dasGate

by das·nano

GUIDELINES 05/2021 ON THE USE OF FACIAL RECOGNITION TECHNOLOGY IN THE AREA OF LAW ENFORCEMENT

Response to public consultation

27th June, 2022

CONTENT

EXECUTIVE SUMMARY 3

0. Introduction 5

1. State-of-the-art biometric technology 5

1.1. AI-based biometric models 6

1.1.1. Irreversibility 8

1.1.2. Non-interoperability 8

1.1.3. Renewability 9

1.1.4. Temporality 9

1.1.5. Controlled use 9

1.2. Accuracy and reliability of state-of-the-art facial biometric systems 10

1.2.1. Standards that guarantee accuracy and reliability 12

1.3. Non-biased and non-discriminatory biometric systems 12

1.4. Presentation attack detection 13

2. How can this biometric technology be implemented? 14

2.1. Biometric verification and Biometric identification 14

2.2. Regulating biometrics depending on its application (risk-based approach) 16

2.2.1. Biometrics as a right vs. biometrics as monitoring means 17

2.2.2. Four categories of biometric technologies application 18

3. Conclusions 21

4. Amendment request to Guidelines 05/2022 23

EXECUTIVE SUMMARY

In response to the public consultation of Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, VERIDAS and DAS-GATE want to summit some amendment proposals since, in their opinion as experts in the biometric technology development sector, the Guidelines include misunderstandings and generalities that need to be qualified and properly contextualized.

This document contains a detailed explanation of **how state-of-the-art biometric technology works**, which we hope will help the EDPB to understand aspects such as its accuracy, the absence of bias, the irreversibility of biometric templates or the possibility of regenerating these templates as many times as necessary.

The different applications that biometric technology can have are also presented, categorizing them according to a **risk-based approach**, as already proposed by the European Commission, and the EDPB itself seems to intend to adopt in its Guidelines.

Based on the explanation in sections 1 and 2 of this document, section 3 includes a proposal for amendments:

1. While these are guidelines relating to the use of facial recognition systems for law enforcement purposes, the EDPB ultimately makes a general assessment of all possible uses of biometric technology. Examples are correctly used to illustrate potential undesirable uses of biometric technology by law enforcement authorities. However, conclusions extracted from these examples are used to generalize the risks and potential effects of all biometric systems, which lead to a biased interpretation of this technology. Therefore, **the scope of application of these Guidelines (law enforcement purposes) shall be indicated and recommendations shall be made with respect to that scope**.

2. The Guidelines shall make express reference to the **user's power of disposal over his or her data**. Regulation shall be based on the **four different categories of face recognition use cases** described in section 2.2.2 of this document.

3. In this regard, **distinction shall be made between verification (1:1) and identification (1:N) implementations**, as it has been interpreted since the commencement of GDPR application, as they do not entail the same risks (precisely due to the conclusions in amendment 2 above).

4. **Applications based on the user's consent shall be considered as a legitimate use of biometric recognition**, as long as the user is duly informed of the functioning of the system and how his or her data is being processed (as well as other information requirements under the GDPR).

5. The regulation and implementation of these systems must be **risk-based approach**, balancing the fundamental rights that may be affected, and considering that the right to data protection is not the only right at risk.

6. **Some misunderstandings regarding biometric technology are included in the Guidelines**, such as reference to permanence and immutability and the impossibility of regenerating a biometric template. As explained in the sections above, this is not true when talking about state-of-the-art technologies, so **it shall be updated accordingly so as not to generate and spread misconceptions and myths**.

VERIDAS DIGITAL AUTHENTICATION SOLUTIONS, S.L. is a Spanish company dedicated to the design, development and deployment of digital identity verification solutions using proprietary technologies for identity document verification, face biometrics and voice biometrics. VERIDAS currently has more than 100 private and public entities using its technology worldwide, and more that 50 million validations have already been carried out. VERIDAS is currently one of the leaders in this field.

Our commitment with compliance and, more specifically, data protection and security obligations and recommendations, is the cornerstone of our business, basing our solutions on the principle of privacy by default and by design.

It is therefore our goal that effective regulations and guidelines are in place to ensure that in Europe (and in other countries that pursue the same values) the benefits of this biometric technology can be used, while limiting or prohibiting unwanted uses. To this end, VERIDAS wishes to provide its expertise in the sector, from a technological and legal point of view, to assist the EDPB in drafting its guidelines.

DAS-GATE ACCESS CONTROL SOLUTIONS, S.L. is a company of the same business group that uses VERIDAS' core biometric technologies. DAS-GATE has also submitted a response to these Guidelines 05/2022, the content of such response being identical to that provided by VERIDAS in this document.

0. Introduction

Regarding **Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement**[1], adopted on May 12, 2022 by the European Data Protection Board (EDPB), **VERIDAS DIGITAL AUTHENTICATION SOLUTIONS, S.L.** ("VERIDAS") and **DAS-GATE ACCESS CONTROL SOLUTIONS, S.L.** ("DAS-GATE") appreciate this opportunity to submit certain comments to the public consultation.

VERIDAS and DAS-GATE are Spain-based companies specialized in the provision of Phygital Identity solutions, based on biometric and digital ID verification. Considering VERIDAS and DAS-GATE knowledge of biometric technologies, their teams believe their input on the topic could be interesting for the understanding and regulation of the processing of biometric data.

VERIDAS and DAS-GATE appreciate the European Data Protection Board's intention to continue to provide clarity on the concepts regulated in the General Data Protection Regulation (GDPR) and how systems incorporating biometrics should be implemented.

However, it has been noted that the current regulation and guidelines in this field related to biometrics are sometimes biased or misleading, mainly due to two reasons: on the one hand, the understanding that biometric technology still works as it did 5 or 10 years ago, when in fact there have been great advances in the technique that make it possible to overcome many of the risks that existed a few years ago; and on the other hand, the consideration that all implementations of this technology entail or may entail the same risks for individuals, when in fact there are multiple use cases in which this technology can be used and the risks to the rights of data subjects vary greatly from one to another, being sometimes even nonexistent.

Therefore, it is the intention of VERIDAS and DAS-GATE to provide in this document to the EDPB accurate and complete information on how state-of-the-art biometric technology currently works, as well as the different implementations it may have, with the desire that the EDPB take it into account for the regulation and adaptation of its guidelines on the matter.

1. State-of-the-art biometric technology

According to ISO 2382-37, biometrics is "the automated recognition of individuals based on their biological and behavioral characteristics".

In fact, this is a straightforward definition of a complex technology that is continuously changing and improving in terms of accuracy and safety.

Biometric recognition is based on physical, physiological or behavioral characteristics (biometric characteristics). Since its beginnings, a wide range of systems have been developed, calling on an increasing number of biometric characteristics while, at the same time, broadening the use cases it can be applied to. Nowadays, biometrics based on the physical characteristics of the individual (and

[1] https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf

especially, face image) is arguably the most widespread, developed and, therefore, mature biometric system.

Given the widespread implementation of biometric technologies in a wide range of use cases, which has been further accelerated in the wake of the COVID-19 pandemic, correctly understanding biometrics from a technological point of view is deemed to be of the utmost importance, so that regulation of these systems is based on knowledge of how state-of-the-art technology works, and therefore requires no less than what is already possible when it comes to privacy and security, while at the same time not "over-regulating" aspects that are not necessary anymore.

