

Disaster Risk Management online training seminar series 2023

In cooperation with Disaster Risk Management Knowledge Centre (DRMKC) and CONRIS network

The use of biometrics for security purposes in view of the future European regulation on AI



1. Biometric identification systems: technical aspects.

2. Biometric identification systems in public and private security.

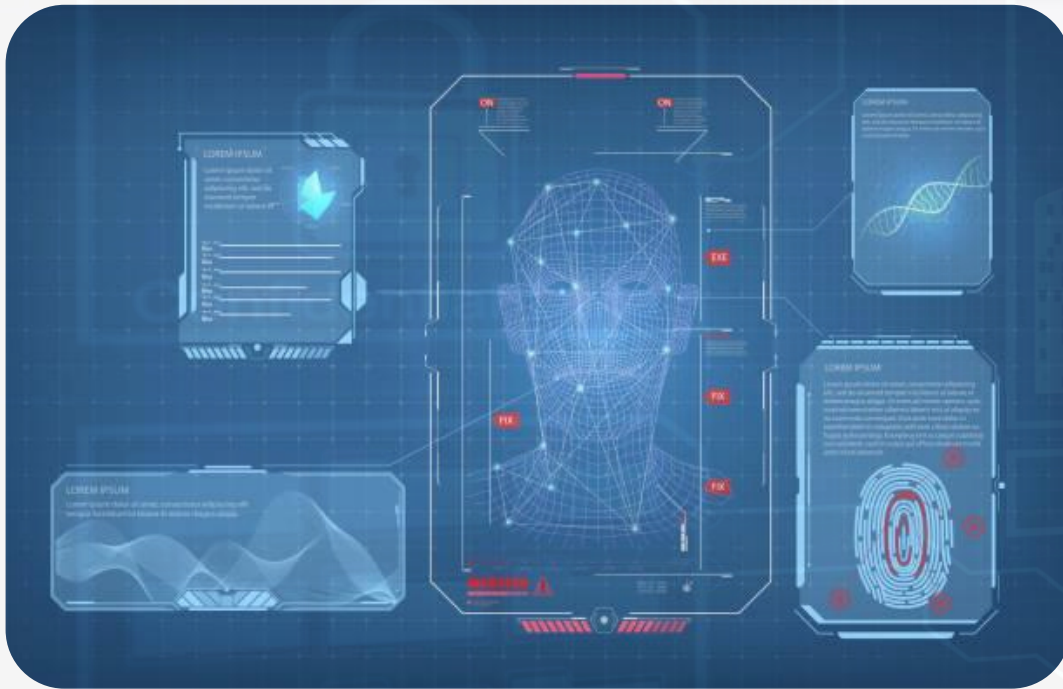
3. Companies marketing biometric identification technology in the field of security.

4. First experiences in the use of biometric identification for security purposes: real cases.

5. Biometric identification systems: legal aspects (GDPR).

6. Future regulation in the EU: the Artificial Intelligence Regulation.

1. Biometric identification systems: technical aspects.




Unlike video capture and processing systems, for example, which require the installation of physical devices, facial recognition is a software functionality which can be implemented within existing systems (cameras, image databases, etc.).

Guidelines on facial recognition, Consultative Committee of Convention 108 the Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, June 2021.

- “A **biometric template** is a digital representation of the unique features that have been extracted from a biometric sample and can be stored in a biometric database.
- This **template** is supposed to be unique and specific to each person and it is, in principle, permanent over time. In the recognition phase, the device compares this template with other templates previously produced or calculated directly from biometric samples such as faces found on an image, photo or video.
- "**Facial recognition**" is therefore a two-step process: the collection of the facial image and its transformation into a template, followed by the recognition of this face by comparing the corresponding template with one or more other templates”

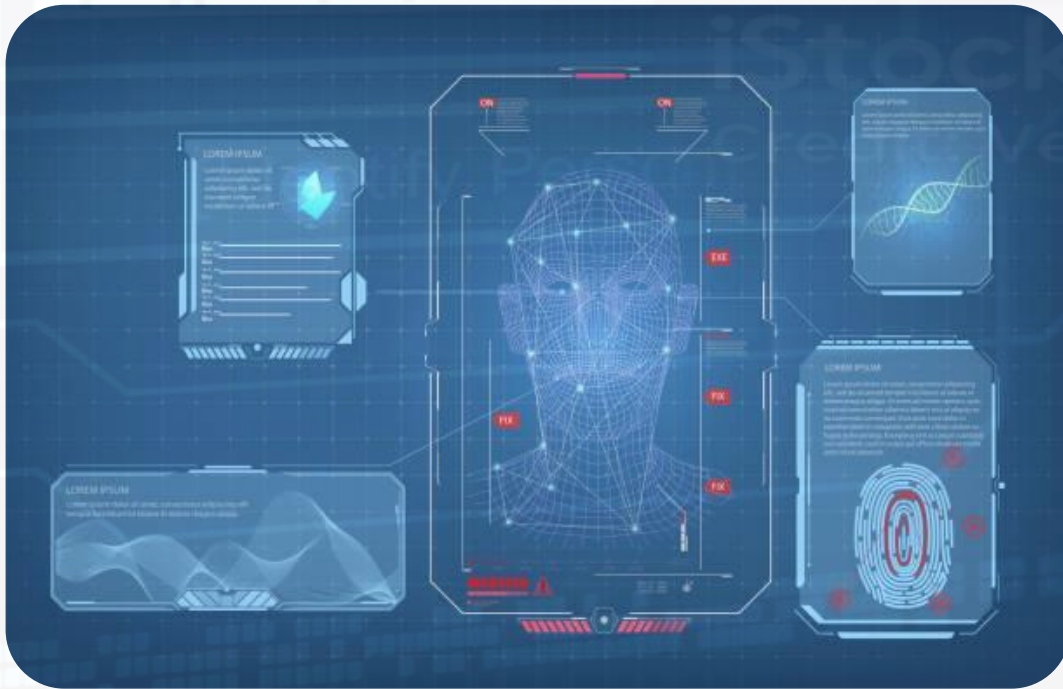
Guidelines on facial recognition, Consultative Committee of Convention 108 the Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, June 2021.



