Asociación Española de Compliance

Grupos de trabajo de ASCOM

Protección de datos y nuevas tecnologías

Sistema de identificación biométrica. Aspectos a tener en cuenta desde la perspectiva del Compliance Officer para su implantación

Septiembre 2023

www.asociacioncompliance.com

Sistema de identificación biométrica.

Aspectos a tener en cuenta desde la perspectiva del Compliance Officer para su implantación.

ÍNDICE DE CONTENIDOS

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

I. Introduccion

Los sistemas de identificación biométrica son herramientas que **se utilizan para verificar la identidad de una persona utilizando características físicas únicas,** como la huella dactilar, el iris, la voz o el rostro. Estos sistemas se basan en la premisa de que cada persona tiene características físicas únicas que se pueden utilizar para identificarla de manera confiable.

Los sistemas de identificación biométrica **se utilizan en una amplia variedad de aplicaciones,** desde el acceso a edificios y áreas restringidas de alta seguridad hasta la verificación de identidad en transacciones financieras y la emisión de pasaportes y certificados de nacimiento. Del mismo modo, estos ofrecen una forma más rápida, precisa y segura de autenticación que los métodos tradicionales basados en contraseñas y tarjetas de acceso.

Algunos ejemplos de sistemas de identificación biométrica son los lectores de huellas dactilares, los escáneres de iris, los sistemas de reconocimiento facial y los sistemas de reconocimiento de voz. Estos sistemas **utilizan algoritmos y tecnologías avanzadas** para capturar y analizar las características biométricas de una persona y compararlas con los datos almacenados previamente en una base de datos para verificar su identidad.

Como Compliance Officer, debemos asegurarnos de que cualquier sistema de identificación biométrica que se implemente **cumpla con los estándares éticos y legales**, y que se implement en **medidas adecuadas de seguridad y privacidad** para proteger los datos biométricos de las personas. Además, debemos estar preparados para **evaluar** y **monitorizar** del sistema para asegurar de que el sistema sigue siendo **efectivo** y **cumple con las políticas y normativas pertinentes**.

II. Identificación y autenticación

II.I . Concepto

La identificación y autenticación biométrica es un **método de verificación de identidad** que utiliza *características únicas y medibles del cuerpo humano* para confirmar la identidad de una persona. Estas características pueden incluir rasgos físicos como huellas dactilares, iris, retina, geometría de la cara, voz, firma y ADN.

La identificación biométrica se refiere al *proceso de verificar la identidad* de una persona mediante el análisis y comparación de sus características biométricas con las que están almacenadas en una base de datos (mediante un proceso de búsqueda de correspondencias **uno-a-varios**). Por ejemplo, un sistema de identificación biométrica podría verificar la identidad de una persona escaneando su huella dactilar y comparándola con una base de datos de huellas dactilares previamente registradas.

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

Por otro lado, **la autenticación biométrica** se refiere al *proceso de confirmar la identidad* de una persona mediante la comparación de sus características biométricas con las que están almacenadas en una base de datos y asegurándose de que sea la misma persona que se registró previamente (proceso de búsqueda de correspondencias **uno-a-uno)**. La autenticación biométrica se utiliza comúnmente en dispositivos electrónicos, como teléfonos móviles y ordenadores portátiles, para desbloquearlos mediante la lectura de huellas dactilares o reconocimiento facial.

Ambas se consideran una forma muy precisa y segura de verificar la identidad de una persona, ya que las características biométricas son únicas e imposibles de falsificar. Sin embargo, es importante tener en cuenta la privacidad y protección de los datos biométricos de las personas, y asegurarse de cumplir con las regulaciones y leyes aplicables en cada país o región.

II.II. Características

Las características de la identificación y autenticación biométrica incluyen:

1. **Unicidad:** cada persona tiene características biométricas únicas que son diferentes de las de cualquier otra persona, lo que las hace una herramienta efectiva para la identificación y autenticación.
2. **Permanencia:** las características biométricas no cambian con el tiempo, por lo que son una forma de identificación y autenticación confiable a largo plazo.
3. **Universalidad:** la mayoría de las personas tienen características biométricas, lo que las hace una herramienta de identificación y autenticación accesible para una amplia gama de personas.
4. **Medible y cuantificable**: las características biométricas se pueden medir y cuantificar con precisión, lo que las hace una herramienta precisa para la identificación y autenticación.

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

5. **Conveniencia:** los sistemas de identificación y autenticación biométricos son convenientes para los usuarios, ya que no requieren el uso de contraseñas o tarjetas de identificación físicas.
6. **Seguridad:** la identificación y autenticación biométrica son altamente seguras, ya que las características biométricas son difíciles de falsificar o copiar.
7. **Rapidez:** los sistemas de identificación y autenticación biométricos pueden ser rápidos y eficientes, lo que los hace útiles en situaciones en las que se requiere una identificación rápida.

En resumen, la identificación y autenticación biométrica ofrecen una serie de ventajas sobre otros métodos de identificación, incluyendo su precisión, seguridad y conveniencia para los usuarios.

II.III. Regulación

A nivel nacional, la regulación de la identificación y autenticación biométrica se rige por varias leyes y regulaciones, entre las que se encuentran:

1. El Reglamento General de Protección de Datos (RGPD) que establece las reglas para la protección de datos personales, incluyendo los datos biométricos, en España.
2. Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD) que regula la protección de datos personales y garantiza los derechos digitales de los ciudadanos, incluyendo el derecho a la protección de los datos biométricos.
3. Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI) que establece reglas claras para la protección de datos personales en el ámbito digital, incluyendo los datos biométricos.
4. Ley de Enjuiciamiento Criminal (LECrim.)que establece las condiciones en las que se pueden utilizar los sistemas de identificación y autenticación biométrica en el ámbito de la justicia penal.

Además de las antes mencionadas, en España también existen otras normativas específicas para la identificación y autenticación biométrica, como el **Real Decreto 3/2010**, que regula el uso de sistemas de identificación biométrica en el ámbito laboral, que más adelante desarrollaremos.

La regulación de la identificación y autenticación biométrica varía según el país o región en la que se utilice. En muchos países, las leyes y regulaciones que protegen la privacidad y seguridad de los datos personales también se aplican a los datos biométricos. A continuación, se mencionan algunas de las regulaciones más importantes a nivel internacional:

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

1. Ley de privacidad de información personal (PIPA): esta es una ley canadiense que establece reglas claras para la recopilación, uso y divulgación de datos personales, incluyendo los datos biométricos.
2. Ley de protección de datos personales (PDPA): esta es una ley de Singapur que establece principios claros para la protección de los datos personales, incluyendo los datos biométricos.
3. Ley de protección de datos personales (LGPD): esta es una ley brasileña que establece requisitos claros para el tratamiento de los datos personales, incluyendo los datos biométricos.
4. Ley de protección de datos personales (DPA): esta es una ley de la India que establece principios claros para la protección de los datos personales, incluyendo los datos biométricos.

Asimismo, existen **normas internacionales** para el tratamiento de los datos biométricos, como las especificaciones de la Organización Internacional de Normalización (**ISO**) para el almacenamiento y transmisión de datos biométricos.

Es esencial que las organizaciones que utilizan la identificación y autenticación biométrica tanto en España como otros países se aseguren de cumplir con las leyes y regulaciones aplicables, y de proteger los datos biométricos de acuerdo con los estándares de privacidad y seguridad establecidos por las autoridades competentes.

II.IV. Factores de autenticación

Los factores de autenticación son los **elementos** o **características** que se utilizan para verificar la identidad de una persona y permitir su acceso a un sistema o servicio. a continuación, se presentan los principales factores de autenticación:

1. **Factor de conocimiento**: este factor se refiere a información que solo el usuario debe conocer, como contraseñas, respuestas a preguntas de seguridad o frases de paso.

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

2. **Factor de posesión**: este factor se refiere a algo que el usuario debe tener en su poder para demostrar su identidad, como una tarjeta inteligente, un token de seguridad o un teléfono móvil.
3. **Factor biométrico**: este factor se refiere a la identificación de una persona a través de características físicas únicas, como la huella dactilar, el iris, la voz o el rostro.
4. **Factor de ubicación**: este factor se refiere a la identificación de la ubicación física del usuario a través de la dirección IP o el GPS del dispositivo utilizado.
5. **Factor temporal**: este factor se refiere a la identificación del momento temporal en que se realiza la autenticación, como la fecha y hora de acceso.

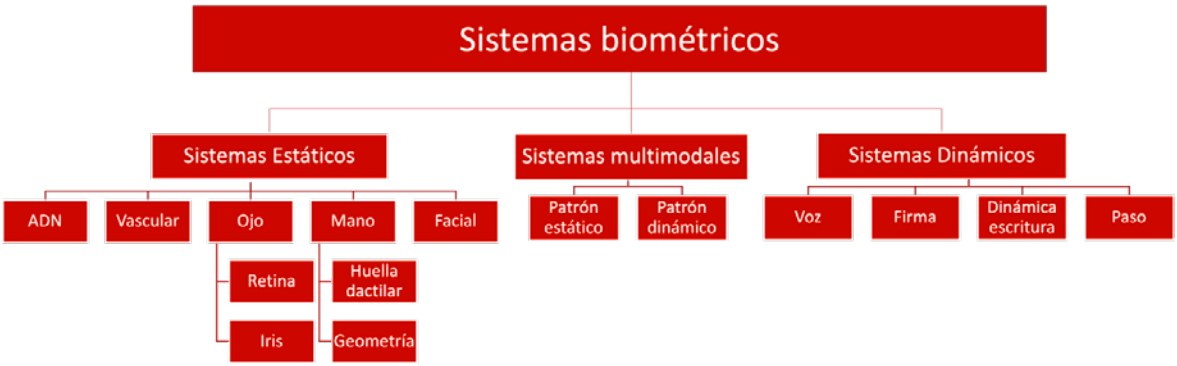
Cuando se combinan dos o más factores de autenticación se conoce como **autenticación multifactorial**, lo que aumenta la seguridad y reduce el riesgo de acceso no autorizado a sistemas y servicios.

III. Sistemas de identificacion biométrica

III.I. Tipos de identificación biométrica

Existen los siguientes tipos de identificación biométrica:

1. La **biometría estática** (o física), que es la medición de las características anatómicas de las personas que permanecen inalterables en el tiempo como huellas dactilares, gestos faciales y geometría.
2. La **biometría dinámica**, que es la medición de las características del comportamiento de las personas, capturadas durante la actividad de un individuo, como la voz, firma, etc.
3. La **biometría multimodal**, que combina dos o más tipos de identificación biométrica, como, por ejemplo, el reconocimiento facial y de voz.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

III.II. Funcionamiento de los sistemas de identificación y autenticación biométrica

Se debe tener en cuenta que los sistemas de identificación y autenticación biométrica pueden variar en relación con las tecnologías y algoritmos utilizados, pero de manera general, la **captura**, **procesamiento**, **almacenamiento**, **comparación**, **verificación/autenticación** y **acción** de características biométricas es común al funcionamiento de la mayoría de dichos sistemas.

