TÍTULO

LA BIOMETRÍA Y LA PROTECCIÓN DE DATOS

AUTOR

Mariano Nicolás Peláez Bartolomé

Esta edición electrónica ha sido realizada en 2025

Directora	Dra. Susana Ruiz Tarrías
Institución	Universidad Internacional de Andalucía
Curso	*Diploma de Especialización en Protección de Datos en la Sociedad Digital (2022-23)*
©	Mariano Nicolás Peláez Bartolomé
©	De esta edición: Universidad Internacional de Andalucía
Fecha documento	2023

LA BIOMETRIA Y LA PROTECCION DE DATOS

DIPLOMA DE ESPECIALIZACIÓN PROTECCIÓN DE DATOS EN LA SOCIEDAD DIGITAL II EDICIÓN (2022)

Alumno: Mariano Nicolás Peláez Bartolomé

Director: Pfra. Susana Ruiz Tarrías. Profesora Titular de Derecho Constitucional. UGR.

Universidad Internacional de Andalucía, 2025

Resumen: La biometría es la medición estadística y matemática de características físicas o biológicas únicas con fines de identificación. En ciberseguridad, la definición de biometría se refiere al uso de características biológicas únicas para la autenticación digital y el control de acceso. Los datos biométricos es un procedimiento destinado facilitar y garantizar la correcta identificación de las características únicas de cada persona.

Palabras clave: Biometría, RGPD, LOPD, huella dactilar, reconocimiento facial, iris, escritura, proteccion datos, autenticación, doble factor, geometría de la mano, retina, vascular, comportamiento, firma, voz, escritura,escritura de teclado, form de andar, datos de categoría especial, AEPD, convención 108, dictamen 3/2012, inteligencia artificial, riesgo aceptable, alto riesgo.

Abstract: Biometrics is the statistical and mathematical measurement of unique physical or biological characteristics for identification purposes. In cybersecurity, the definition of biometrics refers to the use of unique biological characteristics for digital authentication and access control. Biometric data is a procedure designed to facilitate and guarantee the correct identification of the unique characteristics of each person.

Keywords: Biometrics, RGPD, LOPD, fingerprint, facial recognition, iris, writing, data protection, authentication, two-factor, hand geometry, retina, vascular, behavior, signature, voice, writing, keyboard typing, gait, data special category, AEPD, convention 108, opinion 3/2012, artificial intelligence, acceptable risk, high risk.

ÍNDICE

1. Introducción.

Ante todo debemos partir de la definición de biometría contemplada en el [1]RGPD en su artículo 4.14 como aquellos *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* por lo tanto, se trata de un método mediante el cual se procede a la identificación de una persona, haciendo uso de algún rasgo fisiológico o de una pauta de comportamiento.

Según la ISO 2382-37, la biometría es "el reconocimiento automático de los individuos en función de sus características biológicas y de comportamiento"

A su vez el art 9.1 del RGPD incluye entre los **datos de categoría especial** aquellos "*datos biométricos dirigidos a identificar de manera unívoca a una persona física*".

A eso, debemos tener en cuenta que los datos de categoría especial de conformidad con el RGPD se exige una garantía reforzada. El Reglamento requiere la existencia de un interés público especial. El interés público esencial como base de legitimación requiere de una norma con rango de ley. Si no existe norma que lo contemple, se exigiría una especial justificación de la necesidad a fin de poder emplear ese dato biométrico.

Con respecto a esta clasificación como datos de categoría especial debemos acudir al considerando 51 del RGPD el cual señala que "…***no debe considerarse sistemáticamente tratamiento de categoría 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*".

Del mismo modo, según la [2]**AEPD**, "*en una interpretación conjunta de ambos preceptos* **parece dar a entender que los datos biométricos solo constituirían una categoría especial de datos en el caso de que se sometan a un tratamiento técnico especifico dirigido a identificar de manera univoca a una persona física".**

En consecuencia, todo tratamiento de datos personales (sensibles o no), requiere en primer lugar que se cumpla alguna de las bases de legitimación recogidas en el artículo 6 del RGPD. Entre estas bases podemos encontrar el consentimiento del interesado, la ejecución de un contrato, el cumplimiento de una obligación legal, la protección de intereses vitales, el cumplimiento de una misión realizada en interés público o la satisfacción de intereses legítimos.

[1] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

[2] La Agencia Española de Protección de Datos, creada en 1992, es el organismo público encargado de velar por el cumplimiento de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales en España.

2. Las tecnologías biométricas: Aproximación conceptual y antecedentes.

Al objeto de aclarar las dudas interpretativas, la AEPD atiende al [3]Dictamen 3/2012 sobre la evolución de las tecnologías biométricas del Grupo del Artículo 29, en el que se distingue:

Identificación biométrica: la identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno-a-varios). Se comprueba si un individuo particular es uno de los miembros de un grupo predeterminado, comparándose sus datos con los datos de todos los integrantes de ese grupo. Por ejemplo, se toma una nueva imagen facial de la persona y se compara contra todas imágenes faciales existentes en una determinada base de datos; si la nueva imagen coincide con alguna de las registradas, la persona es "identificada" como un usuario preexistente y se le concederán los permisos o derechos asociados a dicha identidad.

Verificación/autenticación biométrica: la verificación de un individuo por un sistema biométrico es normalmente el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo. Se comprueba si una persona es quien dice ser, comparándose sus datos únicamente con otros datos asociados a la identidad en cuestión. Por ejemplo, se toma una nueva imagen facial de la persona y se compara con otra imagen facial previamente registrada; si ambas coinciden, la persona es "verificada" o "autenticada" y se le concederán los permisos o derechos asociados a dicha identidad.