“**Facial recognition technology (FRT)** may be used to automatically recognise individuals based on their face. FRT often is based on artificial intelligence such as machine learning technologies. Applications of FRT are increasingly tested and used in various areas, from individual use to private organisations and public administration use. Law enforcement authorities (LEAs) also expect advantages from the use of FRT. It promises solutions to relatively new challenges such as investigations involving a big amount of captured evidence, but also to known problems, in particular with regard to understaffing for observation and search tasks”


[**Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement**](#)

1. Biometric identification systems: technical aspects.



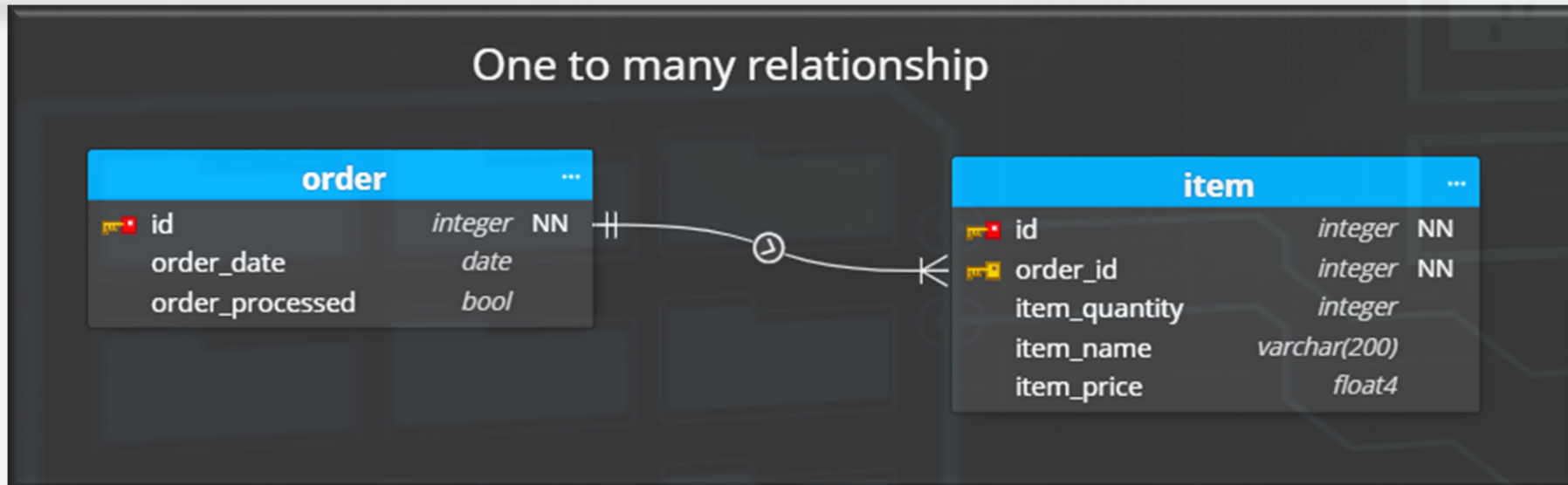
‘**biometric data**’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data (GDPR, Art. 4)

‘**personal data**’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;



‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

1. Biometric identification systems: technical aspects.



Source: Datsen <https://www.datasen.com/blog/er-diagram/one-to-many-relationships/>

In a relational database, a one-to-many relationship exists when one row in table A may be linked with many rows in table B, but one row in table B is linked to only one row in table A. It is important to note that a one-to-many relationship is not a property of the data, but rather of the relationship itself.

1. Biometric identification systems: technical aspects.

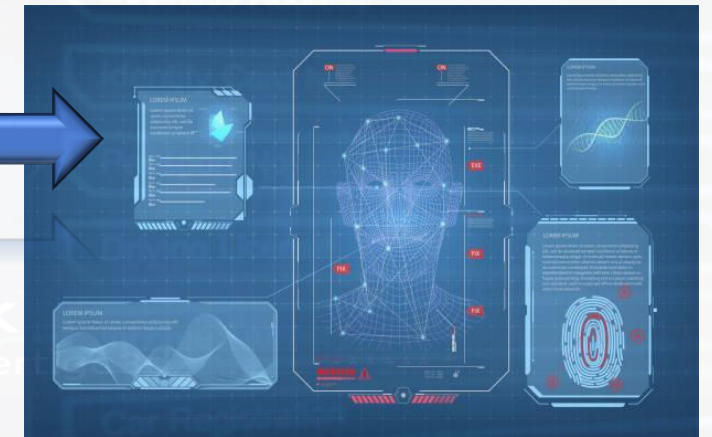


Customers table

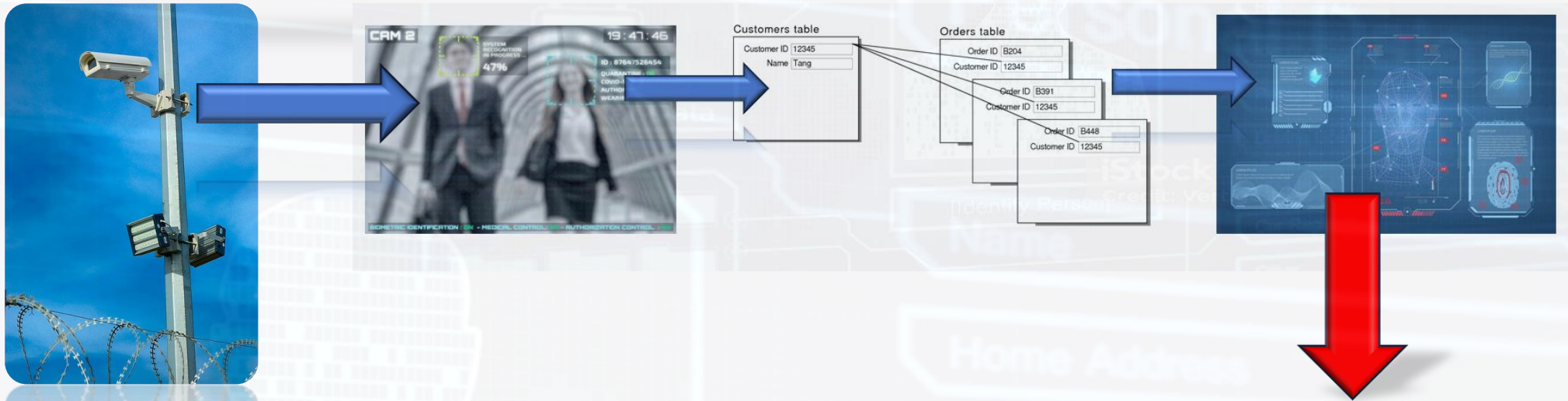
Customer ID	12345
Name	Tang

Orders table

Order ID	B204	Customer ID	12345
Order ID	B391	Customer ID	12345
Order ID	B448	Customer ID	12345