1. **Captura**: el primer paso del proceso de consiste en la recopilación de los datos de una muestra biométrica del individuo (huella, cara, etc.).
2. **Procesamiento**: posteriormente, la muestra se procesa para extraer las características distintivas que se reflejan en una plantilla que resume la información única de los rasos biométricos del individuo para ser comparados con los de los otros individuos en el caso de la identificación, o ser confirmados, en el caso de la autenticación.
3. **Almacenamiento**: la plantilla biométrica se almacena en una base de datos para posterior identificación o autenticación dependiendo del sistema utilizado.
4. **Comparación**: cuando se necesita identificar o confirmar la identidad de un individuo, se recoge una nueva muestra de las características a través de una plantilla y se compara con las plantillas almacenadas en la base de datos.
5. **Identificación** o **autenticación**: según la finalidad, en la identificación biométrica, se busca la coincidencia de la plantilla en toda la base de datos para determinar la identidad del individuo, como puede ser el caso de la identificación de un individuo por los cuerpos de seguridad; por mientras que en la autenticación se compara la plantilla creada con la plantilla asociada previamente al individuo que reclama la identidad, como puede ser el caso del acceso mediante reconocimiento facial a un smartphone.

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

6. **Resultado** o **acción**: como paso final y siempre que haya una coincidencia, la solución emite una acción específica como, por ejemplo, verificar la identidad del individuo, en el caso de identificación; u otorgar acceso, en el caso de autenticación.

IV. Obligaciones de cumplimiento normativo a tener en cuenta en la implantación y uso de sistemas de identificación biométrica

IV.I. Obligaciones en materia de protección de datos personales

Con la entrada en aplicación del RGPD, se dota de una definición específica al concepto de "dato biométrico". Concretamente el artículo 4.14 RGPD, define esta tipología de dato del siguiente modo: "**datos personales obtenidos a partir de un tratamiento técnico específico,** relativos a las características físicas, fisiológicas o conductuales de una persona física **que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos**".

En este sentido, el Considerando 51 del RGPD, a su vez realiza una especificación limitando el concepto de tratamiento de datos biométricos a aquellos que se realicen exclusivamente a través de medios técnicos específicos de biometría. Adicionalmente, advierte de la especial protección que merece esta tipología de datos, debido a su sensibilidad y naturaleza:

"Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, entendiéndose que el uso del término "origen racial" en el presente Reglamento no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas. **El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física**. Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento (…)".

Dicho lo anterior, el tratamiento de datos biométricos queda amparado bajo las disposiciones recogidas el RGPD y resto de normativa aplicable como dato de carácter personal.

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

A diferencia de lo dispuesto en el RGPD, la LOPD no contiene ninguna mención específica o previsión en relación con el tratamiento de datos biométricos.

IV.II. El uso de inteligencia artificial en los sistemas de identificación biométrica: Prácticas prohibidas

Es innegable que el uso de **inteligencia artificial** (IA) en los sistemas de identificación/autenticación biométrica ha **revolucionado** la forma en la que se **verifica o confirma la identidad del individuo**. La IA supone una herramienta clave para mejorar estos el uso de estos sistemas, así como la seguridad y eficacia de estos. Sin embargo, es también importante abordar los desafíos éticos y de privacidad que pueden surgir con el uso de estos sistemas para garantizare que se apliquen manera responsable y transparente, respetando en todo momento los derechos y libertades de los individuos.

En este sentido, la **Propuesta de Reglamento de Inteligencia Artificial**[1] garantizando la tutela de los derechos fundamentales de los individuos frente a los riesgos que conlleva el uso de los sistemas basados en IA, establece un enfoque basado en el riesgo clasificando el tratamiento como riesgo bajo, medio o alto, así como **prohibiendo** totalmente **ciertos usos** de la inteligencia artificial en el tratamiento de datos.

En la propuesta de reglamento de IA, los usos prohibidos quedan resumidos en:

1. Técnicas subliminales manipuladoras perjudiciales que exploten a grupos vulnerables específicos (discapacidad o mental).
2. Usos por las autoridades públicas, o en su nombre, con fines de puntuación social.
3. Utilización de datos biométricos a distancia “en tiempo real” en espacios de acceso público para la aplicación de la ley, excepto en un número limitado de casos.

1. EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu)

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

Estas prohibiciones han sido ampliadas por la **orientación general establecida el Consejo Europeo** el 6 de diciembre de 2022[2], incluyendo: *"a los agentes privados la prohibición de utilizar la IA con fines de **puntuación ciudadana**."*

Además, la disposición por la que se prohíbe el uso de sistemas de IA que explotan las vulnerabilidades de grupos específicos de personas ahora incluye también a las personas vulnerables por su situación social o económica.

Por lo que respecta a la prohibición relativa al uso de sistemas de identificación biométrica remota "en tiempo real" en espacios de acceso público por parte de las autoridades encargadas de la aplicación de la ley, el texto aclara los objetivos para cuya consecución dicho uso es estrictamente necesario con fines de aplicación de la ley y a qué autoridades encargadas de la aplicación de la ley se les debe, por tanto, permitir excepcionalmente el uso de dichos sistemas."

A posteriori, en junio de 2023, el Parlamento Europeo[3] adoptó su posición negociadora sobre la ley de Inteligencia Artificial, ampliando la lista propuesta por la Comisión Europea como sigue:

- los sistemas de identificación biométrica remota, en tiempo real, en espacios públicos;
- los sistemas de **identificación biométrica remota, a posteriori**, con la única excepción de usos policiales en investigaciones por delitos graves y con autorización judicial;
- los sistemas de **categorización biométrica** que utilicen ciertas características identitarias (por ejemplo el género, la raza, la etnia, el estatus de ciudadanía, la religión o la orientación política);
- los sistemas policiales predictivos (basados en la elaboración de perfiles, la ubicación o el historial delictivo);
- los sistemas de **reconocimiento de emociones** por las fuerzas de seguridad, en la gestión de fronteras, los lugares de trabajo o las instituciones de enseñanza; y
- el rastreo indiscriminado de imágenes faciales sacadas de Internet o de circuitos cerrados de televisión para crear bases de datos de **reconocimiento facial** (que violan los derechos humanos y el derecho a la intimidad)."

Como podemos observar, desde la publicación del reglamento de IA, se ha pasado de la prohibición del uso de sistemas inteligencia artificial que traten

2. Reglamento de Inteligencia Artificial: el Consejo pide que se promueva una IA segura que respete los derechos fundamentales - Consilium (europa.eu)
3. La Eurocámara, lista para negociar la primera ley sobre inteligencia artificial | Noticias | Parlamento Europeo (europa.eu)

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

datos biométricos en tiempo real, a la extensión de prohibición propuesta por los eurodiputados sobre las prácticas que conlleven el uso de datos biométricos en la "***identificación biométrica remota, en tiempo real"; "identificación biométrica remota, a posteriori", "categorización biométrica", "reconocimiento de emociones" y "reconocimiento facial".*** Resulta pues evidente el grado de preocupación por parte de las Autoridades cuando los datos biométricos son utilizados por sistemas o prácticas de IA, defendiendo que la futura normativa de inteligencia artificial "se ajuste plenamente a los derechos de los individuos, respetando la supervisión humana, la seguridad, la privacidad, la transparencia, la no discriminación o el bienestar social y medioambiental."

IV.III. Biometría como categoría especial de datos personales

A partir del concepto de dato biométrico, el artículo 9 del RGPD regula las condiciones para llevar a cabo el tratamiento de categorías especiales de datos personales. En este sentido, y como ya adelantaba el anteriormente mencionado Considerando 51 del RGPD, el artículo 9.1 prohíbe por defecto el tratamiento de datos considerados como especiales en los siguientes términos:

"**Quedan prohibidos el tratamiento de** datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, **datos biométricos dirigidos a identificar de manera unívoca a una persona física**, datos relativos a la salud o datos relativos a la vida o la orientación sexuales de una persona física".

No obstante, el artículo 9.2 del RGPD matiza esta prohibición general indicada en el artículo 9.1 y, de manera excepcional, permite el tratamiento de las categorías especiales de datos siempre que ocurran determinadas circunstancias, tales como:

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

"El **apartado 1 no será de aplicación** cuando concurra una de las circunstancias siguientes:

a. el interesado dio su **consentimiento explícito** para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b. el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado"

Interpretando estos preceptos, el RGPD establece que no todos los datos biométricos, sino los "**dirigidos a identificar de manera unívoca a una persona física**" deben catalogarse como una categoría especial de datos al amparo del artículo 9 del RGPD.

Por tanto, no siempre que haya un tratamiento de datos biométricos procede aplicar la prohibición estipulada en el artículo 9.1 RGPD, únicamente cuando el tratamiento esté dirigido a identificar de manera unívoca a una persona física.

No obstante, la definición que otorga el RGPD sobre el concepto de "dato biométrico" ha sido objeto de interpretación por parte de la AEPD, que ha llegado a considerar que sólo hay tratamiento de datos biométricos en el momento en que se empleen medios técnicos dirigidos a la identificación biométrica de los individuos.

La AEPD comenzó a pronunciarse sobre el tratamiento de datos biométricos como categoría especial de datos en el año 2020. Desde entonces, el argumento que adoptó para determinar si un dato biométrico era de categoría especial, fue el tenor literal del artículo 9.1 del RGPD, que prevé que los *"datos biométricos [estén] dirigidos a identificar de manera unívoca a una persona física".*

No obstante, el criterio de la AEPD ha evolucionado y parece experimentar importantes cambios en los últimos años. La interpretación de la AEPD sobre el tratamiento de los datos biométricos en 2020 era que, en caso de emplear técnicas o procesas dirigidos a la identificación biométrica se consideran datos de categoría especial, quedando así sujetos al régimen del artículo 9 RGPD. No obstante, en caso de emplear otras técnicas -como puede ser la autenticación biométrica- no se consideran datos de categoría especial y, por tanto, no sería de aplicación el mencionado artículo 9 RGPD.

