Identidad, Biometría e IA

Ética, Mitos y Realidades

Facebook acaba de reconocer que en 2019 **perdió información**, entre las que se encontraban contraseñas y datos personales de 500 millones de usuarios. Una de las prioridades estratégicas definidas por la Unión Europea, y de todos los Estados miembros, es la lucha **contra el blanqueo de capitales**, que impulsada por las operaciones digitales, amenaza con erosionar el sistema fiscal que dota al estado del bienestar. La **adicción al juego on-line de menores**, se ha convertido en un nuevo problema para el que los padres, educadores y autoridades, buscan respuestas y soluciones. Los **delitos de fraude cibernético** ya son un 25% de los denunciados en diferentes policías en España.

Los hechos anteriores son algunos de los ejemplos en los que la **Identidad de las Personas** y su reflejo en el mundo **digital** juegan un papel clave. El modo de asegurar la certeza, su seguridad, control y eficacia son la piedra angular para una Transformación Digital segura y confiable. La inteligencia artificial y la biometría son la piedra angular para habilitarla. **Europa tiene la capacidad**, no sólo de **regular** de acuerdo a los más altos

estándares éticos, sino también de de hacerlo desde el **liderazgo** tecnológico, como lo ha hecho históricamente en industrias tan importantes como el automóvil y la aeronáutica.

Identidad física en un mundo digital

El **derecho a la identidad** es uno de los derechos **fundamentales** de todo ser humano, y es necesario para poder beneficiarse de los otros derechos fundamentales. La identidad incluye el nombre, el apellido, la fecha de nacimiento, el sexo y la nacionalidad. Es la prueba de la existencia de una persona como parte de una sociedad, como individuo que forma parte de un todo; es lo que la caracteriza y la diferencia de las demás.

En el **mundo físico**, la identidad es un atributo que los estados otorgan a sus ciudadanos al nacer, y que se manifiesta en forma de: **pasaporte, documento de identidad**, carnet de conducir, credencial para votar y otras formas de identificación oficiales que cada país establece. Los primeros pasaportes datan del Imperio Persa en el siglo V a.C., si bien su forma moderna data de mediados del siglo XIX aparejados al ferrocarril, y el desplazamiento masivo de personas. Este sistema ha funcionado de forma "razonable" para acreditar la identidad de las personas en el "mundo físico": el **fraude de identidad** siempre está en el centro de la mayoría de los hechos delictivos, y desde hechos menores como acceder a una discoteca siendo menor a otros, como el blanqueo de capitales necesitan del falseo y suplantación de identidad para su consumación.

Cuando hablamos de **Identidad** en el **mundo digital**, no nos referimos al perfil de Facebook, Instagram, Twitter o cualquier otra en red sociales, donde el mismo no tiene porqué guardar una relación con la Identidad física o real, y en la que el anonimato, pseudónimo o avatar es inherente a esas nuevas formas de expresión. La Identidad Digital, en este contexto, se refiere a la posibilidad de **ejercer el derecho a reclamar nuestra identidad individual**, de forma inequívoca, para poder operar y acceder a todo tipo de información y realizar transacciones de manera segura en el ámbito de internet, de tal manera en que la confianza a ambos lados de la pantalla sea máxima.

El acceso a una página web o una APP, la apertura de una cuenta corriente, la emisión de un certificado digital, la fe de vida para el cobro de una prestación, la firma digital de un documento, el alta de una tarjeta SIM, la reserva de un vehículo, la compra-venta de un bien, el *check-in* en un hotel, una recogida de firmas, asegurar que es un mayor de edad quien accede a determinados contenidos e incluso poder ejercer el derecho al voto, son

una pequeña **muestra de operativas donde la confianza en la certeza de la identidad** es la clave para poder realizar transacciones rápidas y seguras.

El modelo actual de Identidad Digital está roto: la identidad "presumida"

La identificación en el ámbito digital se compone de dos pasos: un **primer** proceso en el que la persona da **prueba de su identidad** demostrando que es quien dice ser mostrando que es el genuino propietario de un documento de identidad válido. Este proceso se puede realizar de manera presencial o digital (como se verá más adelante). Verificado este paso, la persona **obtiene una credencial de identidad** (un usuario y contraseña, un certificado digital y contraseña, una tarjeta de coordenadas, etc). Este proceso no es perfecto: la verificación inicial de identidad muchas veces se realiza sin documento acreditativo, e incluso en un entorno presencial, la persona que verifica no es experta en verificar documentos, reconocer caras y no está entrenada para "enfrentarse" a un caso de fraude.

