

Learning-based Multimedia Processing

1 – Introduction to Multimedia and to Biometrics

Prof. Paulo Lobato Correia

IST, DEEC – Área Científica de Telecomunicações

1

Outline

Introduction to Multimedia and to Biometrics

- Multimedia: what it is and its applications
- Multimedia acquisition and human perception
- Multimedia representation

- **Focusing on biometrics:** definition and applications
- Ethics and data protection



Prof. Paulo Lobato Correia

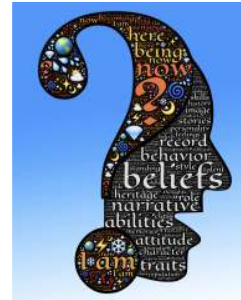
2

2

Identity and Identification

What is **Identity**?

- Identity is “shaped by individual characteristics, family dynamics, historical factors, and social and political contexts”.



Paulo Lobato Correia

3

3

Identity and Identification

What is Identity?

- “Identity” and “sameness” mean the same; their meanings are identical.

However, they have more than one meaning¹:

Used for identification

- Things with **qualitative identity** share properties, so things can be more or less qualitatively identical.

Philosophers definition of identity

- Numerical identity** requires absolute, or total, qualitative identity, and can only hold between a thing and itself. (who one is in essence – a metaphysical statement)



¹ The Stanford Encyclopedia of Philosophy - <https://plato.stanford.edu/entries/identity/>

Paulo Lobato Correia

4

4

Identity and Identification



Identification

- ... we need to save the idea of “identity” chiefly because we need to provide a foundation to the notion of “identification,” which is not an abstract concept, but it is a term describing a specific human activity and practice.¹
- “I argue that the idea of **identification** does not descend from the notion of identity, rather it is vice versa”¹



Identification is a practical question:

- **how (or in virtue of what) one may be recognized**

¹ E. Mordini, “Biometrics, identity, recognition and the private sphere where we are, where we go”, 2017
https://digital-library.theiet.org/content/books/10.1049/pbse004e_ch16

Recognition over Time

First urban societies
 (Neolithic agricultural revolution ~10000 years ago)



Recognition is needed to **establish trust with unknown strangers**¹:

- **Physical appearance** (e.g., body size and shape, skin and hair colour, face shape, physical deformities and particularities, wrinkles and scars, etc.)
- Artificial **body modifications** (e.g., branding, tattooing, scarification, etc.)
- **Physical objects** (e.g., passes, seals, rings, etc.)
- **Mental tokens** (e.g., memories, poems, music, recollection of family and tribal links, etc.)



¹ E. Mordini, “Biometrics, identity, recognition and the private sphere where we are, where we go”, 2017
https://digital-library.theiet.org/content/books/10.1049/pbse004e_ch16

Recognition over Time

Ancient Egypt – first documented examples¹:

Khasekem, assistant to chief administrator, used **phenotypic biometrics** to take notes about every worker (100 000 or more), detailing:

- **physical characteristics** (e.g., age, height, weight, deformities)
- **behavioural characteristics** (e.g., general disposition, speech particularities, etc.)



¹ J. Ashbourn, "Biometrics: Advanced Identity Verification the Complete Guide"

Recognition over Time

Ancient Egypt – first documented examples¹:

"Nechutes, son of Asos, aged 40, of middle size, sallow complexion, cheerful countenance, long face with straight nose and a scar upon the middle of his forehead."

"If required such descriptions were accompanied by anatomical measurements such as the distance measured between the individuals outstretched thumb and the tip of the elbow."



¹ J. Ashbourn, "Guide to Biometrics for large-Scale Systems"

Recognition over Time

Biblical reference example:

- “Then said the men of Gilead unto him,
Say now Shibboleth:
and he said Sibboleth: for he could not frame to pronounce it right.
Then they took him, and slew him at the passages of the Jordan:
and there fell at that time of the Ephraimites forty and two thousand.” – Judges 12:5-6

Phenotypic biometrics, and in particular speech, was used to identify Ephraimites, the enemy of the Gileadites.

- Ephraimites pronounced “Sh” as “S”.



9

9

Recognition over Time – Biometrics

Some biometric recognition milestones:

- **1871 – Adolphe Quetelet**, Belgian mathematician and astronomer made a contribution to the modern use of biometrics with his treatise: “*Anthropométrie ou Mesure des Différentes Facultés de l’Homme*”
- **1882 – Alphonse Bertillon**, French law enforcement officer applied Quetelet’s work to develop a system to identify criminals based on **anatomical measures**.
- **1888 – Juan Vucetich**, Argentinean police officer (born in Croatia) was the first to use **dactyloscopy** (taking of fingerprints using ink). He created an efficient system of fingerprints classification.

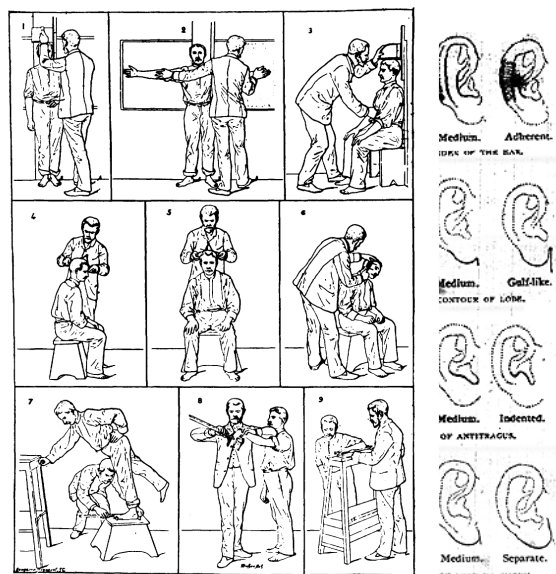


10

Alphonse Bertillon's *Identification anthropométrique* (1893): anthropometric measurements as basis of identification system.



RELEVÉ
DU
SIGNALEMENT ANTHROPOMÉTRIQUE

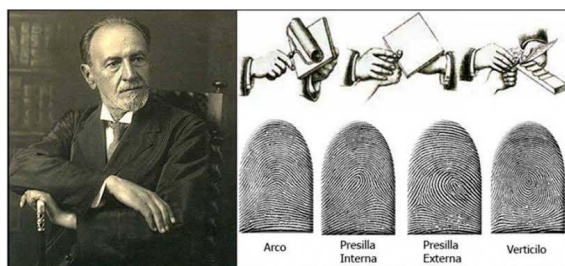


1. Taille. — 2. Envergure. — 3. Buste. —
4. Longueur de la tête. — 5. Largeur de la tête. — 6. Oreille droite. —
7. Pied gauche. — 8. Mèlus gauche. — 9. Couée gauche.

11

11

Juan Vucetich (1904)



Paulo Lobato Correia

12

12

Biometric Recognition

Typical recognition mechanisms:

Something you
know

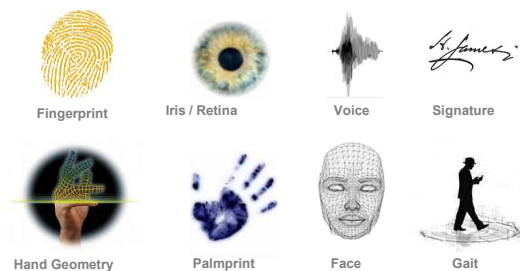


Something you
have



Something you
are / produce

Commonly used biometric traits:



Paulo Lobato Correia

13

13

Biometrics - Definition

“theory, design, and application of **biometric characterization of human beings**, based on physiological and/or behavioural features and traits, in particular for *identification, identity verification, authentication, encryption, recognition and medical diagnosis*” ¹



[¹ IEEE Biometrics Council - <http://ieee-biometrics.org/>]

Paulo Lobato Correia

15

15

Recognition: Identification and Verification

Biometric recognition according to ISO/IEC JTC1 SC37:

- “automated recognition of individuals based on their biological and behavioural characteristics”.¹
 - **biometric identification** – process of searching against a biometric enrolment database (3.3.9) to find and return the biometric reference identifier(s) (3.3.19) attributable to a single individual
 - **biometric verification** – process of confirming a biometric claim (3.6.4) through biometric comparison (3.5.7)



¹ Standards by ISO/IEC JTC 1/SC 37 Biometrics: <https://www.iso.org/committee/313770/x/catalogue/>
<https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v1:en>

Biometrics: Operation Types

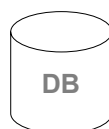
Two **phases** for biometric recognition:

- **Enrolment** – Register the person with the system;
- **Recognition** – Automatically recognize the person.