La AEPD indica que, atendiendo a la citada distinción, puede interpretarse que, de acuerdo con el artículo 4 del RGPD, el concepto de dato biométrico incluiría ambos supuestos, tanto la identificación como la verificación o autenticación. Sin embargo, y según la AEPD, **con carácter general, los datos biométricos únicamente tendrán la consideración de categoría especial de datos en los supuestos en que se sometan a tratamiento técnico dirigido a la identificación biométrica (uno-a-varios) y no en el caso de verificación o autenticación biométrica (uno-a-uno), caso de [4]Biometric Vox.**

A la hora de proceder a la identificación biométrica se pueden emplear distintas técnicas, algunas de forma simultánea, y, a su vez, una misma técnica se puede implementar de formas diferentes. Las operaciones con datos biométricos en un tratamiento concreto tendrán un grado distinto de intrusión e impacto en la privacidad de los individuos que dependerá de la técnica empleada, pero también de la propia definición del tratamiento, su naturaleza, el ámbito o alcance en el que se va a desarrollar, su contexto y, en especial, los fines que se persiguen.

---

[3] Dictamen 3/2012 sobre la evolución de las tecnologías biométricas
https://www.aepd.es/sites/default/files/2019-12/wp193_es.pdf

[4] Empresa de soluciones biométricas de voz
https://biometricvox.com/biometric-vox-empresa/

Las técnicas de proceso de datos biométricos se basan en recoger y procesar rasgos físicos, conductuales, fisiológicos o neuronales de las personas mediante dispositivos o sensores, creando firmas o patrones que posibilitan la identificación, seguimiento o perfilado de las personas. Algunos métodos requieren la cooperación de la persona, mientras que otros métodos pueden capturar datos biométricos a distancia, sin requerir la cooperación del individuo y sin que pueda tener conciencia de ello.

3. Tecnologías aplicadas a la biometría.

La biometría usada como forma única de autenticación o combinada con otras medidas (tarjetas Inteligentes, claves de cifrado o firmas digitales). A su vez podemos hacer una clasificación más específica de las distintas técnicas biométricas en tres categorías, que son:

- Dinámicas: Utilizan tecnologías de comportamiento que compraran acciones o movimiento.
- Estáticas: Utilizan tecnologías fisiológicas que miden y comparan rasgos físicos.
- Multimodales: Combinan técnicas estáticas y dinámicas.

Sin duda, la implementación de medidas de control y acceso biométrico presenta una serie de ventajas para aquellos organismos o empresas, tales como:

Aumento de la seguridad en el control de acceso, al tratarse de rasgos únicos y de imposible duplicación, ya que los rasgos están unidos de forma exclusiva a su legítimo usuario. A diferencia de tarjetas de acceso, que se puede extraviar o prestar para su uso y permitir el acceso a una determinada area, los rasgos biométricos son únicos y exclusivos, garantizando el acceso solo y exclusivamente a aquella persona que está autorizada y cuyos datos constan en una base de datos.

La implantación de tecnologías biométricas contribuye a que una empresa sea más eficiente, más segura y reduzca el fraude interno.

Tramitaciones remotas, esto implica que al usar dispositivos móviles se puede llevar a cabo una identificación mediante varios sistemas biométricos (video, voz, huella dactilar). Por ejemplo, a administración durante la pandemia uso este sistema para poder llevar a cabo la tramitación de los certificados digitales y así evitar desplazamientos innecesarios. Toda la tramitación se realizaba mediate los móviles a través de un sistema de doble factor de autentificación, mediante videollamada y muestra de DNI a fin de comprobar la identidad del solicitante. Son tramites que se dieron durante la pandemia y que con el impulso de la administración electrónica han venido para quedarse. Téngase en cuenta que todos estos trámites son potestativos no exclusivos, ya que de conformidad con el art. 14 de la [5]ley 39/2015 en las comunicaciones del administrado con la

[5] Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

administración puede escoger libremente el sistema mediante el cual puede dirigirse a ella, pudiendo cambiarlo el administrador en cualquier momento.

Aumento de la Seguridad: Es la consecuencia de usar medio biométricos, al tratarse de características únicas aumenta la dificultad de la falsificación de los datos biométricos con el objetivo de acceder a datos personales de un usuario final.

3.1. Técnicas biométricas fisiológicas

Las tecnologías biométricas fisiológicas se caracterizan por considerar parámetros derivados de la medición directa de algún rasgo estrictamente físico del cuerpo humano a la hora de identificar personas.

a) **Huella dactilar**: Hace uso de las huellas dactilares, las cuales son únicas e inalterables. Es el sistema más usado para autenticación. Alta precisión y facilidad de uso, y es NO INVASIVA.
b) **Facial**: hace uso del rostro de la persona, hay que tener en cuenta que va cambiando con la edad.
c) **Iris**: Usa las características del iris humano.
d) **Geometría de la mano**: Utiliza la forma de la mano para confirmar la identidad del individuo. No fiable por alteraciones por lesión.
e) **Retina**: Basado en los vasos sanguíneos de la retina. No varía, es bastante fiable, se usa una cámara de infrarrojos.
f) **Vascular**: Patrón biométrico a partir de la geometría del árbol de las venas del dedo. Es un método muy difícil el robo de la identidad.
g) **Otras formas**.

3.2. Tecnologías biométricas de comportamiento

Las tecnologías biométricas de comportamiento se caracterizan por considerar en el proceso de identificación rasgos derivados de una acción (al escribir, al caminar, etc.) realizada por una persona. Por tanto, incluyen la variable tiempo, ya que toda acción tiene un comienzo, un desarrollo y un final.

a) **Reconocimiento de firma**: Analiza la firma manuscrita para confirmar la identidad del firmante.

b) **Reconocimiento de escritor**: Análisis de escritura.
c) **Reconocimiento de voz**.
d) **Reconocimiento de escritura de teclado**: Patrón de escritura de teclado.
e) Reconocimiento de forma de andar.

