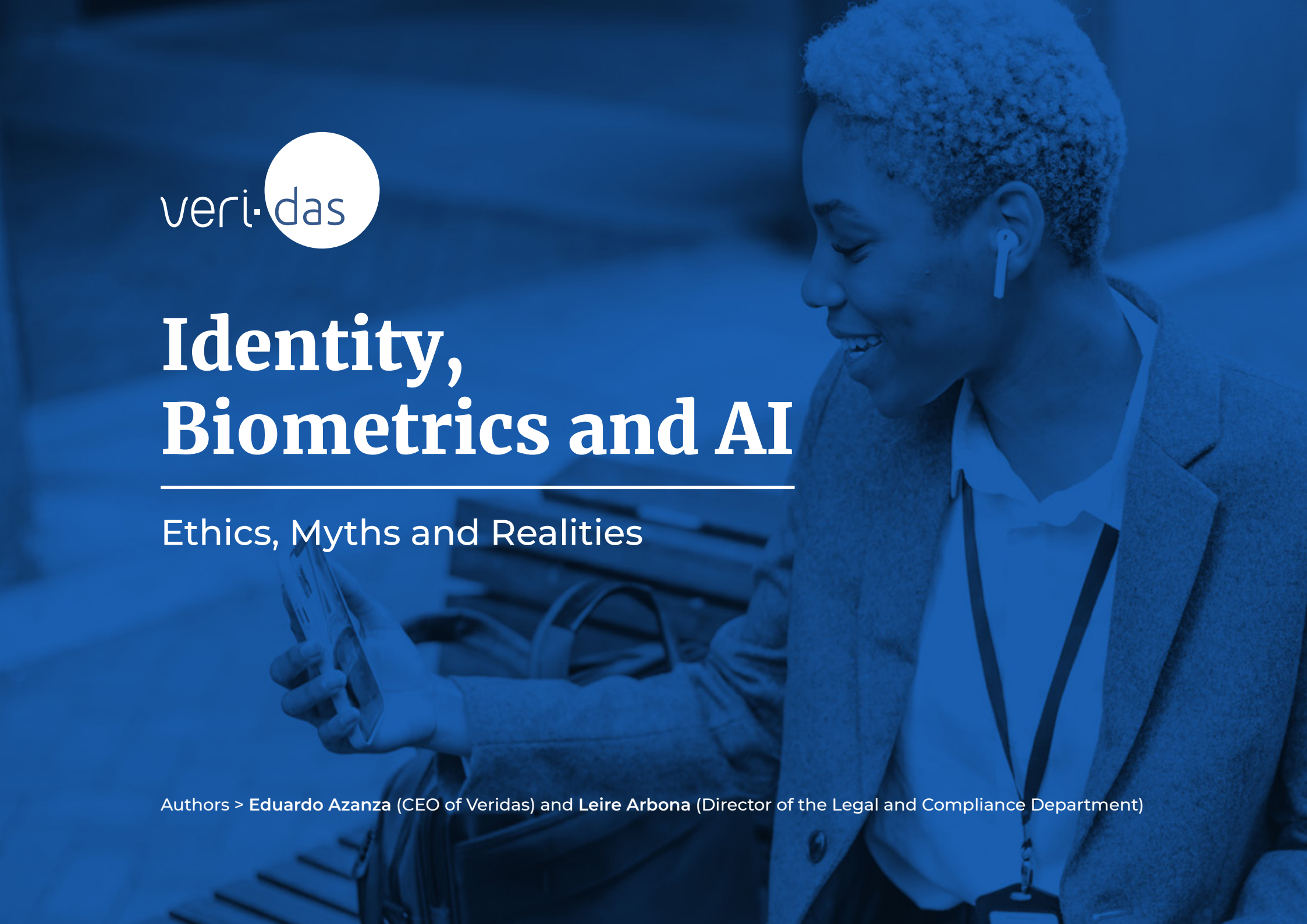


Identity, Biometrics and AI

Ethics, Myths and Realities

Authors > **Eduardo Azanza** (CEO of Veridas) and **Leire Arbona** (Director of the Legal and Compliance Department)

The content of this eBook was presented by Eduardo Azanza in his presentation on the study of the adoption of a regulation for the new technological, disruptive and social realities, framed within the Committee on Economic Affairs and Digital Transformation in the Senate of Spain. Its content is updated in accordance with current regulations. Read the article.