1. Biometric identification systems: technical aspects.



“More and more law enforcement authorities (LEAs) apply or intend to apply facial recognition technology (FRT). It may be used to authenticate or to identify a person and can be applied on videos (e.g. CCTV) or photographs. It may be used for various purposes, including to search for persons in police watch lists or to monitor a person’s movements in the public space”

[Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement](#)



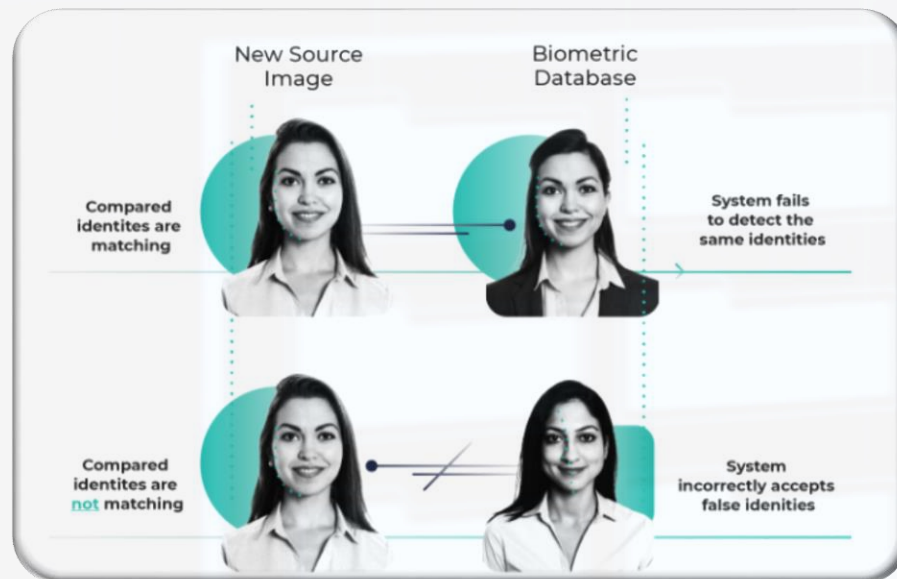
1. Biometric identification systems: technical aspects.

ISO/IEC 19795-1:2021

Information technology — Biometric performance testing and reporting — Part 1: Principles and framework

Establishes general principles for testing the performance of biometrics systems in terms of error rates and throughput rates for purposes including measurement of performance, prediction of performance, comparison of performance, and verifying conformance with specified performance requirements;

1. Biometric identification systems: technical aspects.



Accuracy Terms + Definitions

In biometrics, errors occur when two samples of one person do not match – this is called a **false negative**. Correspondingly, errors occur when samples from two persons do match – this is called a **false positive**.

1. Biometric identification systems: technical aspects.

This degree of accuracy is only possible in ideal conditions where there is consistency in lighting and positioning, and where the facial features of the subjects are clear and unobscured. In real world deployments, accuracy rates tend to be far lower. For example, the US Department of Commerce found that the error rate for one leading algorithm climbed from 0.1% when matching against high-quality mugshots to 9.3% when matching instead to pictures of individuals captured “in the wild,” where the subject may not be looking directly at the camera or may be obscured by objects or shadows



1. Biometric identification systems: technical aspects.



Photo: Kevin Frayer/Getty Images

Gender and race biases have been especially documented, with the accuracy of facial recognition technology varying significantly and being less accurate for women and people of colour than for white men.

J. Buolamwini and T. Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 2018. See also J. Cavazos et al., Accuracy Comparison Across Face Recognition Algorithms: Where Are We on Measuring Race Bias?, IEEE Transactions on Biometrics, Behaviour and Identity Science, 2021.

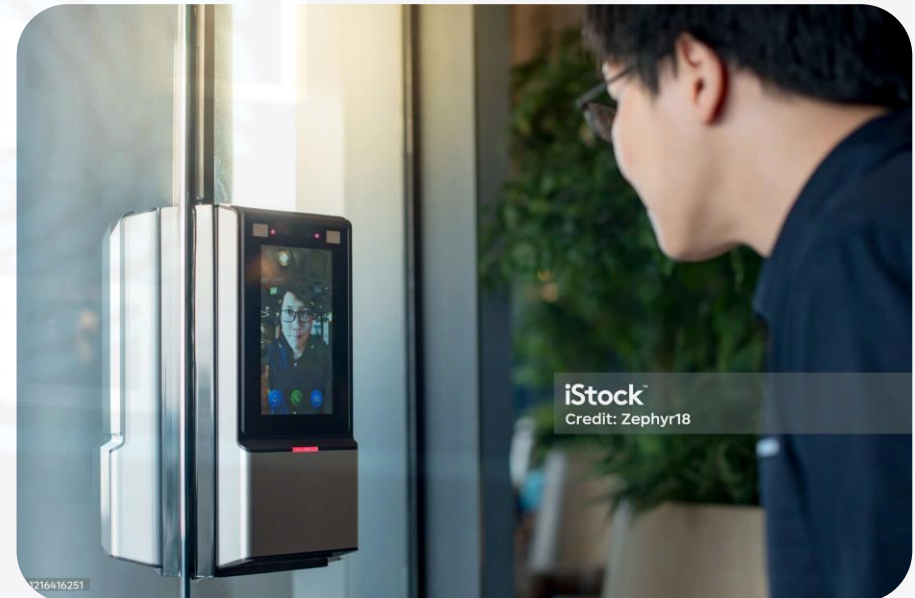
2. Biometric identification systems in public and private security.

“More and more law enforcement authorities (LEAs) apply or intend to apply facial recognition technology (FRT). It may be used to authenticate or to identify a person and can be applied on videos (e.g. CCTV) or photographs. It may be used for various purposes, including to search for persons in police watch lists or to monitor a person’s movements in the public space”
[Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement](#)

- **Searching**, in a database of photographs, for the identity of an **unidentified person** (victim, suspect, etc.); -
- **Monitoring of a person’s movements** in the public space. His or her face is compared with the biometric templates of people travelling or having travelled in the **monitored area**, for example when a piece of luggage is left behind or after a crime has been committed;
- **Reconstructing a person’s journey** and their subsequent interactions with other persons, through a delayed comparison of the same elements in a bid to identify their contacts for example;
- **Remote biometric identification** of wanted persons in public spaces. All faces captured live by video-protection cameras are cross-checked, in real time, against a database held by the security forces.