The precision and accuracy of biometric technologies rests on the type of biometric data captured, how it is captured, how it is processed and how it is used to identify and authorize the individual whose identity is to be confirmed. Nevertheless, these technological variables not only influence the accuracy of the result but also, and primarily, its security, risk mitigation and strict compliance with the requirements of the European General Data Protection Regulation.

This Section 1 sets out **how biometric technologies work, explaining in particular those issues that are of most concern from the data protection and respect of fundamental rights perspective**. For example, aspects such as non-discrimination of biometric systems, mechanisms for the detection of presentation attacks, the irreversibility and non-interoperability of biometric data,... are discussed.

1.1. AI-based biometric models

Article 25 of the General Data Protection Regulation (Regulation EU 2016/679) sets forth the **principles of data protection by design and default**. These principles aim to, taking into account the state of the art, the costs and the nature, scope, context and purposes of the processing, and the potential risks that could arise, apply the most appropriate technical and organizational measures to ensure the principles of data protection and protect the rights of data subjects. This may come in the form of multiple actions, however, when it comes to biometric recognition, we must refer to the use of advanced and state-of-the-art technologies that provide a high level of protection.

It could be said that the key element in a biometric recognition system is the biometric engine used. Logically, this is from a technical point of view, insofar as the most advanced engines provide greater precision and reliability, better system accuracy; however, it is also so in terms of guaranteeing data protection and user privacy. The fact is that the cutting-edge biometric technologies that have become state-of-the-art have some basic characteristics themselves that make them highly secure with regard to privacy.

To understand the above, we can distinguish between two types of biometric engine models:

- **Biometric models based on landmarks or "Old-school" models**

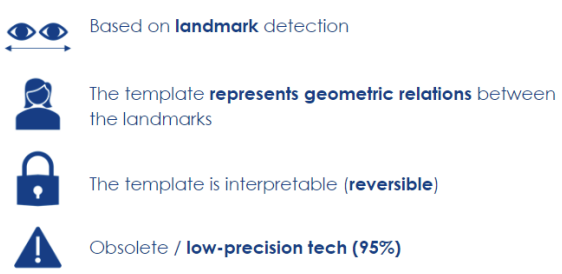
  "Old-school" biometric engines were the most widespread until around 5 or 10 years ago, and are based on 'landmarks' or characteristic points to recognize a face, for example. This method involves taking measurements between multiple points of the biometric characteristic, such as a facial image, resulting in a mathematical

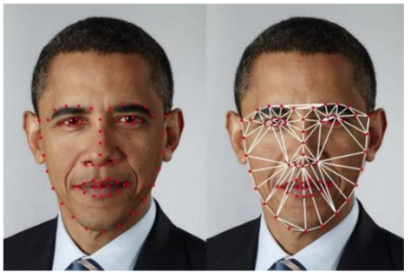
representation (usually known as “template” or “vector”), which is a summary of these measurements. This is where the name *bio-metrics* comes from.

Nevertheless, this type of model carries a data protection risk, since an individual with sufficient knowledge of the system could be capable, in view of the vector generated with this engine, of interpreting the measurements that this template is representing of the characteristic points of the subject’s face (e.g. facial image: the distance between the eyes, between the ears, etc.), and therefore obtain an estimation of the original image. Therefore, with this information, it could be possible to reconstruct the original image and identify the subject (something similar to how we would do a composite picture).

Furthermore, these systems are mostly standardized, which means that anyone can learn how to use them (the standards are public through organizations such as NIST). While this makes these technologies interoperable (such as fingerprint recognition systems), the data protection implications could be severe and non-desirable.

It should be noted that **this was the biometric technology used back in 2012 when first guidelines on this field were published by the Article 29 Working Group, and in 2016 when the GDPR was approved. But this is not the case anymore**.



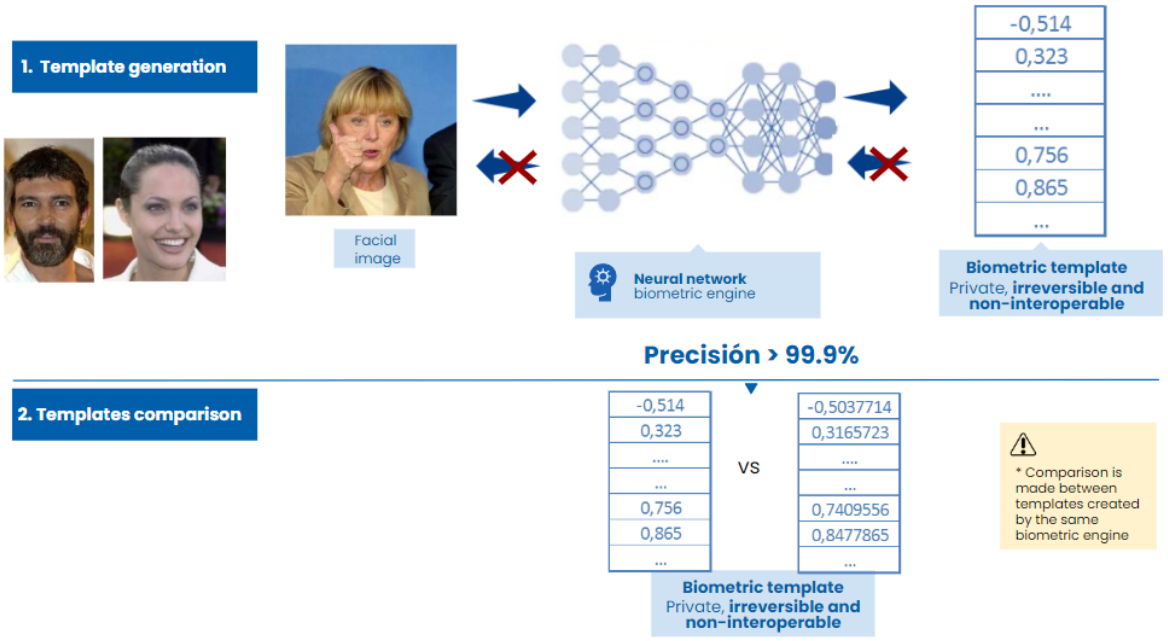


- **Biometric models based on Artificial Intelligence**

Companies developing state-of-the-art technology have moved away from “old-school” models towards models based on Artificial Intelligence and, more specifically, neural networks.

With this model, the mathematical representation is not generated as simply as measuring the subject’s biometric characteristic points. In this case, the result is going to be a mathematical vector that relies on the Artificial Intelligence of the biometric engine (the system may have other mathematical variables; however, the Artificial Intelligence algorithms are the key components of the model). This implies that if, for example, a facial image is run through two different biometric engines (or even through two different versions of the same engine), the resulting vector will be completely different.

As a result, in the Artificial Intelligence-based model, not even the expert engineer who has designed the system is able to interpret the vector with the aim of extracting information from the individual who provided their data. Therefore, by having a vector, it is not possible to extract information about the individual it belongs to or to identify them. Having such a vector, therefore, does not mean that the biometric information has been compromised or that it can no longer be cancelled.



