BORRA

GUÍA SOBRE TRATAMIENTOS EN EL CONTROL DE ACCESO MEDIANTE SISTEMAS BIOMÉTRICOS

v. mes de 2026

BORRADOR

ÍNDICE

1. Introducción 3
2. Definiciones 3
   2.1. Datos, características y sistemas biométricos 3
   2.2. Identificadores: referencias biométricas y de identidad 4
   2.3. Irreversibilidad, no vinculación y revocabilidad 4
   2.4. Registro biométrico. Almacenamiento de los datos biométricos 5
   2.5. Acceso biométrico: identificación y autenticación 5
3. Análisis legal 6
   3.1. Principio de proporcionalidad 6
      3.1.1. Idoneidad 6
      3.1.2. Necesidad 7
      3.1.3. Proporcionalidad en sentido estricto 8
   3.2. Categorías especiales de datos 9
      3.2.1. Excepción basada en el consentimiento 10
      3.2.2. Excepción autorizada por ley 10
   3.3. Licitud del tratamiento 11
   3.4. Decisiones automatizadas 11
4. Gestión del riesgo 12
   4.1. Evaluación de impacto relativa a la protección de datos 12
   4.2. Alto riesgo 13
   4.3. Superación del análisis de idoneidad, necesidad y proporcionalidad 14
   4.4. Implementación y contexto del tratamiento 14
   4.5. Garantías y medidas 15
      4.5.1. Organizativas 15
      4.5.2. Técnicas 16
   4.6. Brechas de datos personales 17
5. Acceso al entorno laboral. Registro de jornada 17
   5.1. Excepción del art. 9.2.b RGPD: Existencia de una norma de rango legal 18
   5.2. Licitud del tratamiento 19
   5.3. Subcontratación de trabajadores 19
6. Conclusiones 20

BORRADOR

1. INTRODUCCIÓN

El presente documento analiza los criterios para los tratamientos en el control de acceso mediante sistemas biométricos, de acuerdo con el 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, en adelante "RGPD").

Los sistemas biométricos y el tratamiento de los datos obtenidos a partir de ellos están evolucionando muy rápidamente. Los nuevos sistemas permiten recoger información con un mayor detalle y, a veces, sin la cooperación o el conocimiento de la persona. Estos datos biométricos se pueden recoger y usar de forma transversal entre múltiples servicios físicos y de Internet. Por último, el desarrollo de la Inteligencia Artificial (en adelante "IA") permite inferir información adicional sobre el sujeto mediante, incluso, categorías de datos sensibles.

Como consecuencia de esta evolución, se han producido cambios en el contexto normativo, social y tecnológico que hacen necesario revisar los criterios aplicables al tratamiento de datos biométricos y las garantías que pueden establecerse para asegurar el cumplimiento de la normativa de protección de datos.

Cuando los sistemas biométricos incorporen técnicas de inteligencia artificial, deberá tenerse en cuenta, además, la normativa europea en materia de inteligencia artificial, que puede establecer prohibiciones, limitaciones y obligaciones adicionales en función de las características, la finalidad y el contexto de utilización del sistema. La aplicación de esta normativa se entiende sin perjuicio del pleno cumplimiento del RGPD y del resto de las disposiciones aplicables en materia de protección de datos personales.

Este documento tiene carácter informativo, orientador y de apoyo al cumplimiento. No constituye una circular ni una disposición de carácter general, no introduce obligaciones nuevas ni modifica el contenido de las previstas en el RGPD, en la LOPDGDD o en otras normas aplicables. Su contenido refleja una síntesis de fuentes normativas, jurisprudenciales, resoluciones, informes y materiales técnicos disponibles en la fecha de su aprobación. Las referencias interpretativas incluidas en este documento no sustituyen el análisis jurídico del caso concreto ni predeterminan por sí solas el ejercicio de las potestades de investigación, supervisión o corrección de la Agencia, que se ejercerán de conformidad con la normativa aplicable a la vista de las circunstancias de cada expediente.