TABLE OF CONTENTS

Context

Facebook has just recognized that in 2019 **it lost information**, which included the passwords and personal data of 500 million users. One of the strategic priorities defined by the European Union, and by all Member States, is the fight **against money laundering**, which, driven by digital operations, threatens to erode the tax system that funds the welfare state. Youth **addiction to online gambling** has become a new problem for which parents, educators and the authorities are searching for answers and solutions.

Cyber fraud crimes already represent 25% of the crimes reported in the different police forces in Spain.

The above facts are just a few examples in which the **identities of people** and their reflection in the **digital** world play a key role.

Guaranteeing certainty, security, control and efficiency is the cornerstone for a safe and reliable Digital Transformation. Artificial intelligence and biometrics are the cornerstone to make this possible.

Europe has the capacity not only to **regulate** in accordance with the highest ethical standards, but also to do so from a position of technological **leadership**, as it has historically done in such important industries as the automobile and aeronautics sectors.

Physical identity in a digital world

The **right to identity** is one of the **fundamental rights** of every human being, and it is a necessity in order to be able to benefit from the other fundamental rights. Identity includes first name, last name, date of birth, gender and nationality. It is the proof of the existence of a person as part of a society, as an individual who is part of a whole. It is what characterizes the person and sets them apart from everyone else.

In the **physical world**, identity is an attribute that countries grant to their citizens at birth, and that manifests itself in the form of a: **passport, ID card**, driver's license, voting cards and other forms of official identification that each country establishes.

The first passports date back to the Persian Empire in the 5th century BC, although their modern form dates back to the mid-19th century, together with the first railroads and the mass movement of people.

This system has worked in a "reasonable" way to prove the identity of people in the "physical world": **identity fraud** is always at the center of most criminal acts, and ranges from minor offenses such as accessing a nightclub when underage to others such as money laundering that require identity falsification and theft for their commission to take place.

When we talk about **identity** in the **digital world**, we're not referring to your profile on Facebook, Instagram, Twitter

or any other social media platform, where identity does not have to be related to the person's real physical or identity, and in which anonymity, pseudonyms or avatars are inherent to these new forms of expression.

Digital Identity, in this context, refers to the ability to **exercise the right to claim our individual identity**, unequivocally, in order to be able to operate and access all kinds of information and carry out transactions safely on the internet, in such a way that the level of trust felt on both sides of the screen is as high as possible.

Accessing a website or an app, opening a bank account, issuing a digital certificate or a certificate of life to receive benefits, a digital signature on a document, the registration of a SIM card, renting a car, buying a property, checking in at a hotel, collecting signatures, ensuring that the person accessing certain content is of legal age, and even being able to exercise the right to vote, are just a small **sample of operations where the trustworthiness of a person's identity is** the key to being able to carry out fast and secure transactions.

The current Digital Identity model is broken: the “presumed” identity

Identification in the digital field consists of two steps: a **first** process in which the person gives **proof of their identity** by showing that they are who they say they are, demonstrating that they are the genuine owner of a valid identity document. This process can be done in person or digitally (as we will see later on).

Once this step has been verified, **the person obtains an identity credential** (a username and password, a digital certificate and password, a coordinate card, etc.). This process is not perfect: the initial identity verification is often carried out without documentary proof of identity, and sometimes it is not even done face-to-face, or the person who verifies the identity may not be an expert in verifying documents, recognizing faces or is not trained to “deal” with a case of fraud.

The **second** step occurs at the moment in which the person is **“authenticated”** and proves, in a digital environment, that they have a credential that proves their identity. This credential (a password, an SMS, a coordinate card) does not directly link the person with their identity, but rather the **identity is “presumed”**.

Said credential, even if it has been obtained lawfully, **can be transferred** so that one person can act on behalf of another. The credential can be **obtained illegally** (remember the mass theft of Facebook passwords, hacking or social engineering maneuvers), or the user can even claim that their identity credential has been used illegitimately by **contesting** an operation

that they themselves carried out - “they stole my password and signed as me” - associated with the intrinsic weakness of the system.