Finally, it should also be noted that the accuracy levels achieved with a model using neural networks are much higher (99.8%) than those of landmark-based models (95%). In other words, the error level of a landmark-based model is about 100 times higher than that of a landmark-based model.

As can be deduced from the above, opting for a system based on one type of engine or another is decisive with regard to the privacy of the processing and its results, as well as with regard to the rights of individuals, since a much higher level of accuracy is guaranteed in Artificial Intelligence-based engines.

The usage of AI-based biometric systems has important implications that are summarized below.

1.1.1. Irreversibility

Biometric data (templates) resulting from these AI-based models cannot be reversed to obtain the original raw data used (for example, the exact image of the individual's face in facial biometrics, or the audio with their voice in voice biometrics) to create this template.

In this regard, the template is irreversible and private, similar to a hash.

1.1.2. Non-interoperability

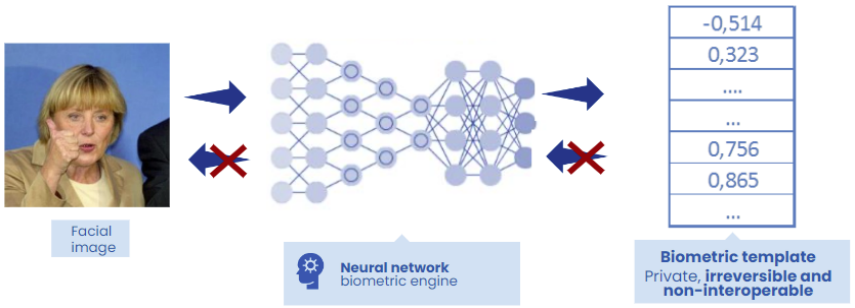
Interoperability is one of the most common concerns when speaking about biometric data. However, with AI-based biometric models this has also been overcome: as it was explained before, from the same original data (i.e. face image) each version of a biometric engine will create a different template, and the same would be true the other way around: each template can only be interpreted by the exact version of the biometric engine that created it.

While this may be inconvenient from a technological point of view, it is beneficial from a data protection perspective, as **the scope in which a biometric template can be used is restricted**.

1.1.3. Renewability

It is very common to hear (in fact, the current version of Guidelines 05/2022 includes it) that the template is permanent over time: *If I lose my password I can reset it… but what if I lose my biometrics? I cannot change who I am…* Well, **it must be stated that this "invariability" of biometric data is a myth, as it can also be reseted**.

It is true that (in the EDPB's own words in Guidelines 05/2022, par. 36) "unlike an address or a telephone number, it is impossible for a data subject to change his or her unique characteristics, such as the face or the iris". However, it should be noted that **the template is not the face of the data subject, but the result from specific technical processing of such unique characteristic (i.e. the face)**.



As it has been explained before, the template is the result of the processing of a face by a biometric engine. And each biometric engine is different and unique; even more, each version of the same biometric engine is different and unique. Therefore, **if a template is compromised, it does not mean that the person's face has been compromised and that his or her biometric authentication means is not longer secure, but it would be as simple as generating a completely new template with a different version of the biometric engine**, being this template totally different from the previous one, and incompatible with it.

1.1.4. Temporality

In any case, it is worth mentioning that a vector is only a representation of the subject's biometric characteristic for the purpose of comparison (in a specific biometric engine), and that it does not provide any further information about the subject..

1.1.5. Controlled use

As a consequence of the above, the biometric vector is data with a reduced scope and only usable by the person it belongs to.

A potential theft of the biometric vector, even if additional security measures such as encryption techniques are not taken, would have a very limited impact on the user. The

vector itself does not allow access to any system. For identification and authentication processes, two pieces of data are used for comparison, at least one of which is always captured at the same time (the second can be a vector if there has been a previous registration, or another piece of data captured at that moment when there is no registration). In this way, if capture is controlled and anti-spoofing techniques are applied, it is ensured that a biometric vector will only be useful in a process carried out by its legitimate owner. In other words, an individual will not be identified or authenticated by the system if it is compared against another individual's vector, and technologies are also applied to prevent it from deceiving the system by impersonating the legitimate user.

Likewise, the subject can only use their vector in systems that incorporate a specific biometric engine. Furthermore, when the vector is to be delivered to the subject, signature and/or encryption techniques are usually used, which means that even systems with the same engine but implemented by different entities are not interoperable.

The above characteristics are inherent to the usage of Artificial Intelligence-based recognition systems, which is the state-of-the-art in biometric technology.

1.2. Accuracy and reliability of state-of-the-art facial biometric systems

As previously mentioned, the improvement facial recognition has experienced in the last few years makes it possible to say that, in ideal conditions, facial recognition systems can have near-perfect accuracy.

Verification (also known as 1:1 or one-to-one matching) algorithms used to match subjects to clear reference images (like a passport photo or mugshot) can achieve accuracy scores as high as 99.97% on standard assessments like NIST's Facial Recognition Vendor Test (FRVT) 1:1[2]. This is comparable to the best results of iris scanners. This kind of face verification has become so reliable that even banks feel comfortable relying on it to log users into their accounts.

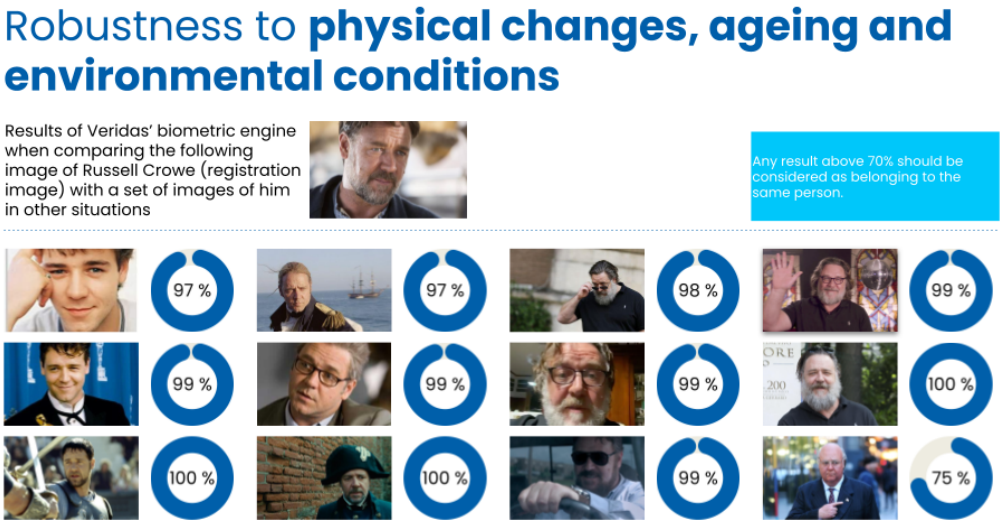
Identification (also known as 1:N or one-to-many matching) is when software takes an unknown face and compares it to a large database of known faces to determine the unknown person's identity. There is also available a separate track to evaluate accuracy of these systems, NIST Recognition Vendor Test FRVT 1:N[3].

