INFORME LEGAL CASOS DE USO EN LA UTILIZACIÓN DE TECNOLOGÍAS BIOMÉTRICAS

autelsi
Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información

Grupo de Regulación de Autelsi

Marzo 2021

ÍNDICE

RESUMEN EJECUTIVO

La transformación digital y la aplicación de las tecnologías a distintos campos de actuación en el ámbito social y empresarial es una realidad. El presente trabajo tiene por objeto analizar las implicaciones derivadas del empleo de tecnologías en relación con el uso de datos biométricos. Con ello, pretendemos dar respuesta a las dificultades suscitadas en la práctica sobre los riesgos asociados al empleo de dichas tecnologías y la adopción de los necesarios controles para garantizar la indemnidad de la ciudadanía.

En primer lugar, debemos delimitar el concepto de "dato biométrico" y "biometría". Por dato biométrico se entiende aquella información relacionada con características físicas, fisiológicas o de conducta de una persona que permiten la identificación de la misma. Son datos biométricos, entre otros, la huella dactilar, las imágenes faciales, la geometría de la palma de la mano, etc. Por biometría se entiende el método de reconocimiento de personas basado en sus características fisiológicas o de comportamiento.

Para realizar el reconocimiento biométrico es frecuente acudir a diferentes tecnologías como la videovigilancia, escáneres de última generación y demás dispositivos de reconocimiento fisiológico o comportamental. La interacción de herramientas de Inteligencia Artificial, de M*achine Learning* y Big Data, dotan a la información biométrica de un alto potencial, pero también de un extraordinario impacto para los derechos e intereses de las personas físicas.

En el presente análisis, abordaremos distintos casos de uso que se dan en la práctica; en concreto:

Identificación biométrica a distancia de las partes intervinientes para la contratación de servicios en remoto.

Video-identificación facial en el que se utilizan herramientas de *machine learning* en espacios abiertos al público tales como infraestructuras aeroportuarias, estaciones de tren, eventos deportivos, etc. y donde se intenta detectar entre una multitud a un sujeto en concreto.

Identificación facial, auditiva y por huella a través de móviles, tabletas y dispositivos tecnológicos a disposición del ciudadano.

Utilización de datos biométricos asociados a la voz en *call centers* que con herramientas de inteligencia artificial permiten realizar patrones y predecir conductas.

LEGISLACIÓN DE REFERENCIA Y ESTÁNDARES INTERNACIONALES.

El legislador trata de proteger los intereses de los agentes implicados en las relaciones afectadas. La tecnología evoluciona y la legislación se adapta. Como veremos a lo largo del presente estudio, entre las aplicaciones actuales de las tecnologías biométricas podemos encontrar el control de accesos físicos y lógicos, el control de presencia o la lucha contra la criminalidad y el fraude entre otras. A tal efecto, en el uso de tecnología biométrico se ha de tener en cuenta las distintas normativas, y especialmente:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, "**RGPD**").

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, "**LOPDGDD**"). REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (eIDAS), pendiente de revisión este año, homogeneizará los requisitos para la video identificación a nivel europeo. También se espera defina los requisitos a nivel de uso de inteligencia artificial en el reconocimiento. Ahora mismo diferente enfoque a nivel país.

- REGLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº. 526/2013 («Reglamento sobre la Ciberseguridad»), que exige la parte de auditorías de los productos.

- Video-identificación: en España existe una norma del Centro Criptográfico Nacional-CCN (CCN-STIC-140) que define a nivel de detalle las características que debe tener el producto de video-identificación para ser válido en la identificación a distancia para la emisión de un certificado.

- La orden ministerial que tiene que publicarse en marzo establecerá la obligatoriedad de obtener la certificación CommonCriteria o Lince para que un producto sea admitido en la emisión de un certificado cualificado, y en consecuencia que la firma realizada en un contrato a distancia tenga unas mínimas garantías legales.

Acerca de los estándares internacionales, existen normas ISO que definen la estructura de los datos biométricos que se recogen, pero no sobre el procedimiento para hacer esta recogida. Con la revisión del Reglamento eIDAS se espera que se publiquen normas ETSI que definan la parte de detalle técnico y de procedimiento.

Además, con relación al DNI Electrónico y su Identidad Biométrica resultarían aplicables:

- ISO/ 19.785, ISO 19.794-2 Formatos de cabecera y datos de referencia.