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

Sin embargo, en el año 2022 hubo un cambio de paradigma por parte de la AEPD a raíz de la publicación de unas Directrices del Comité Europeo de Protección de Datos (CEPD) - Directrices 05/2022 del CEPD de 12 de mayo de 2022, sobre el uso de técnicas de reconocimiento facial, que otorgan mayor claridad sobre la interpretación de los tratamientos de la huella dactilar como dato biométrico especial, y que se alejaba claramente de la diferenciación que hacía la AEPD, sobre autenticación e identificación.

IV.III.I. Base legitimadora del tratamiento

Uno de los principales objetivos del RGPD es la adecuación de los tratamientos al régimen de protección de datos europeo. Las tecnologías empleadas en el tratamiento de datos biométricos no son una excepción, debiendo ser utilizadas para fines determinados, explícitos y legítimos.

Cuando se utilicen estas tecnologías, los artículos 6 y 9 del RGPD establecen los criterios que deben cumplirse para que el tratamiento sea lícito. En el caso de que el consentimiento sea necesario, el artículo 7 del RGPD establece las condiciones para su validez. Por otro lado, el artículo 8 del RGPD establece otros requisitos cuando se recurre al consentimiento para tratar datos de menores de edad.

Concretamente, en el artículo 6.1 del RGPD se describen las bases jurídicas que legitiman el tratamiento de datos personales en general, incluidas las categorías especiales de datos, como los tratamientos de datos biométricos dirigidos a identificar de manera unívoca a una persona física.

Sin perjuicio de lo anterior, el punto de partida general del artículo 9 del RGPD es que el tratamiento de estas categorías especiales de datos está prohibido. No obstante, existen varias excepciones a esta prohibición contempladas en el apartado segundo de dicho artículo.

En consecuencia, aunque exista una base jurídica que legitime el tratamiento de datos biométricos al amparo

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

del artículo 6.1 del RGPD, será necesaria la concurrencia de una de las causas del artículo 9.2 del RGPD, que levantan la prohibición del tratamiento de categorías especiales de datos. Esta es la postura manifestada por distintas autoridades de control en numerosas resoluciones y pronunciamientos (por ejemplo, la AEPD en su Informe Jurídico N/REF 0047/2021).

Si un tratamiento no cumple con ambos requisitos, es decir, no dispone de una base jurídica del artículo 6.1 del RGPD y no puede beneficiarse de una de las excepciones por las que pueden tratarse categorías especiales de datos, entonces no será posible llevar a cabo el tratamiento de datos biométricos para la identificación de interesados.

Con carácter general, para el tratamiento de datos biométricos considerados como una categoría especial de datos, las principales excepciones aplicables para salvar la prohibición expresan de su uso serán el consentimiento explícito, la normativa en el ámbito laboral y el interés público. Así se desprende de las distintas guías y directrices de las autoridades de control (por ejemplo, la guía para la protección de datos en las relaciones laborales de la AEPD o las Directrices 05/2022 del CEPD, sobre el uso de tecnologías de reconocimiento facial). No obstante, no se ha de descartar la aplicación de las restantes excepciones del artículo 9.2 del RGPD para otros casos concretos.

Adicionalmente, debido al mayor nivel de protección concedido a las categorías especiales de datos, el responsable del tratamiento deberá prestar especial atención a garantizar que se cumplen también las demás obligaciones de la normativa de protección de datos.

IV.III.II. Información previa asociada al tratamiento

Teniendo en cuenta que la interpretación del CEPD sobre los datos biométricos supone el tratamiento de una categoría especial de datos personales, dicho tratamiento está sujeto a algunos requisitos adicionales. Concretamente, tanto el RGPD, como las autoridades de control, exigen a las organizaciones que traten esta categoría de datos a proporcionar a los interesados información previa y específica sobre el tratamiento de sus datos biométricos antes de su recogida y uso.

La **información previa** que debe facilitarse según el RGPD puede encontrarse en sus artículos 13 y 14, entre los que se incluyen los siguientes aspectos:

1. Los fines para los que se utilizarán los datos biométricos (por ejemplo, la identificación de personas, el control de acceso a una instalación o la prevención del fraude);
2. Los tipos de datos biométricos que se recogerán (por ejemplo, huellas dactilares o datos de reconocimiento facial);

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

3. Cómo se almacenarán y protegerán los datos biométricos;
4. Quién tendrá acceso a los datos biométricos;
5. Cuánto tiempo se conservarán los datos biométricos;
6. Los derechos de los interesados a acceder a sus datos biométricos, rectificarlos o suprimirlos, entre otros;
7. Cualquier otra información necesaria para garantizar la protección de los interesados.

La información previa debe facilitarse de forma clara y concisa, de manera que resulte fácil de comprender para los interesados. También debe facilitarse en una lengua que los interesados puedan entender. Esta información puede darse de varias maneras, por ejemplo, a través de una política de privacidad, de formularios web, de una aplicación móvil, o de cualquier otro medio adecuado a las circunstancias. Algunas buenas prácticas y consejos adicionales para proporcionar la información previa consisten en:

1. Utilizar un lenguaje sencillo, evitando jerga técnica o acrónimos;
2. Ser específico y transparente, la información previa debe ser precisa y honesta;
3. Facilitar que la información se encuentre disponible en diversos formatos e idiomas.

Es importante señalar que la información previa debe facilitarse antes de recoger o utilizar los datos biométricos. Salvo que exista alguna excepción, las organizaciones no pueden recoger o utilizar datos biométricos sin proporcionar primero a los interesados esta información previa.

En España, la AEPD ha publicado algunos informes jurídicos respecto al tratamiento de datos biométricos que aportan información adicional sobre cómo las organizaciones deben cumplir con su deber de información a los interesados. Por ejemplo, en el Informe Jurídico N/REF 010308/2019 y en el Informe

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

Jurídico N/REF 0036/2020, la AEPD se pronuncia sobre la información que debe proporcionarse cuando se empleen sistemas de reconocimiento facial en los servicios de videovigilancia proporcionados por empresas seguridad privada y en exámenes, respectivamente.

IV.III.III. Idoneidad y proporcionalidad del tratamiento

Una de las principales preocupaciones en relación con el tratamiento de datos biométricos es que puedan utilizarse sin el conocimiento o consentimiento de los interesados. Esto se debe a que los datos biométricos son muy difíciles o imposibles de modificar, por lo que su control y seguridad debe ser una prioridad.

En consecuencia, la idoneidad y proporcionalidad del tratamiento de datos biométricos debe considerarse cuidadosamente. En algunos casos, los beneficios del tratamiento de esta categoría de datos pueden ser superiores a los problemas de privacidad. Por ejemplo, el uso de datos biométricos para prevenir el terrorismo u otros delitos graves puede estar justificado. Sin embargo, en otros casos, los problemas de privacidad pueden superar a los beneficios. Por ejemplo, el uso de datos biométricos para seguir los movimientos de los empleados puede resultar desproporcionado.

Hay una serie de medidas que pueden adoptarse para garantizar que el tratamiento de datos biométricos sea idóneo y proporcional. En primer lugar, las organizaciones deben contar con políticas y normas internas claras que rijan la recogida, el uso y la conservación de los datos biométricos.

Estas políticas y normas deben estar diseñadas para proteger la privacidad de los interesados y garantizar que los datos biométricos sólo se utilizan para fines legítimos. En segundo lugar, las organizaciones deben obtener el consentimiento de los interesados (o disponer de otra base jurídica aplicable) antes de recoger o utilizar sus datos biométricos. En tercer lugar, las organizaciones deben tomar medidas para proteger los datos biométricos del acceso, uso o divulgación no autorizados.

El tratamiento de datos biométricos es una cuestión compleja que plantea diversos problemas de privacidad. Sin embargo, si se toman medidas para garantizar que el tratamiento de los datos biométricos sea idóneo y proporcional, las organizaciones pueden ayudar a proteger la privacidad de los interesados y, al mismo tiempo, aprovechar las ventajas de las tecnologías que hagan uso de estos datos.

En sus Directrices 3/2019, sobre el tratamiento de datos personales mediante dispositivos de vídeo, el CEPD también proporciona algunas orientaciones sobre el tratamiento de datos biométricos. Estas directrices sugieren una serie de medidas que las organizaciones pueden cumplir para garantizar que su tratamiento de datos biométricos sea lícito y justo.

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

Además de lo anterior, existen otros aspectos que deben tenerse en cuenta a la hora de evaluar la idoneidad y proporcionalidad del tratamiento de datos biométricos como la naturaleza de los datos recogidos, la finalidad de la recogida de datos (si los datos se recogen con un fin legítimo, como la prevención de delitos, su uso puede estar más justificado que si se recogen con un fin menos relevante, como el marketing), o el impacto sobre los interesados.

La decisión de tratar o no datos biométricos es compleja y debe tomarse caso por caso. A continuación, se ofrecen algunas preguntas que se pueden realizar para evaluar la idoneidad y proporcionalidad de los tratamientos de datos biométricos:

A) Idoneidad:

1. ¿Los datos se recogen con un fin legítimo?
2. ¿Los datos son necesarios para lograr el fin para el que se recogen?
3. ¿Los datos se recogen de manera justa y transparente?
4. ¿El interesado ha prestado su consentimiento previo a la recogida de los datos?

B) Proporcionalidad:

1. ¿Los beneficios del tratamiento superan los perjuicios para los interesados?
2. ¿Los datos se recogen por el medio menos intrusivo para lograr el fin propuesto?
3. ¿Los datos se almacenan de forma segura?
4. ¿Los datos se destruyen de forma adecuada cuando ya no son necesarios?

IV.IV. Supuestos de hecho/pronunciamientos de las autoridades de control europeas

IV.IV.I. Acceso y control laboral

La aplicación de la biometría en el entorno laboral cuenta ya con un largo recorrido. El avance de estas

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

tecnologías ha atraído a numerosos empleadores a la hora de contemplar su utilidad para el control laboral y la adopción de medidas de seguridad tales como el control de acceso y situaciones similares en las que el uso de este tipo de dato personal es considerado como un recurso reforzado a la hora de proteger los activos empresariales y su empleo.

La particularidad de este tipo de datos basados en procesar rasgos físicos, conductuales o fisiológicos es que pueden facilitar la identificación inherente del interesado del que se recogen datos. Esta acción puede realizarse incluso sin la consciencia del propio individuo, lo cual dota de mayor riesgo cualquier acción encaminada al tratamiento de este tipo de datos.

Igualmente, implica una serie de dificultades y su efectividad no es plena, siendo refutada en supuestos en las que personas de un mismo núcleo familiar comparten parte de esa información, pudiendo hacer inefectivo el patrón biométrico usado. Asimismo, su aplicación conlleva una serie de dificultades en casos en los que los interesados estén imposibilitados por motivos de salud pudiendo afectar al funcionamiento o efectividad del recurso, haciendo necesario un sistema alternativo para poder aplicarse a estas personas.