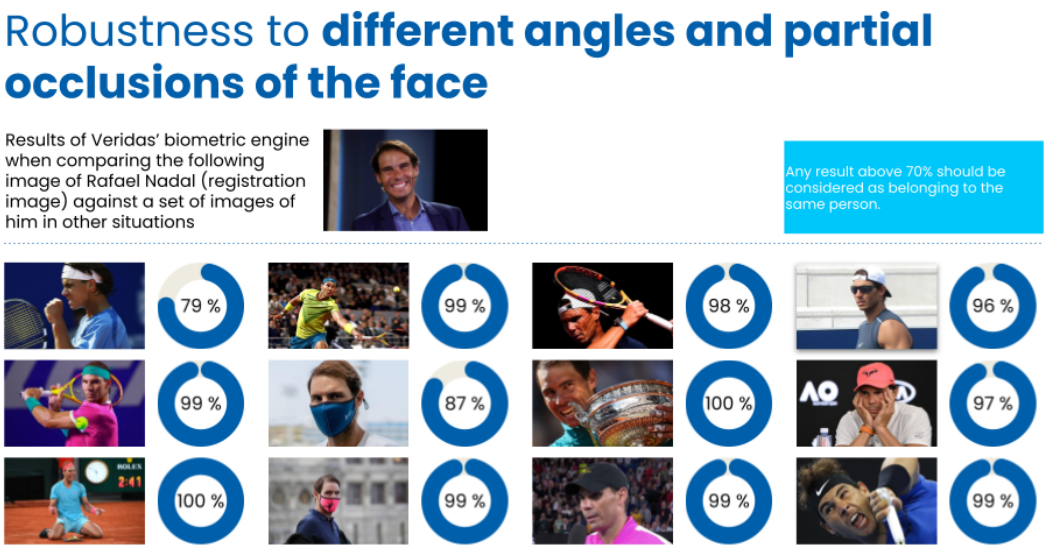
The results of the identification track are also available on the NIST Recognition Vendor Test FRVT 1:N, conducting identifications among a database of 1.6 million registered users. The state of the art, considering WILD category (uncooperative images, which is the most difficult category in the evaluation), is having a false negative rate (incorrectly rejects a legitimate subject) of less than 0.2% for a false acceptance rate (incorrectly accepts a non-legitimate subject) of 1%.

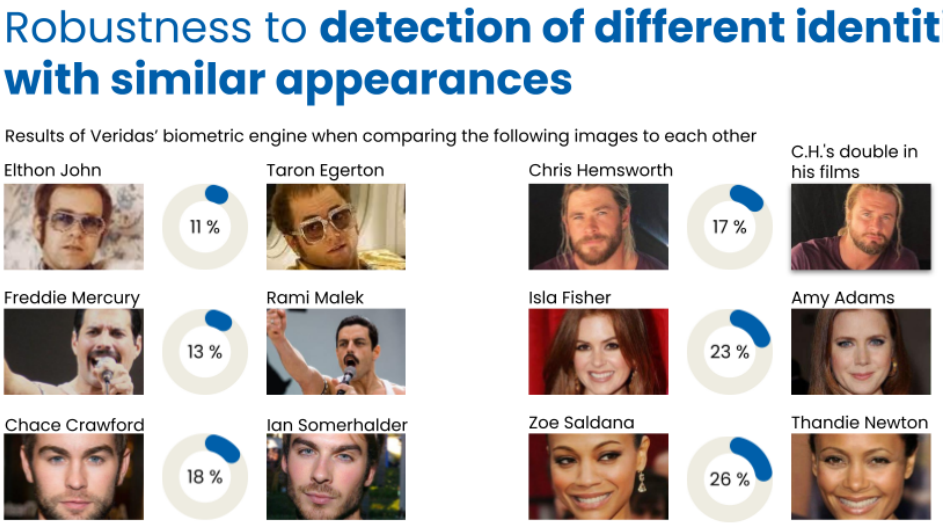
In fact, in the NIST *FRVT Part 2: Identification report* published on March 27th, 2020, comparing the results between 2020 and 2014, stated that the facial recognition accuracy had improved by a factor of 27 relative to 2014. Over the past two years, biometric technology has continued to improve substantially.

[2] https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf
[3] https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf

The following images show performance of VERIDAS' facial biometric engines, but can also illustrate other state-of-the-art biometric systems' performance. VERIDAS and DAS-GATE would like to point out that the following information is not provided with commercial purpose, but only to illustrate in a visual way the high performance that current facial recognition systems based on neural networks (AI) allow to achieve.







1.2.1. Standards that guarantee accuracy and reliability

Regarding the face recognition systems, for the past 20 years, the **National Institute of Standards and Technology (NIST) Facial Recognition Vendor Test (FRVT)** program has been the world's most respected evaluator of facial recognition algorithms, examining technologies voluntarily provided by developers for independent testing and publication of results.

- https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf
- https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf

An equivalent European organism would be desirable, or at least a direct cooperation between both regions.

With regard to **PAD (Presentation Attack Detection)**, the purpose of **ISO/IEC 30107** is to provide a foundation for PAD by defining terms and establishing a framework through which presentation attack events can be specified and detected so that they can be categorized, detailed and communicated for subsequent decision making and performance evaluation activities.

- https://www.iso.org/standard/53227.htm
- https://www.iso.org/standard/67381.html

1.3. Non-biased and non-discriminatory biometric systems

Biometrics are our inherent physical or behavioral attributes, but we should first focus on physical traits for now. The color of our eyes, the scar on our left cheek,... these are all distinctive biometric markers. By training machine learning to scan, understand and recognize these unique features, biometric systems can later operate.

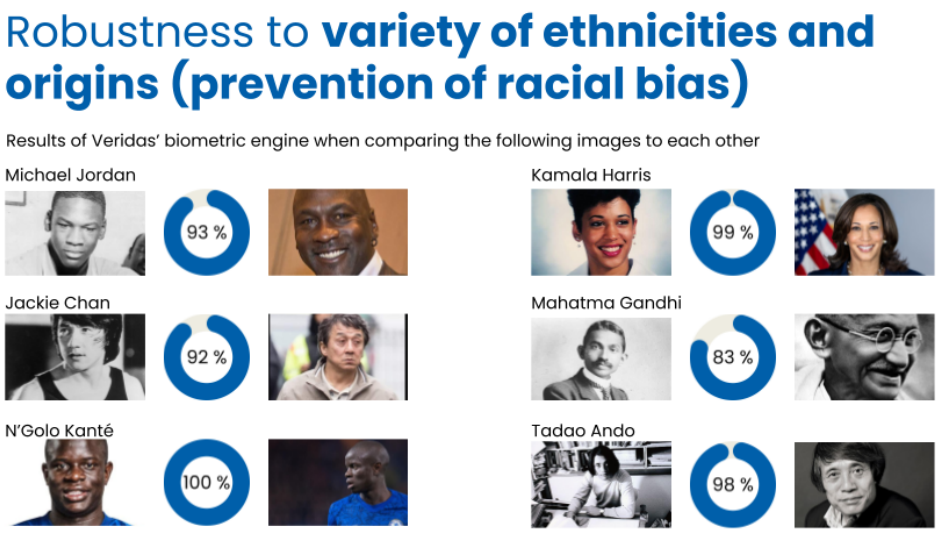
The problem with bias arises when the training data is skewed towards a specific demographic. This results in a very specific type of error known as overfitting. When data sets disproportionately exhibit certain features, a machine learning model will inherently focus more on that feature. That means a biometric system isn't biased against any particular race or

gender, but instead is less able to identify patterns typically found in that face's demographics if it has not been duly trained with data from such origin, gender or age.