2. Biometric identification systems in public and private security.

Facial recognition authentication can aim at controlling physical access to one or more predetermined locations, such as entrances to buildings or specific crossing points.

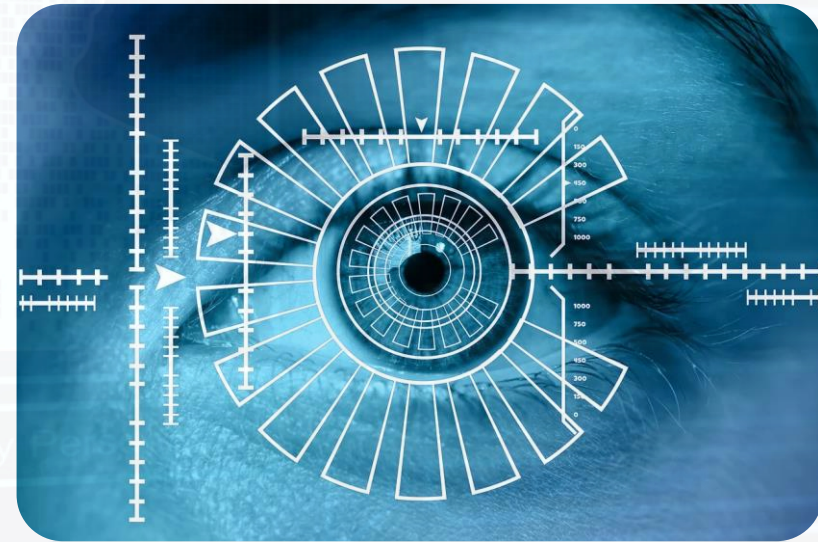


3. Companies marketing biometric identification technology in the field of security.

Top Biometrics Companies

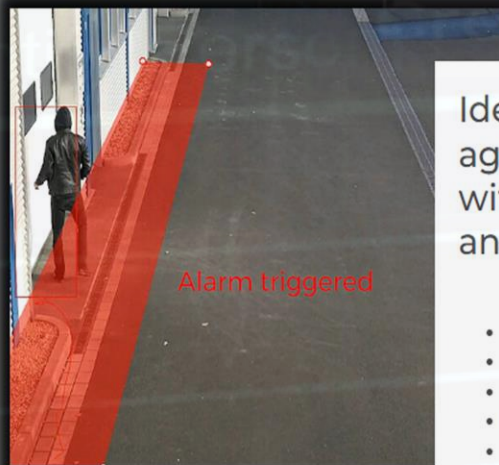
- Uniphore. Private Company. Founded 2008....
- ID-Pal. Private Company. Founded 2016. ...
- Oloid AI. Private Company. Founded 2018. ...
- Yoti. Private Company. Founded 2015. ...
- Cipher Skin. Private Company. Founded 2014. ...
- ThoughtSpot. Private Company. Founded 2012. ...
- Torche. Private Company. Founded 2021. ...
- IDEMIA SA. n/a. Founded 2007.

Source: Venture Radar



<https://www.ventureradar.com/keyword/Biometrics>

3. Companies marketing biometric identification technology in the field of security.



Identify what's important in your images using tailored artificial intelligence with the help of our intelligent video analysis software.

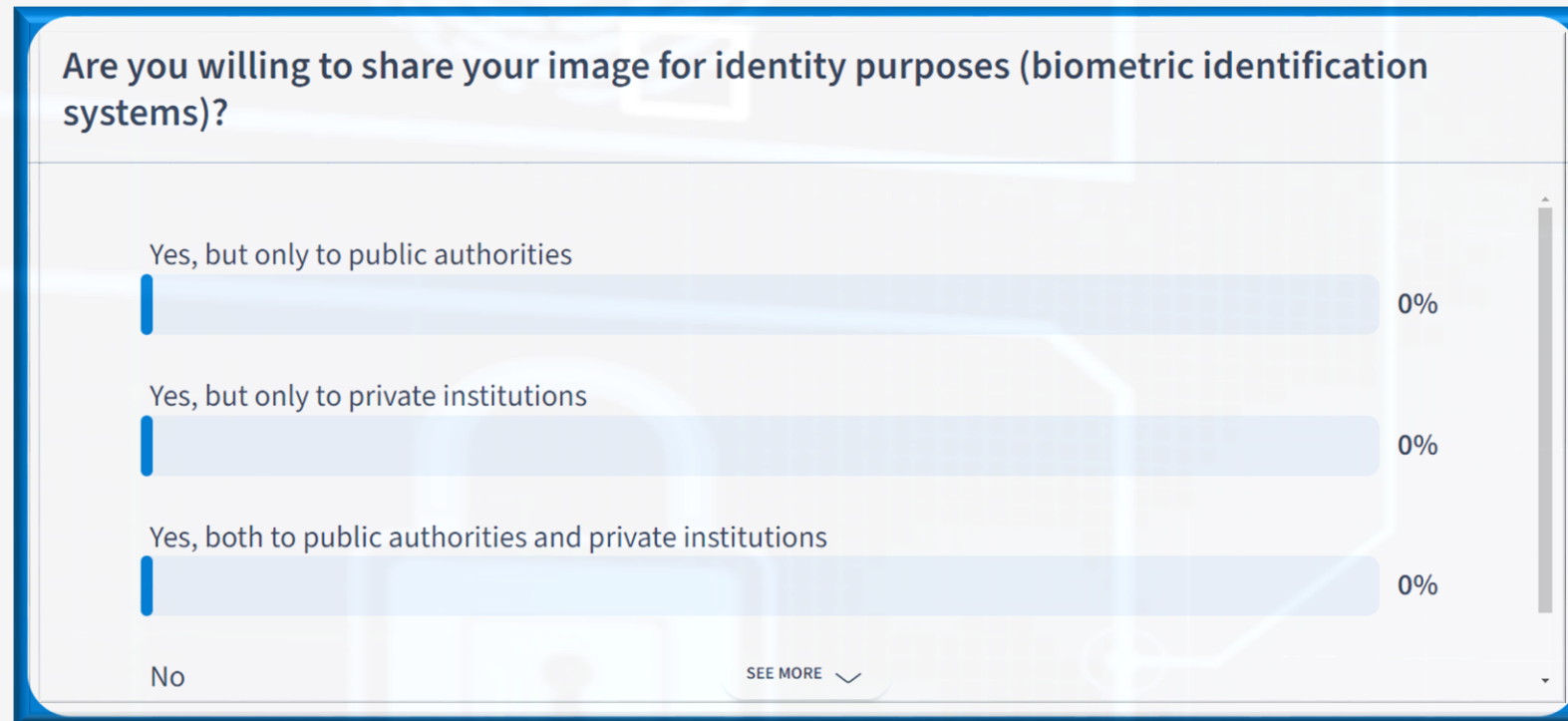
- Recognise and count objects using artificial intelligence
- Reliable perimeter protection day and night
- Evaluation based on size, direction and speed
- Number plate recognition for vehicle management
- Cross-site facial recognition
- Redundant and scalable