2. DEFINICIONES

2.1. DATOS, CARACTERÍSTICAS Y SISTEMAS BIOMÉTRICOS

El artículo 4.14) del RGPD define "datos biométricos" como *"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;"*[1].

En la definición se establece que los datos biométricos permiten la identificación o la autenticación de la identidad declarada por una persona. La diferencia entre estos dos términos se aborda más adelante (véase sección 2.5).

El término "característica biométrica"[2] se refiere a las características físicas (rostro, yema dactilar o palma de la mano, por ejemplo), fisiológicas (tono de la voz o actividad neuronal,

[1] El resaltado no está en el texto original.

BORRADOR

por ejemplo) o conductuales (forma de hablar, de escribir o de caminar, por ejemplo) de una persona física. En el ámbito del control de acceso mediante datos biométricos, las características físicas suelen ser las más tratadas habitualmente.

Los sistemas de procesamiento de datos biométricos se basan en recoger y procesar características biométricas, mediante dispositivos o sensores, creando datos biométricos que posibilitan la identificación, el seguimiento y el perfilado de las personas (esto es, "tratar", conforme al artículo 4.2) del RGPD).

2.2. IDENTIFICADORES: REFERENCIAS BIOMÉTRICAS Y DE IDENTIDAD

En los sistemas descritos anteriormente, los datos biométricos se procesan (crean, almacenan, acceden y comparan) en forma de "referencias biométricas"[2], creadas a partir de las características biométricas de las personas y que permiten su identificación. Pueden ser una "muestra biométrica"[2] (como una huella dactilar o una fotografía, por ejemplo), o bien un "rasgo biométrico"[2] (como una representación vectorial del rostro, por ejemplo), o bien una "plantilla biométrica"[2] (conjunto de rasgos biométricos), o bien un "modelo biométrico"[2] (función almacenada o modelo, basado en IA o no), o cualquier combinación de todos ellos.

La referencia biométrica no está orientada a ser interpretada por una persona, como una fotografía, sino a ser tratada en un proceso automatizado, es decir, a ser eficiente y eficazmente interpretada por una máquina, para un propósito o propósitos determinados.

Para que sean eficaces, es necesario que las referencias biométricas generadas a partir de dos individuos distintos sean claramente distinguibles, es decir, que actúen como un identificador de la persona y la singularice, permitiendo distinguirla de todos los demás miembros de un grupo o dominio determinado.[3]

Por lo tanto, una referencia biométrica que permite la identificación o autenticación de una persona no sólo es un dato personal, sino también un identificador y un dato biométrico, con independencia de la finalidad de su tratamiento. Adicionalmente, en caso de que sea tratada con la finalidad de identificación o autenticación, tendrá también la consideración de categoría especial de datos (véase sección 3.2).

En los sistemas utilizados para el control de acceso, es también habitual el uso de otros identificadores no biométricos, denominados "referencias de identidad"[2]. Son identificadores que permanecen inalterables mientras la persona exista dentro del dominio (como un número de DNI, código de empleado o de cliente, por ejemplo). A ambos tipos de identificador, a las referencias biométricas y a las de identidad, se les pueden asociar datos personales, como los atributos de autorización (véase sección 2.4) y otros atributos adicionales.

2.3. IRREVERSIBILIDAD, NO VINCULACIÓN Y REVOCABILIDAD

A diferencia de las referencias de identidad, las referencias biométricas de una persona se generan directamente a partir de la observación de sus características biométricas, únicas e inalterables. Por ello y como se abordará más adelante en materia de riesgos (véase sección 3.3), es recomendable que las referencias biométricas se generen con ciertas características de diseño, como las de ser 'irreversibles', 'no vinculables' y 'revocables'.

Una referencia biométrica es 'irreversible' si a partir de ella no se puede reconstruir la muestra biométrica original (como la captura del rostro de la persona, por ejemplo).

[2] Términos usados en estándares, como la norma ISO/IEC 24745 *Protección de información biométrica*, por ejemplo.

[3] Grupo del Artículo 29 Documento de trabajo sobre biometría WP80 de 1 de agosto de 2003 apartado 3.8 Identificador único y WP 136 Dictamen 4/2007 sobre el concepto de datos personales, III.3. Tercer componente: "identificada o identificable", página 13.