Derived from the above, it can be concluded that the bias is not inherent to the technology, it is the result of inaccessibility of unbiased data bases on which the engines can be trained. VERIDAS and DAS-GATE support the goal of erasing all bias from biometric technology at all cost, in fact we are of the opinion that this is essential in the time we live in. However, in order to achieve this goal we should correct the root cause. By making unbiased data bases more accessible, to solution providers we will be able to offer unbiased technology. Thus, it is important to bear in mind that this goal will always be dependable on the quality of data bases, which we encourage the EDPB to promote.

Nevertheless, the existence of bias cannot be generalized, as state-of-the-art facial recognition technologies have improved a lot in this regard, and this is something that is also evaluated by the NIST.

For example, the following image shows performance of VERIDAS' biometric engine while verifying people from different ethnicities and origins. Also, when analyzing these examples, it shall be borne in mind that ageing, occlusions and other environmental conditions appear in the images and the engine is very robust to all those changes.



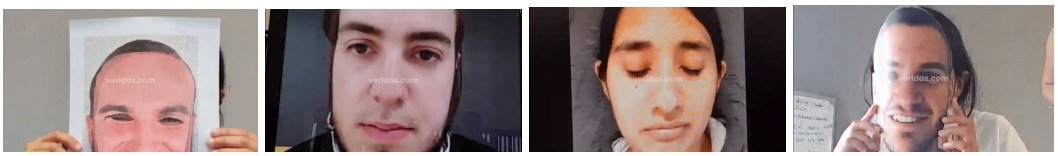
1.4. Presentation attack detection

The presentation of an artifact or of human characteristics to a biometric capture subsystem in a way intended to interfere with system policy is referred to as a presentation attack. In other words, attempts of impersonation or spoof. **International standard ISO/IEC 30107** addresses techniques for the automated detection of presentation attacks. These techniques are called presentation attack detection (PAD) mechanisms.

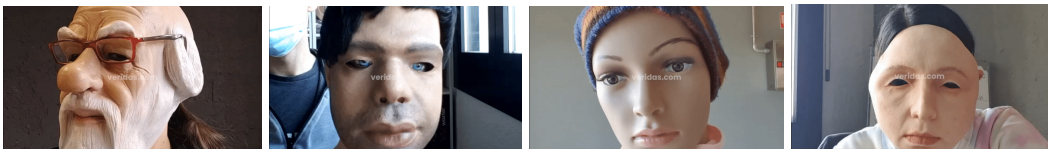
Compliance with ISO/IEC 30107 can be assessed by accredited laboratories, specially by those accredited by the NIST. This certification considers two levels of compliance, that could be

translated into two levels of difficulty or complexness of the presentation attacks the system is able to detect.

- **Level 1**: focused on simpler attacks, it focuses on high-resolution digital and paper photos, high-definition challenge/response videos, and paper masks. A few examples of this level kind of attacks are shown below:



- **Level 2:** focused on more sophisticated attacks, perform the test with realistic dolls and 3D masks made of resin, latex and silicone, as well as faces synthesized by digital image. A few examples of this level kind of attacks are shown below:



2. How can this biometric technology be implemented?

In the previous section it was shown how biometric technology works, and the privacy characteristics of biometric systems based on Artificial Intelligence, which allows us to talk about "privacy by default and by design" in terms of technology.

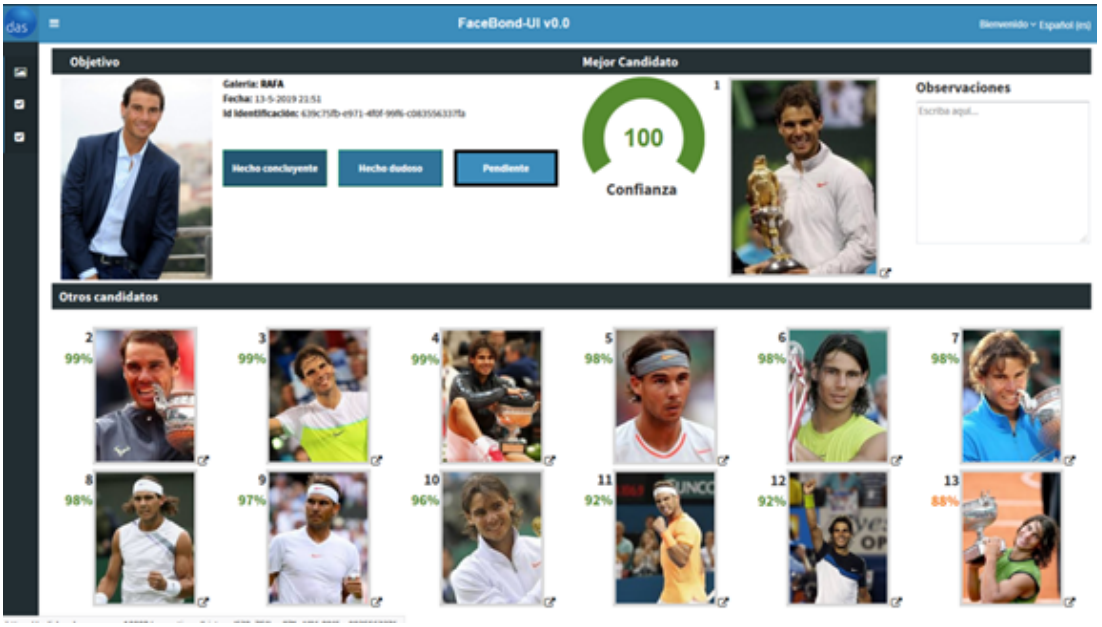
However, this technology can be used for a multitude of different use cases. Herein lies **the key to its regulation: biometric technology is not good or bad *per se*, but some uses of biometric technology are more or less desirable (or should even be prohibited)**.

This section seeks to address the various groupings of biometric technology use cases that can be made, in an attempt to analyze the proportionality, benefits and risks associated in each case.