- ISO 7816-4, ISO 7816-11 Para la definición de los comandos de la tarjeta.
- ANSI X.9.84 – 2003 – Reconocimiento de firmas, huellas digitales.
- ISO/IEC 27N2949 – Condiciones de los sistemas biométricos para la industria de servicios financieros.
- ISO / IEC 19784-1:2005, también conocido como BioAPI 2.0. Conexión entre dispositivos biométricos y diferentes tipos de aplicaciones, interfaz de programación de aplicaciones biométricas (API).
- *Common Biometric Exchange Fice Format* – formatos comunes de intercambio de archivos biométricos.

CASOS DE USO

CASO 1: IDENTIFICACIÓN A DISTANCIA Y FIRMA EN TABLETA.

En la actualidad es posible realizar ciertos trámites, tanto en el sector público como en el privado, de forma telemática, sin tener que acudir presencialmente. La banca inició el proceso hace unos años permitiendo la contratación de algunos servicios, como la apertura de una cuenta corriente, tan sólo con un *selfie* (autorretrato) o un video, realizado por el propio móvil del cliente. Para ello, la banca tiene en cuenta la normativa de Blanqueo de Capitales y las resoluciones del SEPBLAC (Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias), la cual establece los requisitos mínimos para garantizar la identidad del cliente.

Otros servicios que requieren de presencia física en un notario, como por ejemplo la firma de un préstamo o una compraventa, actualmente se podrían realizar íntegramente de forma remota. No obstante, existen aún ciertas limitaciones. En este sentido, para que el proceso de firma remota sea legalmente equivalente a la manuscrita, la legislación actual exige la utilización de un certificado electrónico (además de utilizar un dispositivo seguro), para cuya obtención se requiere la presencia física. En el ámbito de los servicios públicos, el artículo 7 de la Ley 6/2020 del 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, ya establece la posibilidad de acreditar nuestra identidad a distancia mediante el uso de video-identificación o videoconferencia, pero las condiciones concretas para hacerlo las deja en manos de una Orden Ministerial, la cual se espera que esté aprobada para el próximo mes de marzo (2021). Los diferentes actores (fabricantes de productos de identificación biométrica, prestadores de servicios de identificación, etc.) deberán adaptarse a la nueva normativa durante el año 2021. Este cambio debería suponer una mejora sustancial en el acceso a los servicios telemáticos, lo que debería traducirse en un incremento notable de la oferta de dichos servicios.

Otra solución basada en biometría es la firma en tableta para proceder a la contratación de un servicio. En la actualidad está muy extendido, y es un procedimiento habitual en entidades bancarias, comercios, en algunos servicios públicos, etc. El trámite se realiza habitualmente de forma local, utilizando el dispositivo proporcionado por la propia entidad. Su uso ofrece una serie de ventajas respecto a la firma en papel, entre ellas, mayor control del fraude, gestión de evidencias, reducción de papel, etc.

A continuación, se muestra un cuadro **DAFO** que resume las Debilidades, Amenazas, Fortalezas y Oportunidades de este tipo de soluciones de uso de la biometría para la contratación:

Debilidades	**Amenazas**
• Riesgos sobre la privacidad • Dependencia de los dispositivos • En el caso de contratación a distancia, desconocimiento o poco control sobre algoritmos de reconocimiento, o soluciones de IA poco maduras	• Riesgo de brecha digital en caso de contratación a distancia • Riesgo de ciberataques • Riesgo de identificaciones fraudulentas

- Dependencia de infraestructura
- Dependencia de terceros de confianza
- En el caso de firma en tableta, problema sanitario por compartición de lápiz de firma

Fortalezas

- Reducción del fraude por incremento del aseguramiento de la identidad
- Menor necesidad de personal
- Mayor garantía de las evidencias recogidas
- Reducción de papel
- No repudio
- Control de la trazabilidad
- Control de ciclo de vida del dato personal

Oportunidades

- Mayor accesibilidad al público en general
- Regulación europea va en este sentido
- Modernización de la administración y de empresas
- Adaptación de regulaciones vigentes
- Accesibilidad a servicios por parte de personas vulnerables
- Automatización de procesos
- Simplificación de trámites
- Dar respuesta a nuevas necesidades
- Validez de firma por parte de la AAPP

CONCLUSIONES CASO DE USO 1

Podemos concluir que el uso de esta tecnología:

1. Facilita llegar a más público con menor esfuerzo, especialmente en la contratación de servicios. Actualmente, muchos servicios incluyen en sus procesos esta tecnología: identificación, autenticación, firma de servicios, registro de entrolamiento.