Details about the products >>

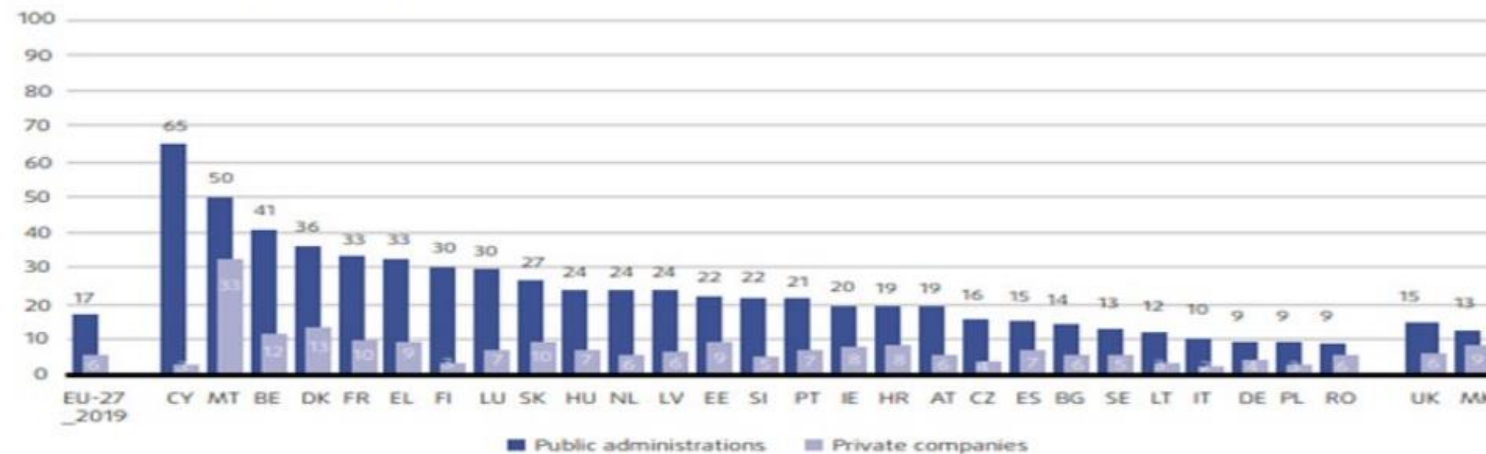
4. First experiences in the use of biometric identification for security purposes: real cases.

[PollEv.com/javierdoradoferrer843](https://poll-ev.com/javierdoradoferrer843)



4. First experiences in the use of biometric identification for security purposes: real cases.

Figure 2 – Willingness to share facial images for identity with public authorities and private companies, by country



Source: European Union Agency for Fundamental Rights, [Your rights matter: Data protection and privacy](#), 2020.

4. First experiences in the use of biometric identification for security purposes: real cases.

- Look for real cases in which biometric identification systems were applied for security purposes
 - It can be cases of private or public security
 - Preferably, it should be from your own country

4. First experiences in the use of biometric identification for security purposes: real cases.

Country	Use cases	Relevant case law, administrative decisions and legislation
France	<p>FRT pilot projects at schools in Nice and Marseille:</p> <p>FRT was tested to help safety agents to control access to two high schools, to prevent intrusions and identity theft and to reduce the duration of these controls.</p> <p>ALICEM ID system:</p> <p>In 2020, the French Ministry of Home affairs launched ALICEM (Certified online authentication on mobile phones), a smartphone application using FRT to allow individuals to prove their identity on the internet in a secure manner, using their smartphone and their passport or residence permit.</p>	<p>The administrative court of Marseille annulled the Marseille municipality decision to authorise FRT testing in the two schools in Nice and Marseille.</p> <p>The French data protection authority (CNIL) released a positive opinion on a draft decree authorising the creation of the <i>ALICEM</i> system.</p>

4. First experiences in the use of biometric identification for security purposes: real cases.

Germany	Crime prevention at train station: In 2019, the police piloted the use of FRT to detect suspicious behaviour at the Südkreuz train station in Berlin.	Name
	Crime investigation at G20 summit: During the 2017 G20 summit , the police authorities of the city of Hamburg deployed FRT for the detection and investigation of crimes.	In the G20 context , a first instance court overruled the Hamburg DPA's order to delete the police database of biometric templates. The Hamburg DPA has appealed . The police authorities initially relied on Sections 161 and 163 in conjunction with Section 98c of the German Criminal Procedure Code (GCPC). Subsequently, they referred to Sections 161, 163 or, alternatively, Section 483 GCPC.

4. First experiences in the use of biometric identification for security purposes: real cases.

Spain	Surveillance at bus station: A live face recognition system was deployed in Madrid's South Station in 2016 to fight acts of vandalism and petty crime.
	Airport: Aena and Iberia operate a facial recognition system in the boarding process since 2019.
	Immigration: Facial recognition technology is used to improve border control and to increase security at border crossings in Ceuta.
	Supermarkets: The Spanish supermarket chain Mercadona rolled out FRT to detect people who received a restraining order or who have been banned by a court from supermarket premises.