Digital identity with biometrics **is expressly provided for in the Spanish Public Administration’s 2021-2025 Digital Transformation Plan** in axis 1 “Digital Transformation Plan for the General Administration and Public Agencies”, where a “new digital identity model” is advocated for in the following terms:

“It is a challenge to improve how citizens and companies identify themselves easily and effectively with the Administrations.

The objective of this measure is twofold. On the one hand, systems and services will be developed that allow the identity of citizens and companies to be digitally verified in a 100% online way, using secure technologies such as biometrics, image, etc.

and, on the other hand, new identification and signature systems will be developed that are simple, secure and easy to use for citizens, in line with the applicable regulations in this matter.”

In the midst of the technological change in which are immersed, accelerated by the pandemic, it is absolutely necessary to equip ourselves with instruments that make this **Digital Transformation safe, private and reliable**, for which instruments must be assembled to **apply our Real Identity**.

Biometrics: “from presumption to certainty”

Biometrics is defined according to **ISO** as the automatic recognition of individuals based on their biological and behavioral characteristics. In the world of biometrics, a distinction is always made between **verification/authentication (1:1)**, in which an individual verifies themselves against themselves (e.g., comparing their ID photo with their selfie photo) and **identification (1:N)** in which an individual is searched for within a list.

Modern biometric technology, thanks to its precision, ease of use, security and privacy, allows identity to be applied in the digital space in a unique and secure way. This allows a person to carry out a digital operation and **have their identity be unambiguously verified**, with all legal certainty, **thus preventing fraud** and identity theft, in addition to having all the conveniences of operating in the digital space, improving the efficiency of the Public Administrations, companies and avoiding wasted time, resources and unnecessary travel, **thereby reducing the carbon footprint** of each transaction.

Digital Identity Verification technologies: automatic validation of identity documents, facial and voice biometrics, allow us to prove our identity in a simple, safe and efficient way in the digital world, **just as human beings have historically done in the physical world: with their face and voice** if we had already met the person previously, or we ask for a document that proves their identity (verifying its authenticity, personal data and relationship between the photograph

and the person), if we did not already know them.

Finally, it should be noted that these systems **do not allow other characteristics to be inferred with regard to the subject**, such as behaviors, attitudes, emotions, tendencies, gender, ethnicity, skin colors, etc., nor does it lead to the classification of the person in a profile that could determine future characteristics or behaviors.

These systems do not allow other characteristics to be inferred with regard to the subject, such as behaviors, attitudes, emotions, tendencies, gender, ethnicity, skin colors, etc., nor does it lead to the classification of the person in a profile that could determine future characteristics or behaviors.

Artificial Intelligence and Biometrics: an “irreversible” couple

Thanks to the impulse of **Artificial Intelligence (AI)**, and, in particular, of Machine Learning, which has taken place in recent years, facial and voice recognition technologies have reached extremely high levels of precision, well above the best human physiognomists. The biometric models of Machine Learning are created from complex mathematical algorithms, which are “trained and taught” as would be done with the human brain, although their “intelligence” is very specific and tailored for a certain task, instead of being generalist. The results that they obtain are much more effective, accurate and with less bias than a person.

As an example, we can look at the last evaluation of **Facial Identification (1:N) carried out by NIST**[1] where there are already many systems with rates of False Positives (making a mistake in the candidate who is found) of **3 per 1,000** associated with a rate of False Negatives (not finding the person on the list when they are indeed on it) below 2 percent in searches of 1.6 million people.

The systems also have very low levels of **bias between race, gender and age.** This last issue was analyzed by NIST in a December 2019 report, which concluded that biases in 1:1 systems had little effect, and that in 1:N systems only some algorithms showed a bias, since “algorithms perform differently”, and the most equitable (least biased) also coincide with the most accurate algorithms. Therefore, it all boils down to the quality of the biometric system, which allows not only for greater precision, but

[1]*National Institute of Standards and Technology, in the USA, is a laboratory that neutrally and systematically evaluates all biometric technologies from manufacturers that voluntarily submit to their examination: https://pages.nist.gov/frvt/html/frvt1N.html

also less discrimination. In any case, the biases of automatic systems **are much less than those in which a human being make an inference**.

Modern AI-trained biometric engines are private by design and by default, so the myth that “if I lose a password I reset it, but if I lose my biometrics, I have lost my identity” can be done debunked once and for all.