2. Es una identificación que puede darse de 1:1 o 1: N.

3. Permite la trazabilidad de punto a punto; sistema cualificado de verificación y evidencia digital.

4. En general, el producto o servicio tienen el reto de garantizar su propia seguridad en tanto que pueden darse incidentes y vulnerabilidades de ciberseguridad, especialmente en el marco de IoT.

5. En relación con la legitimación para el uso de datos personales, no requiere consentimiento previo de la persona para el uso d estas tecnologías, pero sí una información clara y específica previa a la firma. La legitimación se obtendrá con la firma del contrato.

CASO 2: VERIFICACIÓN A DISPOSITIVOS (FACIAL, AUDITIVA Y HUELLA)

La verificación de la identificación a través del reconocimiento facial la voz o de la huella está muy extendido en la actualidad.

¿Cómo funciona? Para realizar una verificación debe hacerse un patrón biométrico que podrá ser de la simetría facial, minucias de la huella o patrón de venas de la mano, o de timbre de voz,

por ejemplo, esto implica un enrolamiento previo del cliente ya que esta verificación siempre será siempre 1:1.

Estos patrones se transforman a formato digital lo que permite su uso en algoritmos de identificación o de verificación. Normalmente el uso es de uno a uno, en una video llamada, cámara inteligente, conversación con *Call Center* o *Chat Bot* o incluso ya en el propio hogar con dispositivos tipo "Alexa" o en vehículos para instrucciones vocales en llamadas o búsquedas de música, en el caso de la huella para acceso al propio smartphone, control de accesos a CPD, Tornos de acceso a salas, habitaciones de hotel, al propio ordenador, etcétera. En todos los casos exige un patrón biométrico. No se almacena el dato biométrico en claro, sino que se transforma a bits y se cifra, la verificación posterior se realiza siempre comparando cadenas cifradas o hashes. Son accesos y verificaciones modulares, ya que los usos son casi todos los que nos ocurran.

¿Que casos de uso están más extendidos?

- Uso de huella dactilar para salvaguardar la información y los sistemas de un CPD.
- Uso de la imagen facial para acceso a ordenador.
- Utilización de reconocimiento de voz para acceder a un edificio o sala específica.
- Identificar, verificar y operar con *Call Center* o *Chat Bot*, Vehículo, Domótica Alexa, etc.

A continuación, se muestra un cuadro **DAFO** que resume las Debilidades, Amenazas, Fortalezas y Oportunidades de este tipo de soluciones de reconocimiento de la identidad:

Debilidades

- Es posible que el *machine learning* pueda ser capaz de usurpar identidades.
- Dependencia del hardware. (Si se quiere incluir cualquier patrón biométrico requiere un dispositivo en cámara, lector de huellas).
- Falta de conocimiento de la población en estas tecnologías.
- Dependencia de factores físicos (luz ambiental, ruido ambiental, falta de mantenimiento del hardware)

Amenazas

- Almacenamiento de la información y en qué momento están.
- Tratamiento de datos especialmente protegidos por la normativa de protección de datos.
- Tratamiento de una gran cantidad de datos personales.
- Algoritmos o Cifrados no robustos
- Falsos Positivos y Falsos Negativos
- Usurpación con técnicas de grabación, fotos, captura de huellas, etc.

Fortalezas

- Se reduce el error en la identificación de las personas físicas.
- El Machine learning es capaz de superar el paso del tiempo; es capaz de aprender los cambios físicos.
- Comodidad y facilidad de uso

Oportunidades

- Agilidad. Se gana tiempo de procesado.
- Opción de usar distintas biometrías en el mismo proceso.
- Identificación fuerte y robusta multimodal.
- Simplificación de trámites
- Dar respuesta a nuevas necesidades
- Validez de firma por parte de la AAPP

CONCLUSIONES CASO DE USO 2

Podemos concluir que el uso de esta tecnología:

1. Son ya usadas desde hace años en accesos que requieren mayor seguridad como accesos a zonas restringidas o sensibles, también accesos a dispositivos como smartphones, portatiles, tablets, tornos, vehiculos, edificios e incluso hogares.