Técnicas biometricas fisiologicas:

a) HUELLA DACTILAR:

La primera referencia del uso de la huella dactilar como medida de seguridad la tenemos en los años 70 en la empresa de Wall Street Shearson Hamill instaló [6]**Identimat**, un sistema de identificación automática basado en huella dactilar que se utilizó para el control de acceso físico a instalaciones, siendo la primera solución biométrica de uso comercial.

La huella dactilar es la antigua de las técnicas biométricas y ha sido utilizada en un gran número de aplicaciones debido a que se considera que las huellas dactilares son únicas e inalterables. La huella presenta una alta tasa de precisión (se considera una tecnología madura) y fácil de usar. A la hora de buscar coincidencias en la huella dactilar existen dos vías:

Basada en minucias: Identifica determinadas formas fácilmente identificables presentes en la huella dactilar del individuo a identificar. Una vez localizadas esas minucias se hacen una serie de mediciones obteniendo una plantilla para cada individuo.

No obstante, existen algunas dificultades asociadas a este método. Por un lado, no es sencillo extraer de forma precisa las mencionadas minucias cuando la calidad de la muestra no es buena. Por otro lado, no se tiene en cuenta el patrón global de crestas y surcos.

Basada en correlación: Esta técnica analiza el patrón global seguido por la huella dactilar, se centra en el conjunto de la huella y no en las minucias. Esta técnica requiere un registro preciso, pero su principal inconveniente es que se ve afectada por la traslación y la rotación de la imagen.

b) RECONOCIMIENTO FACIAL

El reconocimiento facial es un sistema mediante el cual se reconoce a una persona a partir de una imagen o Para ello, se utilizan programas de calculo que analizan de rostros humanos. Entre los aspectos clave empleados para la se encuentran mediciones como la distancia entre los ojos, la longitud de la nariz o el ángulo de la mandíbula.

A diferencia de otros sistemas el reconocimiento facial puede ser utilizado para la vigilancia general, habitualmente mediante de video. Este sistema se puede ver afectado por las

[6] El sistema Identimat 2000 fue usado como un escaner biométrico por el gobierno de los Estados Unidos en sus instalaciones militares en la decada de los de 70 y los 80. Funciona midiendo y verificando la goemtria de la mano para conceder el acceso. Este sistema se pudo ver en la película Encuentros en la tercera fase.

modificaciones en el rostro como llevar barba, gafas de sol, etc.… A pesar de estos inconvenientes el reconocimiento facial ha podido distinguir entre personas reales y la fotografía, pero el verdadero retro estará con la aparición de la Inteligencia Facial en el que no se podrá distinguir o será muy difícil distinguir entre una persona real y un avatar generado por I.A.

c) RECONOCIMIENTO DE IRIS

Utiliza las características del iris humano para poder identificar a la persona. Los patrones del iris vienen marcados desde el nacimiento, raramente cambian y son extremadamente complejos, contienen más de 200 propiedades únicas.

d) RECONOCIMIENTO DE LA GEOMETRIA DE LA MANO

Esta utiliza la forma de la mano para confirmar la identidad del individuo. Mediante una cámara se realizan varias capturas de la mano desde distintos ángulos. Entre las características extraídas se incluyen las curvas de los dedos, su grosor y longitud, la altura y la anchura del dorso de la mano

e) RECONOCIMIENTO DE RETINA

Se basa en el mapeado de los vasos sanguíneos de la retina, dicho patrón es único e inalterable, por lo que es el método perfecto para entornos de alta seguridad.

f) RECONOCIMIENTO VASCULAR

Se basa en el mapeado del árbol de las venas del dedo o de la muñeca. Al tratarse de algo interno es imposible el robo de identidad. Se recomienda el uso de este sistema biométrico para entornos de alta seguridad.

g) OTRAS FORMAS:

Existen otras técnicas de identificación biométrica de carácter fisiológico, pero que a día de hoy son novedosas y poco maduras, entre ellas podemos enumerar las siguientes.

1. Líneas de la palma de la mano.
2. Forma de las orejas.
3. Piel, superficie dérmica.
4. ADN, patrones basados en el genoma.
5. Composición química del olor corporal.

Tecnologias biometricas de comportamiento

a) RECONOCIMIENTO DE FIRMA

Esta técnica analiza la firma manuscrita para confirmar la identidad del usuario firmante. Existen dos variantes a la hora de identificar a las personas según su firma:

Comparación simple: Se considera el grado de parecido entre dos firmas, la original y la que está siendo verificada.

Verificación dinámica: Se hace un análisis de la forma, la velocidad, la presión de la pluma/bolígrafo y la duración del proceso de firma. No se considera significativa la forma o el aspecto de la firma, sino los cambios en la velocidad y la presión que ocurren durante el proceso, ya que sólo el firmante original puede reproducir estas características.

b) RECONOCIMIENTO DE ESCRITOR

El objetivo del reconocimiento de escritor es averiguar o confirmar la identidad del autor de un determinado texto manuscrito valiéndose de un software [7]OCR (o reconocimiento óptico de caracteres). Cada persona tiene una forma de escribir diferente, teniendo rasgos propios e inconfundibles para cada letra. Asimismo, cada persona tiene un grado de inclinación en la escritura y nivel de presión al escribir. Uniendo todos estos datos, un software de reconocimiento de escritor puede ser capaz de detectar la persona que está escribiendo un texto manuscrito.

c) RECONOCIMIENTO DE VOZ:

Se basa en Inteligencia Artificial (redes neuronales) para aprender a identificar voces. La identificación se complica debido a factores como el ruido de fondo, por lo que siempre es necesario considerar un margen de error.