A la hora de determinar las **medidas de seguridad** necesarias para los supuestos en los que se emplee el tratamiento de datos personales en la relación laboral, se debe partir de la necesidad de conocer el contexto en el que se lleva a cabo, dado que va a marcar el planteamiento a realizar por el empleador como responsable del tratamiento de datos.

De inicio, confluyen derechos y obligaciones de ambas partes con un encaje aparentemente complejo. En primer lugar, se parte de la delgada línea que fija el uso de esta tipología de datos con fines que pueden confundirse, como son la **identificación** y la **autenticación** de los interesados. Dicha diferenciación radica, en esencia, en el tipo de **verificación** que se hace de los **datos**, conllevando la primera **una coincidencia unívoca (uno-a-varios); frente a la segunda, en la que la misma se realiza de uno-a-uno**. La primera, que en este ámbito a priori resulta desproporcionada por lo general, implica de forma irrechazable la categorización como dato de especial categoría, llevando a contar con unas exigencias reforzadas para dicho tratamiento.

En la práctica, sería más complicado justificar la necesidad para su tratamiento a la vista del artículo 9 RGPD, cuestión que llegó a confirmar la AEPD en su Informe 2009-324 indicando que *los datos biométricos permiten la identificación de una persona, haciendo imposible la coincidencia de tales aspectos en dos individuos*.

Respecto a las obligaciones inherentes a la relación laboral, el empleador se encuentra sometido a la relativa al control laboral efectivo. Para ello, el único límite

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

legal que se encuentra es el fijado por el Estatuto de los Trabajadores y la discrecionalidad que otorga a la hora de seleccionar las medidas llevadas a cabo para realizar el control laboral en su artículo 20.3.

En este sentido, esta obligación legal no escapa al riesgo potencial del uso de esos datos personales pudiendo implicar la afectación a derechos fundamentales como la intimidad. La percepción de intrusión e impacto que puede tener debería justificarse, de forma sólida, con los rasgos esenciales del **tratamiento** como son la **finalidad** de este, su **necesidad** y la **proporcionalidad** de esta decisión. Respecto a estos atributos, dependerá mucho de la técnica empleada en el tratamiento, la cual deberá ser analizada previamente para asegurarse de cuál es el flujo completo de datos y que no implica un riesgo para los derechos y libertades de los empleados.

De inicio, se debe tener presente en todo momento y desde el inicio las exigencias planteadas por la Recomendación 2015 del Consejo de Europa en su apartado 5 estableciendo que su recogida y tratamiento únicamente tiene cabida cuando sean necesarios para proteger los intereses legítimos de los trabajadores, empresarios o terceros, poniendo como premisa que no haya alternativa posible de emplear otro tipo de técnica. Además, llegado el caso, igualmente debe estar alineado con las exigencias de seguridad y considerar la proporcionalidad necesaria. En conclusión, dicha definición establece un marco muy restringido en el que cabría la adopción de este tipo de tratamiento de datos.

Si dicha obligación legal no tiene fundamento, la única base legitimadora para ese potencial tratamiento sería el interés legítimo del empleador. Y para ello, la clave será el poder determinar que dicho interés viene soportado por una verdadera necesidad, tal y como lo ha corroborado la AEPD.

En consecuencia, una primera medida a adoptar debería incluir la realización del potencial responsable de **Evaluación del Interés Legítimo (LIA)** que permita confirmar dicho rasgo en base a la necesidad y que el

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

mismo es proporcional teniendo en cuenta las circunstancias específicas del caso, y que dicho interés no colisiona con los derechos y libertades de los empleados, y que la decisión es equilibrada en base a estas premisas.

El **LIA** debería formar parte de una **Evaluación de Impacto** detallada en la que se analicen y reflejen todas las circunstancias atenientes al ciclo completo del dato, desde su recogida, partiendo de la necesidad y proporcionalidad de la decisión; el acceso por parte de los perfiles claramente definidos y debidamente justificados; su uso para la acción de autenticación en cualquier sistema de acceso o control laboral; su conservación en un repositorio adecuadamente protegido; su posible acceso y comunicación a terceros que proporcionen algún tipo de servicio vinculado (software de lectura de datos, repositorio de los datos biométricos, etc.); hasta su eliminación, en los casos en los que el empleado cese la relación laboral, debiendo comprobarse que la supresión es efectiva y no hay posibilidades de recuperación de esa información.

Esta adopción de un sistema biométrico debe tener presente en todo momento una justificación sólida partiendo de la base de la necesidad comentada; y, en ese supuesto, que se siga respetando la minimización y limitación de los datos, de forma que los datos efectivamente recogidos sean adecuados, pertinentes y los mínimos imprescindibles para los fines buscados, evitando tratamientos desproporcionados resultando intrusivo y carente de justificación.

Además, será conveniente seguir el **principio de minimización** establecido en la normativa vinculante, llevando a cabo el tratamiento empleando el volumen y tipos de datos exclusivamente necesarios. Así, no se debe olvidar que no debe resultar intrusivo, tal y como establecía el Grupo del Artículo 29 en su Dictamen 2/2017 acerca de los tratamientos de datos en los entornos laborales.

En el supuesto que finalmente se decida realizar el tratamiento de datos biométricos resulta imperante elaborar y poner a disposición de los interesados la **información**, de manera previa, acerca del tratamiento, indicando en qué consiste, la finalidad y todas aquellas cuestiones requeridas por el artículo 13 del RGPD. Particular importancia ostenta la finalidad como comentamos, dado que únicamente cabrá confirmar si finalmente se soporta mediante una obligación legal o se motiva a través del interés legítimo, recordando que el consentimiento no cabe en estos casos dada la relación contractual entre los intervinientes.

A nivel de derechos, también se deberán adoptar las medidas oportunas para contemplar que el empleador está preparado para **gestionar** las posibles **solicitudes de derecho** de oposición invocadas por los interesados, debiendo tramitarlas y adoptar las resoluciones pertinentes de acuerdo a lo establecido en la normativa vigente en los plazos de tiempo establecidos.

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

Otro tipo de **medidas de seguridad** a implantar serían aquellas de índole **técnico**, las cuáles podríamos disgregar en diferentes aspectos.

Por un lado, conviene adoptar las medidas que conlleven **proteger el patrón biométrico** empleado (Ej. *Hash*, *biohash*) destinadas a evitar su reversibilidad y que permitan el acceso e identificación de los interesados. Así, debe evitarse este riesgo y garantizar la protección de acceso a dicha fuente de información permitiendo la reconstrucción de este. A pesar de la aparente robustez, no obsta a que se siga recomendando el refuerzo del proceso de autenticación mediante el uso de un doble factor de autenticación que impida el acceso indebido por terceros.

Por otro lado, conviene analizar desde su **diseño**, **prueba** en desarrollo y efectiva **implantación** las medidas implantadas para proteger los sensores y dispositivos empleados para el registro y lectura del patrón usado para la autenticación del empleado.

Así, conviene que los dispositivos de **cotejo de los patrones,** empleados para comparar los patrones, en los que se asegura la coincidencia de la información empleada y validar esa autenticación, se dispusiesen en servidores centralizados y supervisados que hayan implantado las medidas de seguridad adecuadas para la protección y acceso limitado a la información en función de los roles que sea necesario que administren y supervisen dicha información.

Finalmente, aplicarlo al repositorio en el que dicha información se conserva, debiendo contar con las restricciones oportunas de acceso únicamente a aquellos perfiles que sea realmente necesario para evitar el acceso indiscriminado a los datos de carácter especial.

En relación con el repositorio, la adecuación de las medidas también dependerá del tipo de repositorio, bien interno, gestionado por el propio responsable del tratamiento; bien externo, alojado en los servidores de un proveedor externo, el cual podría también proporcionar

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

algún servicio adicional, implicando un análisis individualizado de las circunstancias para determinar las medidas apropiadas y valorando la posible necesidad o falta de fundamento para tener acceso de este tercero al repositorio. Igualmente, otro factor, con independencia de la titularidad del repositorio, es el medio de este, multiplicándose las combinaciones posibles si consideramos aquellos de carácter físico o alojado en la nube.

Otra alternativa que permitiría proteger la información biométrica sería el uso de ***tokens*** criptográficos para reforzar la protección e impedir el acceso a terceros no autorizados, de forma que únicamente los roles que dispusiesen de la contraseña maestra pudiesen acceder a la información personal.

Por último, y vinculado a los principios de minimización y limitación referidos anteriormente, deberían adoptarse las medidas oportunas en aquellos supuestos en los que se empleasen terminales que permitiesen la **recogida** de datos personales **fuera del entorno y horario laboral**, de forma que también puede afectar a la privacidad de las personas.

En estos casos, debería habilitar los mismos para que el usuario pudiese realizar las acciones oportunas para que la recogida de datos fuese suspendida durante el espacio temporal que no se corresponde con las horas de trabajo efectivo. Estas cuestiones deberían preverse ya en la fase de concepto para asegurar el respeto al principio de la privacidad desde el diseño.

IV.IV.II. Reconocimiento facial en los aeropuertos

El reconocimiento facial se puede utilizar para mejorar la seguridad en aeropuertos y acelerar el procesamiento en el check-in de los vuelos.

Mediante el sistema de reconocimiento facial es posible identificar a una persona a partir de sus datos biométricos. Además de brindar una precisión ideal y rapidez en el proceso, es altamente efectivo en sus resultados cuando se combina con otro dato biométrico, como las huellas dactilares, el iris, las venas, entre otros.

Varios aeropuertos en el mundo ya disponen de tecnología biométrica. La terminal 4 del aeropuerto de Shanghái, en Singapur, posee un sistema de reconocimiento facial automatizado, que permite ahorrar alrededor de un 20% de los costes habituales de mano de obra.

Otro caso similar se da en Australia o Argentina, que a comienzos del año 2023, ha comenzado a implementar en sus aeropuertos sistemas de reconocimiento facial, de iris y huella dactilar, para permitir a los pasajeros entrar y salir del aeropuerto sin tener que mostrar su pasaporte.

En Europa se ha llevado a cabo por primera vez un proceso de integración en aeropuertos que permite a los pasajeros **realizar todos los pasos necesarios sin**

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

tener que mostrar documentación de identificación. Esto incluye la facturación del equipaje. Se utilizan sistemas biométricos basados en el reconocimiento de características físicas únicas de las personas.

Los **equipos biométricos se han ubicado en la zona de facturación, en el acceso al filtro de seguridad y en la puerta de embarque,** validando los datos biométricos del pasajero, como su rostro, y su documentación. Este proceso agiliza el flujo y mejora la seguridad desde el registro online del viajero en casa hasta el abordaje del avión.