El **segundo** paso se produce en el momento en el que la persona se **"autentica"** y prueba, en un entorno digital, que tiene una credencial que prueba su identidad. Esa credencial (un password, un SMS, una tarjeta de coordenadas), no liga a la persona con su identidad de forma directa, sino que **ésta se "presume"**. Dicha credencial, aún en caso de que se haya obtenido lícitamente, **se puede transferir** para que una persona actúe en nombre de otra. Ésta, se puede **obtener de forma ilícita** (recuérdese el robo masivo de passwords de Facebook, el hacking, o maniobras de ingeniería social), o el usuario puede incluso reivindicar un uso espurio de su credencial de identidad **repudiando** una operación que él mismo hizo - "me robaron el password y firmaron por mi"- asociado a la debilidad intrínseca del sistema.

La identidad digital con biometría está **expresamente contemplada en el Plan de digitalización de Administraciones Públicas 2021-2025** en el eje 1 "Transformación Digital de la Administración General del Estado", donde se propugna un "nuevo modelo de identidad digital" en los siguientes términos:

"Es un reto mejorar cómo los ciudadanos, ciudadanas y empresas se identifican de forma sencilla y efectiva ante las Administraciones.

> *El objetivo de esta medida es doble. Por una parte, se desarrollarán sistemas y servicios que permitan acreditar digitalmente a ciudadanos, ciudadanas y empresas de forma 100% telemática,* ***utilizando tecnologías tales como biometría, imagen, etc, de forma segura*** *y, por otra,*

desarrollar nuevos sistemas de identificación y firma sencillos, seguros y usables por los ciudadanos y ciudadanas, en línea con la normativa aplicable en esta materia."

En medio del cambio tecnológico en el que estamos inmersos, acelerado por la pandemia, es absolutamente necesario dotarnos de instrumentos para hacer que esta **Transformación Digital sea segura, privada y confiable**, para lo que se deben articular instrumentos para **ejercer nuestra Identidad Real**.

La biometría: "de la presunción a la certeza"

La **biometría**, definida según la **ISO,** como el reconocimiento automático de los individuos en función de sus características biológicas y de comportamiento. Se diferencia siempre en el mundo de la biometría, la **verificación o autenticación (1:1)** en la que un individuo se verifica contra sí mismo (p.ej: comparar la foto de su DNI con su foto selfie) de la **identificación (1:N)** en la que se busca a un individuo dentro de una lista.

La tecnología biométrica moderna, gracias a su precisión, facilidad de empleo, seguridad y privacidad, permite ejercer la identidad en el espacio digital de forma unívoca y segura. Ésta permite que una persona realice una operación digital, y **sea acreditada de forma unívoca** a su persona, aportando toda la **seguridad jurídica**, **evitando el fraude**, la suplantación de identidad, además de tener toda conveniencia de operar en el espacio digital, mejorando la eficacia de las AAPP, las empresas, evitando pérdida de tiempo, recursos y desplazamientos innecesarios, **reduciendo la huella de carbono** de cada transacción.

Las tecnologías de **Verificación Digital de Identidad**: validación automática de documentos de identidad, biometría facial y de voz, nos permiten probar la identidad de forma sencilla, segura y eficiente, en el mundo digital **igual que lo hemos hecho los seres humanos históricamente en el físico: por su cara y su voz** si ya la habíamos conocido anteriormente, o les pedimos un documento que acredite su identidad (verificando su autenticidad, datos personales y relación entre la fotografía y la persona), si no lo conocíamos.

Finalmente, debe resaltarse que estos sistemas **no permiten inferir otras características del sujeto** como comportamientos, actitudes, emociones, tendencias, género, etnia,

colores de piel, etc., ni supone la clasificación de la persona en un perfil que pueda determinar características o comportamientos futuros.