Enrolment



Enrol



Recognition

Query

1:1 (Verification)
1:N (Identification)

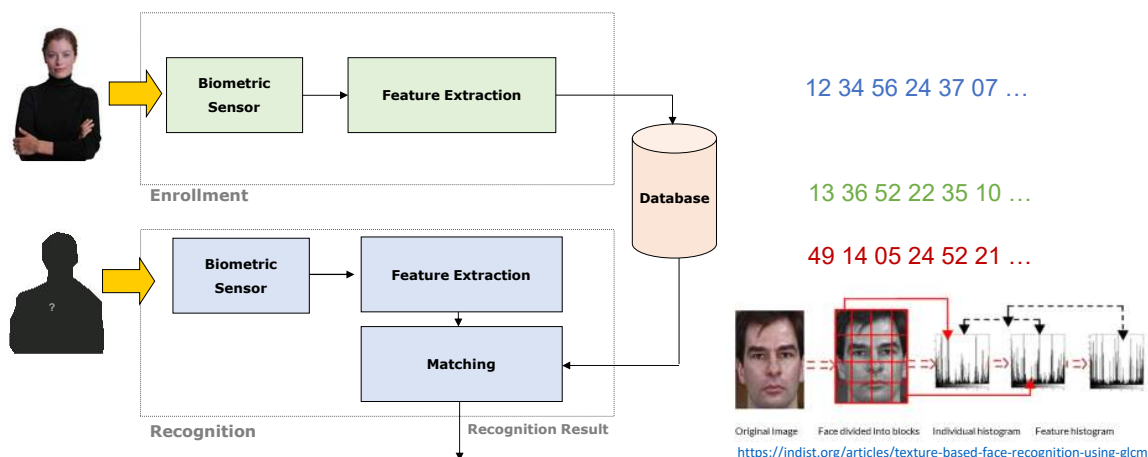


Two **operation types**:

- **Verification** – Is this person who she claims to be? (1:1)
- **Identification** – Who is this person? (1:N)

Biometric Recognition: Architecture

Overall architecture of biometric recognition system:



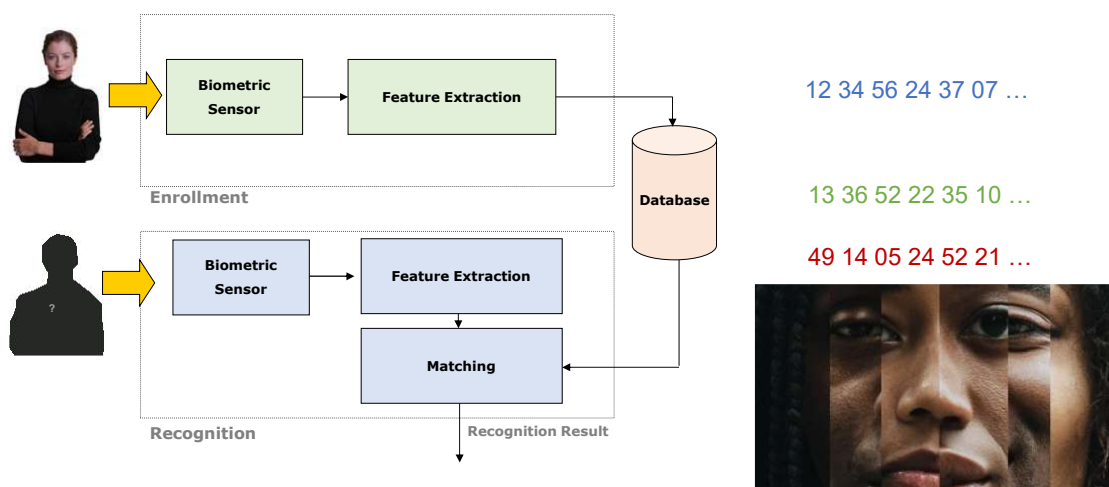
Paulo Lobato Correia

18

18

Biometric Recognition: Architecture

Overall architecture of biometric recognition system:



Paulo Lobato Correia

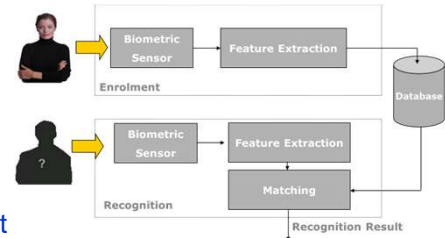
19

19

Biometric Recognition: Architecture

Biometric Sensor:

- ❑ measure biometric characteristic with appropriate device
- ❑ the resulting data may be an image, a sound, ...
- ❑ multiple samples may be used
- ❑ a quality metric may be associated with the measurement



Feature extraction:

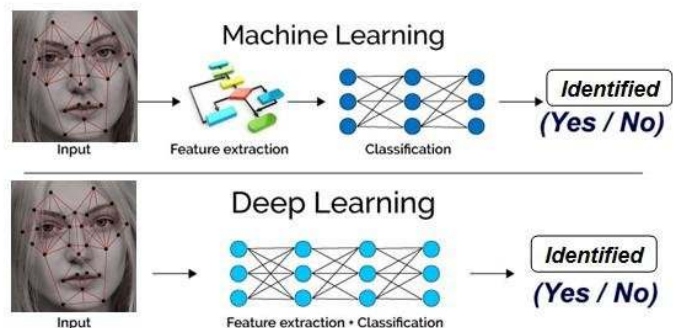
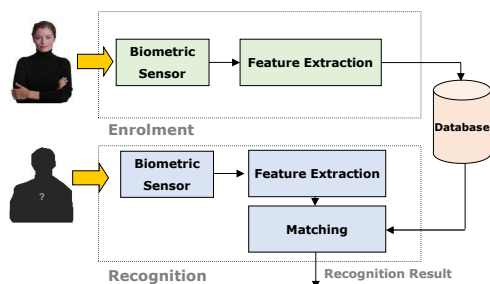
- ❑ *pre-processing* (sometimes appears as a *separate module*) – useful for noise removal, for removal of unwanted data, normalization, ...
- ❑ possible problems, such as *failure to enroll*
- ❑ main goal: convert input data into a “numeric” feature template

Paulo Lobato Correia

20

20

Deep Learning vs. Handcrafted Feature Extraction



[Hayder Najm, Hayder Ansaf, Oday A. Hassen; "An Effective Implementation of Face Recognition Using Deep Convolutional Network", Journal of Southwest Jiaotong University, Oct. 2019]

Paulo Lobato Correia

21

21

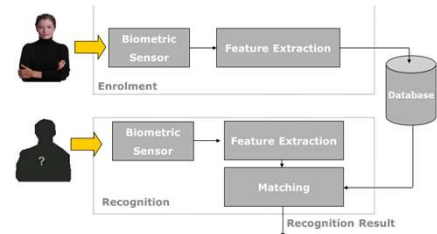
Biometric Recognition: Architecture

Matching:

- compare the extracted template with the previously enrolled biometric templates
- determine a degree of similarity (or a distance/error metric)
- output a **matching score**

Decision:

- matching scores are compared to a threshold
 - above threshold -> **match**
 - below threshold -> **no match**



Paulo Lobato Correia

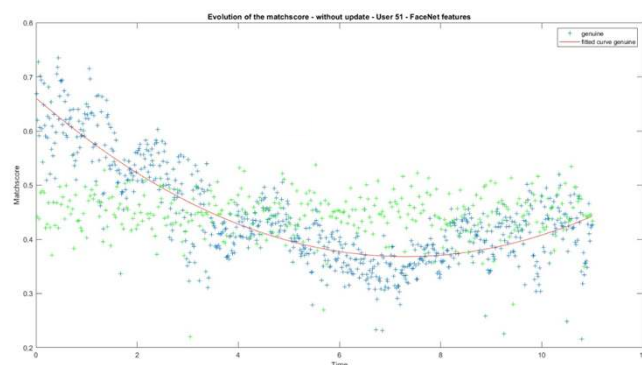
22

22

Biometric Recognition: Template

Biometric templates:

- Can be obtained from one or from multiple samples.
- Should be updated along time, e.g., using information from successful recognition attempts.



very low matchscore

Sample input to the authorization system after 10 years



[Giulia Orru, "Template update algorithms and their application to face recognition systems in the deep learning era", PhD Thesis, 2021, Università di Cagliari]

Paulo Lobato Correia

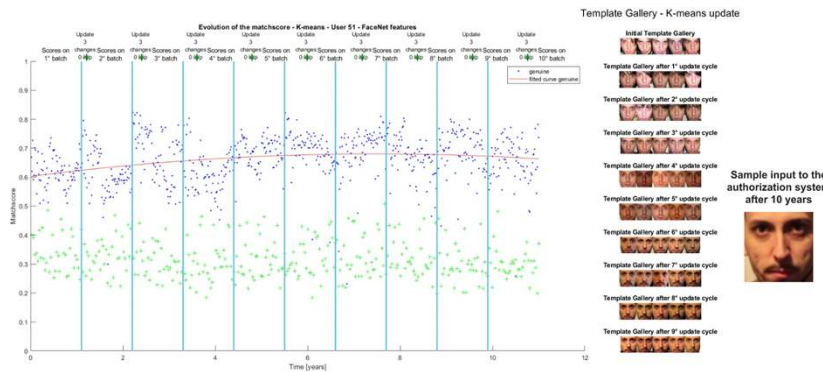
23

23

Biometric Recognition: Template

Biometric templates:

- Can be obtained from one or from multiple samples.
- Should be updated along time, e.g., using information from successful recognition attempts.



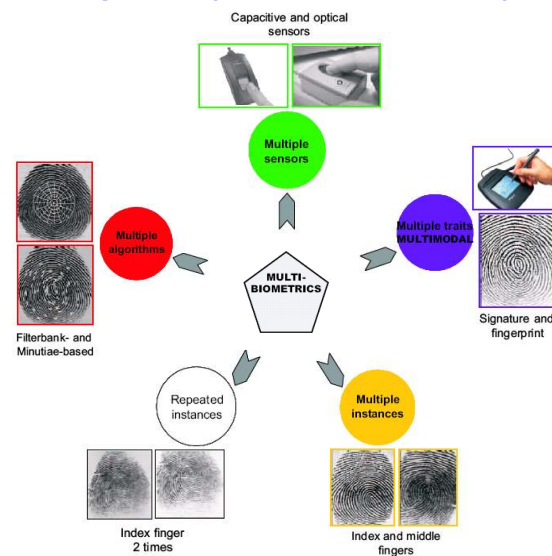
[Giulia Orru, "Template update algorithms and their application to face recognition systems in the deep learning era", PhD Thesis, 2021, Università di Cagliari]

Paulo Lobato Correia

24

24

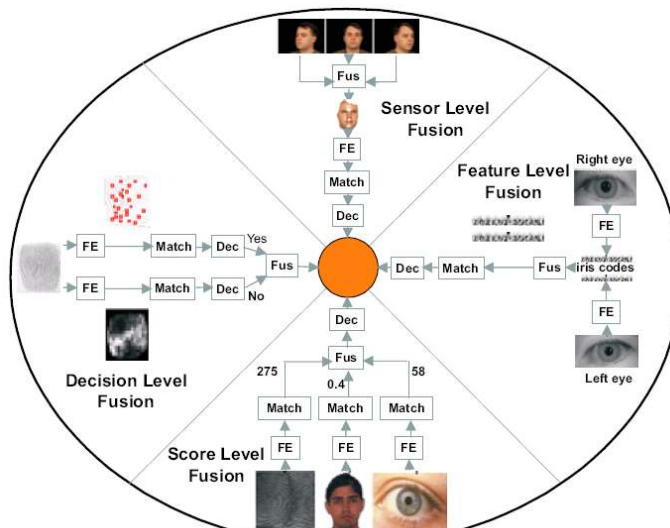
Using Multiple Biometric Samples



[Aguilar, J., Adapted Fusion Schemes for Multimodal Biometric Authentication, 2006]

25

Fusion of Multiple Biometric Traits



[Aguilar, J., Adapted Fusion Schemes for Multimodal Biometric Authentication, 2006]

26

Aadhaar

Biometric information:

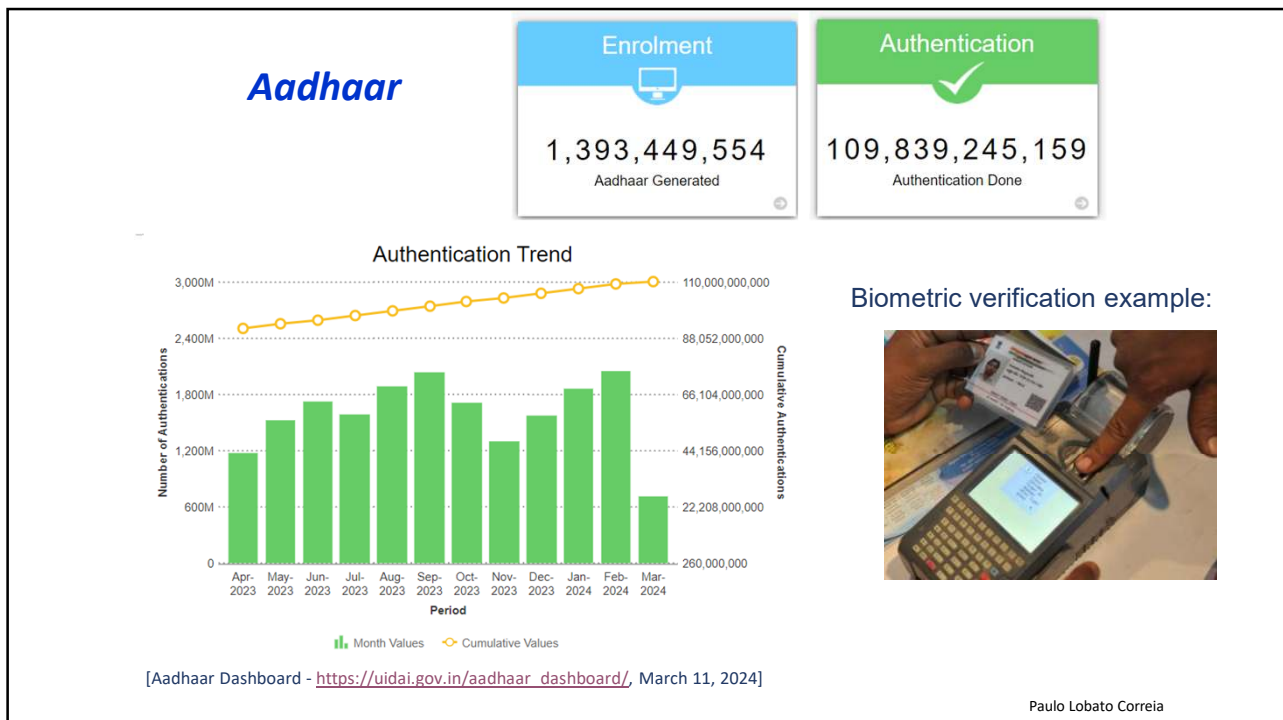
- ▶ Ten Fingerprints
- ▶ Two Iris Scans
- ▶ Facial Photograph




[Aadhaar Dashboard - https://uidai.gov.in/aadhaar_dashboard/, March 1, 2023]

Paulo Lobato Correia

27



28




Biometric Recognition: Evaluation metrics


Verification (1:1) evaluation metrics (algorithm eval):

- ❑ **False Non-Match Rate (FNMR)**
 - ❑ proportion of mated comparison trials (same biometric trait from same user – a genuine trial) that result in a false non-match– related to FRR (false reject rate)
 → *algorithm rejects true identity* $FNMR(t) = \int_0^t \Phi_g(s) ds$
- ❑ **False Match Rate (FMR)**
 - ❑ proportion of non-mated comparison trials (impostor trials) that result in a false match– related to FAR (false accept rate)
 → *algorithm accepts “zero-effort” impostor*

$$FMR(t) = \int_t^1 \Phi_i(s) ds$$

$\Phi_g(s)$: PDF of genuine similarity score $s(Q, R)$
 $\Phi_i(s)$: PDF of imposter similarity score $s(Q, R)$