BORRADOR

Dos o más referencias biométricas son 'no vinculables' si no se puede determinar una asociación entre ellas o con la persona de la que se obtuvieron. Lo contrario posibilitaría vincular a las personas entre diferentes aplicaciones y contextos.

Una referencia biométrica es 'revocable' si es posible prevenir futuras operaciones de identificación o autenticación basadas en dicha referencia biométrica. A su vez, es 'renovable' cuando es posible generar un nuevo y distinto identificador para la misma persona.

Cabe señalar que las referencias biométricas, incluidas aquellas irreversibles, no vinculables o revocables, conservan su condición de dato biométrico siempre que permitan la identificación o autenticación de una persona.

2.4. REGISTRO BIOMÉTRICO. ALMACENAMIENTO DE LOS DATOS BIOMÉTRICOS

El registro es un requisito necesario y previo en los procesos de control de acceso. Se realiza durante el alta de una persona (un empleado, por ejemplo) para poder acceder a un espacio o actividad. En este proceso, es necesario confirmar la identidad de la persona de forma correcta pues, de lo contrario, todo el tratamiento en el control de acceso podría estar viciado. Para ello, se recogen una serie de atributos acreditables de su identidad. Así, podría confirmarse la identidad del individuo (por ejemplo, con el DNI) y, a continuación, recoger datos adicionales en el proceso de alta, en particular, sus datos biométricos.

Adicionalmente, durante el registro, los identificadores de las personas se asocian con sus atributos de autorización (como *'Asiento 1A confirmado para el Vuelo 123'*, *'Área1:Autorizada'* o *'Área2:no autorizada'*, por ejemplo). Estos atributos pueden quedar almacenados junto con los indicadores o de forma separada. Su asociación con los identificadores puede ser directa con las referencias biométricas o indirecta a través de referencias de identidad. En otras palabras, el uso de referencias de identidad es opcional en casos donde baste con atributos de autorización asociados directamente a las referencias biométricas.

Como resultado del proceso de registro, las **referencias biométricas** pueden quedar **almacenadas bajo el control**

- **del responsable**, en una base de datos;
- **del individuo**, en una tarjeta o dispositivo personal y, opcionalmente, cifradas con un secreto conocido por el individuo; o
- **compartido**,
  - **distribuidas** en partes, entre la base de datos del responsable y el dispositivo del individuo,
  - en una base de datos del responsable, pero **cifradas** con un secreto conocido por el individuo,
  - o de ambas maneras a la vez (**distribuidas** y **cifradas**).

2.5. ACCESO BIOMÉTRICO: IDENTIFICACIÓN Y AUTENTICACIÓN

Tras el registro, se realizan de forma regular procesos de control de acceso de las personas, en los que se realizan tratamientos de sus datos personales en la entrada y, en su caso, la salida de un determinado lugar o espacio (por ejemplo, su inicio/fin de la jornada laboral). En el caso de emplear sistemas biométricos, ya sea mediante un proceso de autenticación o de identificación, se realiza una comparación entre las referencias biométricas generadas en el punto de control y las previamente almacenadas durante el registro. De determinarse una coincidencia, se accede a los atributos de autorización asociados a la persona. Finalmente, se toma una decisión.

En los procesos de autenticación, el individuo realiza en primer lugar una declaración de su identidad, por ejemplo, mediante la presentación de una tarjeta o dispositivo personal. La

BORRADOR

referencia biométrica generada en el proceso de autenticación se compara (comparación uno-a-uno) con la obtenida previamente en el proceso de registro. Como se ha comentado anteriormente, la referencia biométrica registrada puede estar almacenada bajo el control del individuo en su dispositivo, bajo control del responsable en una base de datos, o de forma compartida. En el caso de estar almacenada bajo el control del responsable, con objeto de recuperar la referencia biométrica asociada a la identidad reclamada, es necesaria una búsqueda en la base de datos (véase sección 4.2 para implicaciones en materia de riesgos).