Let’s review why. Two types of biometric engine models can be distinguished:

> Biometric models by landmarks (old-school)

Based on the detection of landmarks

The vector is a representation of the geometric relationships between the landmarks

The vector is interoperable (reversible)

Obsolete/low precision technology (95%)

They were the most widespread until about 5 to 7 years ago, and **they were based on landmarks** to recognize, for example, a face.

This method involves taking measurements between multiple points of the biometric feature, such as a facial image, resulting in a mathematical comparison vector, which is a summary of these measurements. In this type of technology, precision was limited and, in view of the vector generated with this engine, it would be possible to interpret the measurements that said vector represented of the landmark on the subject's face (for example, as a facial image: the distance between the eyes, between the ears, etc.) and thus obtain an estimate of the original image.

In addition, these systems are mostly standardized, which means that the way they operate can be uncovered by just about anyone.

This makes the technologies **interoperable** (such as fingerprint recognition **systems**), and as such there can be negative implications at the data protection level. Due to these circumstances, landmark-based biometric engines can be considered an **outdated technology** for digital identity verification, which we can define as the “old-school technology”.

> Biometric models based on Artificial Intelligence

Companies that develop cutting-edge technologies have left behind the old-school models to switch over to models based on Artificial Intelligence and, more specifically, on deep neural networks (DNN).

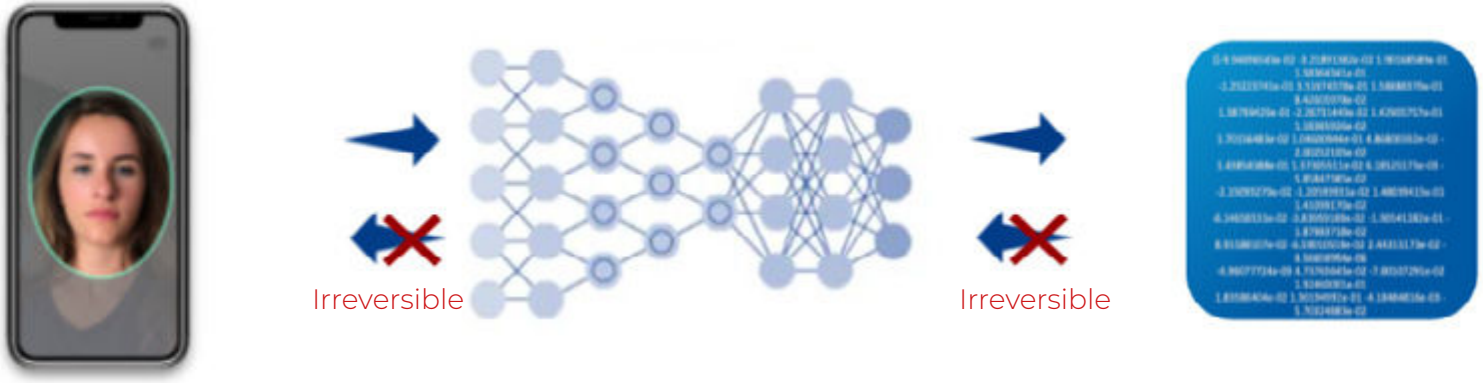
This IRREVERSIBILITY means that, as a consequence, **not even the manufacturer is able to interpret** the mathematical vector in order to extract information from the individual who provided their data. Therefore, obtaining it, even if it were illegal, does not mean that the biometric information has been compromised, nor that it can no longer be canceled.

Illegitimately obtaining this vector represents a **risk** to privacy that is substantially **less** than the loss of an identity document or the publication of an image on social networks.

The **non-interoperability** that is intrinsic to these systems is an important technical drawback, but it has the advantage of guaranteeing that, in the event of the potential theft of this data, it does not allow it to be used in any other biometric system from the same or another manufacturer.

Likewise, it is important to ensure **transparency** in the operation of the system once it is in a productive environment. It is important to guarantee that the **data** of the subjects who are using the recognition service **is not used to** automatically train

the engine. This should only be done in the development phase of the system, to guarantee the quality of the data (in order to guarantee that a precise and unbiased model is obtained) and the legitimacy of its processing for this purpose.