Durante el piloto**, la validación de la documentación con datos biométricos se realiza una sola vez,** siempre que el pasajero dé su consentimiento para futuros vuelos. Aena es la única propietaria de la base de datos biométrica y se encarga de su gestión, asegurando el cumplimiento del Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

Este proyecto, realizado en colaboración entre Vueling y Aena, comenzó varios meses atrás con pasajeros en la ruta Barcelona-Málaga. Se trata de la prueba piloto más completa que se ha llevado a cabo en un aeropuerto de Aena, ya que incluye tecnología biométrica en cuatro procesos del viaje: check-in, facturación de equipaje, filtro de seguridad y embarque.

Por otro lado, el proyecto de biometría del Aeropuerto Josep Tarradellas Barcelona-El Prat, ha sido premiado por el Consejo Internacional de Aeropuertos.

En los aeropuertos de Aena, se ha implementado la biometría como parte del Programa Estratégico de Identidad Digital de la compañía. Este programa tiene como objetivo utilizar tecnología biométrica en múltiples puntos del aeropuerto, con el fin de ofrecer a los pasajeros una experiencia de viaje segura, fluida y cómoda en todo momento. Mediante el uso de la biometría, se busca simplificar los procesos de identificación y agilizar el flujo de pasajeros, proporcionando una experiencia más eficiente y agradable en el aeropuerto.

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

IV.IV.III. Acceso a grandes intalaciones de ocio (Estadios)

El proyecto de ley de inteligencia artificial presentado por el Parlamento Europeo y el Consejo establece normas armonizadas para regular el uso de la inteligencia artificial (IA). En este proyecto se prohíben ciertas prácticas de IA, como el uso de sistemas de identificación biométrica remota en tiempo real en espacios públicos con fines de aplicación de la ley, aunque se contemplan excepciones específicas. Además, se proponen restricciones y garantías para ciertos usos de los sistemas de identificación biométrica remota.

Destacamos la implementación de un sistema pionero de acceso biométrico en el estadio El Sadar, casa del equipo de fútbol CA Osasuna.

El acceso biométrico permite a los aficionados ingresar al estadio sin necesidad de llevar consigo su carnet físico, utilizando en su lugar el reconocimiento facial lo que **resulta más cómodo y evita posibles pérdidas u olvidos**.

Además, el acceso biométrico **es rápido y eficiente**, con la capacidad de permitir la entrada de hasta 20 personas por minuto, lo que **reduce significativamente los tiempos de espera en las puertas de acceso**.

El sistema de acceso mediante datos biométrico se ha implementado de **manera voluntaria**, lo que significa que los aficionados tienen la total libertad de elegir la opción de utilizar sus tarjetas físicas o pases móviles. Esto demuestra que la implementación de la biometría **no excluye otras formas de acceso**, sino que ofrece una alternativa adicional y conveniente y que el uso de la biometría está a disposición de todo aquel que considere oportuno consentir su utilización, una modalidad que cada vez está siendo más utilizada por los aficionados mejorando así la celeridad de los procesos de acceso a los estadios.

En la Opinión conjunta 5/2021 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas sobre inteligencia artificial el Comité Europeo de Protección de Datos (CEPD) y el Supervisor Europeo de Protección de Datos (SEPD) **solicitan de manera general la prohibición de cualquier utilización de la IA para el reconocimiento automático** de características humanas en espacios de acceso público.

Esto incluye el reconocimiento de rostros, huellas dactilares, ADN, voz, pulsaciones de teclas y otras señales biométricas o de comportamiento. Asimismo, consideran altamente indeseable el uso de la IA para inferir las emociones de una persona física, **y abogan por su prohibición en cualquier contexto**.

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

IV.IV.IV. Acceso a instalaciones (Gimnasios)

La utilización del control del control de acceso (a través de la autenticación) mediante biometría facial es una opción que permite **digitalizar la entrada a las instalaciones y brindar una experiencia más cómoda, rápida y segura, sin necesidad de utilizar credenciales físicas.**

El acceso para gimnasios puede hacerse bien con tecnología biométrica o con una tarjeta con codificación y proximidad[4].

Según el artículo 4.1 de la Ley Orgánica de Protección de datos, "los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".

El Dictamen 3/2012 del GT29, el Grupo de Autoridades europeas de protección de datos en el que está incluida la Agencia Española, usa precisamente el gimnasio como ejemplo de **uso desproporcionado (y por tanto, ilícito)** de los controles de acceso por lectura de huella digital.

"En un gimnasio se instala un sistema biométrico centralizado basado en la recogida de impresiones dactilares a fin de permitir el acceso a las instalaciones y servicios conexos únicamente a los clientes que han pagado su cuota. Para que funcione dicho sistema, es preciso almacenar las huellas dactilares de todos los clientes y miembros del personal. Esta aplicación biométrica parece desproporcionada en relación con la necesidad de controlar el acceso al club y facilitar la gestión de las inscripciones. Es fácil imaginar que otras medidas, como una mera lista de control, el uso de etiquetas RFID o tarjetas de banda magnética, que no requieren el tratamiento de datos biométricos, serían igualmente factibles y eficaces."

4. https://www.avpd.euskadi.eus/contenidos/dictamen_avpd/d17_005/es_def/adjuntos/CN17-004_DIC_D17-005.pdf

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

El GT29 considera que hay medios menos lesivos para controlar el acceso de los socios y que, por tanto, su uso es desproporcionado e innecesario. Pero tenemos un precedente aún más cercano, un informe jurídico del año 2010 sobre un caso similar en España donde la finalidad que motiva el tratamiento de datos es otorgar un servicio a un cliente. Aquí la Agencia Española de Protección de Datos dice exactamente lo mismo:

"Atendiendo al juicio de proporcionalidad que el Tribunal Constitucional exige en la adopción de este tipo de medidas, la Agencia concluye que resulta desproporcionado la necesidad de recabar la huella dactilar para prestar un servicio comercial a los clientes, cuando dicho servicio puede prestarse con otros medios menos intrusivos en los derechos y libertades de los clientes, tales como el uso de las tarjetas de fidelización."

En conclusión: la biometría es cómoda y todo lo cómodo es popular. En un gimnasio, elimina la necesidad de llevar la tarjeta, pulsera o identificador encima. En un festival, impide que se cuelen varias personas con la misma pulsera, o con una entrada que ha perdido otro.

El usuario que prefiere renunciar a esa protección para no llevar carnet está en su justo derecho, pero necesita **saber qué tratamiento se aplicará a esa delicada información(derecho de información)**: si será guardado en una base de datos, con qué finalidad y bajo qué tipo de protección. También debe saber si tiene derecho de acceso, rectificación, cancelación y oposición a esos datos, y qué pasará con ellos si la empresa quiebra o es adquirida por otra empresa, o cuando cancele la suscripción.

IV.IV.V. Prevención del fraude y prevención de blanqueo de capitales

El uso de la tecnología de reconocimiento facial para el alta de clientes en oficina o en canal online fue analizado por la AEPD en su informe jurídico 0047/2021.

El proyecto que fue presentado ante la AEPD por las entidades bancarias, para evaluar el tratamiento de datos biométricos con la finalidad de cumplir con el deber de identificación y cumplir con la normativa de prevención del blanqueo de capital y financiación del terrorismo.

Esta consulta se centra en las posibles **alternativas** a la utilización del **consentimiento** como base legitimadora en el tratamiento de datos biométricos, ya que, al tratarse de categorías especiales de datos, el consentimiento no es la base jurídica adecuada por depender el tratamiento de la autorización de los clientes, considerándose un consentimiento obligatorio que no sería lícito. Por este motivo, se plantea en la consulta el empleo del **interés público** como base jurídica, estando limitada la **finalidad del tratamiento** a la **prevención del blanqueo de capitales y financiación del terrorismo**, así como **control** de **fraude**.

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

La AEPD especifica que este tratamiento se encuentra enmarcado dentro del grupo de **identificación unívoca** de la persona, por lo que considera que se trata de categorías especiales de datos y sujeto a la regla general de prohibición de tratamiento de estos según el art. 9 RGPD.

Este tratamiento fue analizado por la AEPD en tres informes anteriores:

1. 36/2020, reconocimiento facial de los alumnos para exámenes on-line, con el objetivo de verificar la identidad y evitar suplantación de identidad.
2. 31/2019 sobre la incorporación de sistemas de reconocimiento facial en los servicios de videovigilancia.
3. 97/2020 sobre métodos de identificación no presencial para la expedición de certificados electrónicos.

En estos informes, la AEPD analiza las **posibilidades de levantar la prohibición** del art. 9, mediante dos excepciones:

1. consentimiento; e
2. interés público.

En cuanto al **consentimiento**, puede aplicarse con las siguientes condiciones:

1. cuando cumpla las condiciones marcadas por RGPD: libre, informado, específico e inequívoco; y
2. que el Derecho de la Unión o de los Estados miembros establezca que la prohibición del tratamiento no puede ser levantada por el interesado.

En cuanto al **interés público** debe tener las siguientes características:

1. esencial;
2. proporcional al objetivo conseguido;
3. respetar el derecho a la protección de datos; y
4. establecer medidas adecuadas y específicas para proteger los derechos fundamentales del interesado.

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

En cuanto a la consideración de "***esencial***", según la doctrina constitucional, requiere que se encuentre regulado en una norma con rango de ley, que debe especificar el interés público esencial que justifica la limitación del derecho a protección de datos y las limitaciones aplicables, debiendo estar justificado por la protección de otros derechos fundamentales, por lo que debe especificar las reglas que hagan limitar el derecho a la protección de datos y las consecuencias. Dicha ley además debe contener la descripción de las garantías de carácter técnico y organizativo para prevenir y mitigar los riesgos para los interesados.

Respecto a la **proporcionalidad**, debe seguirse lo establecido por el Tribunal Constitucional en sentencia 14/2003, debiendo evaluar si cumple con los tres requisitos siguientes:

1. juicio de idoneidad: si la medida es susceptible de conseguir el objetivo propuesto.
2. juicio de necesidad: no existe otra medida más moderada para conseguir el fin con igual eficacia.
3. juicio de proporcionalidad: si la medida es ponderada y equilibrada porque supone más beneficios o ventajas para el interés general que perjuicios para los valores en conflicto.

Para la evaluación de este caso, debemos considerar que se trata de una obligación establecida por la Ley 10/2010, que exige a los sujetos obligados la identificación de las personas físicas o jurídicas que pretendan establecer una relación de negocio. esta identificación requiere la comprobación de la identidad mediante documentos fehacientes.