Inteligencia Artificial y Biometría: una pareja "irreversible"

Gracias al impulso de la **Inteligencia Artificial (IA)**, y en particular del *Machine Learning,*que se ha producido en los últimos años, las tecnologías de reconocimiento facial y de voz han alcanzado unos niveles de precisión elevadísimos, muy por encima de los mejores fisonomistas humanos. Los modelos biométricos de *Machine Learning* se crean a partir de complejos algoritmos matemáticos, a los que se "entrena y enseña" como se haría con el cerebro humano, si bien su "inteligencia" es muy específica para una determinada tarea, y no generalista. Los resultados que éstos obtienen son muchísimo más eficaces, precisos y con menos sesgo que una persona.

Valga como ejemplo la última evaluación de **Identificación Facial (1:N) realizada por el NIST**[1] dónde se encuentran ya muchos sistemas con tasas de Falsos Positivos (equivocarse en el candidato encontrado) del **3 por 1.000** asociados a una tasa de Falsos Negativos (no encontrar la persona en la lista cuando está) por debajo del dos por ciento en búsquedas de 1.6 millones de personas.

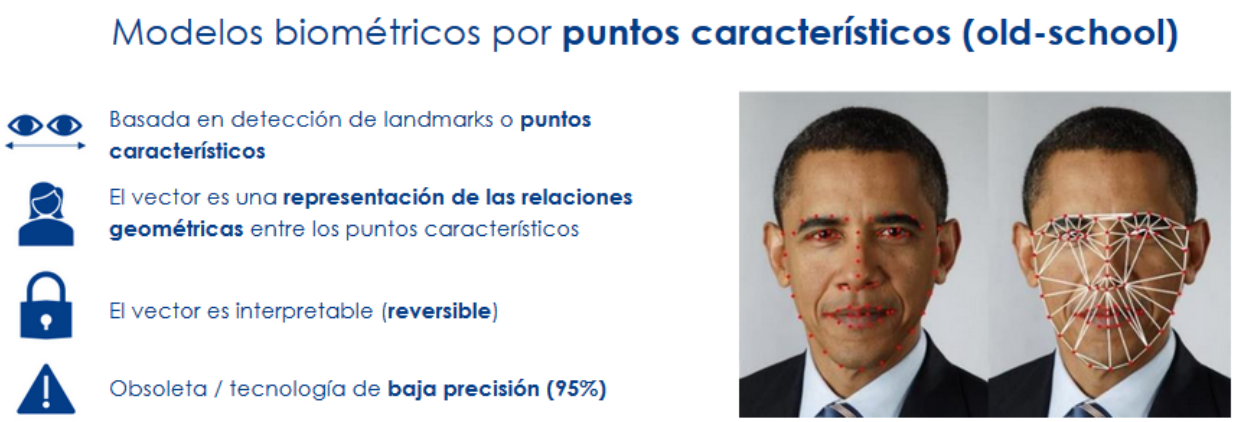
Los sistemas, además, presentan niveles de **sesgo entre razas, géneros y edades,** muy **bajos**. Esta última cuestión fue objeto de análisis por el NIST en un informe de diciembre de 2019, que concluyó que los sesgos en los sistemas 1:1 apenas tenían incidencia, y que en los sistemas 1:N solo algunos algoritmos evidenciaron un sesgo, dado que "los algoritmos tienen un rendimiento diferente", y los más equitativos (menos sesgados) coinciden también con los algoritmos más precisos. Por consiguiente, es una cuestión de calidad del sistema biométrico, lo cual permite no sólo una mayor precisión sino también una menor discriminación. En cualquier caso, el sesgo de los sistemas automáticos son **mucho menores que aquellos en los que infiere un ser humano**.

[1] **National Institute of Standards and Technology, en EEUU, es un laboratorio que evalúa de forma neutral y sistemática todas las tecnologías biométricas de los fabricantes que voluntariamente se someten a su exámen: https://pages.nist.gov/frvt/html/frvt1N.html*

Los motores biométricos modernos entrenados mediante IA son privados por diseño y por defecto, por lo que se puede **desterrar el mito de que "si pierdo un password lo reseteo, pero si pierdo mi biometría, he perdido mi identidad"**.