False Negative


False Positive


29

29

Verification (1:1) evaluation metrics (algorithm eval):

False Non-Match Rate (FNMR)

- proportion of mated comparison trials (same biometric trait from same user – a genuine trial) that result in a false non-match– related to FRR (false reject rate)

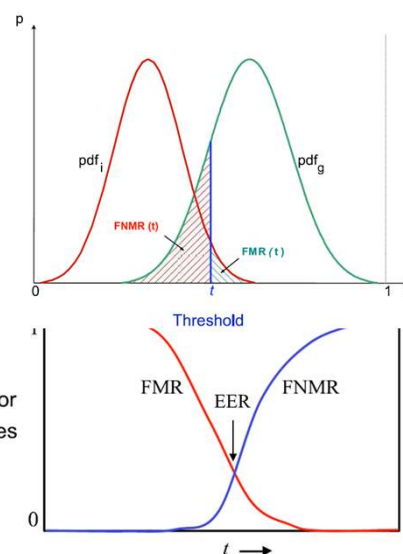
→ algorithm rejects true identity $FNMR(t) = \int_0^t \Phi_g(s) ds$

False Match Rate (FMR)

- proportion of non-mated comparison trials (impostor trials) that result in a false match– related to FAR (false accept rate)
- algorithm accepts “zero-effort” impostor

$$FMR(t) = \int_t^1 \Phi_i(s) ds$$

$\Phi_g(s)$: PDF of genuine similarity score $s(Q, R)$
 $\Phi_i(s)$: PDF of impostor similarity score $s(\hat{Q}, R)$



30

30

Evaluation metrics (system eval):

- Failure to capture rate (FTC)** – proportion of failures to capture a biometric sample (e.g. image of insufficient quality)
- Failure to extract rate (FTX)** – proportion of failures to extract features from the acquired sample to generate a template
- Failure to acquire rate (FTA)** – proportion of acquisition trials that failed to be accepted for subsequent processing (failure to capture or to extract)

$$FTA = FTC + FTX \times (1 - FTC)$$

- Failure to enrol rate (FTE)** – proportion of failures to create and store a biometric record during enrolment



31

31

Verification (1:1) evaluation metrics

For system evaluation:

False Accept Rate (FAR)

$$FAR = FMR \times (1 - FTA)$$

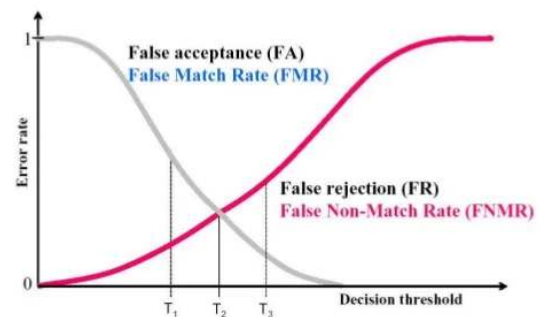
False Reject Rate (FRR)

$$FRR = FTA + FNMR \times (1 - FTA)$$

For algorithmic evaluation:

$$FMR = FAR$$

$$FNMR = FRR$$



Paulo Lobato Correia

32

32

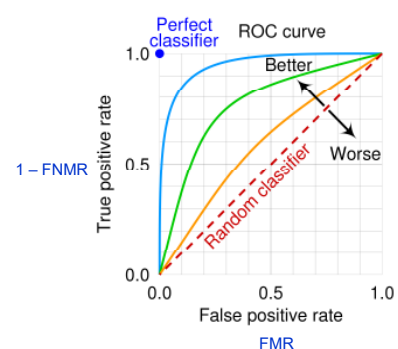
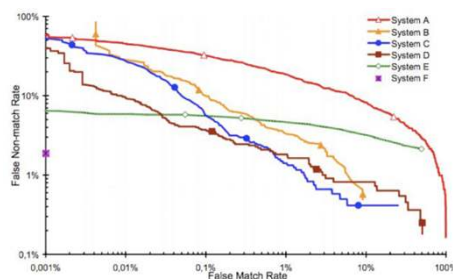
Verification (1:1) evaluation metrics:

Receiver operating characteristic (ROC)

- plots of $(1 - FNMR)$ vs FMR (or TP vs FP)
- illustrates binary classifier performance, as the discrimination threshold is varied

Detection error trade-off curve (DET)

- plots of FNMR vs FMR (or FN vs FP)



Paulo Lobato Correia

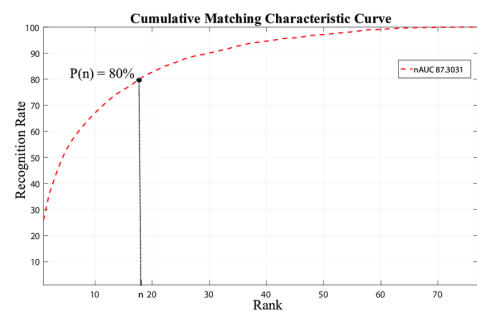
33

33

Biometric Recognition: Evaluation metrics

Identification (1:N) evaluation metrics:

- **Rank-1** identification rate – proportion of identification trials that return the correct subject's ID at rank 1
- **Rank-N** identification rate, or True Positive Identification Rate (**TPIR**) – proportion of identification trials that return the correct subject's ID among the top N ranks ($TPIR = 1 - FPIR$)
- False Negative Identification Rate (**FNIR**) – fraction of trials where the correct subject's ID is not among the top N ranks or the similarity comparison score is below the threshold
- **Cumulative match characteristic curve (CMC)** – plots the true positive identification rate (TPIR) vs the rank



Paulo Lobato Correia

34

34

Biometrics: Applications

Biometric recognition is everywhere:

- access control to facilities
- passport control
- employee attendance control
- unlocking smartphones/computers
- in-vehicle configurations
- multifactor authentication
- ...

Fingerprint and facial recognition are routinely used.

Biometrics provide additional security, also for online transactions.



Paulo Lobato Correia

35

35

Biometrics: Applications

E-Commerce and Remote Banking

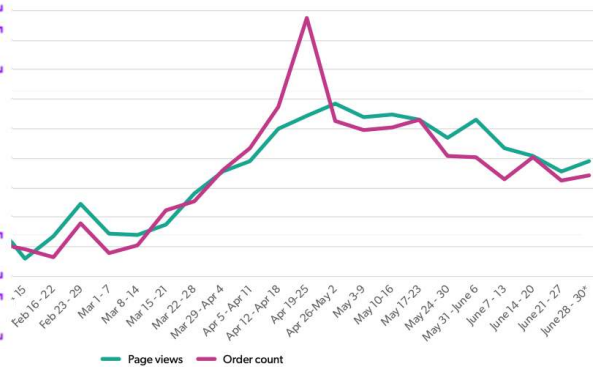
CUSTOMERS ARE READY FOR BIOMETRICS



500 MILLION
Biometric sensors globally by 2018



Weekly shopping activity, global
Year-over-year percent growth — 2020 v. 2019



Source: Bazaarvoice Network data

[Connect to Your Customer with Secure Biometric Banking", Accenture, 2018]

bazaarvoice:

CUSTOMERS WANT BIOMETRICS



Paulo Lobato Correia

36

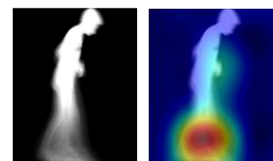
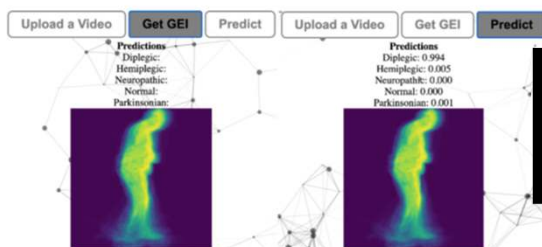
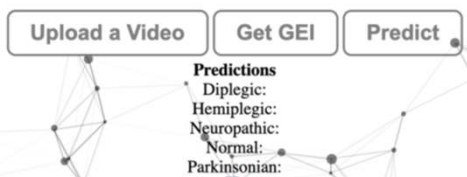
36

Biometrics: Applications

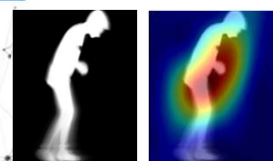
Biomedical applications



Pathological gait classification



Diplegic gait



Parkinsonian gait

Paulo Lobato Correia

37

37

Biometrics in Portugal

Business (also) in Portugal

- Many “commercial companies” (e.g. Bioglobal, Gateway, ...)
- Polygon – remote biometric authentication (face, voice, fingerprint) and liveness detection, for banking applications, ...