La citada Ley establece los documentos fehacientes a efectos de identificación de las personas físicas y jurídicas, y adicionalmente, el artículo 12 recoge las condiciones para realizar una identificación por medios no presenciales, que no incluye la posibilidad de identificación por medios biométricos.

Por consiguiente, al encontrarnos con un tratamiento de categorías especiales, según el artículo 9.1 del RGPD, requiere alguna de las circunstancias recogidas en el apartado 2 para posibilitar su tratamiento. En este caso, la normativa de aplicación (Ley 10/2010) no habilita este tratamiento.

No siendo posible levantar la prohibición del tratamiento por una norma, **debemos recurrir al consentimiento expreso** del afectado siempre que se cumplan con los requisitos para un consentimiento válido según el RGPD.

Adicionalmente, la AEPD dictamina que la base jurídica que legitime el tratamiento no puede basarse en el interés público.

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

Para detallar el ámbito de aplicación del interés público se remite a la Constitución, que lo clasifica como concepto jurídico indeterminado que tiene una doble función: dar cobertura legitimadora a la actuación de la Administración y además constituye una de las formas de delimitar las potestades administrativas.

Según la AEPD, aunque se puede determinar que existe un interés público en la prevención del blanqueo de capitales, no se justifica el tratamiento de datos biométricos, ya que la Ley 10/2010 no atribuye a las entidades financieras competencias de las Administraciones públicas.

El informe aclara que el uso de tratamientos biométricos por las entidades financieras para evitar la suplantación de identidad no se realizaría por interés Público sino como medida de control de fraude, que es un interés privado y no público.

Sin embargo, la Ley 10/20210 establece las medidas de diligencia debida de los sujetos obligados por razones de interés público, aplicando la base legitimadora recogida en el artículo 6.1 c) del RGPD, según el informe de la AEPD 195/2017.

Para cumplir con las obligaciones de los sujetos obligados en cuanto a la identificación de las personas, debe utilizarse el DNI como documento identificativo fehaciente, ya que acredita por sí solo y a todos los efectos la identidad y los datos personales de su titular.

La Agencia, por último, recuerda el cumplimiento de los principios de finalidad y minimización de datos.

Respecto al principio de minimización, se destaca que el uso de estos sistemas de forma generalizada por las Entidades Bancarias supondría tratamiento a gran escala de categorías especiales de datos por el elevado número de clientes de las entidades financieras.

Además, este tratamiento afectará a gran número de clientes que no estarán dentro de la aplicación de medidas específicas de diligencia debida, lo que supone una aplicación indiscriminada que se considera por la Agencia como no proporcional.

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

La AEPD remite al DNI como documento identificativo básico y por tanto la identificación biométrica se considera injustificada y desproporcionada.

Como consecuencia de todo lo anterior, emite un **informe desfavorable para el uso de técnicas de identificación biométrica para la identificación de personas** dentro de la prevención del blanqueo de capitales y financiación del terrorismo tomando en consideración, como principales argumentos, los siguientes:

1. Se trata de categorías especiales de datos y debe encontrarse una base legitimadora y una excepción a la prohibición del tratamiento.
2. La Ley 10/2010 no establece una excepción para el tratamiento de estos datos
3. Excluye el uso de interés público.
4. En el caso de uso de datos biométricos deben valorarse los principios de necesidad, proporcionalidad y minimización.

IV.IV.VI. Persecución de delitos (Mercadona)

La biometría tiene una función cada vez más relevante para la persecución y prevención de la comisión de delitos y ello requiere el análisis y desarrollo de nuevas normas y la emisión de mejores prácticas por los diferentes organismos internacionales[5] que resulten aplicables en España, en el ámbito Europeo[6] e internacional, principalmente mediante la emisión de:

1. resoluciones y procedimientos sancionadores de las diferentes autoridades de protección de datos europeas y en especial por la AEPD con la sanción a un conocido grupo de supermercados español;
2. autos o resoluciones judiciales; y
3. nuevos informes jurídicos de la AEPD y diversos organismos internacionales especializados.

En relación con el tratamiento de datos biométricos para la persecución y prevención de delitos, comenzaremos por diferenciar si se trata de:

1. un tratamiento de datos realizado por un organismo público/administración en interés público o bien,
2. se corresponde con el tratamiento de datos realizado por una empresa privada para satisfacer las medidas de control y prevención de seguridad ante la potencial comisión de delitos.

5. Compendio de prácticas recomendadas de las Naciones Unidas" Uso responsable y el uso compartido de la biometría en la lucha contra el terrorismo https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_on_biometrics_es.pdf

6. **Libro Blanco de la Inteligencia Artificial** https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0065

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

IV.IV.VI.I. Cuestiones en común y principales aspectos diferenciadores del empleo de la biometría en el ámbito público y privado

El principal marco normativo lo encontramos en la Constitución Española, el RGPD, la LOPDGDD y también en la Ley específica 7/2021 de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales[7].

Si bien, como explica la AEPD *"el marco legal de las operaciones biométricas dependerá de la normativa de protección de datos, normativa específica sobre biometría y también la normativa sectorial que es aplicable al responsable y al tratamiento concreto. Esto puede implicar habilitaciones o limitaciones al uso de operaciones biométricas, también obligaciones adicionales (por ejemplo, podrían obligar a realizar una Evaluación de Impacto en la Protección de Datos, EIPD), así como a la validez legal de sus resultados."*[8]

Este tratamiento ha sido analizado parcialmente por la AEPD en varios informes:

1. 36/2020, reconocimiento facial de los alumnos para exámenes on-line, con el objetivo de verificar la identidad y evitar suplantación de identidad.
2. 31/2019 sobre la incorporación de sistemas de reconocimiento facial en los servicios de videovigilancia.
3. 010308/2019 Informe sobre el uso de la tecnología de reconocimiento facial por los servicios de seguridad privada.
4. 97/2020 sobre métodos de identificación no presencial para la expedición de certificados electrónicos.

7. Boletín Oficial del Estado https://www.boe.es/buscar/pdf/2021/BOE-A-2021-8806-consolidado.pdf
8. AEPD https://www.aepd.es/es/prensa-y-comunicacion/blog/datos-biometricos-evaluacion-perspectiva-proteccion-datos

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

Al mismo tiempo, nos encontramos en momento de gran avance de la inteligencia artificial y de otros tantos sistemas de innovación tecnológica, sobre todo en estos últimos años y como consecuencia, en el ámbito normativo:

1. en algunos casos no se han tenido en cuenta en la redacción inicial, por ejemplo, la Norma Penal u otras normas de desarrollo; o bien,
2. se encuentra esta materia en fase de análisis y desarrollo mediante, por ejemplo, el futuro Reglamento Europeo de Inteligencia Artificial que esperamos en versión final dentro de 2023.

En línea con lo expuesto, destacamos también el Informe del CEPD *"Directrices 05/2022 sobre el uso de técnicas de reconocimiento facial"*[9] el tratamiento de datos biométricos constituye, en cualquier circunstancia, una intromisión grave en los derechos reconocidos en la Carta de Derechos Fundamentales de la Unión Europea, especialmente en el respeto de la vida privada y familiar (art.7) y en la protección de datos (art. 8). Se trata de un tratamiento de una categoría especial de datos, las principales excepciones respecto a la prohibición expresan de su uso (art. 9.1 RGPD):

1. el consentimiento explícito;
2. la normativa en el ámbito laboral; y
3. el interés público artículo 9.2 a, b y c RGPD.

En todo caso, como bien se ha descrito en otros apartados anteriores, existe una recomendación común respecto a la manera de proceder por parte de las organizaciones públicas y privadas y de la labor de los especialistas del Compliance y de la protección de datos (relativa a la diligencia debida), en los casos en los que se lleve a cabo el **tratamiento de datos especialmente sensibles de datos biométricos que requiere analizar y documentar entre otros:**

1. valorar si disponemos de una habilitación normativa al tratamiento de datos biométricos;
2. determinar si requiere o no consentimiento expreso del interesado;
3. cumplimiento del deber de información;
4. medidas de seguridad, deberá ser un tratamiento proporcional al fin perseguido (análisis de riesgos y en su caso evaluación de impacto conforme al Reglamento y al ENS si se trata de infraestructura crítica);

9. Comité Europeo de Protección de Datos. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_es

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

5. valoración ética de la inteligencia artificial empleada; y
6. mantener un adecuado equilibrio de la protección de la privacidad y de los derechos fundamentales de los individuos.

Y además documentar y renovar periódicamente este análisis o *"Due Diligence".*

IV.IV.VI.II. Análisis de la aplicación de tratamiento de datos biométricos en el Ámbito Público

En el presente apartado analizaremos la utilización de la biometría conforme a la normativa de protección de datos y resto de resto de normativa relevante aplicable, diferenciando si se emplea ésta en interés público por parte de las Autoridades, el Estado, Administraciones Públicas, etc.

En la Ley 7/2021, encontramos la habilitación al tratamiento de datos biométricos en interés de la seguridad pública y la prevención de delitos, en el Artículo 13.2, en concreto: *"las autoridades competentes, en el marco de sus respectivas funciones y competencias, podrán tratar datos biométricos dirigidos a identificar de manera unívoca a una persona física con los fines de* ***prevención, investigación, detección de infracciones penales,*** *incluidas la* ***protección y la prevención frente a las amenazas contra la seguridad pública."***

Aquí podemos encontrar casos de forma práctica, por ejemplo, el empleo de tecnologías biométricas en los controles transfronterizos como complemento a la identificación documental de los individuos con el fin de identificar y detectar posibles compromisos de la seguridad ante ataques terroristas, identificación de criminales de guerra y otros delincuentes penales, en los que el interés público y las medidas de las Autoridades pueden encontrar cabida en la norma[10].

10. Caso INTERPOL – Sistema IFRS **https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Reconocimiento-facial**

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

Cabe destacar el *"Compendio de prácticas recomendadas de las Naciones Unidas" donde hablamos del uso responsable y el uso compartido de la biometría en la lucha contra el terrorismo"*[11].

En los apartados anteriores se han explicado varios de los informes, en este apartado destacamos, **el Informe sobre el uso de la tecnología de reconocimiento facial por los servicios de seguridad privada,** que fue analizado por la AEPD en su informe jurídico 0039/2019 (N/REF 010308/2019). La consulta relativa a:

1. la **potencial exclusión de las actividades de seguridad privada**, por tratarse de actividades subordinadas a la seguridad pública, del ámbito de aplicación del Reglamento conforme a su artículo 2.2, letra d); y
2. la licitud de la incorporación de sistemas de reconocimiento facial en los servicios de videovigilancia al amparo del artículo 42 de la Ley de Seguridad Privada.