En los procesos de identificación, el individuo no declara su identidad. Esto implica necesariamente la existencia de una base de datos, bajo el control del responsable, que almacena las referencias biométricas de todas las personas registradas en el sistema. Por tanto, la referencia biométrica generada en el proceso de identificación se compara (comparación uno-a-varios) contra todas las referencias biométricas existentes en la base de datos.

3. ANÁLISIS LEGAL

3.1. PRINCIPIO DE PROPORCIONALIDAD

El principio de proporcionalidad es uno de los principios generales del Derecho de la Unión. Requiere que las medidas sean idóneas, necesarias y proporcionadas en sentido estricto, como recuerda la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero:

> *"En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto; STC 66/1995, de 8 de mayo, F. 5; STC 55/1996, de 28 de marzo, FF. 7, 8 y 9; STC 270/1996, de 16 de diciembre, F. 4.e; STC 37/1998, de 17 de febrero, F. 8; STC 186/2000, de 10 de julio, F. 6)."*

En el RGPD, el principio de proporcionalidad interactúa con los principios relativos al tratamiento, en particular con el de minimización de datos, con el enfoque basado en riesgos y con la evaluación de impacto en materia de protección de datos.

3.1.1. IDONEIDAD

Para que un tratamiento se pueda considerar idóneo (o adecuado, en términos del principio de minimización del RGPD) ha de permitir cumplir con la finalidad última del tratamiento con unos niveles adecuados de calidad, teniendo en cuenta que no hay tratamiento que esté libre de errores ni de posibilidad de fraude.

Para establecer la idoneidad del tratamiento biométrico hay que evaluar que exista un vínculo lógico y directo entre el tratamiento y el objetivo perseguido, y determinar la eficacia real del tratamiento, es decir, determinar mediante prueba objetiva que éste es capaz de alcanzar un nivel mínimo de efectividad en resolver la necesidad planteada.

BORRADOR

Para ello, es recomendable que estén definidas métricas[4] sobre los objetivos necesarios en los tratamientos en el control de acceso. Es preciso realizar un análisis objetivo sobre la adecuación de las distintas opciones técnicas, incluida la biométrica, a dichos requerimientos.

En particular, hay que determinar si puede existir una falta de exactitud de los datos obtenidos con relación a la operación biométrica al no adecuarse al tipo humano medio o estándar según criterio del responsable. Esto se puede materializar en sesgos en los perfilados, identificaciones incorrectas, suplantación de identidad, discriminación en segmentos de población (mayores, discapacitados, tipos raciales, enfermos, etc.) o denegación de acceso a servicios por errores en la captación del dato.

Por otra parte, dada una finalidad de control de acceso, un tratamiento basado en datos personales no biométricos (es decir, que no trate características del propio individuo) podría ser inadecuado (no idóneo), en función de su utilidad para lograr dicha finalidad específica. Por ejemplo, basarse únicamente en tarjetas (algo en posesión del individuo) o códigos (algo que el individuo conoce), podría ser inadecuado en casos donde éstos pudiesen ser fácilmente compartidos o utilizados por otros individuos, de forma incompatible con la finalidad.

Del mismo modo, por sí solas, algunas características biométricas como la temperatura corporal o la frecuencia cardíaca, por ejemplo, pueden no ser idóneas o adecuadas para la identificación o verificación biométrica a menos que contribuyan eficazmente a tal fin.

3.1.2. **NECESIDAD**

El principio de proporcionalidad requiere también que las medidas, además de idóneas (o adecuadas) sean necesarias. Esto significa que no deben ser más gravosas que otras medidas, basadas en biometría o no, que también logran la finalidad con igual eficacia.

Uno de los principios del RGPD es el principio de minimización que establece en el art. 5 apartado 1 letra c que los datos serán:

"adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);"

Los datos que se traten han de ser pertinentes y limitados a lo necesario para conseguir los fines del tratamiento. El considerando 39 explica que unos datos que no son necesarios para cumplir con la finalidad del tratamiento no deben ser tratados:

"…Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios…".