4. First experiences in the use of biometric identification for security purposes: real cases.

Italy	<p>Automatic Image Recognition System: An Automatic Image Recognition System (SARI) is <u>used</u> by the police forces for identification purposes since 2019.</p>	<p>On 16 April 2021, the Italian data protection authority issued an <u>opinion</u> stating that the SARI system would result in a form of indiscriminate/mass surveillance if used as designed.</p> <p>A draft bill <u>proposed</u> a moratorium on the use on the use of facial recognition technologies in public spaces.</p>
-------	--	--

4. First experiences in the use of biometric identification for security purposes: real cases.

<p>Netherlands</p>	<p>Events control: Municipalities are using facial recognition technology during carnivals and other large events.</p> <p>Police control: Since 2016, the Dutch police use a system of facial recognition technology called CATCH, aimed at identifying suspects or convicts of crimes through a criminal justice database.</p> <p>Police are also trialling the use of real-time facial recognition technology through smartphone pictures, body cams, and the cloud.</p>	<p>The Dutch DPA issued a Recommendation in which it is critical of the current biometric legal framework (<i>Wet Biometrie Vreemdelingenketen</i> (Wbvk)) and disapproves of the extension of its application period.</p>
--------------------	--	--

4. First experiences in the use of biometric identification for security purposes: real cases.

TECHNOLOGY

Wrongfully arrested man sues Detroit police over false facial recognition match

The case could fuel criticism of police investigators' use of a controversial technology that has been shown to perform worse on people of color

By Drew Harwell
April 13, 2021



<https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>

A faulty system

A nationwide debate is raging about [racism in law enforcement](#). Across the country, millions are protesting not just the actions of individual officers, but bias in the systems used to surveil communities and identify people for prosecution.

Facial recognition systems have been used by police forces for [more than two decades](#). Recent studies by [M.I.T.](#) and the [National Institute of Standards and Technology](#), or NIST, have found that while the technology works relatively well on white men, the results are less accurate for other demographics, in part because of a lack of diversity in the images used to develop the underlying databases.

4. First experiences in the use of biometric identification for security purposes: real cases.

European Convention on Human Rights



ARTICLE 14

Prohibition of discrimination

The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

4. First experiences in the use of biometric identification for security purposes: real cases.

Charter of Fundamental Rights of the European Union

Article 20

Equality before the law

Everyone is equal before the law.

Article 21

Non-discrimination

1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.
2. Within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited.



4. First experiences in the use of biometric identification for security purposes: real cases.



Charter of Fundamental Rights of the European Union

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

4. First experiences in the use of biometric identification for security purposes: real cases.

In 2021, we witnessed the failed "pilot" of the Mercadona organisation, based on the installation of biometric identification systems in its shops, which culminated in a sanction by the Spanish Data Protection Agency (hereinafter, AEPD) of 3.15 million euros. However, due to the organisation's voluntary payment, the amount was reduced to 2 million.

As alleged by Mercadona, the system was implemented to detect "solely and exclusively" individuals who had been previously convicted by a final judgment for acts committed against the persons, goods or workers of the organisation.



4. First experiences in the use of biometric identification for security purposes: real cases.



The system installed, in fact, automatically captured indiscriminately and indiscriminately the image of any person who entered its establishments, storing a pattern that was subsequently compared with the stored pattern of those persons previously convicted. In this way, the organisation was dealing with biometric data; data considered as special category data under Article 9 of the General Data Protection Regulation.

4. First experiences in the use of biometric identification for security purposes: real cases.

It has also been stressed that using facial recognition technologies **to process facial images captured by video cameras in the public space may interfere with a person's freedom of opinion and expression** and have a negative effect on their freedom of assembly and of association.



5. Biometric identification systems: legal aspects (GDPR).



5. Biometric identification systems: legal aspects (GDPR).

Since the use of FRT implies the processing of data for the purpose of identification, its use by public authorities constitutes an interference with the **right to data protection**, as set out in Article 8 CFR and the **right to private life** under Article 7CFR. More specifically, the initial video-recording, the subsequent retention of the footage, and the comparing of footage with database records for the purpose of identification (matching), all present interferences with or limitations on this right. **Any limitation on these fundamental rights must be strictly necessary and proportionate pursuant Article 52(1) CFR**



Regulating facial
recognition in
the EU

5. Biometric identification systems: legal aspects (GDPR).

Article 9

Processing of special categories of personal data

1. 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 prohibited**.

Exceptions

Explicit consent

Social security and social protection law

Vital interests

public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued

Others...

5. Biometric identification systems: legal aspects (GDPR).

Article 10

Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences, or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.



5. Biometric identification systems: legal aspects (GDPR).



Article 22

Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph 1 shall not apply if the decision:
 - (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
 - (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
 - (c) is based on the data subject's explicit consent.

6. Future regulation in the EU: the Artificial Intelligence Regulation.

The European Parliament has called for limits to the use of facial recognition in the EU on several occasions. The Parliament has highlighted that the gathering and use of biometric data for remote identification purposes (such as facial recognition) in public areas bears particular risks for fundamental rights and stressed that such technology should only be deployed and used by Member States' public authorities for substantial public interest purposes



6. Future regulation in the EU: the Artificial Intelligence Regulation.



The European Commission unveiled a new proposal for an EU regulatory framework on AI in April 2021. The legal framework focuses on the specific utilisation of AI systems and associated risks. The Commission proposes to enshrine a technology-neutral definition of AI systems in EU law and to lay down a classification for AI systems with different requirements and obligations tailored on a 'risk-based approach'.