La utilización de este método está más extendida en sistemas de respuesta por voz y en centros de atención de llamadas telefónicas (call centers) que en el control de acceso físico a edificios o a redes y equipos informáticos.

d) RECONOMIENTO DE ESCRITURA DE TECLADO

Esta técnica se basa en el hecho de la existencia de un patrón de escritura en teclado que es permanente y propio de cada individuo. De este modo, se mide la fuerza de tecleo, la duración de la pulsación y el periodo de tiempo que pasa entre que se presiona una tecla y otra.

[7] El reconocimiento óptico de caracteres (ROC), generalmente conocido como reconocimiento de caracteres y expresado con frecuencia con la sigla OCR (del inglés Optical Character Recognition), es un proceso dirigido a la digitalización de textos, los cuales identifican automáticamente a partir de una imagen símbolos o caracteres que pertenecen a un determinado alfabeto, para luego almacenarlos en forma de datos. Así podremos interactuar con estos mediante un programa de edición de texto o similar.

e) **RECONOCIMIENTO DE LA FORMA DE ANDAR**

Este método toma como referencia la forma de caminar de una persona. Este acto se graba y se somete a un proceso analítico que genera una plantilla biométrica única derivada de dicho comportamiento.

Esta tecnología está todavía en desarrollo y no ha alcanzado aún los niveles de rendimiento necesarios para ser implantada de manera similar al resto de tecnologías biométricas.

4. La regulación jurídica de los datos biométricos

4.1. Los datos biométricos como datos sensibles en el RGPD y la LOPDGDD.

La definición de biometría contemplada en el **RGPD** en su artículo 4.14 establece que se trata de aquellos *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* por lo tanto, se trata de un método mediante el cual se procede a la identificación de una persona, haciendo uso de algún rasgo fisiológico o de una pauta de comportamiento.

Según la ISO 2382-37, la biometría es "el reconocimiento automático de los individuos en función de sus características biológicas y de comportamiento"

A su vez el art 9.1 del RGPD incluye entre los **datos de categoría especial** aquellos "*datos biométricos dirigidos a identificar de manera unívoca a una persona física*".

A eso debemos tener en cuenta que los datos de categoría especial de conformidad con el RGPD se exige una garantía reforzada. El Reglamento requiere la existencia de un interés público especial. El interés público esencial como base de legitimación requiere de una norma con rango de ley. Si no existe norma que lo contemple, se exigiría una especial justificación de la necesidad a fin de poder emplear ese dato biométrico.

Con respecto a esta clasificación como datos de categoría especial, debemos acudir al considerando 51 del RGPD el cual señala que "…***no debe considerarse sistemáticamente tratamiento de categoría 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*".

Asimismo, según la **AEPD**, "*en una interpretación conjunta de ambos preceptos* **parece dar a entender que los datos biométricos solo constituirían una categoría especial de datos en el caso de que se sometan a un tratamiento técnico especifico dirigido a identificar de manera univoca a una persona física".**

Otra referencia legislativa se podría encontrar en la [8]LOPDGDD, pero apenas se hace referencia a los datos biométricos en la protección de datos y solo los menciona en las disposiciones adicionales relativas a datos relacionados con la salud.

A lo que sí hace referencia en su artículo 9, es a las categorías especiales de datos, señalando que «el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico».

Por su parte, la disposición final undécima matiza que «si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley».

La base jurídica para poder tratar datos biométricos la encontramos en el artículo 9 del RGPD:

1. Por consentimiento explícito del interesado.
2. Para proteger el interés vital del interesado cuando este se encuentre incapacitado tomar decisiones.
3. Cuando sea necesario para el cumplimiento de obligaciones establecidas o para llevar a cabo los derechos de la protección de datos.
4. Si esos datos son públicos y han sido publicados por el interesado.
5. Por interés público esencial siempre que sea proporcional al objetivo perseguido.
6. Y también con fines de medicina preventiva, cuestiones sociales o para evaluar las capacidades del trabajador.

4.2. Consideración internacional de los datos biométricos:

a) Informe de la aplicación de la Convención 108 a la recogida y al proceso de los datos biométricos del Comité Consultivo del Consejo de Europa 2005.

El [9]Convenio n.º 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal fue el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos. Tiene como fin garantizar a cualquier persona física el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona. Con el Protocolo

[8] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
[9] https://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion-de-los-datos-personales

que ha modificado el Convenio se pretende ampliar su ámbito de aplicación, aumentar el nivel de protección de los datos y mejorar su eficacia.

En 1981 el Consejo de Europa emite el primer texto normativo vinculante, el Convenio 108 de 28 de enero de Estrasburgo, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (en adelante, Convenio o Convención 108).

La denominada "Convención 108" se encuentra en vigor tras la actualización realizada por el propio Consejo de Europa, mediante el Protocolo de 18 de mayo de 2018.El objetivo ha sido adaptarse al Reglamento 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

El Convenio 108 es el único tratado internacional que aborda el derecho de las personas a la protección de sus datos personales, y está abierto a la firma y ratificación de cualquier país. Las partes actuales de la Convención son los 47 Estados miembros del Consejo de Europa, más Mauricio, Senegal, Túnez y Uruguay, mientras que Argentina, Burkina Faso, Cabo Verde, México y Marruecos han sido invitados a adherirse al tratado. Asimismo, es utilizado como modelo para la legislación de protección de datos.