Revisemos el porqué. Se puede distinguir dos tipos de modelos de motores biométricos:

- **Modelos biométricos por puntos característicos (*old-school*).**



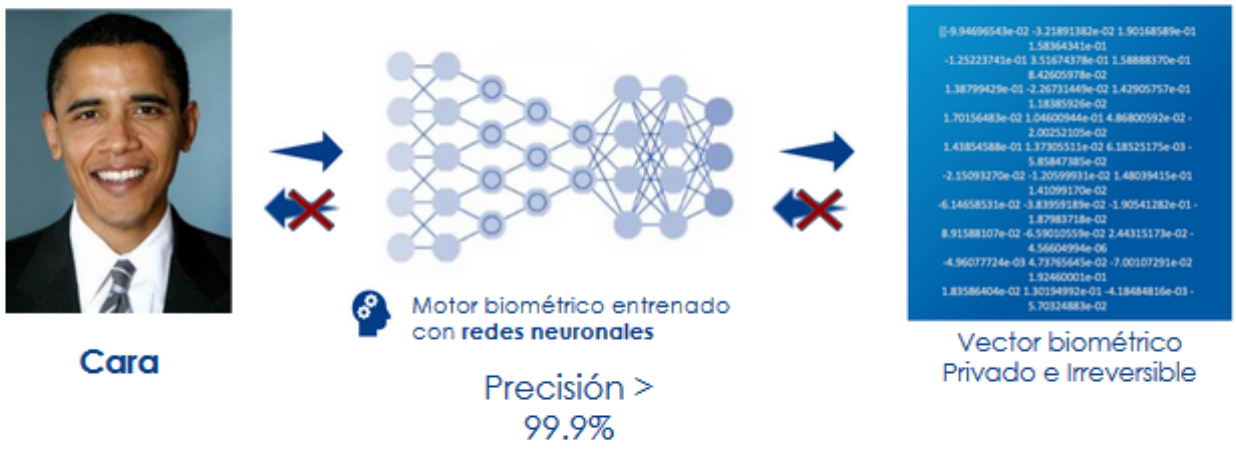
Eran los más extendidos hasta hace unos 5 ó 7 años, y **estaban basados en *'landmarks'* o puntos característicos** para reconocer, por ejemplo, una cara.

Este método implica tomar medidas entre múltiples puntos de la característica biométrica, como una imagen facial, obteniendo como resultado un vector matemático de comparación, que es un resumen de dichas medidas. En este tipo de tecnologías, la precisión quedaba limitada y se podría ser capaz, a la vista del vector generado con este motor, de interpretar las medidas que dicho vector está representando de los puntos característicos de la cara del sujeto (p.ej. siendo una imagen facial: la distancia entre los ojos, entre sus orejas, etc.), y obtener así una estimación de la imagen original. Además, estos sistemas se encuentran en su mayoría estandarizados, lo cual implica que su funcionamiento pueda ser conocido por cualquiera. Esto hace que las tecnologías **sean interoperables** (como los sistemas de reconocimiento de huella **dactilar**), las implicaciones a nivel de protección de datos pueden ser negativas. Por estas circunstancias, los motores biométricos basados en puntos, pueden considerarse una

tecnología ya superada para la verificación de identidad digital, que podemos definir como la "old School technology".

- **Modelos biométricos basados en Inteligencia Artificial**

Las empresas que desarrollan tecnologías punteras, han dejado atrás los modelos "Old-school" para pasar a modelos basados en Inteligencia Artificial y, más específicamente, en redes neuronales (deep neural network, DNN)



Cuando una cara (o una voz) se procesa por el motor biométrico, el **resultado es un vector matemático irreversible y no-interoperable con otros sistemas**.

Esta IRREVERSIBILIDAD hace que, como consecuencia, **ni siquiera el fabricante** sea capaz de **interpretar** el vector matemático con la finalidad de extraer información del individuo que prestó sus datos. Por tanto, la obtención del mismo, aunque fuera ilícita, no supone que la información biométrica haya sido comprometida, ni que ya no se pueda cancelar.

La obtención ilegítima de este vector representa un **riesgo** para la privacidad sustancialmente **menor** que el extravío de un documento de identidad o la publicación de una imagen en redes sociales.