- Vision-Box - security in government services, travel, border control, and smart facilities ...



Paulo Lobato Correia

38

38

Biometric Recognition – Advantages

Biometrics are increasingly attractive tools for authentication and access control.

Advantages (as replacement for passwords or cards):

- Inherently linked to the user
- Cannot be forgotten, lost or given away
- Higher entropy than poorly chosen passwords
- Require very little user expertise



39

Biometric Recognition – Limitations

Potential problems:

- ❑ Personal data protection (centralized databases, function creep, ...)
- ❑ Privacy violation
- ❑ May require significant computational resources
- ❑ Can it be “fooled”?
- ❑ Biometric traits cannot be changed ...



→ Presentation attack detection

→ Secure template storage

- *Human bodies are words made flesh, they are embodied biographies* – much more than a set of measurable physical or behavioural characteristics¹
- If biometric systems are intrusive, physically, psychologically or socially, is often due to operational procedures, rather than to technology; they should not contribute to humiliate people

¹ E. Mordini, “Biometrics, identity, recognition and the private sphere where we are, where we go”, 2017

Biometric Recognition – Limitations

ThreatList: A Third of Biometric Systems Targeted by Malware in Q3



3/12/2020 - Kaspersky researchers found that in the third quarter of 2020, one in three (37 percent) of computers within the firm's telemetry that collect, process and store biometric data were targeted by malware attacks.

[<https://threatpost.com/threatlist-a-third-of-biometric-systems-targeted-by-malware-in-q3/150778/>]

The man in the latex mask: **BLACK** serial armed robber disguised himself as a **WHITE** man to rob betting shops

- Henley Stephenson wore the disguise during a 12-year campaign of hold-ups at betting shops and other stores across London
- He was part of a three-man gang jailed for a total of 28 years
- CCTV footage showed him firing a semi-automatic pistol into the ceiling during a raid on a betting shop
- The mask was bought from the same London shop which supplied masks used in the £40m Graff Diamonds heist

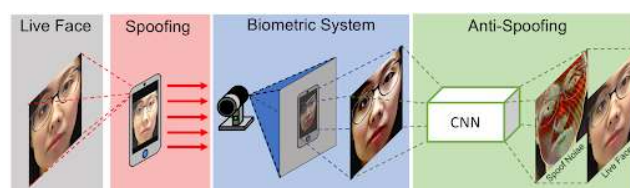
By ROB PREECE and REBECCA CAMBER FOR THE DAILY MAIL

PUBLISHED: 17:22 GMT, 1 June 2012 | UPDATED: 18:21 GMT, 2 June 2012

Most masked robbers opt for a balaclava to hide their identity.

Not this one. Henley Stephenson, 41, eluded police for more than ten years thanks to an extraordinarily lifelike latex mask, which turned him into a white skinhead.

Officers discovered that their man was in fact black when they finally caught up with Stephenson after a string of armed raids dating back to 1999.



[<http://www.dailymail.co.uk/news/article-2153346/Black-armed-robber-disguised-white-man-using-latex-mask.html>]

<http://cvlab.cse.msu.edu/project-face-anti.html>]

Paulo Lobato Correia

42

42

Introduction to Multimedia and to Biometrics

- Multimedia: what it is and its applications
- Multimedia acquisition and human perception
- Multimedia representation
- Focusing on biometrics: definition and applications
- Ethics and data protection

Prof. Paulo Lobato Correia

43

43



Biometrics and privacy has always been a topic of discussion

“Biometrics: privacy's foe or privacy's friend?” (J. Woodward):

- *“Critics inevitably compare biometrics to **Big Brother** and the loss of individual privacy.”*
- *“The pro-biometric lobby generally stresses the **greater security and improved service** that the technology provides.”*

Biometrics as a friend to privacy, by establishing identity depending on unique characteristics of an individual, versus an externalized comparator such as a password.

[J. D. Woodward, "Biometrics: privacy's foe or privacy's friend?," in Proceedings of the IEEE, vol. 85, no. 9, pp. 1480-1492, Sept. 1997]

Prof. Paulo Lobato Correia 44

44



General Data Protection Regulation (GDPR):

- *Regulation (EU) 2016/679 of the European Parliament and of the Council.*
- *Lays down rules relating to the **protection of fundamental rights and freedoms of natural persons**, and in particular their **right to the protection of personal data**.*
- *Aims to improve consumer protection and general levels of **privacy for individuals**, includes mandatory reporting of data protection breaches and has an increased emphasis on **gaining explicit consent to process information**.*

Prof. Paulo Lobato Correia 45

45

Personal data is **any information relating to a natural person who can be identified**, directly or indirectly, by that information.

- Examples: name, identification number, location data, online identifier, pseudonymised data, as well as factors specific to physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data ("**sensitive data**"):

- Examples are personal data relating to: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or **biometric data** processed for purpose of identification, health, sex life or sexual orientation.

Personal and sensitive data – examples:

Personal information	Special categories of personal data ('sensitive data').
Name	Race
Address	Religion
Date of birth	Political opinion
Email address	Trade union membership
Photographs	Sexual orientation
IP address – the unique digital address attributed to your digital devices	Sex life
Location data	Gender identity
Online behaviours – traced through 'cookies'	Health information
Profiling and analytics data	Biometric data
	Genetic data

Case study – identify the **personal information** being shared:

Mr Silva, 45, of Av. Rovisco Pais, n.37, 1st E, in Lisbon, has been recovering in St. Maria Hospital after successful kidney transplantation on March 16. The operation was a complete success and we are sending his family all our good wishes.

Mr Silva has been a member of Portuguese kidney patient association since his diagnosis in 2001, and has raised several thousand euros in funding over the last few years, helped by connections made through his membership of the Socialist Party. He is also an active member of the community of St João de Deus local church.

If you would like to wish him a speedy recovery, you can visit him on the 6th floor between 2 and 3 pm, on week days at St. Maria Hospital or you can contact his wife, Joana, on 912345678 or joana@maildossilva.pt.

Personal information

- Address
- Date of birth
- Email address
- Photographs
- IP address
- Location data
- Online behaviours – traced through 'cookies'
- Profiling and analytics data

Prof. Paulo Lobato Correia 48

48

Case study – identify the **personal information** being shared:

Mr Silva, 45, of Av. Rovisco Pais, n. 37, 1st E, in Lisbon, has been recovering in St. Maria Hospital after successful kidney transplantation on March 16. The operation was a complete success and we are sending his family all our good wishes.

Mr Silva has been a member of Portuguese kidney patient association since his diagnosis in 2001, and has raised several thousand euros in funding over the last few years, helped by connections made through his membership of the Socialist Party. He is also an active member of the community of St João de Deus local church.

If you would like to wish him a speedy recovery, you can visit him on the 6th floor between 2 and 3 pm, on week days at St. Maria Hospital or you can contact his wife, Joana, on 912345678 or joana@maildossilva.pt.

Personal information

- Name
- Age
- Postal address
- Link to Portuguese kidney patient association
- Current location
- Relationship to Joana
- Joana's name
- Joana's mobile number
- Joana's email address

Prof. Paulo Lobato Correia 50

50

Case study – identify the **sensitive personal information** being shared:

Mr Silva, 45, of Av. Rovisco Pais, n.37, 1st E, in Lisbon, has been recovering in St. Maria Hospital after successful kidney transplantation on March 16. The operation was a complete success and we are sending his family all our good wishes.

Mr Silva has been a member of Portuguese kidney patient association since his diagnosis in 2001, and has raised several thousand euros in funding over the last few years, helped by connections made through his membership of the Socialist Party. He is also an active member of the community of St João de Deus local church.