El Consejo de Europa (Council of Europe) ha publicado un documento llamado: "Informe de situación relativo a la aplicación de los principios de la convención 108 sobre la recogida y al proceso de los datos biométricos", el informe contiene una serie de pronunciamientos respecto a los datos biométricos y su uso. A continuación, se presenta la idea básica de cada punto:

1. Los datos biométricos deben ser considerados como una categoría específica de datos, ya que estos siguen siendo los mismos en distintos sistemas y son inalterables de por vida.
2. Antes de recurrir a la biometría, se deben evaluar: las finalidades previstas para los datos, las ventajas contra los inconvenientes que afecten la vida privada de la persona involucrada, y se deben tener posibles soluciones alternativas que supongan un menor atentado contra la privacidad.
3. No se debería optar por la biometría únicamente por el hecho de que su uso resulte práctico.
4. Los datos biométricos deben ser utilizados con fines determinados, explícitos y legítimos. No deben ser procesados de manera incompatible con esas finalidades.
5. Los datos deberían ser adecuados, pertinentes y no excesivos en comparación con la finalidad del proceso; si basta con patrones, se debería evitar el almacenamiento de la imagen biométrica.
6. A la hora de elegir la estructura del sistema, se debería proceder teniendo en mente los aspectos de seguridad.
7. La estructura de un sistema biométrico no debería ser desproporcionada respecto a la finalidad del proceso; si basta con la verificación, no se debería desarrollar una solución de identificación.
8. La persona afectada debería ser informada de la finalidad del sistema y de la identidad del responsable del proceso. Además, conocer los datos procesados y las categorías de personas a las que se comunicarán esos datos.

9. La persona afectada tiene derecho de acceso, rectificación, bloqueo y cancelación de sus datos.
10. Se deben prever medidas, técnicas y organizativas, que sean adecuadas para proteger los datos biométricos contra la destrucción y la pérdida accidental, también se deben proteger contra el acceso, modificación o comunicación no autorizada y deben ser resguardados de cualquier otra forma de procesamiento ilícito.
11. Se debería desarrollar un procedimiento de certificación y de control, con el fin de establecer normas de calidad para el software y la formación del personal responsable del registro y la verificación de datos biométricos. Se recomienda una auditoría periódica que pruebe las cualidades técnicas del sistema.
12. Si una persona, registrada en un sistema biométrico, es rechazada, el responsable de proceso debería, a petición de ésta, volver a examinar el caso y si fuese preciso, ofrecerle soluciones de sustitución adecuadas.

b) Dictamen 3/2012, sobre la evolución de las tecnologías biométricas, del Grupo de Trabajo del Art. 29.

El Dictamen 3/2012 del grupo de trabajo del artículo 29 de la UE sobre la evolución de las tecnologías biométricas estableció los requisitos que se deberían cumplir para que un sistema biométrico se considerase adecuado y proporcional para la finalidad pretendida.

En el caso del uso de sistemas biométricos para el cumplimiento de la obligación de registro diario de jornada, el margen para su aplicación y utilización es mínimo o nulo, debiendo tenerse en cuenta:

1) La necesidad del sistema, esto es, que sea esencial para satisfacer la necesidad. La biometría no es necesaria para responder a esa necesidad de que sea esencial

2) La eficacia del sistema para responder a la necesidad teniendo en cuenta para ello la tecnología empleada. EXISTE TECNOLOGÍA QUE NO ES INVASIVA.

3) Si la pérdida de intimidad que resulta de la utilización del sistema es proporcional a los beneficios del mismo. NO, LA PERDIDA DE INTIMIDAD NO APORTA BENEFICIOS.

4) Si el uso de medios menos lesivos alcanzaría la misma finalidad. SI, EXISTEN MEDIOS MENOS LESIVOS.

Por lo tanto es evidente que para llevar a cabo el registro de jornada existen sistemas digitales que aplican el principio de minimización y no requieren de datos biométricos para conseguir el objetivo.

4.3. Regulación Europea de la Inteligencia Artificial y la biometría.

En abril de 2021, la Comisión propuso el primer marco regulador de la UE para la [10]IA. Propone que los sistemas de IA que puedan utilizarse en distintas aplicaciones se analicen y clasifiquen según el riesgo que supongan para los usuarios. Los distintos niveles de peligro implicarán una mayor o menor regulación.

La prioridad del Parlamento es garantizar que los sistemas de IA utilizados en la UE sean seguros, transparentes, trazables, no discriminatorios y respetuosos con el medio ambiente. Los sistemas de IA deben ser supervisados por personas, en lugar de por la automatización, para evitar resultados perjudiciales. La intención de regularizar la IA por parte de la UE está en el hecho de que podemos estar ante una revolución industrial por lo que el crecimiento y desarrollo economico de la UE dependerá en gran medida del uso e intercambio de datos y de las tecnologías.

El Parlamento también quiere establecer una definición uniforme y tecnológicamente neutra de la IA que pueda aplicarse a futuros sistemas de IA. La nueva normativa establece obligaciones para proveedores y usuarios en función del nivel de riesgo de la IA. Aunque muchos sistemas de IA plantean un riesgo mínimo, es necesario evaluarlos todos.

Riesgo inaceptable

Los sistemas de IA de riesgo inaceptable son los que se consideran una amenaza para las personas y serán prohibidos. Incluyen:

1. manipulación cognitiva del comportamiento de personas o grupos vulnerables específicos: por ejemplo, juguetes activados por voz que fomentan comportamientos peligrosos en los niños.
2. puntuación social: clasificación de personas en función de su comportamiento, estatus socioeconómico o características personales.
3. sistemas de identificación biométrica en tiempo real y a distancia, como el reconocimiento facial.

Aunque existen algunas excepciones a esta calificación. Por ejemplo, los sistemas de identificación biométrica a distancia "a posteriori", en los que la identificación se produce tras un retraso significativo, se permitirán para perseguir delitos graves y sólo cuando haya previa aprobación judicial.

Alto riesgo

Los sistemas de IA que afecten negativamente a la seguridad o a los derechos fundamentales se

[10] La inteligencia artificial (IA), en el contexto de las ciencias de la computación, es una disciplina y un conjunto de capacidades cognoscitivas e intelectuales expresadas por sistemas informáticos o combinaciones de algoritmos cuyo propósito es la creación de máquinas que imiten la inteligencia humana para realizar tareas, y que pueden mejorar conforme recopilen información.

considerarán de alto riesgo y se dividirán en dos categorías.