Sobre estos puntos:

1. Siendo criterio de la Agencia que los tratamientos de datos personales que lleven a cabo las **empresas de seguridad, despachos de detectives privados y personal de seguridad privada,** *incluida la comunicación de datos a las Fuerzas y Cuerpos de Seguridad en cumplimiento de la obligación legal establecida en el artículo 14.2 de la Ley de Seguridad Privada, no están incluidos en el ámbito de aplicación de la Directiva 2016/680, quedando sujetos a lo dispuesto en el RGPD.*

   Criterio que incluye la LOPDGDD, en el artículo 22 los tratamientos con fines de videovigilancia, señala en su apartado 6 que *"El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva (UE) 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.*

   Fuera de estos supuestos, dicho tratamiento se regirá por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica".

11. Compendio de prácticas recomendadas de las Naciones Unidas" Uso responsable y el uso compartido de la biometría en la lucha contra el terrorismo https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_on_biometrics_es.pdf

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

Por el contrario, los tratamientos que realicen las empresas y personal de seguridad quedan sujetos a lo dispuesto en el citado precepto, "sin perjuicio de lo previsto en la **Ley 5/2014, de 4 de abril, de Seguridad Privada y sus disposiciones de desarrollo**".

2. En estos casos nos encontramos que se requiere un **análisis de la idoneidad y proporcionalidad del tratamiento de datos biométrico**s, generando un beneficio superior en el tratamiento de dichos datos con respecto a los problemas o el impacto que genere en la privacidad.

   Será necesario demostrar y evidenciar en el análisis efectuado que por ejemplo la prevención de la comisión de delitos de terrorismo u otros delitos graves justifican la implantación de los sistemas

   "la existencia de un interés público no legitima cualquier tipo de tratamiento de datos personales, sino que deberá estarse, en primer lugar, a las condiciones que haya podido establecer el legislador, tal como prevé el propio artículo 6 del RGPD, en sus apartados 2 y 3, así como a los ya citados principios del artículo 5 del RGPD, especialmente a los de limitación de la finalidad y minimización de datos. Y en el caso de que vayan a ser objeto de tratamiento alguno o algunos de los datos personales incluidos en las categorías especiales de datos a los que se refiere el artículo 9.1. del RGPD, que concurra alguna de las circunstancias contempladas en su apartado 2 que levante la prohibición de tratamiento de dichos datos, establecida con carácter general en su apartado 1".

   Un ejemplo de empleo de esta tecnología para la persecución de delitos la encontramos en el caso de la INTERPOL mediante el sistema de **Reconocimiento Facial (IFRS)**[12] que conforme se describe en su web *"se almacenan las imágenes faciales enviadas por más de 179 países, lo que la convierte en una*

12. INTERPOL – IFRS https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Reconocimiento-facial

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

base de datos policiales de ámbito mundial única. Combinado con un software automatizado de identificación biométrica, este sistema es capaz de identificar a una persona o de comprobar su identidad mediante la comparación y el análisis de los modelos, formas y proporciones de sus rasgos y contornos faciales".

IV.IV.VI.III. Análisis de la aplicación de tratamiento de datos biométricos en el Ámbito Privado

En el anterior apartado, mediante el análisis efectuado por la AEPD en el Informe jurídico, se perfila qué recae en el concepto de "interés público" y qué otros ámbitos como la seguridad privada deberán contar con un análisis exhaustivo, con consentimiento expreso de los usuarios, entre otros, y con sujeción a la normativa de protección de datos o el amparo del artículo 6.1. del RGPD sobre la base del interés público.

En relación con la resolución del principal expediente sancionador de la AEPD con **Referencia PS/00120/2021 relacionado con el sistema de detección** de aquellas personas con sentencias firmes y órdenes de alejamiento en vigor contra Mercadona o contra alguno de sus trabajadores, es importante destacar que la sanción es resultado de la consideración a juicio de la AEPD de que se producido una vulneración de la privacidad, a consecuencia de realizar un tratamiento de datos biométricos sin la concurrencia de una base de legitimación que habilitara para ello.

En concreto, al analizar el caso, destacamos que:

1. La finalidad del sistema de reconocimiento facial implantado la empresa, ésta indica que se trata únicamente y de forma exclusiva para el fin de" detectar la entrada a sus establecimientos de personas con sentencias firmes y medida cautelar de orden de alejamiento" en pro de proteger la seguridad de los clientes y empleados, sin generar una base de datos de condenas penales y que el sistema comparase "una muestra biométrica dubitada, obtenida a través de una o varias imágenes de una persona, frente a una base de datos de muestras biométricas ya asociadas de forma indubitada a la identidad de una persona, que han sido registradas previamente a través de una o varias fotografías".

2. Las "muestras biométricas dubitadas" de los condenados que obraban en poder de la empresa y obtenidas mediante el sistema de reconocimiento facial, se transformaban en "patrones" que, a posteriori, se comparaban con esas fotos. Y por ende consideraba la empresa que dicho patrón no constituye un dato de carácter personal, por lo que no necesita base legal para su tratamiento".

3. Adicionalmente, la empresa interpretó en base a la resolución judicial previa, que ostentaba legitimación conforme al art. 9.2.f) del RGPD tanto para los

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

condenados como para el resto de los ciudadanos que accedían a los locales.

Respecto a la valoración de la AEPD;

1. LA AEPD consideró que en la fotografía y sobre el denominado como "patrón biométrico" en ambos recae la consideración de dato personal y requería por tanto dicha base jurídica que legitimara el tratamiento de datos.
2. Produciendo en los interesados (usuarios y potenciales usuarios, incluidos menores) una limitación de facto con respecto al derecho a la autodeterminación, libertad e intimidad, al no informar, por ejemplo, de en qué centros en concreto estaba implantado o no el sistema.
3. Además, tratándose de tecnologías tan invasivas sobre los menores y otros colectivos vulnerables que merecen una especial protección, la información suministrada debería ser específica para los mismos (Considerando 58).
4. De nuevo aquí cobra especial relevancia lo expuesto en el apartado anterior respecto a los principios que analizar y documentar en la evaluación previa a la instalación de cualquier sistema biométrico conforme a lo recogido por el Tribunal Constitucional en sentencia 14/2003.
5. Finalmente, la AEPD consideró que esta valoración era contraria a los principios de necesidad, proporcionalidad y minimización del Reglamento, en especial; Imponiendo la sanción superior a 2 millones de euros.

IV.IV.VI.V. Conclusiones y recomendaciones adicionales:

1. El tratamiento de datos biométricos supone el uso de categorías especiales de datos y debe encontrarse una base legitimadora y una excepción a la prohibición del tratamiento. O bien que podamos evidenciar que se trata de un tratamiento en interés público.

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

2. En el caso de uso de datos biométricos deben valorarse los principios de necesidad, proporcionalidad y minimización.
3. Conveniencia conforme a lo expuesto en el apartado 4.3.4 relativo a la PREVENCIÓN DEL FRAUDE Y PREVENCIÓN DE BLANQUEO DE CAPITALES, la creación y revisión continua de políticas y procedimientos internos de gestión que operan como medida para garantizar que el tratamiento de datos biométricos sea idóneo y proporcional. Mediante procesos claros respecto a las fases de tratamientos de datos (en especial, recogida, uso, conservación y expurgo), velando por la privacidad desde el diseño y por defecto, medidas de seguridad y con cuestiones como la incorporación de medidas de privilegios de acceso.

IV.IV.VII. Utilización para perfilado comercial/publicitario

A nivel local, no contamos con ningún cuerpo normativo que regule expresamente este tipo de actividad, a diferencia de otras jurisdicciones en las que están proliferando nuevas leyes que regulan los tratamientos de datos biométricos empleados para determinados fines, como es el caso del surgimiento de leyes estatales en Estados Unidos.

Se debe considerar que el tratamiento de datos biométricos con esta finalidad implicaría, en sí mismo, un doble tratamiento de dicha información con alcances diferenciados:

1. Por un lado, la actividad propiamente del **perfilado** realizado, abarcando todo el ciclo (desde la recogida, acceso, potenciales interconexiones y cruces de datos conservados en diferentes repositorios, etc.) de procesamientos necesarios para obtener un patrón con rasgos comunes (físicos, psíquicos o de conducta) sobre el público objetivo con el fin de adecuar y personalizar la oferta a trasladar, y así obtener una mayor receptividad.

   La primera cuestión a tener en cuenta es el contar con una **base legitimadora** que permitiese un tratamiento de esta naturaleza, encuadrando esta obligación dentro del principio de privacidad desde el diseño, aportando una evidencia de la cultura de cumplimiento existente en la empresa y que sirviese con medida de seguridad en sí mismo para asegurarse de la ausencia de un tratamiento que carece de legitimación.

   Teniendo en cuenta el tipo de tratamiento comentado las opciones se reducen, debiendo limitar el mismo a aquellos casos en los que podamos basarlo en el **consentimiento** del interesado; o, en caso contrario, el **interés legítimo** del responsable.

   En el caso del consentimiento, implicaría la necesidad de establecer una serie de medidas organizativas incluyendo desde la obtención al manejo adecuado

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

del consentimiento otorgado por los interesados. En este sentido, es fundamental disponer de un sistema de gestión de consentimientos eficiente, teniendo en cuenta los rasgos que debe cumplir el consentimiento para ser válido, disponiendo de todo el ciclo de vida de este desde su recogida hasta su revocación. Las evidencias deben permitir conocer el momento y forma en que se ha otorgado, como medida preventiva que el responsable del tratamiento debería implantar.

Si bien el interés legítimo, generalmente, se contempla como la otra vía de legitimación para este tipo de tratamiento, lo cierto es que el responsable del tratamiento debe tener en consideración las orientaciones planteadas por el CEPD y la AEPD en lo referente a las actividades de perfilado. En estos casos, dichos organismos exigen estas actividades que se realicen con datos de especial categoría, como es el caso, y, a mayor abundancia, que puedan considerarse intrusivas, únicamente se limiten los tratamientos a aquellos que cuenten con el consentimiento expreso del afectado. Por tanto, el escenario se reduce de manera considerable a la primera base legitimadora comentada, el consentimiento.

La naturaleza de la propia actividad, así como el tratamiento a gran escala de datos de especial categoría y, a mayores, biométricos; o el uso de nuevas tecnologías, nos lleva a asegurar la necesidad de realizar una evaluación de impacto para plantear la necesidad, proporcionalidad y justificación de la actividad, además de tener en cuenta los riesgos y las medidas de seguridad a implantar para su mitigación o eliminación.