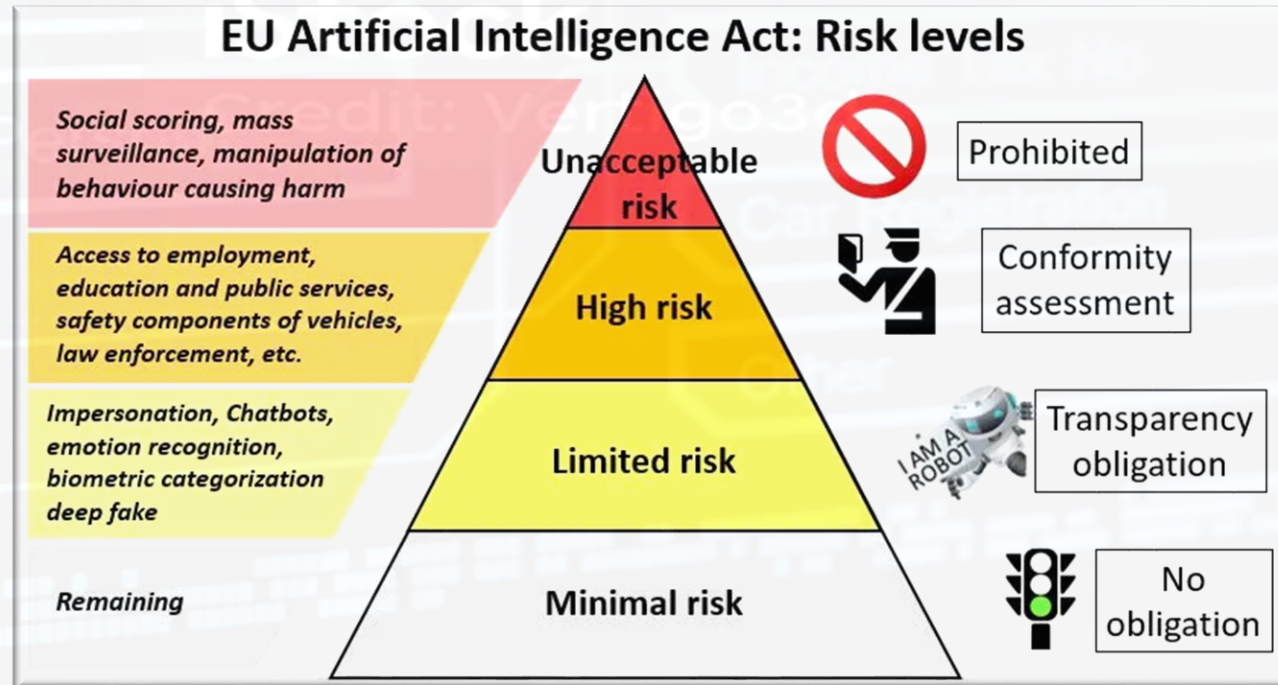
6. Future regulation in the EU: the Artificial Intelligence Regulation.

‘**Artificial intelligence system**’ (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with

ANNEX I ARTIFICIAL INTELLIGENCE TECHNIQUES AND APPROACHES

- (a) **Machine learning approaches**, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;
- (b) **Logic- and knowledge-based approaches**, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;
- (c) **Statistical approaches**, search and optimization methods.

6. Future regulation in the EU: the Artificial Intelligence Regulation.



(Source: Telefónica)

6. Future regulation in the EU: the Artificial Intelligence Regulation.

Social scoring, mass surveillance, manipulation of behaviour causing harm

Unacceptable risk



Prohibited

Title II establishes a list of prohibited AI. The regulation follows a risk-based approach, differentiating between uses of AI that create:

- (i) **an unacceptable risk,**
- (ii) a high risk, and
- (iii) low or minimal risk.

The list of prohibited practices in Title II comprises all those AI systems whose use is considered unacceptable as contravening Union values, for instance by violating fundamental rights.

6. Future regulation in the EU: the Artificial Intelligence Regulation.

Social scoring, mass surveillance, manipulation of behaviour causing harm

Unacceptable risk



Prohibited

Certain particularly harmful AI practices are prohibited as contravening Union values (article 5). They are considered a clear threat to people's safety, livelihoods and rights and are banned because of the 'unacceptable risk' they create. This includes systems that are designed to manipulate human behaviour through subliminal techniques and social scoring by governments.

6. Future regulation in the EU: the Artificial Intelligence Regulation.

REGULATED FRTs ²⁰⁹	Real-time [remote] facial recognition systems in publicly accessible spaces for law enforcement purposes	
Rule	prohibited as matter of principle (unacceptable risk)	permitted for specific exceptions (high risk) <ul style="list-style-type: none">- search for victims of crime- threat to life or physical integrity or of terrorism- serious crime (EU arrest warrant)
Conditions		- ex-ante authorisation (judicial authority or independent administrative body)

EPRS | European Parliamentary Research Service Authors:
Tambiana Madiega and Hendrik Mildebrath Members'
Research Service PE 698.021 – September 2021

6. Future regulation in the EU: the Artificial Intelligence Regulation.



PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES



Art. 5.1 The following artificial intelligence practices shall be prohibited

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

(I) the targeted search for specific potential victims of crime, including missing children;

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

6. Future regulation in the EU: the Artificial Intelligence Regulation.

Art. 5.1 The following artificial intelligence practices shall be prohibited



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

(III) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA [62](#) and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State.



Scope of the European arrest warrant

6. Future regulation in the EU: the Artificial Intelligence Regulation.

Scope of the European arrest warrant

The following offences, if they are punishable in the issuing Member State by a custodial sentence or a detention order for a maximum period of at least three years and as they are defined by the law of the issuing Member State, shall, under the terms of this Framework Decision and without verification of the double criminality of the act, give rise to surrender pursuant to a European arrest warrant:



6. Future regulation in the EU: the Artificial Intelligence Regulation.



- participation in a criminal organisation,
- terrorism,
- trafficking in human beings,
- sexual exploitation of children and child pornography,
- illicit trafficking in narcotic drugs and psychotropic substances,

- illicit trafficking in weapons, munitions and explosives,
- corruption,
- fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests,
- laundering of the proceeds of crime,
- counterfeiting currency, including of the euro,
- computer-related crime,

- environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,
- facilitation of unauthorised entry and residence,
- murder, grievous bodily injury,
- illicit trade in human organs and tissue,
- kidnapping, illegal restraint and hostage-taking,
- racism and xenophobia,
- organised or armed robbery,
- illicit trafficking in cultural goods, including antiques and works of art,
- swindling,
- racketeering and extortion,
- counterfeiting and piracy of products,
- forgery of administrative documents and trafficking therein,
- forgery of means of payment,
- illicit trafficking in hormonal substances and other growth promoters,
- illicit trafficking in nuclear or radioactive materials,
- trafficking in stolen vehicles,
- rape,
- arson,
- crimes within the jurisdiction of the International Criminal Court,
- unlawful seizure of aircraft/ships,
- sabotage.

6. Future regulation in the EU: the Artificial Intelligence Regulation.

The use of ‘real-time’ remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall take into account the following elements:

- (a) the nature of the situation giving rise to the possible use, in particular the seriousness, **probability and scale of the harm** caused in the absence of the use of the system;
- (b) the **consequences of the use of the system for the rights and freedoms of all persons concerned**, in particular the seriousness, probability and scale of those consequences.



6. Future regulation in the EU: the Artificial Intelligence Regulation.



As regards paragraphs 1, point (d) and 2, each individual use for the purpose of law enforcement of a ‘real-time’ remote biometric identification system in publicly accessible spaces **shall be subject to a prior authorisation granted by a judicial authority or by an independent administrative authority** of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law.

However, in a **duly justified situation of urgency**, the use of the system may be commenced without an authorisation and the authorisation may be requested only during or after the use.