La **no-interoperabilidad** intrínseca a estos sistemas, supone un inconveniente técnico importante, pero tiene la ventaja de garantizar que, ante un eventual robo de esos datos, no permite su uso en ningún otro sistema biométrico del mismo u otro fabricante.

Asimismo, es importante asegurar la **transparencia** en el funcionamiento del sistema una vez está en un entorno productivo. Debe garantizarse que los **datos** de los sujetos que están haciendo uso del servicio de reconocimiento **no son usados para el entrenamiento** automático del motor. Éste debe realizarse sólo en la fase de desarrollo del sistema, para garantizar la calidad de los datos (para poder así garantizar que se obtiene un modelo preciso y sin sesgos) y la legitimidad en su tratamiento para esta finalidad.

- **La captura de los datos**

Un sistema de reconocimiento biométrico, sea para autenticación o identificación, debe partir siempre de la **captura EXPLÍCITAMENTE CONSENTIDA de los datos del individuo** (salvo que exista otra base legitimadora para su tratamiento suficientemente justificada). La elección de los datos biométricos que se usan, determinan la accesibilidad y el alcance del sistema de identificación. Un sistema de biometría facial es prácticamente accesible para todas las personas, con independencia de potenciales problemas de salud o características físicas (p.ej. cicatrices), sean temporales o permanentes. Los sistemas de biometría de voz también son accesibles para un elevadísimo porcentaje de las personas. Además de tener en cuenta qué tipo de datos se recopilan, es fundamental a efectos de seguridad y de protección de la privacidad, el diseño del modo en que se capturan esos datos. En primer lugar, la seguridad se eleva si la captura es **controlada en tiempo para una acción determinada**. Cuando la captura está integrada en el proceso, se garantiza que el usuario no pueda aportar muestras tomadas previamente, o incluso manipuladas o fruto de una sustracción de un documento de identidad o de una fotografía, video o audio disponible en la red.

Es también común la introducción de técnicas de ***anti-spoofing,*** que **eviten la suplantación**, recogidas por la norma ISO-30107 y certificadas por laboratorios independientes.

Aspectos regulatorios en el uso de la biometría: mitos vs. realidades

La biometría, como se ha descrito anteriormente, es una potente herramienta para realizar una Transformación Digital segura y confiable. No se puede obviar, no obstante, que es una tecnología, que por el uso que han hecho de la misma determinados Gobiernos y el

desconocimiento profundo de su funcionamiento real, ha dado lugar a determinados titulares de prensa y posicionamientos extremos, que haciendo *tabula rasa* la han puesto, en el centro de una polémica, que es positiva para inducir el debate, pero que en ocasiones aporta más ruido que razones. Es habitual escuchar en los debates sobre esta materia que el uso de la tecnología biométrica no está regulado en el marco normativo vigente. No es cierto; **existen normas, legales y técnicas**, que han establecido las líneas en las que deben desarrollarse y prestarse estos sistemas.

En primer lugar, el **Reglamento (UE) 2016/679 General de Protección de Datos (RGPD)** o la Ley Orgánica 3/2018 de Protección de Datos y Garantías de Derechos Digitales. Estas normas, en materia de protección de datos, incluyen la definición de "dato biométrico", incluyendo además como categoría especial de datos aquellos "datos biométricos dirigidos a identificar de manera unívoca", derivandose de todo ello unos derechos y obligaciones para los ciudadanos y para las entidades que tratan estos datos.

Asimismo, en su artículo 22 el RGPD establece que los interesados tienen derecho "a **no ser objeto de una decisión basada únicamente en el tratamiento automatizado**, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar". En estos casos, debe existir siempre, como mínimo, el derecho a obtener intervención humana, "a expresar su punto de vista y a impugnar la decisión"; es decir, el ciudadano siempre debe tener derecho a la revisión por una persona, intervención que en algunos sectores (p.ej. autorizaciones del SEPBLAC) se torna siempre obligatoria.