If you would like to wish him a speedy recovery, you can visit him on the 6th floor between 2 and 3 pm, on week days at St. Maria Hospital or you can contact his wife, Joana, on 912345678 or joana@maildossilva.pt.

Sensitive information

Race
Religion
Political opinion
Trade union membership
Sexual orientation
Sex life
Gender identity
Health information
Biometric data
Genetic data

Prof. Paulo Lobato Correia

52

52

Personal data shall be:

- ❑ **processed lawfully, fairly and in a transparent manner;**
- ❑ **collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes;
- ❑ **adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed;
- ❑ **accurate** and, where necessary, **kept up to date;**
- ❑ kept in a form which **permits identification of data subjects for no longer than is necessary** for the purposes for which the personal data are processed;
- ❑ processed in a manner that **ensures appropriate security of the personal data.**

The **controller** shall be responsible for and be able to **demonstrate compliance** with the above → **Accountability Principle**

Prof. Paulo Lobato Correia

55

55

The GDPR provides the following rights for individuals:

- The right to **be informed** (privacy notice / data collection notice)
- The right of **access** (subject access request)
- The right to **rectification** (if data is inaccurate or incomplete)
 A response is due within a month; if not possible the individual must receive an explanation.
- The right to **erasure** (was: right to be 'forgotten')
 Personal data shall be erased and no longer processed in specific circumstances:
 - Personal data is **no longer necessary** for the purpose for which it was originally collected/processed.
 - **The individual withdraws consent, or objects to the processing.**
 - If data is being processed on the basis of legitimate interest, the individual objects, and the entity **cannot demonstrate that there are overriding legitimate grounds for the processing.**
 The right to erasure does not apply:
 - For the exercise of the right of **freedom of expression and information**;
 - For compliance with a **legal obligation**
 - For the performance of a **public interest task or exercise of official authority**
 - For **public health reasons**
 - For **archival, research or statistical purposes**
 - If required for to **establish, exercise or defend legal claims**

The GDPR provides the following rights for individuals:

- The right to **restrict processing**
 Where an **individual contests the accuracy of the personal data**, where an individual has objected to the processing and the organisation is considering their legal reason for processing, where processing is unlawful and the **individual opposes erasure and requests restriction instead**, where the organisation no longer need the personal data but **the individual requires the data to establish, exercise or defend a legal claim.**
- The right to **data portability**
 Must respond **within a month**. Individuals can **move, copy or transfer personal data** to obtain and reuse for their own purposes across different services.
- The right to **object**
 - **To direct marketing**: this is an absolute right.
 - **To processing** for scientific / historical research / statistical purposes: there must be grounds which specifically relate to the individuals situation.
 - **To processing for legitimate interests / public interest.**
- Rights in relation to **automated decision making and profiling**
 Safeguards individuals against the risk that a potentially damaging decision is taken without human intervention.

GDPR explicitly **prevents using biometric data** for either *authentication or identification*, **except** in the conditions listed in Article 9 (2):

- a) *the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;*
- b) ***processing is necessary for** the purposes of carrying out the obligations and **exercising specific rights** of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;*
- c) ***processing is necessary to protect the vital interests of the data subject** or of another natural person where the data subject is physically or legally incapable of giving consent;*

GDPR explicitly **prevents using biometric data** for either *authentication or identification*, **except** in the conditions listed in Article 9 (2):

- d) *processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the **processing relates solely to the members** or to former members **of the body** or to persons who have regular contact with it in connection with its purposes and that the **personal data are not disclosed outside that body without the consent of the data subjects**;*
- e) *processing relates to personal data which are manifestly **made public by the data subject**;*
- f) *processing is necessary for the establishment, **exercise** or defence of **legal claims** or whenever courts are acting in their judicial capacity;*

Biometrics and the GDPR

GDPR explicitly **prevents using biometric data** for either *authentication or identification*, **except** in the conditions listed in Article 9 (2):

- g) *processing is necessary for reasons of **substantial public interest**, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;*
- h) *processing is necessary for the purposes of **preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services** on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;*

Biometrics and the GDPR

GDPR explicitly **prevents using biometric data** for either *authentication or identification*, **except** in the conditions listed in Article 9 (2):

- i) *processing is necessary for **reasons of public interest in the area of public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;*
- j) *processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes** in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.*

Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Conditions for consent

- ❑ **Implied consent is unacceptable** for processing
- ❑ Demonstrable by a **statement or clear affirmative action**
- ❑ **Freely given**, specific, informed, unambiguous
- ❑ Consent must be obtained **for every processing scenario**
- ❑ Consent **can be withdrawn at any time**

New and expanded rights

- ❑ Data subjects must be aware of their rights
- ❑ Responses within one month
- ❑ If a right is exercised, *any third party we've shared the relevant data with must be notified*

→ Data Protection by Design

Must explain

- personal data being processed,
- purpose of processing,
- intended retention,
- subject rights,
- source of data,
- conditions of processing,
- intended sharing or international transfer
- existence of automated decision making, including profiling

Prof. Paulo Lobato Correia

62

62

GUIÃO PARA UM CONSENTIMENTO INFORMADO

O consentimento informado consiste no assentimento, em regra, individual, **prévio, instruído, esclarecido, livre, expresso, específico, positivo e revogável em qualquer altura** por parte dos indivíduos, ou seus representantes, participantes em estudos científicos¹.

O IST rege-se por altos padrões de cumprimento legal e ético na prossecução da sua missão pública, pelo que qualquer tipo de investigação realizada no seu âmbito está vinculada a perseguir um consentimento assente em uma aceitação voluntária e esclarecida pelo participante (ou representante) sobre a natureza, finalidades, procedimentos, implicações e riscos dessa participação, todos a comunicar pelos responsáveis da investigação, ou investigadores intervenientes com a devida qualificação académica, de forma inteligível, clara, simples, aberta e apropriada para o nível de compreensão dos participantes (incluindo, explicação de conceitos, jargões, abreviaturas, siglas e acrónimos relativos à investigação e participação).

[<http://etica.tecnico.ulisboa.pt/en/>]

Prof. Paulo Lobato Correia

63

63

A declaração de consentimento constitui, pois, um estágio derradeiro do processo de comunicação integral destinado a informar o participante (ou representante legal²), pelos competentes investigadores conforme a prossecução dos fins e padrões acima enunciados. Assim, da sobredita declaração **deve constar inequívoco consentimento do participante** (ou representante legal) **e reconhecer ou mencionar os elementos seguintes**:

- ☑ Identificação do participante (e representante legal, se aplicável) e investigador responsável (e terceiros citados);
- ☑ **Descrição da investigação** e participação visada (dados, procedimentos, intervenções, tempo, modo, lugar, duração);
- ☑ **Garantia de confidencialidade dos dados recolhidos e anonimato**;
- ☑ Explicitação clara e aberta que a **participação é voluntária e livre**;
- ☑ Se aplicável, descrição dos **possíveis riscos, desconfortos ou desvantagens** para o participante;
- ☑ Explicitação clara do **direito** do participante questionar e **desistir** da sua participação sem qualquer prejuízo pessoal, bem como de obter informações sobre a entidade de acolhimento da investigação;
- ☑ Local, data e assinaturas devidas em dois originais, um para o participante, outro para o responsável da investigação.

[<http://etica.tecnico.ulisboa.pt/en/>]

Prof. Paulo Lobato Correia

64

64

Se a investigação envolver tratamento de dados pessoais³ dos participantes, a declaração de consentimento inclui, ainda, menção da comunicação e autorização do devido tratamento quanto aos elementos seguintes:

- ☑ **Finalidades, fundamentos, procedimentos e garantias do tratamento dos dados**, incluindo enunciação, **recolha, confidencialidade, armazenamento e prazo de conservação** (ou critérios/condições se aplicável) dos dados a tratar;
- ☑ **Identidade e contactos do responsável pelo tratamento e os contactos do encarregado de protecção de dados**, se aplicável, sem prejuízo da referência aos contactos para esclarecimento de eventuais questões pertinentes;
- ☑ **Direito de saber as entidades a quem possam os dados ser comunicados** e possibilidade da transferência dos dados para países terceiros (fora do Espaço Económico Europeu);
- ☑ Direito de solicitar ao responsável pelo tratamento **acesso aos dados pessoais** que lhe digam respeito, bem como os **direitos de rectificação, apagamento, limitação e oposição do tratamento**, incluindo o **direito de retirar consentimento em qualquer altura**, sem prejuízo da licitude do tratamento eventual e previamente consentido;
- ☑ Direito de apresentar reclamação à CNPD.