6. Future regulation in the EU: the Artificial Intelligence Regulation.

Title II establishes a list of prohibited AI. The regulation follows a risk-based approach, differentiating between uses of AI that create:

- (i) an unacceptable risk,
- (ii) a **high risk**, and
- (iii) low or minimal risk.

The list of prohibited practices in Title II comprises all those AI systems whose use is considered unacceptable as contravening Union values, for instance by violating fundamental rights.



6. Future regulation in the EU: the Artificial Intelligence Regulation.

Biometric identification and categorisation of natural persons:

AI systems intended to be used for the ‘real-time’ and ‘post’ remote biometric identification of natural persons.



6. Future regulation in the EU: the Artificial Intelligence Regulation.



Management and operation of critical infrastructure:

AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity.

6. Future regulation in the EU: the Artificial Intelligence Regulation.

Education and vocational training:

- (a) AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions;
- (b) AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions.



6. Future regulation in the EU: the Artificial Intelligence Regulation.



Employment, workers management and access to self-employment:

- (a) AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests;
- (b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behavior of persons in such relationships.

6. Future regulation in the EU: the Artificial Intelligence Regulation.

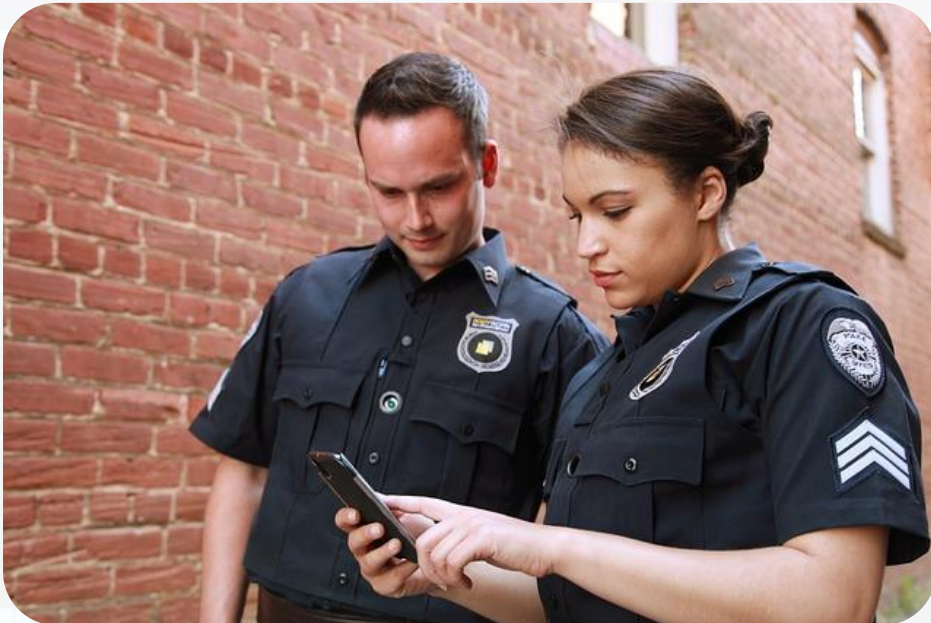
Access to and enjoyment of essential private services and public services and benefits:

(c) AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid.



6. Future regulation in the EU: the Artificial Intelligence Regulation.

Law enforcement:



- (a) AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences;
- (b) AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person;
- (c) AI systems intended to be used by law enforcement authorities to detect deep fakes as referred to in article 52(3);

6. Future regulation in the EU: the Artificial Intelligence Regulation.

Law enforcement:

(d) AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences;



(e) AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups;



6. Future regulation in the EU: the Artificial Intelligence Regulation.

Migration, asylum and border control management:



(a) AI systems intended to be used by competent public authorities as polygraphs and similar tools or to detect the emotional state of a natural person;

(b) AI systems intended to be used by competent public authorities to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State;

6. Future regulation in the EU: the Artificial Intelligence Regulation.

Administration of justice and democratic processes:

- (a) AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts.



6. Future regulation in the EU: the Artificial Intelligence Regulation.

Requirements for high-risk AI systems



The **risk management system** shall consist of a continuous iterative process run throughout the entire lifecycle of a **high-risk AI system**, requiring regular systematic updating. It shall comprise the following steps:

- (a) **identification and analysis** of the known and foreseeable risks associated with each high-risk AI system;
- (b) **estimation and evaluation of the risks** that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse
- (c) evaluation of other possibly arising risks based on the **analysis of data gathered from the post-market monitoring** system.
- (d) **adoption of suitable risk management measures** in accordance with the provisions of the following paragraphs.

6. Future regulation in the EU: the Artificial Intelligence Regulation.

Requirements for high-risk AI systems



Training, **validation and testing data sets** shall be subject to appropriate data governance and management practices. Those practices shall concern in particular,

- (a) the relevant **design** choices;
- (b) **data collection**;
- (c) **relevant data preparation processing operations**, such as annotation, labelling, cleaning, enrichment and aggregation;
- (d) the **formulation of relevant assumptions**, notably with respect to the information that the data are supposed to measure and represent;
- (e) a **prior assessment of the availability**, quantity and suitability of the data sets that are needed;
- (f) examination in view of **possible biases**;
- (g) the identification of any possible **data gaps or shortcomings**, and how those gaps and shortcomings can be addressed.

6. Future regulation in the EU: the Artificial Intelligence Regulation.

Requirements for high-risk AI systems

Human oversight



The measures referred to shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances:

- (a) fully understand the capacities and **limitations of the high-risk** AI system and be able to duly monitor its operation, so that signs of anomalies, **dysfunctions and unexpected performance** can be detected and addressed as soon as possible;
- (b) remain aware of the possible tendency of automatically relying or **over-relying on the output produced** by a high-risk AI system (**‘automation bias’**), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons;

6. Future regulation in the EU: the Artificial Intelligence Regulation.

Requirements for high-risk AI systems

Human oversight



The measures referred to shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances:

- (c) be able to correctly **interpret the high-risk AI system's output**, taking into account in particular the characteristics of the system and the interpretation tools and methods available;
- (d) be able to **decide**, in any particular situation, not to use the high-risk AI system or otherwise **disregard, override** or **reverse** the output of the high-risk AI system;
- (e) be able to **intervene on the operation of the high-risk AI system** or interrupt the system through a “stop” button or a similar procedure.

Thank you for your attention