Photo

Biometric engine trained with neural networks

Private and irreversible biometric vector

PRECISION > 99,9%

*VS

*The comparison is made between vectors created by the same biometric engine

When a face (or a voice) is processed by the biometric engine, the result is an irreversible mathematical vector that is non-interoperable with other systems.

The engine is never trained with customer data from production.

MYTH

If I lose my password, I reset it.
But what if I lose my biometrics?

Privacy by default and by design.

> Capturing the data

A biometric recognition system, whether for authentication or identification, **must always start with the individual's EXPLICIT CONSENT for the capture of their data** (unless there is another legal basis for its sufficiently justified processing). The choice of the biometric data used determines the accessibility and scope of the identification system. A facial biometric system is accessible to practically everyone, regardless of potential health problems or physical characteristics (e.g. scars), whether temporary or permanent.

Voice biometric systems are also accessible to a very high percentage of people. In addition to taking into account what type of data is collected, the design of how that data is captured is essential for security and privacy protection purposes. First, the level of security is elevated if the capture is controlled in time for a certain action. When the capture is integrated into the process, it is guaranteed that the user cannot provide samples that have been taken previously, or even manipulated or that are the result of a theft of an identity document or of a photograph, video or audio that is available on the internet.

It is also common to introduce **anti-spoofing** techniques, which are included in the **ISO-30107 standard and certified** by independent laboratories.

Regulatory aspects in the use of biometrics: myths vs. realities

Biometrics, as described above, is a strong tool for carrying out a secure and reliable Digital Transformation process. We shouldn't ignore, however, that it's a technology that, due to how certain governments have used it and the profound ignorance surrounding how it actually works, has given rise to certain headlines in the press and extremist positions, which, by wiping the slate clean, have managed to place it at the center of a controversy that is positive in sparking a debate, but that sometimes contributes more noise than reason.

It is common to hear in debates on this matter that the use of biometric technology is not regulated in the current regulatory framework. This is simply not true; **there are legal and technical standards** that have established the lines along which these technologies must be developed and provided.

1. Regulation on data protection

1.1 General Data Protection Regulation (EU) 2016/679 (GDPR)

First, there is the **General Data Protection Regulation (EU) 2016/679 (GDPR)** or Organic Law 3/2018 on Data Protection and Guarantee of Digital Rights. These regulations, in terms of data protection, include the definition of "biometric data", while also including a special category of data for "biometric data aimed at uniquely identifying a natural person", derived from which are all rights and obligations for citizens and for the entities that process

this data.

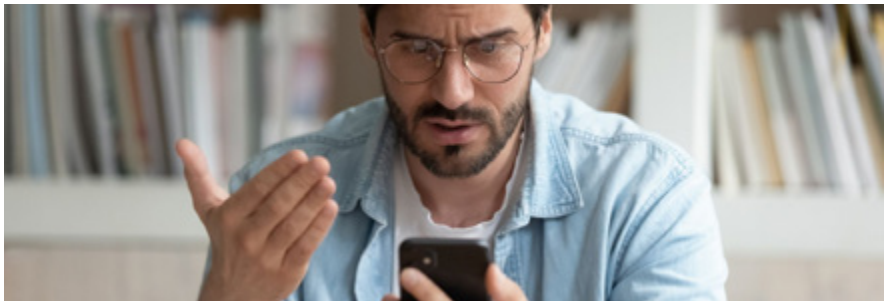
Likewise, in Article 22 of the GDPR, it establishes that the data subjects shall have the right "**not to be subject to a decision based solely on automated processing**, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

In these cases, there must always be, at a minimum, the right to obtain human intervention, "to express his or her point of view and to contest the decision"; in other words, the citizen must always have the right to a review by a person, an intervention that in some sectors (e.g. SEPBLAC authorizations) is always mandatory.

1.2 Regulation on a European approach for Artificial Intelligence

In its proposal for a **"Regulation on a European approach for Artificial Intelligence"** which was published on April 21, 2021 by the European Commission2, it emphasizes what it calls **"High Risk"** applications, including **remote (1:N) Biometric Identification Systems** (meaning that the individual may be identified without being aware of it).

[2] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence



These systems, in addition to complying with the GDPR, must be subject to strict obligations:

· Risk assessment and mitigating actions.