1. Los sistemas de IA que se utilicen en productos sujetos a la legislación de la UE sobre seguridad de los productos. Esto incluye juguetes, aviación, automóviles, dispositivos médicos y ascensores.
2. Los sistemas de IA pertenecientes a ocho ámbitos específicos que deberán registrarse en una base de datos de la UE:

- Identificación biométrica y categorización de personas físicas.
- Gestión y explotación de infraestructuras críticas.
- Educación y formación profesional.
- Empleo, gestión de trabajadores y acceso al autoempleo.
- Acceso y disfrute de servicios privados esenciales y servicios y prestaciones públicas.
- Aplicación de la ley.
- Gestión de la migración, el asilo y el control de fronteras.
- Asistencia en la interpretación jurídica y aplicación de la ley.

Todos los sistemas de IA de alto riesgo serán evaluados antes de su comercialización y a lo largo de su ciclo de vida.

IA generativa

La IA generativa, como ChatGPT, tendría que cumplir requisitos de transparencia:

- Revelar que el contenido ha sido generado por IA.
- Diseñar el modelo para evitar que genere contenidos ilegales.
- Publicar resúmenes de los datos protegidos por derechos de autor utilizados para el entrenamiento.

Riesgo limitado

Los sistemas de IA de riesgo limitado deben cumplir unos requisitos mínimos de transparencia que permitan a los usuarios tomar decisiones con conocimiento de causa. Tras interactuar con las aplicaciones, el usuario puede decidir si desea seguir utilizándolas. Los usuarios deben ser conscientes de cuándo están interactuando con la IA. Esto incluye los sistemas de IA que generan o manipulan contenidos de imagen, audio o vídeo (por ejemplo, deepfakes).

Con respecto a esta materia durante las Jornadas del [11]CCN CERT de 2022 en Madrid tuve la ocasión de asistir a la conferencia impartida por Chema Alonso, popularmente conocido como el Hacker de Telefónica, bajo el título Humanos Sintéticos con Inteligencia Artificial, en la misma se centraba en la creación de deepfakes y como estos podrían dar lugar a lo que el llamo ataque al

[11] El Centro Criptológico Nacional Computer Emergency Response Team, también conocido por su sigla CCN–CERT, es el organismo español, creado en 2006, encargado de contribuir a la ciberseguridad de la administración pública, los organismos públicos y empresas estratégicas del país

CEO, básicamente suplantar a una persona, en el 2019 hicieron la prueba de como con una webcam virtual podían copiar la imagen de una persona y hacer creer que estaban hablando con esa persona sin que se diera cuenta el otro interlocutor de que estaba hablando con una IA. La única manera de combatir esto es mediante algoritmos de machine learning basados en faceforensics (Repositorios) a fin de poder detectar cualquiera de las variantes que pueden darse.

Tengamos en cuenta que la IA permite el desarrollo de una nueva generación de productos y servicios, incluso en sectores en los que las **empresas** europeas ya tienen posiciones sólidas.

5. Gestión de riesgos de los datos biométricos:

5.1. Amenazas y vulnerabilidades en los procesos de identificación biométricos.

Desventajas de la autenticación biométrica

A pesar del aumento de la seguridad, la eficacia y la comodidad, la autenticación biométrica y sus usos en las aplicaciones digitales y tecnológicas actuales también tienen desventajas:

- Costes. Es necesario hacer una inversión significativa en biometría para seguridad.
- Violación de datos. Las bases de datos biométricas pueden ser hackeadas.
- Monitorización y datos. Los dispositivos biométricos, como los sistemas de reconocimiento facial, pueden limitar la privacidad de los usuarios.
- Sesgo. El aprendizaje automático y los algoritmos tienen que ser muy avanzados para minimizar el sesgo demográfico biométrico.
- Positivos falsos e imprecisiones. Es posible que ocurran falsos rechazos y falsas aceptaciones que impidan a los usuarios acceder al sistema.

Costes

Como es lógico, un sistema de seguridad más avanzado requiere más inversión y su implementación tiene más costes. En 2018, en una encuesta hecha por Spiceworks, el 67% de los profesionales de IT afirmaba que los costes son «la razón principal por la que no adoptan la autenticación biométrica». La transición a la autenticación biométrica no sería la única cosa por la que la empresa tendría que pagar. El 47% de los encuestados afirmaba que es necesario actualizar los sistemas actuales para poder integrar la autenticación biométrica en sus dispositivos.

Violación de datos

Las empresas y los gobiernos que recogen y almacenan datos personales de los usuarios están bajo la constante amenaza de los hackers. Como los datos biométricos no son reemplazables, las organizaciones necesitan tratar los datos biométricos sensibles con seguridad y precaución. Algo que es caro y difícil a nivel técnico, para estar un paso por delante de los intentos de fraude. Si una

contraseña o PIN han estado expuestos, siempre existe la posibilidad de cambiarlos. No puede decirse lo mismo de los datos biométricos conductuales o fisiológicos de una persona.

Monitorización y datos

A medida que el mundo empieza a usar sistemas de autenticación biométrica como la tecnología de reconocimiento facial y otras medidas de seguridad biométricas, es necesario tener en cuenta la seguridad de los usuarios. Cuando los datos biométricos se convierten en datos y se almacenan, especialmente en lugares o países que tienen medidas de vigilancia muy estrictas, el usuario corre el riesgo de dejar un registro digital que puede ser monitorizado por agentes maliciosos. Las organizaciones y gobiernos han usado software de reconocimiento facial para monitorizar e identificar a personas con una precisión estremecedora que limita la privacidad de manera significativa. A medida que la vigilancia aumenta, los datos biométricos pueden convertirse en una etiqueta digital permanente que puede usarse para monitorizar a las personas, con o sin su conocimiento.