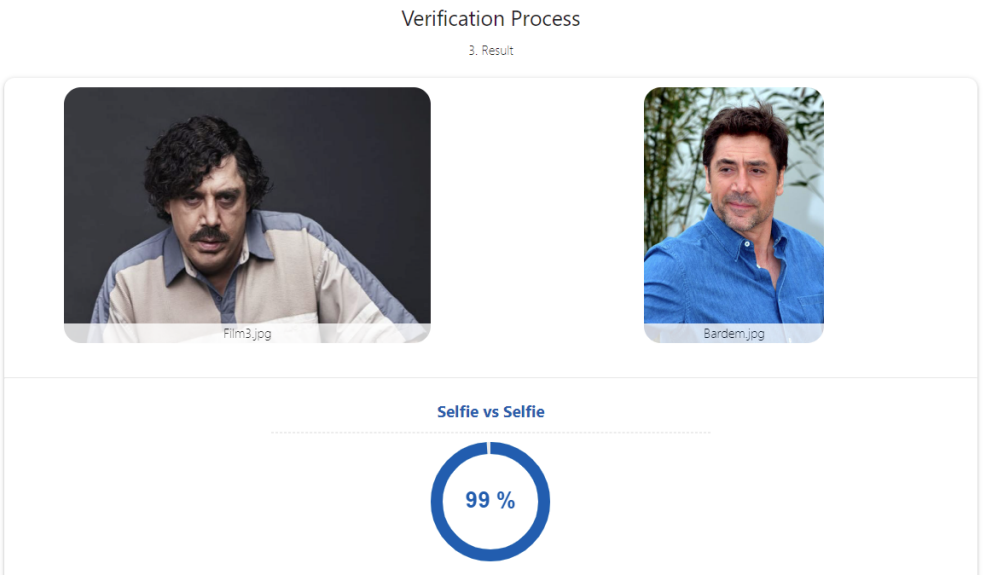
2.1. Biometric verification and Biometric identification

It is well known that biometric technology can be applied in two main different ways:

1. For **identification** purposes. This is the method known as **1:N**, since it compares an individual to a group (i.e. against each of the people who comprise that group). The purpose is to ascertain whether that individual belongs to that specific group.

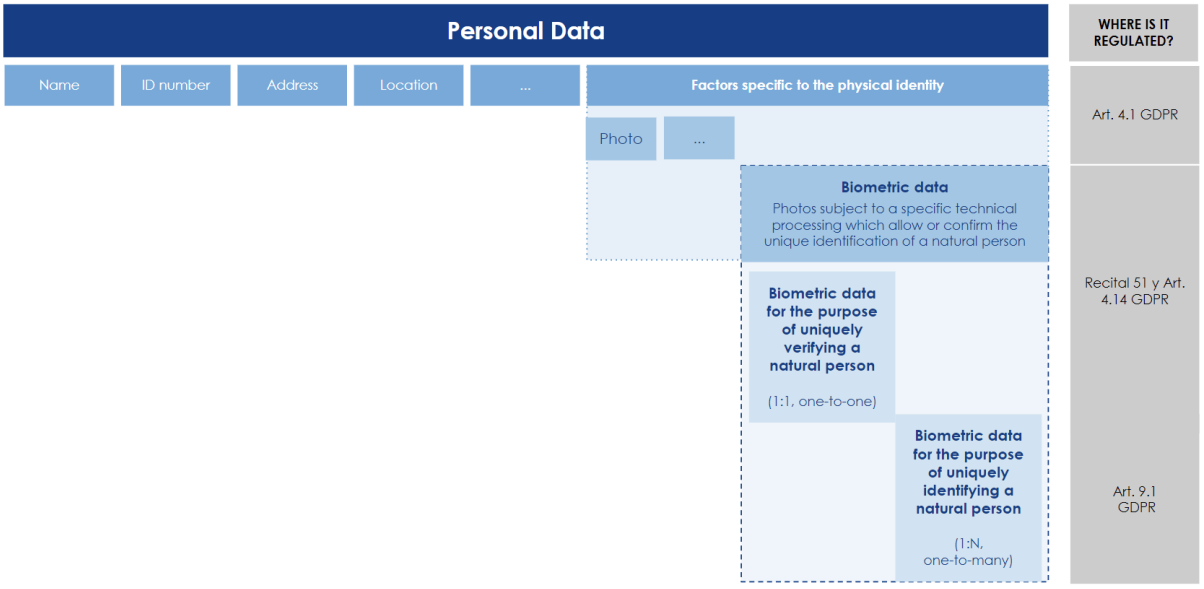


2. For **verification** purposes. This method is based on a **1:1** basis, since the individual's data is compared against other data associated with that same individual. The purpose, in this case, is to verify their identity, in other words, that they are who they claim to be.



This distinction, which is fundamental at a technical level, also has legal implications regarding data protection, as the processing of personal data is different.

And this difference has been addressed by multiple European and national bodies, since from the interpretation of Articles 4.14 and 9.1 and Recital 51 of the GDPR it can be derived that their treatment is different. The following image resumes this:



The classification has been extracted from the interpretation of GDPR provisions and resolutions and guidelines of various data protection authorities.

Consequently, only biometric identification uses (1:N) are considered sensitive data processings and will have to comply with the additional requirements that the GDPR and, where appropriate, national regulations, establish for these special categories of data.

For cases of biometric verification/authentication (1:1), the rest of the standard requirements of the GDPR and national regulations must be complied with, seeking, of course, in any case, the protection of the rights and freedoms of its users.

For further explanation on this regard, a complete document elaborated by VERIDAS and DAS-GATE can be consulted here.

2.2. Regulating biometrics depending on its application (risk-based approach)

However, **the main pillar in the use of biometric technology lies in its purpose**. As previously mentioned, the technology itself is not good or bad, but rather the different applications it can have.

This is the approach adopted by the European Commission in its proposal to the European Parliament and the European Council for a European regulation laying down harmonised rules on Artificial Intelligence[4] or **Artificial Intelligence Act Proposal**. This is not a proposal for the regulation of Artificial Intelligence per se, but rather a regulation of some applications that incorporate Artificial Intelligence.

The Proposal starts from a **risk-based approach** when regulating AI, differentiating between: (i) activities that represent an unacceptable risk and should be prohibited; (ii) those that represent a high risk and should be subject to special requirements for their development; and, finally, (iii) those that represent a low or non-existent risk and are not subject to this regulation

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

but to general regulations and transparency requirements so as not to impose excessive burdens or weigh down innovation. And this is of course the approach followed regarding biometrics.

This approach is key, and the EDPB is also adopting it in its Guidelines 05/2022 when assessing the risks of the different applications of facial recognition in the area of law enforcement.

The risk-based approach to which we are referring is essentially based on the control that the user has over his or her personal data (in this case, his or her biometric data), the processing that a third party may carry out on it and the consequences that may arise from it for the data subject.

This has been in fact state by the EDPB in paragraph 17 of the Guidelines 05/2022:

"More specifically, a scale of potential uses might be considered depending on the degree of control people have over their personal data, the effective means they have for exercising such control and their right to initiative to trigger and use of this technology, the consequences for them (in the case of recognition or non-recognition) and the scale of the processing carried out. Facial recognition based on a template stored on a personal device (smartcard, smartphone, etc.) belonging to that person, used for authentication and of strictly personal use through a dedicated interface, does not pose the same risks as for example usage for identification purposes, in an uncontrolled environment, without the active involvement of the data subjects, where the template of each face entering the monitoring area is compared with templates from a broad cross-section of the population stored in a database. Between these two extremes lies a very varied spectrum of uses and associated issues related to the protection of personal data."

User's power of disposal (transparency, information, consent,...) **is the cornerstone for the understanding and categorization of the different use cases**.