· Establish minimum quality standards for the products used that minimize risks and discriminatory results.

· Log of system activity that allows for the traceability of results.

· Documentation about the system, its purpose and compliance that the competent authorities require.

· Clear and adequate information for the user.

· Human supervision of the results that leads to subsequent actions and minimizes risk and defenselessness.

· High level of robustness and precision of the systems.

The approach of this proposal for a regulation is noteworthy, since it does not intend to regulate or prohibit Artificial Intelligence or the technology itself, but rather proposes regulating several of the specific applications of that Artificial Intelligence, with the aim of guaranteeing that the rights and freedoms of citizens are always respected. This **frame of reference** is very relevant when it comes to providing clarity and security to citizens, in addition to establishing a more focused space for debate.

1.3 AEPD - Data Protection in Labor Relations

In this same sense, on May 18, 2021, the Spanish Data Protection Agency (AEPD) published the guide on "Data Protection in Labor Relations" which, among other considerations, contains a number of guidelines that must be applied to the use biometric data for the management of the employment relationship, but which are equally applicable to other areas. Because, in reality, what the APED is doing is simply reminding us of the principles already established in the GDPR. In particular, it consolidates the distinction between biometric verification and identification, confirming that only in the second case (biometric identification) is the processing of special categories of data carried out according to Article 9 of the GDPR; it indicates in what cases and under what requirements the processing of biometric data is allowed in the field of labor relations and, finally, it recommends he guarantees that must be applied to this type of processing so that it is done in accordance with data protection regulations.

2. Regulation on electronic identification and trust services

2.1 eIDAS Regulation

Likewise, Regulation (EU) 910/2017, known as the eIDAS Regulation, and Implementing Regulation (EU) 2015/1502, expressly mentions biometric technology as a determining element when establishing the framework of security levels for means of electronic identification.

As a result of the development of the eIDAS Regulation in Spain, in November 2020, Law 6/2020 of 11 November came into force, regulating certain aspects of electronic trust services, in which Article 7 refers to the verification of identity prior to the issuance of qualified certificates, allowing this identification to be done remotely.

2.2 Ministerial Order - Remote Identification Methods

This remote identification has finally been regulated in Order ETD/465/2021, of May 6, 2021, which regulates remote video identification methods for the issuance of qualified electronic certificates. The authorized process includes, among other measures, the requirement to verify the authenticity and validity of the identity document, as well as its correspondence with the certificate's applicant, using technologies such as facial recognition (using biometric engines accredited by NIST), and to verify that this is a living

person who is not being impersonated. In addition, a review of the evidence by an operator is required, as well as specific training for said operators.

2.3 EU digital ID "wallet"

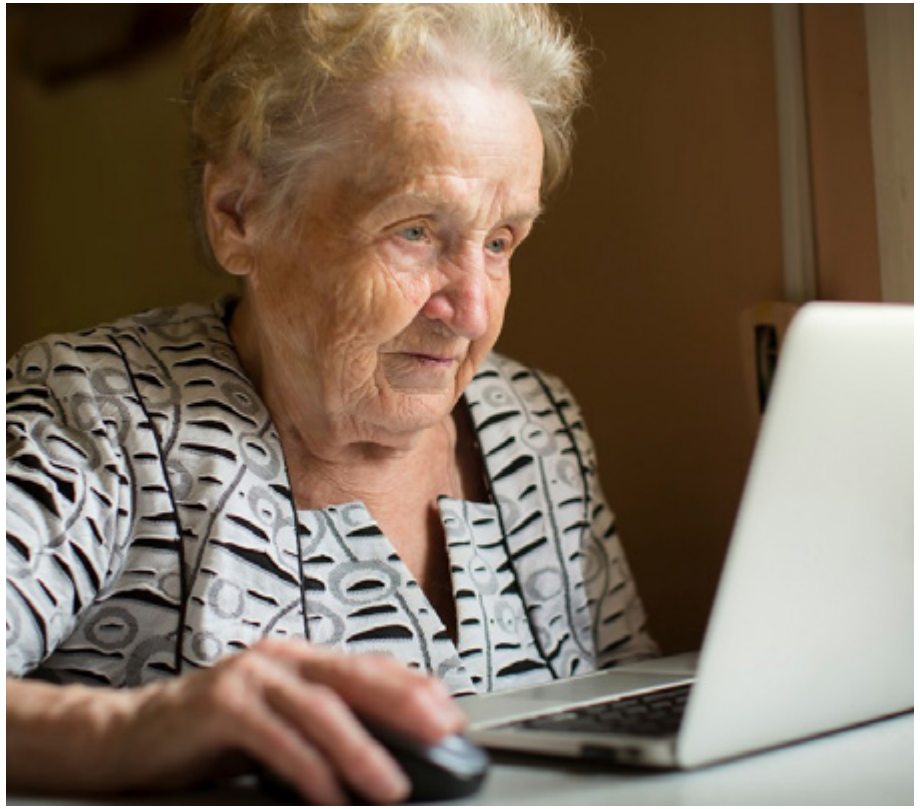
Digital wallets are not unfamiliar to users, as they have already been using these services on their mobile devices to manage their credentials and cards. However, the European Commission wants to offer a solution that allows citizens to control their data. Thus, the new draft of the eIDAS Regulation (already known as **eIDAS2**) includes the Regulation of a digital identification wallet in which all European citizens can securely store their electronic ID cards, driving licenses, bank cards, qualifications, etc. so that they can serve as **proof of identity** for easy and secure access to public and private services within the European Union.