2. Las tecnologías de voz su uso suele ser mayoritario en call center y similares, ahora también en dispositivos tipos Alexa en el hogar y en Domótica.

3. Suelen ser tecnologías bastante testadas, fiables y probadas, si bien requieren igualmente de su análisis y tener muy en cuenta su seguridad y privacidad por diseño y defecto, así como sus tasas de falsos positivos y falsos negativos para garantizar la fiabilidad de las mismas.

4. Apoyadas por Inteligencia Artificial o Machine Learning pueden adaptarse a cambios fisiológicos, de voz e incluso de la huella.

5. Facilitan y agilizan la gestión de accesos, dando un nivel de seguridad de acceso y de identificación al usuario y a quien controle esa identificación que puede y suele ser automatizada.

6. El coste de estas son muy asequibles y hay diferentes modelos y fabricantes especializados para cada tipo de uso.

7. Es muy importante garantizar el nivel de seguridad tanto del dispositivo o componentes y software que interviene como de los datos y cifrados de los mismos para evitar ataques y suplantación.

8. Resulta necesario que antes de proceder a implantar este tipo de tecnologías se analice su adecuación a la normativa de protección de datos. Conforme al principio de proporcionalidad, principalmente, se ha de verificar si hay medidas menos intrusivas para los derechos de los interesados y si la implantación de esta medida genera más beneficios que perjuicios.

CASO 3: VIDEOIDENTIFICACIÓN FACIAL Y CONDUCTUAL CON ESPECIFICACIÓN DE USO DE INTELIGENCIA ARTIFICIAL Y MACHINE LEARNING

A través de esta tecnología, se permite la identificación y descubrimiento de personas y objetos o elementos, así como criterios de carácter conductual, con comportamientos e identificación de los mismos ya sean objetos, elementos o personas. Dicha identificación puede ser Identificación Multimodal, combinando distintas tecnologías y mecanismos, lo que la hacen más robusta y fiable, a la vez que menos suplantable. Esta identificación siempre será concebida como búsquedas 1:N contrastando las imágenes obtenidas contra registros masivos de objetos, conductas o personas.

Podemos hablar de dos tipos principales: identificación contra listas de identidad conocidas por contraste, de personas, objetos, matriculas, etc., con ellas o identificación por un método complementario usando IA (*Inteligencia Artificia) y ML (Machine Learning*) por descubrimiento de patrones de comportamiento. Hay que tener en cuenta aspectos clave en general en cada tecnología como: su facilidad de uso, coste razonable y adecuado al riesgo a proteger, su *Compliance* y su aspecto de seguridad y ciberseguridad que eviten que sea manipulable o atacada.

Hay que destacar que la identificación facial biométrica y de comportamiento puede hacerse respecto a diferentes técnicas como pueden ser: iris del ojo, retina, patrón de simetría facial, micromovimientos faciales a cámara lenta, por temperatura corporal con cámaras térmicas, por modo de andar, incluso de espaldas, etc…

A continuación, se muestra un cuadro **DAFO** que resume las Debilidades, Amenazas, Fortalezas y Oportunidades de este tipo de soluciones de identidad y verificación:

Debilidades

- Alto coste de la tecnología.
  - Que no exista fiabilidad absoluta en cuestiones que afectan a los derechos y libertades de las personas.
  - Posible rechazo por considerar pueda invadir intimidad
  - Integración de Tecnologías de IA, ML, Video, etc.

Amenazas

- Tratamiento de datos especialmente protegidos por la normativa de protección de datos.
- Puede afectar a derechos fundamentales de la ciudadanía.
- Datos expuestos a recibir ataques y especialmente protegidos.
- Necesidad de examinar principio de proporcionalidad

Fortalezas

- Posibilidad de evitar riesgos hacia las personas.
- Herramienta favorable para lucha antiterrorista y frente a hechos delictivos.

Oportunidades

- Ahorro de costes (menor personal de videovigilancia).
- Confort de control de acceso.
- Mayor control de acceso.
- Posibilidad de intervención de las autoridades.

- Se evita la suplantación de identidad. Se reduce el error humano en la identificación de las personas.
- Facilita también identificación masiva en lugares de gran afluencia como estaciones, aeropuertos, eventos, etc. Mejorando movilidad y tiempos de espera en colas.