En su propuesta de **"Reglamento con enfoque Europeo de la Inteligencia Artificial"** que ha sido publicada el **21 de abril de 2021** por la **Comisión Europea**[2] hace hincapié en lo que denomina aplicaciones de **'Alto Riesgo'** entre las que incluye los sistemas de **Identificación Biométrica (1:N) remota** (entendiéndose como tal la que el individuo puede estar siendo identificado sin ser consciente de ello)

Estos sistemas, además de cumplir el RGPD, deben estar sujetos a obligaciones estrictas:

- *Evaluación de riesgo y acciones mitigadoras.*
- *Establecer estándares de calidad mínima de los productos utilizados que minimicen riesgos y resultados discriminatorios.*

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

- *Registro de la actividad del sistema que permita la trazabilidad de los resultados.*
- *Documentación necesaria para las autoridades competentes sobre el sistema, su propósito y cumplimiento.*
- *Información clara y adecuada para el usuario.*
- *Supervisión humana de los resultados que impliquen acciones posteriores y minimicen el riesgo e indefensión.*
- *Alto nivel de robustez y precisión de los sistemas*

Es destacable el enfoque de esta propuesta de regulación, dado que no pretende regular, ni prohibir la Inteligencia Artificial o la tecnología en sí, sino que propone una regulación de algunas aplicaciones específicas de esa Inteligencia Artificial, con el objetivo de garantizar así que siempre se respetan los derechos y libertades de los ciudadanos.

Este **marco de referencia** es muy relevante para aportar claridad y seguridad a la ciudadanía, estableciendo, además el espacio de debate más centrado.

Igualmente, es de especial relevancia el Reglamento (UE) 910/2017, conocido como **Reglamento eIDAS**, y el Reglamento de ejecución (UE) 2015/1502, que expresamente menciona la tecnología biométrica como un elemento determinante al establecer el marco de los niveles de seguridad de los medios de identificación electrónica.

Fruto del desarrollo del Reglamento eIDAS en España, en noviembre de 2020 entró en vigor la **Ley 6/2020, de 11 de noviembre**, reguladora de determinados aspectos de los servicios electrónicos de confianza, en cuyo artículo 7 hace referencia a la comprobación de la identidad previa a la emisión de certificados cualificados, **permitiendo** que esta **identificación se haga a distancia**.

Una **orden ministerial**, que se encuentra actualmente en las últimas fases de su aprobación, regula los métodos de identificación no presencial que se deberán emplear para esta finalidad: tecnologías biométricas y de validación documental certificadas.

Nuestro país, gracias al impulso del regulador, en este caso del Servicio de Prevención de Blanqueo de Capitales (**SEPBLAC**), perteneciente al Banco de España, fue de los primeros en el mundo en **autorizar, ya en 2016,** la identificación remota para la apertura de cuentas corrientes en banca, cumpliendo de forma estricta la **Ley de Blanqueo de Capitales**. Dicha regulación evolucionó en 2017. Tras cinco años de experiencia, el Regulador reconoce que

la identificación electrónica es superior a la física, ya que los sistemas automáticos son mejores que las personas, y en caso de fraude queda trazabilidad y evidencias en el proceso de identificación. Muchos países en el mundo han seguido la regulación española como modelo para establecer las suyas propias.

Cabe por último hacer referencia, dentro de la regulación europea, la **Directiva de servicios de pago (PSD2)**, que al definir en su artículo 4.30 la autenticación reforzada de clientes, introduce la referencia a los posibles elementos de autenticación, "categorizados como conocimiento (algo que solo conoce el usuario), posesión (algo que solo posee el usuario) e inherencia (algo que es el usuario)". Además, la combinación de estos elementos, que son independientes, nos permiten **autenticar a usuarios de forma reforzada.**

Al mismo tiempo, existen otras **normas técnicas** como podrían ser normas ISO relativas a las características que deben cumplir los datos biométricos o a las técnicas de detección de ataques de presentación, las guías del NIST, las guías CCN-STIC emitidas por el Centro Criptológico Nacional (de relevancia la recientemente publicada CCN-STIC-140-F11), etc.