This digital wallet will not replace the current national identity documents but is offered as a complement so that the identity of a European citizen in any Member State can be accredited without the need for additional processes. At the same time, the opportunity to define how to ensure that the digital wallet is in possession of the legitimate user and that it is the user who is proving his identity.

2.4 Resolution Social Security and Pensions

Likewise, the **Resolution of May 25, 2021, of the Secretary of State for Social Security and Pensions** was recently published, which enables procedures and actions to be carried out through the telephone and telematic channels using certain identification systems and regulates aspects related to the submission of applications through electronic forms.

This Resolution highlights the interest in bringing Social Security services closer to citizens through its electronic services and, given the evidence that the current means of identification (e.g., electronic certificates and cl@ve) are not sufficiently widespread among citizens, it adds the possibility of using new, more straightforward means to ensure both the verification of identity and the expression of will and the provision of user consent.



Thus, the following are approved as new recognized identification systems: (i) remote identification systems using videoconference or video-identification and (ii) identification systems, other than video-identification systems, based on biometric data.

In addition, it establishes that this identification of the citizen using videoconference or video-identification may be used for the accreditation of residence to continue to receive the recognized pension and the requirements foreseen in other Social Security procedures.

3. Regulation on payments and prevention of money laundering

3.1 SEPBLAC - Money Laundering Law

Spain, thanks to the initiative taken by the Regulator, in this case the Money Laundering Prevention Service (**SEPBLAC**), belonging to the Bank of Spain, was among the first in the world, back in 2016, to **authorize** remote identification for the opening of checking accounts, strictly complying with the **Money Laundering Law**. This regulation evolved in 2017. After five years of experience, the Regulator recognized that electronic identification is superior to physical identification, since automatic systems are better than people and, in the case of fraud, there is traceability and evidence to be found in

the identification process. Many countries around the world have followed the Spanish regulations as model on which they have based their own.

3.2 Payment Services Directive - PSD2

Finally, also worth mentioning within the European regulations is the **Payment Services Directive (PSD2)**, which, by defining Strong Customer Authentication in its Article 4.30, introduces the reference to the possible elements of authentication, "categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is)". In addition, the combination of these elements, which are independent, allows us to **strengthen the way we authenticate users**.

4. Electronic Judicial Administration

The use of information and communication technologies (ICT) in Spain's Administration of Justice is supervised by the **State Technical Committee of the Electronic Judicial Administration (CTEAJE)**, among whose functions is that of ensuring the interoperability of the systems and applications used in the Justice Administration. In this sense, it has approved the Interoperability and Security Guide for Authentication, Certificates and Electronic Signature **("ISG" Authentication, Certificates and Electronic Signature)**. Within this ISG, the signature systems admitted for electronic proceedings within the Administration of Justice are established.