No caso de tratamento de **dados sensíveis**⁴ deve garantir-se medidas técnicas e organizativas especiais visando, sobretudo, o respeito pelos princípios da **proporcionalidade e da minimização dos dados**, incluindo a **anonimização** ou **pseudonimização** dos mesmos sempre que possível, sem prejuízo da explicitação e justificação dos termos deste tratamento e do consentimento do tratamento dos dados dado pelo seu titular.

[<http://etica.tecnico.ulisboa.pt/en/>]

Prof. Paulo Lobato Correia

65

65

The Artificial Intelligence Act (AI Act)

The European Union “Artificial Intelligence Act”:

- The AI Act is a **proposed European law on artificial intelligence (AI)** – the first comprehensive law on AI by a major regulator anywhere.
- The law assigns applications of AI to **three risk categories**:
 - **Unacceptable risk** applications and systems are banned – example: government-run social scoring of the type used in China.
 - **High-risk** applications are subject to specific legal requirements – example: CV-scanning tool that ranks job applicants.
 - Applications not explicitly banned or listed as high-risk are largely left unregulated.

[<https://artificialintelligenceact.eu/>]

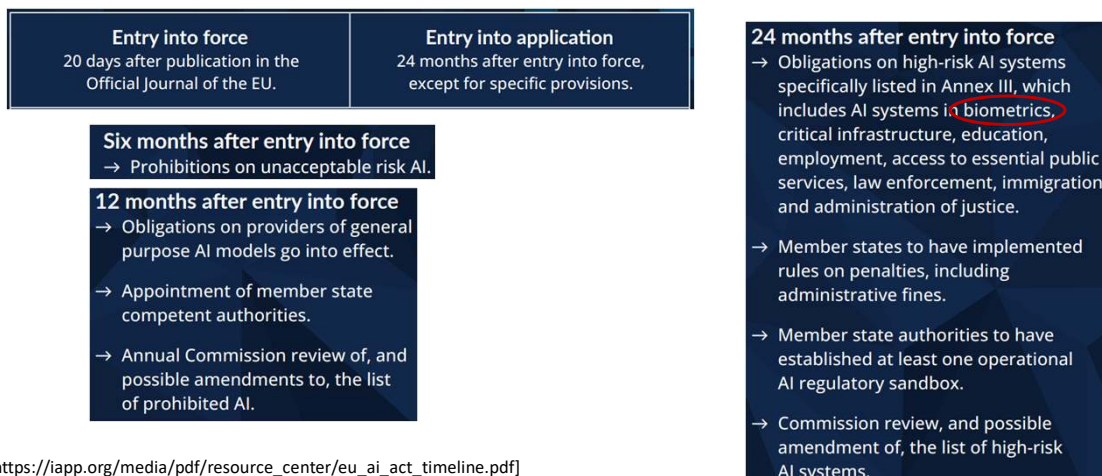
Prof. Paulo Lobato Correia 66

66

AI Act – Timeline

EU AI Act timeline:

- 8 Dec. 2023 – European Parliament, Commission and Council reached a political agreement.



[https://iapp.org/media/pdf/resource_center/eu_ai_act_timeline.pdf]

67

AI Act – Timeline

EU AI Act timeline:

- 8 Dec. 2023 – European Parliament, Commission and Council reached a political agreement.



[https://iapp.org/media/pdf/resource_center/eu_ai_act_timeline.pdf]

Prof. Paulo Lobato Correia 68

68

AI Act Summary

The AI Act classifies AI according to its risk:

- Unacceptable risk** is prohibited (e.g. social scoring systems and manipulative AI).
- High-risk** AI systems are regulated.
- Limited risk** AI systems – subject to lighter transparency obligations: end-users must be aware that they are interacting with AI (e.g. chatbots and deepfakes).
- Minimal risk** is unregulated (majority of current AI applications e.g. AI enabled video games and spam filters).

The **majority of obligations fall on providers/developers**.

Deployers of high-risk AI systems have some obligations, though less than providers.

General purpose AI (GPAI): providers must provide technical documentation, instructions for use, comply with the Copyright Directive, and publish a summary about the content used for training.

[<https://artificialintelligenceact.eu/high-level-summary/>]

Prof. Paulo Lobato Correia 69

69

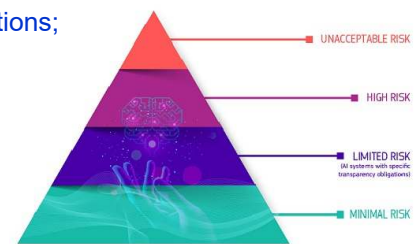
The Artificial Intelligence Act

Identifies “**high-risk**” AI systems, posing significant risks to the health and safety or fundamental rights of persons. Those AI systems will have to comply with a set of horizontal mandatory requirements for trustworthy AI and follow conformity assessment procedures.

Regulation follows a risk-based approach, differentiating between uses of AI that create:

- Unacceptable risk – AI systems whose use is considered **unacceptable**;
- High risk – subject to **strict obligations before they can be put on the market**;
- Low risk – AI systems with specific transparency obligations;
- Minimal risk – free use.

[<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>
<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>]



Prof. Paulo Lobato Correia 70

70

AI Act – Prohibited AI Systems

The following types of AI system are ‘Prohibited’ according to the AI Act:

- Deploying subliminal, manipulative, or deceptive techniques to distort behaviour and impair informed decision-making, causing significant harm.
- Exploiting vulnerabilities related to age, disability, or socio-economic circumstances to distort behaviour, causing significant harm.
- **Biometric categorisation systems** inferring sensitive attributes (race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation), *except labelling or filtering of lawfully acquired biometric datasets* or when *law enforcement* categorises biometric data.
- Social scoring, i.e., evaluating or classifying individuals or groups based on social behaviour or personal traits, causing detrimental or unfavourable treatment of those people.

[<https://artificialintelligenceact.eu/high-level-summary/>]

Prof. Paulo Lobato Correia 71

71

AI Act – Prohibited AI Systems

The following types of AI system are 'Prohibited' according to the AI Act:

- ❑ Assessing the risk of an individual committing criminal offenses solely based on profiling or personality traits, except when used to augment human assessments based on objective, verifiable facts directly linked to criminal activity.
- ❑ **Compiling facial recognition databases** by untargeted scraping of facial images from the internet or CCTV footage.
- ❑ **Inferring emotions** in workplaces or educational institutions, except for medical or safety reasons.
- ❑ **'Real-time' remote biometric identification (RBI)** in publicly accessible spaces for law enforcement, *except* when:
 - ❑ *searching for missing persons*, abduction victims, and people who have been human trafficked or sexually exploited;
 - ❑ *preventing substantial and imminent threat* to life, or foreseeable terrorist attack; or
 - ❑ *identifying suspects in serious crimes* (e.g., murder, rape, armed robbery, narcotic and illegal weapons trafficking, organised crime, and environmental crime, etc.).

[<https://artificialintelligenceact.eu/high-level-summary/>]

Prof. Paulo Lobato Correia

72

72

AI Act – Prohibited AI Systems

Notes on remote biometric identification (RBI):

- ❑ Using AI-enabled real-time RBI is *only allowed when not using the tool would cause considerable harm* and must account for affected persons' rights and freedoms.
- ❑ Before deployment, *police must complete a fundamental rights impact assessment and register the system* in the EU database, though, in duly justified cases of urgency, deployment can commence without registration, provided that it is registered later without undue delay.
- ❑ Before deployment, they also *must obtain authorisation from a judicial authority* or independent administrative authority, though, in duly justified cases of urgency, deployment can commence without authorisation, provided that authorisation is requested within 24 hours. If authorisation is rejected, deployment must cease immediately, deleting all data, results, and outputs.