2.2.1. Biometrics as a right vs. biometrics as monitoring means

Identity accreditation has always been done through who I am (element of inherence); the people around me, my family, my friends, my colleagues, know me and recognize me by my face, my voice,.... Sometimes, for certain procedures, especially when the other party does not know me, I must also provide my identity document (possession element) to prove that I am who I say I am.

Biometrics makes it possible to do this in a digital environment, but also in the physical environment. It allows me to prove that I am who I say I am. And in terms of authentication elements (possession, knowledge and inherence) biometrics is undoubtedly the most secure of all, since it is the only one that proves a **real identity** (who he or she is), while the others rely on presumed identities (who at a given time had an object, or knew a piece of data or password).

And these benefits of biometrics should be available to citizens who want to use them consciously and voluntarily. I have the right to prove my identity for who I am, and it is a legitimate use.

However, there will also be other uses of biometrics where the citizen does not have this complete control over the processing of their biometric data. Sometimes because other

rights predominate (as the EDPB itself points out in the examples mentioned in Guidelines 05/2022 or national supervisory authorities have stated in their own reports), and sometimes because there may be an abuse of power leading to massive and indiscriminate surveillance of users.

Thus, again, we come to the same conclusion: not all applications of biometric technology entail the same risks, and therefore their regulation must be based on a risk-based approach.

ACCREDITATION	vs.	SURVEILLANCE
A right I can voluntarily exercise	vs.	Public or private monitoring

This aspect is closely related to the control that the user has over his or her data, the information he or she receives, and the consequences derived from the processing.

2.2.2. Four categories of biometric technologies application

The difference made between verification (1:1) and identification (1:N) is important in terms of the interpretation and application of the GDPR, but, as it has been pointed out in previous epigraphs, **there is an even more important distinction: data subject control over their data**, or power of disposal.

Taking this into account, and especially considering the classification suggested by the Artificial Intelligence Act Proposal, four main categories should be considered:

Scenarios	Associated risk	Sensitive data
Biometric verification or authentication systems (1:1) Data subject knows the biometric verification is taking place, he/she has been duly informed, and there is a legitimate legal basis (often, consent) for the processing.	Low or non-existent	No
Biometric identification systems (1:N) Data subject knows the biometric identification is taking place, he/she has been duly informed, and there is a legitimate legal basis (often, consent) for the processing.	Low or non-existent	Yes
'Real-time' and 'post' remote biometric identification systems (1:N) of natural persons, and without prior knowledge of the user of the AI system whether the person will be present and can be identified Data subject may not know the biometric identification is taking place or, if he/she knows, there is not an alternative for him/her, adequate information to the data subject is difficult to guarantee and there is a legitimate legal basis for the processing (consent may be difficult to obtain and/or justify).	High	Yes
'Real-time' remote biometric identification systems (1:N) of natural persons in publicly accessible spaces and without prior knowledge of the user of the AI system whether the person will be present and can be identified, for the purpose of law enforcement Data subject may not know the biometric identification is taking place or, if he/she knows, there is not an alternative for him/her, adequate information to the data subject is difficult to guarantee and there is a legitimate legal basis for the processing (consent may be difficult to obtain and/or justify). Processing may have legal consequences for the data subject.	Prohibited, with exceptions	Yes

"Associated risk" classification has been made following the AIA Proposal; "Sensitive data" classification has been made following GDPR and its interpretations.

The previous image shows the classification as it would now look with the Artificial Intelligence Act Proposal. We consider this to be a logical and appropriate classification, since it is based on the real risks that the use of biometric systems could have on citizens' right to data protection, but also on the impact on other fundamental rights.

However, VERIDAS and DAS-GATE agree with the interpretation made by the EDPB that when these biometric systems are to be used for law enforcement purposes, the associated risks would extend to the use of 'post' remote biometric identification systems, so the classification could be as follows (see the change in the last scenario):

Scenarios	Associated risk	Sensitive data
Biometric verification or authentication systems (1:1) Data subject knows the biometric verification is taking place, he/she has been duly informed, and there is a legitimate legal basis (often, consent) for the processing.	Low or non-existent	No
Biometric identification systems (1:N) Data subject knows the biometric identification is taking place, he/she has been duly informed, and there is a legitimate legal basis (often, consent) for the processing.	Low or non-existent	Yes
'Real-time' and 'post' remote biometric identification systems (1:N) of natural persons, and without prior knowledge of the user of the AI system whether the person will be present and can be identified Data subject may not know the biometric identification is taking place or, if he/she knows, there is not an alternative for him/her, adequate information to the data subject is difficult to guarantee and there is a legitimate legal basis for the processing (consent may be difficult to obtain and/or justify).	High	Yes
'Real-time' and 'post' remote biometric identification systems (1:N) of natural persons in publicly accessible spaces and without prior knowledge of the user of the AI system whether the person will be present and can be identified, for the purpose of law enforcement Data subject may not know the biometric identification is taking place or, if he/she knows, there is not an alternative for him/her, adequate information to the data subject is difficult to guarantee and there is a legitimate legal basis for the processing (consent may be difficult to obtain and/or justify). Processing may have legal consequences for the data subject.	Prohibited, with exceptions	Yes

Again, it should be remembered that **technology is neutral, and that the regulation and interpretation of such regulation should focus on the applications this technology may have**.

Therefore, it is neither logical nor appropriate to judge all uses of biometric technology equally, since this would be stopping the use of these systems for entirely legitimate purposes, even those in which it is the citizen himself who voluntarily and consciously requests their use to prove his or her identity.

Biometric systems that seek to establish control over the population or a group are a different matter. Here, of course, an exhaustive analysis of the legitimizing basis must be carried out, and it must be verified whether there are other fundamental rights that should prevail.

We can think of certain examples, such as the use of facial recognition with remote systems (usually linked to video surveillance cameras) for law enforcement purposes in spaces open to the public. By default, these uses should be prohibited, as their generalization can lead to situations such as those being observed in other countries where individual rights and freedoms are less protected; the clearest example of this undesired use in Europe is China, where the government of the country, through its police forces, obtains a huge

amount of information from citizens, including through facial recognition in public (and sometimes even private) spaces, to monitor the population. This is certainly something we do not want to see in Europe, so its widespread use by the police should be prohibited.

However, legitimate exceptions must also be considered, such as those that the EDPB itself already includes among the examples in the guide. For example, the search for missing children who may be the subject of an abduction is expressly mentioned, and we also find among the exceptions provided for in the AIA Proposal the prevention of an imminent terrorist attack. If the use of biometric technology makes it possible to resolve these serious situations (finding these kidnapped minors or preventing a terrorist attack), but implies that for a few hours a facial recognition system must be installed in a station and its use is therefore ruled out, would we not be giving more weight to the right to data protection than to the right to life and the right to the integrity of the person? All of them are rights recognized in the European Charter of Fundamental Rights. Once again, everything is a question of values, rights and freedoms that must be weighed in the balance, so a common resolution for all cases is not appropriate. All this, knowing that it will probably be necessary to develop more European and national legislation, but guidelines that do not judge different situations as if they were the same thing are needed.

Similarly, we can think of examples that are entirely legitimate.