On May 9, 2021, the General Council of the Judiciary (CGPJ), at the request of the CTEAJE, issued a favorable legal report endorsing the electronic signature system based on facial recognition, with QRbiometrics, in the Electronic Judicial Administration proposed at the request of Veridas within the Avantius system that operates in the Justice Administrations of several Autonomous Communities in Spain.

5. Technical regulations

5.1 National scope

At the same time, there are other **technical standards** such as ISO standards regarding the characteristics that biometric data must comply with or that are related to presentation attack detection techniques, NIST guides, CCN-STIC guides issued by the National Cryptologic Center (of relevance are the recently published CCN-STIC 140-F11), etc.

All this has allowed **limits to be set on the use of this technology in Spain and in Europe**.

5.2 International

Likewise, and in a broader geographic area, it should be noted that Latin American countries and several states in the United States (e.g. California, Illinois, New York...) have also reviewed and adopted their own data protection regulations, thus also establishing the limits, rights and obligations applicable to the processing of personal data, including biometric data. Information that is clear and transparent to users, the rights of users regarding their data, the conditions or prohibitions for the communication and sale of data, the conditions for international data transfers... are common denominators in all regulations.

6. Application of European regulations on the matter

The recent decision taken by the **French Council of State** on the ALICEM identification system is a good example of the application of the aforementioned European regulations to a specific case. This system was promoted by the French Government to facilitate secure access by citizens to public services.

The highest administrative body of France has confirmed the legality of this measure and its compliance with the European GDPR and fundamental rights. Likewise, the Spanish Data Protection Agency itself prepared a note in 2020 with warnings about certain uses of facial biometrics that allow some cases to be differentiated from others.

To presume that any use of biometrics is illegal and that it may violate fundamental rights is simply not justified. There are institutions that are charged with the mission of defending rights (judges, courts, supervisory authorities such as the AEPD, etc.), and they should be the ones who differentiate between legal cases and those that are not legal, between technologies that respect privacy and those that are invasive.


CONCLUSIONS

CONCLUSIONS

1

After the description of the Identity Verification and Biometrics technology, we can conclude that the use of a system based on Artificial Intelligence can offer **guarantees** of precision, **security** and data protection in the sense required by the principles of privacy by default and by design.

CONCLUSIONS

2

The use of biometric recognition systems has spread in recent years in a large number of sectors, being very well received by users. It can cover, with the **greatest guarantees**, the objective of **identifying or authenticating** the identity of a person. And, out of the three elements that we have been differentiating when we talk about user authentication (possession, knowledge and inherence), there is no question that **inherence is the only one that can provide certainty,** while the other two remain a presumption.

The latter is an issue that, in the analysis of the specific case and of the technology to be used, must be taken into account when making judgments about proportionality regarding data protection.

CONCLUSIONS

3

The implementation of these technologies drastically reduces **the risk of committing crimes and identity theft**, and allows for secure **access** to public and private services.

Companies and governments in the most advanced countries, including Spain, are betting on this technology.

CONCLUSIONS

4

When we talk about biometric technology, we must keep in mind that not all systems are the same nor do they carry the same risks.

There are internationally recognized advanced technologies, based on artificial intelligence, which are in the current state of the art, and which **can minimize the risks of fraud and fully comply with regulatory requirements in terms of data protection and with the different regulations for the protection of fundamental rights.**

Systems based on artificial intelligence help to make more informed and secure decisions; **when properly configured they are less prone to error and bias than humans.**

CONCLUSIONS

5

Biometric and identity verification systems **are not meant to infer any of the person's other characteristics** such as their behaviors, emotions, gender, ethnicity, race, sexual orientation, lifestyle, etc.

This purpose is not lawful, typical of or inherent to the use of these systems and processes.

CONCLUSIONS

6

European and Spanish data protection regulations clearly regulate the use of biometrics.

It is the responsibility of the public authorities to ensure its application and development in a way that guarantees that the uses and technologies applied respect said regulations.

CONCLUSIONS

7

In short, the technologies described allow us to tackle a **Safe Digital Transformation process**, in line with the guidelines of the Digital Transformation Plan put together by the Government of Spain, in which, in addition, Spanish companies are playing a leading role in terms of technological development and implementation in highly competitive international markets, reflecting the quality and level of training of their human talent.

For more information contact us

Pamplona I Madrid I Ciudad de México I Bogotá I San Francisco

www.veridas.com