[<https://artificialintelligenceact.eu/high-level-summary/>]

Prof. Paulo Lobato Correia

73

73

AI Act – High Risk AI Systems

High risk AI systems are those:

- ❑ Used as a safety component or a product covered by EU laws (Annex II) AND required to undergo a third-party conformity assessment; OR those under Annex III use cases, except if:
 - ❑ the AI system performs a narrow procedural task;
 - ❑ improves the result of a previously completed human activity;
 - ❑ detects decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence human assessment without proper human review;
 - ❑ performs a preparatory task to an assessment relevant for the purpose of the use cases listed in Annex III.
- ❑ AI system is always considered **high-risk if it profiles individuals**, i.e. automated processing of personal data to assess various aspects of a person's life, such as work performance, economic situation, health, preferences, interests, reliability, behaviour, location or movement.
- ❑ Providers that believe their AI system, which fails under Annex III, is **not high-risk, must document such an assessment** before placing it on the market or putting it into service.

[<https://artificialintelligenceact.eu/high-level-summary/>]

Prof. Paulo Lobato Correia 74

74

AI Act – High Risk AI Systems

AI Act Annex III use cases:

- ❑ **Non-banned biometrics:** 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.
- ❑ **Critical infrastructure:** Safety components in the management and operation of critical digital infrastructure, road traffic and the supply of water, gas, heating and electricity.
- ❑ **Education and vocational training:** AI systems determining access, admission or assignment to educational and vocational training institutions at all levels. Evaluating learning outcomes, including those used to steer the student's learning process. Assessing the appropriate level of education for an individual. Monitoring and detecting prohibited student behaviour during tests.
- ❑ **Employment, workers management and access to self-employment:** AI systems used for recruitment or selection, particularly targeted job ads, analysing and filtering applications, and evaluating candidates. Promotion and termination of contracts, allocating tasks based on personality traits or characteristics and behaviour, and monitoring and evaluating performance.

[<https://artificialintelligenceact.eu/high-level-summary/>]

Prof. Paulo Lobato Correia 75

75

AI Act – High Risk AI Systems

AI Act Annex III use cases:

- ❑ **Access to and enjoyment of essential public and private services:** AI systems used by public authorities for assessing eligibility to benefits and services, including their allocation, reduction, revocation, or recovery. Evaluating creditworthiness, except when detecting financial fraud. Evaluating and classifying emergency calls, including dispatch prioritising of police, firefighters, medical aid and urgent patient triage services. Risk assessments and pricing in health and life insurance.
- ❑ **Law enforcement:** AI systems used to assess an individual's risk of becoming a crime victim. Polygraphs. Evaluating evidence reliability during criminal investigations or prosecutions. Assessing an individual's risk of offending or re-offending not solely based on profiling or assessing personality traits or past criminal behaviour. Profiling during criminal detections, investigations or prosecutions.

[<https://artificialintelligenceact.eu/high-level-summary/>]

Prof. Paulo Lobato Correia 76

76

AI Act – High Risk AI Systems

AI Act Annex III use cases:

- ❑ **Migration, asylum and border control management:** Polygraphs. Assessments of irregular migration or health risks. Examination of applications for asylum, visa and residence permits, and associated complaints related to eligibility. Detecting, recognising or identifying individuals, except verifying travel documents.
- ❑ **Administration of justice and democratic processes:** AI systems used in researching and interpreting facts and applying the law to concrete facts or used in alternative dispute resolution. Influencing elections and referenda outcomes or voting behaviour, excluding outputs that do not directly interact with people, like tools used to organise, optimise and structure political campaigns.

[<https://artificialintelligenceact.eu/high-level-summary/>]

Prof. Paulo Lobato Correia 77

77

Requirements for providers of high-risk AI systems:

- ❑ Establish a *risk management system* throughout the high risk AI system's lifecycle;
- ❑ Conduct *data governance*, ensuring that training, validation and testing datasets are relevant, sufficiently representative and, to the best extent possible, free of errors and complete according to the intended purpose.
- ❑ Draw up *technical documentation to demonstrate compliance* and provide authorities with the information to assess that compliance.
- ❑ Design their high risk AI system for *record-keeping* to enable it to automatically record events relevant for identifying national level risks and substantial modifications throughout the system's lifecycle.

[<https://artificialintelligenceact.eu/high-level-summary/>]

Prof. Paulo Lobato Correia 78

78

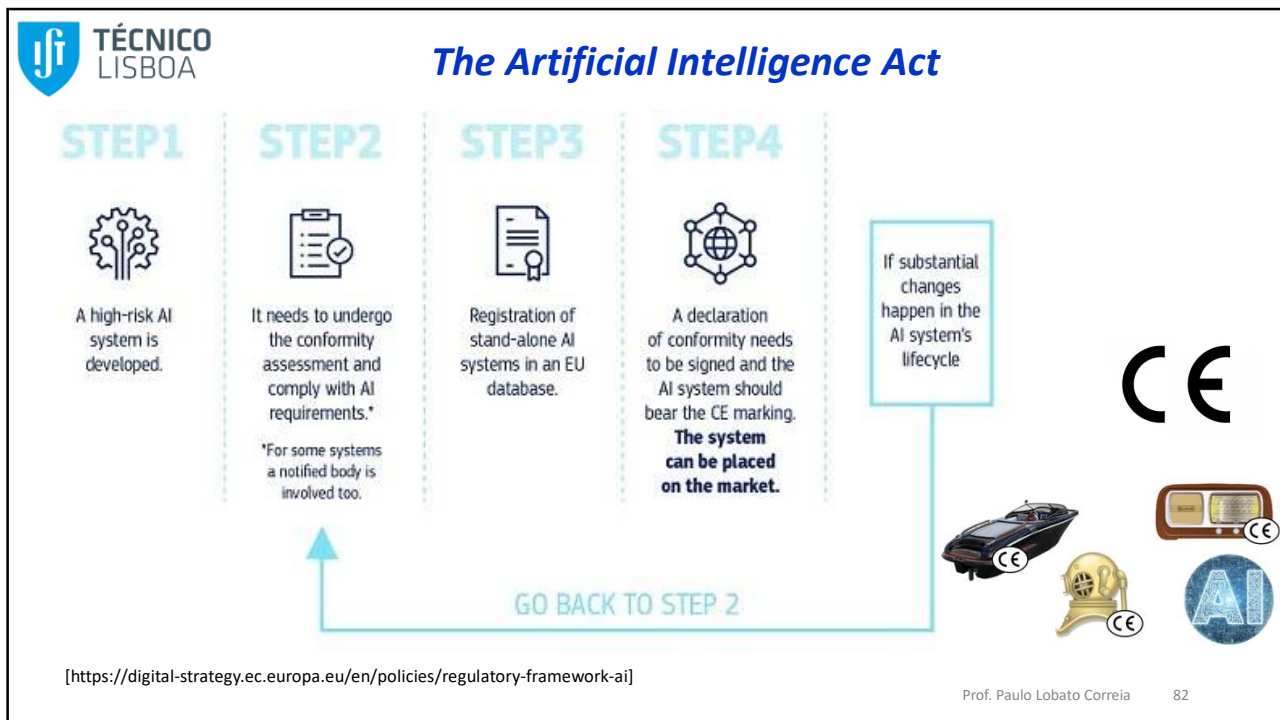
Requirements for providers of high-risk AI systems:

- ❑ Provide *instructions for use to downstream deployers* to enable the latter's compliance.
- ❑ Design their high risk AI system to *allow deployers to implement human oversight*.
- ❑ Design their high risk AI system to *achieve appropriate levels of accuracy, robustness, and cybersecurity*.
- ❑ Establish a *quality management system* to ensure compliance.

[<https://artificialintelligenceact.eu/high-level-summary/>]

Prof. Paulo Lobato Correia 79

79



82

IFT TÉCNICO LISBOA

Outline

Introduction to Multimedia and to Biometrics

- Multimedia: what it is and its applications
- Multimedia acquisition and Human perception
- Multimedia representation
- Focusing on Biometrics: definition and applications
- Ethics and data protection

Suggested reading for next class:

- Chapter 3 of "Digital Image Processing"

"Digital Image Processing", Gonzalez and Woods, 2018, 4th Ed., Pearson

Prof. Paulo Lobato Correia 91

91