Todo ello ha permitido ir configurando **límites al uso de esta tecnología, en España y en Europa.**

La reciente decisión del **Consejo de Estado francés** sobre el sistema de identificación ALICEM es un buen ejemplo de aplicación de las normativas europeas antes mencionadas a un caso concreto. Este sistema fue promovido por el Gobierno francés para facilitar el acceso seguro de la ciudadanía a los servicios públicos. El máximo órgano contencioso administrativo de Francia ha confirmado la legalidad de esa medida y el ajuste de la misma al RGPD europeo y su conformidad con los derechos fundamentales. Asimismo, la propia Agencia Española de Protección de Datos elaboró en 2020 una nota con advertencias sobre ciertos usos de la biometría facial que permite diferenciar entre unos casos y otros.

Presumir que todo uso de la biometría es ilícito y que puede atentar contra derechos fundamentales no está justificado. Existen instituciones que tienen encargada la misión de defender los derechos (jueces, tribunales, autoridades de control como la AEPD, etc.), y deben ser ellas quienes diferencien entre los casos lícitos y los que no lo son, entre tecnologías respetuosas con la privacidad y las invasivas.

Finalmente, y en un **ámbito geográfico más extenso** cabe señalar que también los países de Latinoamérica y varios Estados de Estados Unidos han revisado y adoptado sus normativas de protección de datos, sentando así también los límites, derechos y obligaciones aplicables al tratamiento de los datos personales, y de los datos biométricos entre ellos.

Conclusiones

Tras la descripción de la tecnología de Verificación de Identidad y biometría, se puede concluir que el empleo de un sistema basado en Inteligencia Artificial permite ofrecer unas **garantías** de precisión, **seguridad** y protección de datos en el sentido requerido por los principios de privacidad por defecto y desde el diseño.

El uso de sistemas de reconocimiento biométrico se ha extendido en los últimos años en un amplio número de sectores, obteniendo una muy buena acogida por parte de los usuarios. Permite cubrir, con las **mayores garantías**, el objetivo de **identificar o autenticar** la identidad de una persona. Y es que, de los tres elementos que se vienen diferenciando cuando hablamos de autenticación de usuarios (posesión, conocimiento e inherencia), sin duda el de **inherencia es el único que puede aportar certeza,** mientras que los otros dos se quedan en la presunción. Esta última es una cuestión que, en el análisis del caso concreto y de la tecnología a emplear, deberá tenerse en cuenta a la hora de realizar los juicios de proporcionalidad en materia de protección de datos.

La implantación de estas tecnologías **reducen de forma drástica el riesgo de comisión de delitos** y suplantación de identidad, y permiten un **acceso seguro** a servicios públicos y privados. Empresas y gobiernos de los países más avanzados, entre ellos el de España, están apostando por esta tecnología.

Cuando hablamos de tecnología biométrica, debe tenerse en cuenta que no todos los sistemas son iguales ni entrañan los mismos riesgos. Hay tecnologías avanzadas internacionalmente reconocidas, fundadas en la inteligencia artificial, que se encuentran en el estado del arte actual, que **permiten minimizar los riesgos de fraude y cumplir sobradamente con los requisitos normativos en materia de protección de datos y con las distintas normativas de protección de derechos fundamentales**. Los sistemas

basados en inteligencia artificial ayudan a tomar decisiones más informadas y seguras; **debidamente configurados son menos proclives al error y al sesgo que el ser humano.**

Los sistemas biométricos y de verificación de identidad, **no tienen como objeto inferir otras características de la persona** como sus comportamientos, emociones, género, etnia, raza, orientación sexual, estilo de vida, etc. Esta finalidad no es lícita ni propia o inherente al uso de estos sistemas y procesos.

La normativa europea y española de protección de datos regula el uso de la biometría de manera clara. Corresponde a los poderes públicos velar por su aplicación y desarrollo para garantizar que los usos y tecnologías aplicadas las respetan.

En resumidas cuentas, las tecnologías descritas permiten abordar un **proceso de Transformación Digital Segura**, en línea con las directrices del Plan de Transformación Digital elaborado por el Gobierno de España, en la que, además, las empresas españolas están siendo protagonistas en materia de desarrollo tecnológico e implantación en mercados internacionales de alta competitividad, reflejando la calidad y en nivel de formación de su talento humano.

Eduardo Azanza Ladrón

Co fundador y CEO de *das-Nano* y *Veridas.*