En caso de que la propia evaluación determinase que el tratamiento carece de riesgos considerables para los derechos y libertades de los interesados, sería conveniente poner énfasis en las medidas técnicas para adecuar el tratamiento y limitar los riesgos.

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

Así, una de las primeras medidas sería implantar un sistema de **control de acceso** a la información basada en los roles existentes (RBAc), de forma que el personal únicamente tuviese acceso y derechos ulteriores sobre la información teniendo en cuenta las funciones desempeñadas, basando los mismos en el principio de minimización y estando convenientemente actualizados, además de estar basados en los niveles de riesgo asumidos.

Además, otra de las premisas esenciales sería implantar un sistema de **conservación, archivo y eliminación** de la información que cumpliese con los parámetros contemplados en la normativa vinculante, de forma que, una vez finalizado el tratamiento o revocado el consentimiento por el interesado, esta información se conservase por los plazos legalmente establecidos con las medidas adecuadas evitando su tratamiento. Igualmente, y como fase final de dicha gestión, las acciones de eliminación definitiva de la información deberían ser convenientemente testadas para asegurar que dicha información puede ser borrada definitivamente de los repositorios corporativos empleados y evitar riesgos e incidentes que impliquen un riesgo adicional para el responsable del tratamiento.

2. Por otro lado, no debemos olvidar la consiguiente actividad del envío de las acciones de marketing y comunicaciones motivadas con el fin de hacer llegar la oferta e información al público objetivo.

   En este sentido, además de las premisas fijadas en la normativa vigente en materia de protección de datos, habrá que tener en consideración la Ley de Servicios de Sociedad de la Información, limitando el envío de comunicaciones publicitarias o promocionales a los interesados que hayan dado previamente su **consentimiento** expreso, la ausencia de revocación de consentimiento en caso de basar el tratamiento en el mismo, etc.

En lo que respecta al consentimiento, nos remitimos a lo comentado en el punto anterior.

En caso contrario, y que el tratamiento se basase en el interés legítimo, nos llevaría a la necesidad de disponer de una evaluación de este mediante la realización del ***Legitimate Interest Assessment o evaluación de interés legítimo en el que se plasmase y quedase confirmada la fundamentación de este sobre el estudio de:***

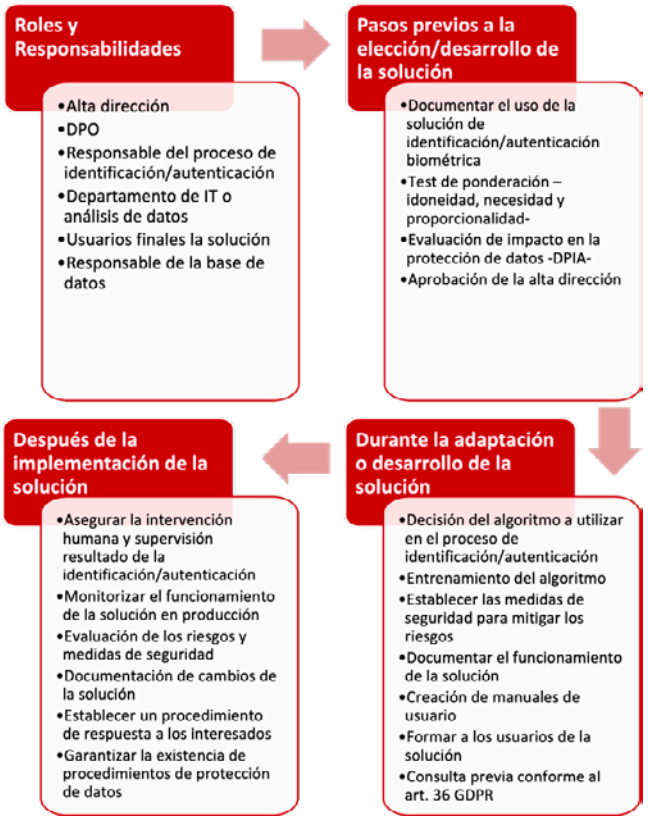
1. **test de finalidad**, donde se exponga el interés legítimo del responsable;
2. **test de necesidad**, donde quede probado que el tratamiento es necesario para llevar a cabo la actividad; y
3. **test de equilibrio**, donde resulte que los intereses del responsable no prevalezcan los intereses o los derechos y libertades del interesado.

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

A partir de la información resultante de los análisis realizados, convendría adoptar las decisiones pertinentes para llevar a cabo la puesta en marcha de ulteriores medidas de seguridad que se adecuasen al alcance y circunstancias del tratamiento en sí mismo (volumen de interesados, actividad de tratamiento, sistemas empleados para el mismo, duración de este, proveedores necesarios, ámbito geográfico, etc.).

V. Test de idoneidad para la implantación y uso de sistemas de identificación biométrica

Tomando como ejemplo las Directrices del Comité Europeo de Protección de Datos 05/2022 sobre el uso de técnicas de reconocimiento facial en el ámbito de aplicación de la ley[13] para la implantación de una solución como producto disponible en el mercado de reconocimiento facial, se propone el siguiente workflow para la implantación de soluciones de identificación/autenticaciones biométricas dentro de las organizaciones.



13. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

VI. Anexo 1.- Principales sanciones relacionadas con el uso de sistemas biométricos

ENT.	PAÍS	EXPTE.	EMPRESA	DESCRIPCIÓN	IMPORTE	ENLACE
AEPD	España	**PS/00120/2021**	Mercadona S.A.	Sistema de detección de aquellas personas con sentencias firmes y órdenes de alejamiento en vigor contra Mercadona o contra alguno de sus trabajadores.	2.5 Mio EUR	https://www.aepd.es/es/documento/ps-00267-2021.pdf
AEPD	España	**PS/00218/2021**	ENTIDAD URBANÍSTICA COLABORADORA DE CONSERVACIÓN EUROVILLAS,	Instalación sistema de registro diario de jornada laboral de los empleados a través de técnica de reconocimiento facial (RF).	Apercibimiento	https://www.aepd.es/es/documento/ps-00218-2021.pdf
AEPD	España	**EXP202100603 PS/0553/2021**	GSMC EVENT PROJECT MANAGEMENT, S.L.	Caso MWC BARCELONA 202	200.000	https://www.aepd.es/es/documento/ps-00028-2023.pdf
AEPD	España	**PS/0597/2022 EXP202209921**	ALBERO FORTE COMPOSITE, S.L	Instalación sistema de registro diario de jornada laboral de los empleados a través de técnica de reconocimiento facial (RF).	20.000 €	https://www.aepd.es/es/documento/ps-00597-2022.pdf
CNIL	Francia	**Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI**	CLEARVIEW AI	La empresa CLEARVIEW AI extrae fotografías de una gran cantidad de sitios web, incluidas las redes sociales, y comercializa el acceso a su base de datos de imágenes de personas en forma de un motor de búsqueda en el que se puede buscar a un individuo utilizando una fotografía. La empresa ofrece este servicio en particular a las fuerzas del orden. Por lo tanto, la tecnología de reconocimiento facial se utiliza para interrogar al motor de búsqueda y encontrar a una persona a partir de su fotografía. En una decisión del 17 de octubre de 2022, el Comité Restringido -órgano de la CNIL responsable de las sanciones- impuso una multa de 20 millones de euros y ordenó a la empresa no proceder, sin base legal, a la recopilación y procesamiento de datos de personas ubicadas en Francia, y eliminar los datos de estas personas después de haber respondido a las solicitudes de acceso que le han sido enviadas. El Comité Restringido acompañó el requerimiento con una multa coercitiva -una cantidad de dinero a pagar en caso de incumplimiento de una decisión- de 100.000 euros por día de retraso al término del plazo de dos meses	20 Mio EUR	https://www.cnil.fr/fr/reconnaissance-faciale-la-cnil-liquide-lastreinte-prononcee-lencontre-de-clearview-ai https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

GPDP	Italia	**CLEARVIEW AI**	CLEARVIEW AI	La autoridad italiana impuso una multa de 20 millones de euros. Además: impuso la prohibición de cualquier recopilación adicional, por medio de técnicas de web scraping, de imágenes y los metadatos relevantes relacionados con personas en el territorio italiano y sobre el procesamiento posterior de los datos estándar y biométricos que son manejados por la Compañía a través de su sistema de reconocimiento facial y preocupación personas en el territorio italiano; ordenó el borrado de los datos, incluidos los datos biométricos, procesados por su sistema de reconocimiento facial con respecto a personas en el territorio italiano, sujeto a la obligación de responder oportunamente a dichas solicitudes para el ejercicio de los derechos en virtud de los artículos 15 a 22 del Reglamento como pueden haberse recibido de los interesados de conformidad con el artículo 12, apartado 3, del Reglamento; ordenó a la Sociedad que designara un representante en el territorio de la Unión Europea.	20 Mio EUR	https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9751362
Autoridad Protección de Datos Alemana	Holanda		DESCONOCIDO	La AP se centró en si la organización podía confiar en una de las excepciones del artículo 9 (2) del RGPD a la prohibición de procesar datos biométricos. Según AP, dos excepciones fueron relevantes en este caso: consentimientoexplícito(artículo9(2)(a)GDPR);y necesario para fines de autenticación o seguridad (artículo 29 de la Ley de implementación del RGPD de los Países Bajos; basado en el artículo 9 (2) (g) del RGPD).	€750,000	https://autoriteitpersoonsgegevens.nl/uploads/imported/boete-besluit_vingerafdrukken_personeel.pdf

VII. Anexo 1.- Guías de referencia

TITULO	ORGANISMO	ENLACE
Libro Blanco de la Inteligencia Artificial	Comisión Europea	https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0065
Propuesta Reglamento Europeo Inteligencia Artificial	Unión Europea	https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52021PC0206
Compendio de prácticas recomendadas de las Naciones Unidas" Uso responsable y el uso compartido de la biometría en la lucha contra el terrorismo	Naciones Unidas	https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_on_biometrics_es.pdf
Directrices 05/2022 sobre el uso de técnicas de reconocimiento facial	Comité Europeo de Protección de Datos	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_es
Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción	AEPD	https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf
Futuro Código de Conducta sobre Inteligencia Artificial (voluntario) EEUU EU	EEUU – EU	https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/31/u-s-eu-joint-statement-of-the-trade-and-technology-council-2/

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

Participantes en el grupo de trabajo que han elaborado este documento

Coordinador del grupo de trabajo:

- Castilla, Yolanda
- Hurtado, Alonso

Participantes (por orden alfabético):

- Baradat, Ramón
- García, Jorge
- Garzón, Fuencisla
- Santillán, Ana
- Trepat, Alicia
- Túnez, Alba
- Usó, Cristina

© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

Asociación
Española
de Compliance