Sesgo

Minimizar el sesgo demográfico en biometría al mismo tiempo que verifican la identidad de los solicitantes durante el onboarding digital es un reto para los proveedores. La implementación deficiente de esta tecnología o hacer mal uso de ella de manera deliberada pueden resultar en discriminación y exclusión. Sin una solución verificada para la comprobación de identidad basada en documentos de identificación, el desempeño demográfico cruzado puede ser poco fiable y limitar el acceso de los clientes a servicios esenciales como créditos y a una amplia gama de servicios digitales.

Falsos positivos e imprecisiones

Los métodos de autenticación biométrica más comunes dependen de información parcial para autenticar la identidad del usuario. Por ejemplo, un dispositivo móvil biométrico puede escanear una huella digital completa durante la fase de registro y convertirla en datos. Sin embargo, la autenticación biométrica de la huella digital del futuro solo usará partes de las impresiones para verificar la identidad, por lo que es más rápida. En 2018, un grupo de investigadores de la Universidad de Nueva York creó una plataforma de inteligencia artificial que consiguió quebrar la autenticación con huella digital de manera fraudulenta, con una tasa de éxito del 20%, haciendo coincidir las similitudes de huellas parciales con los datos biométricos completos.

Claramente los sistemas basados en biometría generan una seguridad superior frente a los sistemas tradicionales de control de acceso o de check-in de credenciales. No obstante, hay sistemas más seguros que otros. El sistema de huella dactilar digamos que es la tecnología más madura, frente a otros como el reconocimiento facial o la voz que se ven amenazadas su fiabilidad y seguridad por la tecnología basada en inteligencia artificial, para que podamos entenderlo mejor, la inteligencia artificial es capaz de generar copias digitales de una persona y facilitar la suplantación de la misma, en situaciones como una charla vía webcam o para pasar el control de doble factor.
Otro riesgo que se puede dar es con respecto a la voz, ya que con plataformas como

[12]ElevenLabs.io se puede clonar la voz de una persona y proceder a suplantarla en una llamada telefónica y asi saltarse un control de acceso a una plataforma, un banco, por lo tanto, la voz como método biométrico ha dejado de ser valido.

En el 2014 se filtró en WikiLeaks un documento de la CIA en el que se exponía las preocupaciones por parte de los servicios de inteligencia de Estados Unidos hacia los sistemas biométricos que se iban a instaurar por parte de los países que formaban parte de la Unión Europea en sus aeropuertos y el riesgo que eso podría suponer para los agentes de inteligencia (Espías), los ciudadanos de Estados Unidos no necesitan aún dar datos biométricos, pero si se entra con una nacionalidad distinta, entonces el riesgo de su identidad crece, ya que los controles son mayores., aunque no se están utilizando como elemento de contra-inteligencia, sino como forma de control migratorio para detectar anomalías en la entrada y salida de personas.

5.2. Prevención y resolución de riesgos

5.2.1 Riesgos

La implantación y el empleo de tecnologías biométricas están expuestos a una serie de riesgos, además debemos tener en cuenta que hay ciertas tecnologías biométricas que cuentan con ciertas limitaciones.
Debemos pensar que los riesgos no son sólo exclusivos de la propia biometría, sino que también se pueden ver afectadas por la tecnología compartida con otras tecnologías de autenticación.

Entre los riesgos que pueden darse, están:

- **Pérdida o robo de información biométrica**: Son invariables y su confidencialidad es esencial. El robo de este tipo de información es extremadamente sensible (incidente de seguridad grave), ya que está vinculada al individuo.
- **Suplantación de identidad**: Implica el usar información biométrica robada o falsificada (Deepfake) para acceder a un espacio físico o virtual.
- **Sabotaje:** Ataques informáticos a los aparatos encargados de hacer la lectura y comprobación de los datos biométricos.
- **Incumplimiento de la normativa de protección de datos personales**: Los datos biométricos son datos de carácter personal, concretamente de categoría especial, por lo que su tratamiento tiene que ser acorde a lo establecido en la LOPD y en el RGPD.

Alguna de las herramientas para poder combatir los riesgos que pudieran tener las técnicas biométricas estaría en el caso de la imagen o video sería utilizar herramientas capaces de detectar *Face Swap*, *Face renaisance*, *Lipsync* o Imágenes generadas en tiempo real**. El *Chief Digital Officer* de Telefónica, el hacker Chema Alonso**, apunta que se debería de crear uno como el

[12] https://elevenlabs.io/ Compañía especializada en generación de voz por IA en mas de 20 idiomas.

[13]**Test de Empatía Voigh-Kampff,** así como el uso de un algoritmo de machine learning nutrido por el sistema Faceforensics de Google a fin de combatir estos deepfakes que pueden comprometer la seguridad de los métodos biométricos.

Las vulnerabilidades de cada método

Método	Vulnerabilidades
Huella dactilar	• condición del dedo en el momento de tomar la muestra: mojado, seco, manchado... • condiciones climatológicas que afectan al lector: humedad, temperatura, etc. • condiciones de la huella: cortes, heridas o inflamaciones • actividad laboral: trabajos que puedan afectar a la huella, por ejemplo, el uso habitual de productos químicos que puedan deteriorarla
Reconocimiento de voz	• enfermedades de la voz: bronquitis, faringitis, gripe, laringitis, afonías, etc. • variación entre el dispositivo de registro y el usado en la captura de muestras. • variación entre entornos de registro y captura de muestras (por ejemplo: interior y exterior). • volumen del habla
Reconocimiento facial	• variación en el aspecto facial: peinado, vello, gafas, sombrero, etc. • condiciones de luminosidad. • variación en el peso.