- Posibilidad de atención rápida sanitaria
- Facultad de intervención rápida para contener Covid-19

CONCLUSIONES CASO DE USO 3

Teniendo en cuenta el DAFO y los aspectos como: Seguridad, Coste, Usabilidad, Aceptación, *Compliance*, Ciberseguridad y Privacidad, podemos concluir que el uso de esta tecnología:

- Requiere ser revisada en los aspectos de proporcionalidad de uso respecto al activo a proteger, las finalidades de interés legítimo o de negocio o de seguridad y los posibles aspectos legales, normativos y de privacidad, con el fin que no invada ningún derecho fundamental.

- Requiere de un Análisis PIA o EIPD (Evaluación de Impacto) con el fin de evaluar los posibles riesgos de uso, así como las medidas adoptadas para la protección de datos y seguridad por diseño y por defecto.

- Presenta un avance en cuanto a evitar suplantación de identidad y detección temprana de conductas o situaciones anómalas o de riesgo permitiendo una alerta temprana y posible intervención de CFS o Seguridad Privada, a más cuando se usan técnicas Multimodales combinando diferentes tecnologías y aplicando comportamiento, IA e ML, además de en otros aspectos de la seguridad incluso ciudadana o de control de accesos a eventos, lugares, etc.

- Facilita la movilidad y el tiempo, evitando procesos de identificación y accesos más complejos, lo que redunda tanto en posibles ahorros de costes como en facilidad de adopción, siempre que se garantice la privacidad.

- Dispone de capacidades de multi-identificación masiva de personas y objetos.

- Puede ser usada además para ayuda en temas de Salud (como el control de la Pandemia COVID 19 que estamos sufriendo en la actualidad)

- Como toda tecnología, puede estar expuesta a ataques de Ciberseguridad o de *Insiders* que puedan hacer un uso indebido de la información y datos, por lo que requiere ser revisada y si procede acreditada para su uso antes de su puesta en producción.

CASO 4: UTILIZACIÓN DE DATOS BIOMÉTRICOS EN TECNOLOGÍA DE VOZ EN CALL CENTERS

Los call centers son servicios telefónicos con los que las empresas buscan mantener el contacto con sus clientes o generar clientes nuevos; las empresas pueden ofrecer a través de los call centers sus servicios. También pueden brindar asistencia, encuestas de satisfacción o darse a conocer en el mercado y captar nuevos clientes.

El uso del reconocimiento vocal biométrico se puede aplicar en todos los procesos de un call center. Dicha tecnología nos permite identificar o autenticar al individuo que tenemos al otro lado de la línea, bien sea a través de telefonía tradicional o por aplicación móvil.

Cuando hablamos de biometría de voz, hablamos de una tecnología no intrusiva para el usuario. De manera que, de una forma natural, al mantener el cliente una conversación con el operador o con el IVR (respuesta de voz interactiva), recogeremos los valores de la voz intrínsecos a cada individuo, y estos podrán ser utilizados para identificar o autenticar a la persona que esta al otro lado del teléfono. Así se facilita el proceso automático o al operador en la toma de decisiones.

Integrar esta tecnología en un call centers nos da la facilidad de explotar todos los posibles usos de este tipo de biometría, bien realizar el uso de la biometría vocal con una frase fija o con un texto libre.

- El uso de una frase fija en donde el usuario registrado repite la misma frase que utilizó para el enrolamiento, el nivel de precisión es máximo y la comprobación casi inmediata.

- En una conversación libre la extracción y el tratado de los datos vocales se producen en una conversación natural. En este caso se podrían aceptar registros mediante la huella vocal extraída de grabaciones previas.

La tecnología de reconocimiento aporta alta fiabilidad tanto en entornos libres de ruido como en entornos de exterior donde el ruido ambiente puede ser más acentuado; además, como ventajas respecto a otras biometrías, los datos extraídos de la voz nunca pueden reproducirse con ingeniería inversa pues se están recogiendo más de 500 valores diferentes de la voz, en comparación con otras biometrías donde los rasgos intrínsecos solo son unas pocas unidades o decenas.

Al mismo tiempo, se puede utilizar la biometría vocal para firmar documentos vía el *call center* estando estas firmas avaladas como firma electrónica avanzada (según reglamento EIDAS) por auditores y gabinetes jurídicos.

Destacamos como principales casos de uso los siguientes:

- *Calls centers* de empresas de telecomunicaciones que quiere realizar la captación de clientes con firma del contrato, mediante evidencias biométricas vocales.