One might mention for example the fact that in order to gain access to a sports stadium, its members are offered the opportunity to prove that they are entitled to enter because they carry a membership card or simply because they are who they are. Just as the doorman of a building knows the faces of all his or her neighbors and allows them access, a technological “doorman” (equipped with a facial recognition system) can give them access because of who they are, without the need to ask them to carry a card as well. However, this use must be optional and based on consent (the user may opt for access by traditional methods), unless, as the EDPB itself points out, there is a national or European regulation that provides another legitimate basis. And being consent the legal basis for the data processing, it should be ensured that people who have not consented on the use of the facial recognition access are not subject to such processing; therefore, no remote identification systems should be used, and only those that require the close presence of the subject, in order to ensure that only those who voluntarily place themselves in front of the system are captured. This is a key factor in the distinction and regulation of RBI systems (remote biometric identification systems) where the data subject cannot choose if he or she wants his or her data to be processed, as opposed to proximity biometric identification systems (as the second category of the previous image shows) where the data subject voluntary action is required for the processing of his or her data.

The same can be said of access to work environments by employees, where there is national legislation requiring the employer to record the entry and exit times of its employees. In these cases, as some national data protection authorities have already interpreted, there may be a legitimate basis in that legal obligation for the use of biometric technology to facilitate time recording and avoid fraud.

But all these legitimate uses (whether general or under accredited exception), must be based on a reliable, accurate, secure and private biometric technology (as the state of the art allows today). And this demands that the regulation of the use of biometric systems requires the use of technology subject to international standards and certified, transparent and explainable.

Likewise, data subjects shall always have the right to obtain human intervention, even if this means going against the result provided by the system.

VERIDAS and DAS-GATE understand that **the approach taken by the EDPB in the Guidelines 05/2022 is intended to follow this same criterion: risk-based approach, not only for data protection but for all fundamental rights**, and this is reflected in the many examples given.

However, it is no less true that in the Guidelines 05/2022 the EDPB generalizes some risks or misunderstandings regarding facial biometric technology, sometimes leading to the interpretation that any use of biometrics is equally intrusive. It has already been explained that this is not the case: **same technology, multiple use cases; the technology is not good or bad by nature, but rather the different applications it may have**.

3. Conclusions

After analyzing how the technology works and the different applications it may have, the following conclusions were reached:

1. In light of the description of biometric technology, it can be concluded that **using an Artificial Intelligence-based system can offer guarantees of precision, security and data protection with regard to those required by the principles of privacy by design and default**.
2. In this regard, the quality of biometric systems can now be **audited worldwide**. These evaluations (currently carried out by NIST, and hopefully soon to be carried out by European organizations as well) analyze issues such as accuracy and reliability, the absence of racial or age bias, etc. In addition, there are also international standards and certifications relating to robustness and security against attempts to spoof them.
3. The use of biometric recognition systems has taken off in recent years across a wide range of sectors and has been received positively by users. It allows to cover, with the highest guarantees, the objective of identifying or authenticating the identity of a person. Of the three elements that are differentiated when discussing user authentication (possession, knowledge and inherence), inherence is without a doubt the only one that can offer certainty, while the other two remain presumptions. The latter is a matter that, when analyzing the specific case and the technology to be used, must be taken into account when making proportionality judgments.
4. **The regulation and legal interpretation of biometric recognition systems must be closely linked to their technical characteristics and their operating conditions**, as this will enable limits and requirements to be set for those systems that entail a greater intrusion on the

rights of individuals, while at the same time systems that do not entail any risk are allowed. In short, "not everything is the same" and therefore "not everything should be treated the same".

5. Only biometric data used for biometric identification (1:N) are classified as **sensitive data under Article 9 of the GDPR**. On the other hand, biometric data used for biometric verification (1:1) are not classified as sensitive data.
6. Without prejudice to the above, it can be stated that **not all biometric identification systems (1:N) pose a risk to the rights and freedoms of individuals**, but only those that may result in a massive and indiscriminate surveillance system and/or otherwise limit the fundamental freedoms and rights of individuals. Thus, they shall be delimited into prohibited systems with duly justified exceptions, high risk systems, and low or non-existent risk systems.
7. The **data subject's power of disposal over his or her data** is key. Access to complete, clear and transparent information must be guaranteed, as well as the right to not be subject to biometric processing, except in those cases in which the **balance with other fundamental rights** so recommends.
8. When considering the fundamental rights of individuals, their right to be able to prove their identity simply by who they are, without further excessive requirements (tokens, passwords, etc.) must also be taken into account, except in those cases where the security of the operation requires additional elements. However, this should be configured as **a right of the individual to make use of their real identity**, and not as an obligation to be authenticated through biometrics (again, unless the security of the transaction requires it).
9. Considering the above, **a distinction is made between using biometrics to enable the user to prove his or her identity or to monitor the user**. The former should be guaranteed as long as the security and privacy of the system has been ensured. The latter must be sufficiently regulated to ensure that biometric technology is prohibited for this purpose, unless there are exceptions that have been authorized by judicial or administrative authorities and always based on European or national legislation. Based on the first perspective indicated in this point, **the legal basis of user consent should not be limited or considered inadequate for biometric data processing, provided that such consent is based on clear, complete and transparent information to the user**.
10. The four categories set out in the AIA Proposal are based on a study of the rights that may be affected in the different applications of biometric systems, and **the same risk-based approach should be followed to ensure that unwanted uses of biometric technology are limited or even prohibited, while ensuring the possibility of using these systems in legitimate cases**.

4. Amendment request to Guidelines 05/2022

Based on the arguments regarding the performance of biometric technology and the use cases in which it can be implemented, VERIDAS and DAS-GATE request the EDPB to revise the Guidelines 05/2022 based on the following aspects:

7. While these are guidelines relating to the use of facial recognition systems for law enforcement purposes, the EDPB ultimately makes a general assessment of all possible uses of biometric technology. Examples are correctly used to illustrate potential undesirable (or sometimes undesirable) uses of biometric technology by law enforcement authorities. However, conclusions extracted from these examples are used to generalize the risks and potential effects of all biometric systems, which lead to a biased interpretation of this technology. Therefore, the scope of application of these Guidelines shall be indicated and recommendations shall be made with respect to that scope.

8. The Guidelines shall make express reference to the user's power of disposal over his or her data. Regulation shall be based on the four different categories of face recognition use cases described in section 2.2.2 of this document.

9. In this regard, distinction shall be made between verification (1:1) and identification (1:N) implementations, as it has been interpreted since the commencement of GDPR application, as they do not entail the same risks (precisely due to the conclusions in amendment 2 above).

10. Applications based on the user's consent shall be considered as a legitimate use of biometric recognition, as long as the user is duly informed of the functioning of the system and how his or her data is being processed (as well as other information requirements under the GDPR). Again, this is directly related to the amendments proposed before.

11. The regulation and implementation of these systems must be based on a risk-based approach, balancing the fundamental rights that may be affected, and considering that the right to data protection is not the only right at risk.

12. Some misunderstandings regarding biometric technology are included in the Guidelines, such as reference to permanence and immutability and the impossibility of regenerating a biometric template. As explained in the sections above, this is not true when talking about state-of-the-art technologies, so it shall be updated accordingly so as not to generate and spread misconceptions and myths.