[13] La prueba o test Voight-Kampff, también llamado test de empatía, es un examen científico-psicológico ficticio que aparece en la novela de ciencia ficción ¿Sueñan los androides con ovejas eléctricas? de Philip K. Dick, así como en su adaptación cinematográfica Blade Runner.

	• uso de vestimenta que puede dificultar la localización o visión de la cara (pañuelos, bufandas, etc.)
Escáner de iris y retina	• excesivo movimiento ocular o de la cabeza. • enfermedades oculares. • uso de gafas. • problemas debidos al uso de lentes de contacto(iris)
Geometría de la mano	• uso de joyería, bisutería o abalorios. • uso de vendajes o guantes. • condiciones de la mano: inflamaciones. en las articulaciones, heridas, etc.
Escáner de firma	• velocidad de la firma: excesivamente rápida o lenta. • diferente postura del sujeto durante la firma: sentado o de pie. • firma no consistente: el sujeto varía su firma.

5.2.2 Resolución de riesgos

Para reducir los riesgos relacionados con el empleo de la biometría y ahcer una adecuado uso de los mismos, por ello deben adoptarse una serie de medidas:

- Reforzar la seguridad del sistema: Se debe garantizar la privacidad y evitar acceso no autorizados donde se encuentren los datos biométricos.
- Almacenamiento de muestras: Fraccionar el almacenamiento de las muestras biométricas, para los supuestos de utilización fraudulenta, pérdida o robo
- Autenticación de doble factor: Implicaría usar biometría bimodal (dos sistemas biométrico) o una combinación de un sistema biométrico junto a una contraseña o una tarjeta de

identificación (tecnología de [14]RFID o [15]NFC)
- Adquisición de tecnología de calidad.
- Formación de los usuarios: Los usuarios deben estar formados para un uso correcto de los mismos.
- Cumplimiento normativo.

6. Conclusiones.

La biometría es una de las mejores formas de autenticar usuarios, debido a que valida características inherentes al usuario y que teoricamente el único que puede tener tales características es el verdadero usuario.
En un sistema biométrico es particulamente importante revisar la seguridad de los procesos de captura y trasnferencia de la muestra biometrica, debido a que son los momentos mas susceptibles de ataques dentro del sistema de autenticación.
Por supuesto esos datos biométricos para que su uso sea acorde al RGPD y la LOPD, deben cumplir con algo tan básico como que dicho tratamiento sea lícito y se encuentre dentro de los supuestos contemplados en el art. 6 del RGPD (consentimiento del interesado, cumplimiento de una obligación legal, la protección de intereses vitales, el cumplimiento de una misión realizada en público o satisfacion de intereses legitimos).

Sin duda el sistema biométrico es una buena medida para regular el acceso a espacios físicos y virtuales siempre y cuando se cumpla con el ambito normativo y se cumplan los aspectos técnicos de seguridad que conlleva usar dichos sistemas, desde mi punto de vista es recomendable utilizar el doble factor de identificación, que impica usar dos sistemas de autenticación a fin de aumentar la seguridad en el control de acceso, recordemos que puede usarse un sistema bimodal biométrico (uso de dos sistemas biometricos como doble factor) o un sistema mixto, es decir, un primer factor biométrico seguido de un segundo factor mediante una tarjeta identificativa (RFID o NFC).

7. Bibliografia

Cuerpo Nacional de Policía, Sistema Automático de Identificación Dactilar – SAID

http://www.policia.es/org_central/cientifica/servicios/id_identificacion.html

CERTSI, Blog, «La problemática de la biometría como medio de autenticación»

https://www.certsi.es/blog/problematica-biometria-autenticacion

CERTSI, Blog, «Patrones biométricos y autenticación dinámica»

https://www.certsi.es/blog/autenticacion-dinamica

Modi, Shimon K., Artech House, 2011

[14] La Identificación por Radio Frecuencia (RFID) o tecnología RFID, es una tecnología que permite identificar objetos mediante ondas de radio de manera única y pudiendo captar cientos de objetos a la vez.
[15] Near-field communication o comunicación de campo cercano es una tecnología de comunicación inalámbrica, de corto alcance y alta frecuencia que permite el intercambio de datos entre dispositivos.

«Biometrics in Identity Management: Concepts to Applications»

Janin, A.K, et al, Springer, 2011,

«Introducction to biometrics»

A. K. Jain, R. Bolle and S. Pankanti (eds.),

«Biometrics: Personal Identification in a Networked Society»

Kluwer Academic Press, 1999.

M. Tapiador y J. A. Sigüenza (coord.)

«Técnicas biométricas aplicadas a la Seguridad»

Ra-Ma, 2005.

El reconocimiento biométrico: Fortalezas y debilidades. Raul Sanchez Reillo – Grupo Universitario de Tecnologias de la Identificación (GUTI) . Universidad Carlos III de Madrid.

14 equivocos con relación a la identificación y autenticacion biométrica. Junio 2020 AEPD.

[4] Agencia Española de Protección de Datos:

- Proporcionalidad del tratamiento de la huella dactilar de alumnos de un colegio. Informe 368/2006
- Tratamiento de la huella digital de los trabajadores.
- Resolución de archivo de actuaciones. Expediente Nº: E/00016/2007

https://www.europarl.europa.eu/news/es/headlines/priorities/inteligencia-artificial-en-la-ue/20200918STO87404/inteligencia-artificial-oportunidades-y-desafios

https://www.europarl.europa.eu/committees/es/aida/home/highlights

https://www.youtube.com/watch?v=0TiE6u__jDI

Chema Alonso (CDO Telefonica): Deepfakes y Técnicas de IA en Ciberseguridad | openclass UNIR

https://youtu.be/IxHWTz0oBCI

Convenio 108 del Consejo de Europa sobre la protección de datos de carácter personal