- *Calls centers* de aseguradoras que quieren verificar al asegurado para realizar un proceso de cobro de pensiones vía telefónica.

- *Calls center* de empresas de fidelización con comprobación en listas de impago.

A continuación, se muestra un cuadro **DAFO** que resume las Debilidades, Amenazas, Fortalezas y Oportunidades de este tipo de soluciones de identificación:

Debilidades

- Necesidad de una infraestructura bien dimensionada.
- Posibles discrepancias en las leyes de protección de datos dependiendo de la regulación vigente.
- Sensible a un ruido ambiente muy alto en el dispositivo cliente.
- Cliente reticente a aceptar su grabación vocal.
- Se requiere de un enrolamiento previo en caso de querer hacer identificación de la persona.

Amenazas

- Tratamiento de datos característicos de la persona regulados por las leyes de protección de datos de la mayoría de los países.
- Casos de falsos positivos y falsos negativos (Como cualquier biometría).
- Todo sistema de IT está expuesto a ciberataques.
- Quien y como almacena y trata esos datos.

Fortalezas

- Sistemas anti *spoofing* para evitar usurpación mediante grabaciones predefinidas.
- Reducción de suplantación de identidad.
- Los algoritmos aprenden al paso del tiempo los cambios de la voz.
- Se utilizan patrones biométricos que incrementan su efectividad al incluir más huellas vocales de la misma persona.
- Biometría poco intrusiva en su uso
- Solo necesitamos un dispositivo con micrófono para su uso

Oportunidades

- Ayuda a operadores en caso de transacciones con cobro de comisiones.
- Reducción de los índices de fraude.
- Posibilidad de consultar listas negras/listas blancas
- Posibilidad de utilizar la misma llamada para la firma del documento utilizando esa misma biometría de voz.
- Doble factor de autenticación en una sola acción: reconocimiento de biometría vocal y reconocimiento de caracteres de contraseña

CONCLUSIONES CASO DE USO 4

Podemos concluir que el uso de esta tecnología:

- El uso de biometrías en *call centers* nos sirve para autenticar, identificar o realizar el proceso de firma facilitando la contratación punto a punto de una manera natural.
- El uso de la biometría combinado con otras tecnologías (ML, IA) ayuda a evitar el fraude como principal fuerte, bien mediante listas de contraste o por estudios conductuales.
- La biometría vocal no está regulada en cuanto a normas ISO de estandarización.
- El estudio de la integración de esta tecnología ajustada a la regulación en contrataciones está en marcha y aporta plena eficacia jurídica.

CONCLUSIONES GENERALES

Actualmente, el crecimiento de las tecnologías biométricas resulta exponencial. Las soluciones que utilizan patrones biométricos se utilizan ya en todo tipo de sectores, e incluso han llegado a nuestras casas. Una vez analizados distintos casos de uso, alcanzamos las siguientes conclusiones:

- El uso de datos biométricos y, en particular, el reconocimiento facial puede conllevar grandes riesgos para la privacidad de los ciudadanos. Por ello es fundamental que la utilización de estas tecnologías se lleve a cabo con el debido respeto a los principios de licitud, necesidad, proporcionalidad y minimización de datos según lo establecido en el RGPD.

- Al percibirse estas tecnologías como particularmente invasivas, los responsables del tratamiento deben evaluar en primer lugar la impacto en los derechos y libertades fundamentales y considerar el uso de medios menos intrusivos para lograr una finalidad legítima en el tratamiento.

- Las soluciones tecnológicas que incorporan inteligencia artificial están expuestas a recibir ataques informáticos, por lo que es totalmente recomendable introducir las máximas garantías de seguridad.

- Desde una perspectiva global a la hora de seleccionar aquella tecnología de identificación y/o autenticación biométrica, se debería ponderar entre aquellas que presenten una combinación más eficiente técnico-operativa y con menor riesgo para la privacidad de los usuarios, minimizando los datos tratados y aplicando las medidas técnicas por diseño y defecto que garanticen su seguridad.

En definitiva, es un conjunto de tecnologías que han venido para quedarse y hacernos la vida más sencilla y segura, pero requiere ser previamente analizada y usarla de forma correcta, proporcional y adecuada a cada finalidad y uso, garantizando el respeto a los fundamentales y la adecuada protección de los riesgos que sobre la seguridad puedan existir.