La justificación de la necesidad de recurrir al tratamiento de datos biométricos debe basarse en elementos objetivos y acreditar que la finalidad perseguida no puede alcanzarse razonablemente de manera igualmente eficaz mediante otras alternativas que ocasionen una menor injerencia en los derechos y libertades de las personas afectadas.

El principio de proporcionalidad no excluye el empleo de sistemas biométricos por la mera existencia de otros medios posibles de identificación o autenticación. Para apreciar la necesidad del tratamiento debe determinarse, atendiendo a las circunstancias concretas en las que este se desarrolla, si existen alternativas menos intrusivas que permitan alcanzar la finalidad perseguida, pero siempre que sea con un nivel de eficacia equivalente. No basta,

[4] Ejemplo de métricas a considerar podrían ser: tasa de falsos positivos y falsos negativos en el control de acceso y por diferentes sistemas, tasas de flujo o controles de autenticación/identificación por unidad de tiempo y por diferentes sistemas, etc.

BORRADOR

por tanto, con que exista otro sistema posible o que este pueda considerarse también eficaz: la alternativa debe permitir satisfacer las necesidades que justifican el tratamiento de manera igualmente eficaz. Además, cabe subrayar que esta valoración corresponde al responsable, que es quien dispone del conocimiento sobre el contexto del tratamiento, las finalidades y necesidades concretas que deben satisfacerse, los medios disponibles y las alternativas técnica y organizativamente viables. Conforme al principio de responsabilidad proactiva y su diligencia, deberá poder justificar tanto la eficacia exigida en ese contexto como la inexistencia de una alternativa menos intrusiva que permita alcanzarla con un nivel equivalente.

En el caso del tratamiento de múltiples características biométricas (multibiometría) como el rostro y la palma de la mano conjuntamente, o ambos iris izquierdo y derecho, por ejemplo, no sólo debe justificarse la necesidad de recurrir al tratamiento de datos biométricos, sino también acreditar que el tratamiento de un número menor de características (sólo una huella dactilar sin recurrir al rostro o a la palma de la mano, o sólo un iris en lugar de ambos, por ejemplo) no es igualmente eficaz en el cumplimiento de la finalidad.

En cumplimiento del principio de minimización, los responsables deberán valorar si la precisión, el detalle o la frecuencia con la que recogen los datos biométricos exceden las necesidades específicas del tratamiento. Por ejemplo, con la finalidad de identificar a una persona, un tratamiento de datos biométricos no se puede considerar limitado a lo necesario si dichos datos biométricos revelan información adicional sobre la persona, como su origen racial o étnico, sus emociones, o atributos relacionados con su salud.

Por último, en la evaluación de posibles alternativas igualmente eficaces y más moderadas se han de explorar también opciones que no sean solo tecnológicas como la utilización de recursos humanos, por ejemplo.

3.1.3. PROPORCIONALIDAD EN SENTIDO ESTRICTO

El principio de proporcionalidad también exige que las medidas sean proporcionales en sentido estricto. Esto significa que no deben suponer una carga excesiva sobre los derechos afectados con relación al beneficio obtenido al lograr la finalidad. Se debe establecer si el tratamiento de datos biométricos es una medida ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto.

Para ello hay realizar una evaluación del nivel de injerencia en los derechos y libertades del interesado, estimando entre otros: la naturaleza de la injerencia: o como se limitan o se ponen en riesgo los derechos y libertades; el alcance/extensión del tratamiento; el contexto en que la medida deberá aplicarse o la naturaleza de la actividad objeto de la medida. Adicionalmente, deben analizarse posibles injerencias en la intimidad de personas distintas al interesado (por ejemplo, la captura de datos biométricos de personas que están en el entorno del interesado).

En este sentido, la aplicación del principio de minimización se extiende, tanto a la obligación de tener en cuenta la condición de necesidad, como también a la de tener en consideración (art. 24.1 RGPD) los riesgos para los derechos y libertades de las personas físicas, como se establece en el art. 25 apartado 1 del RGPD:

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas

BORRADOR

apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

Por lo tanto, un tratamiento de datos biométricos en el control de acceso puede considerarse desproporcionado si supone un alto riesgo para los derechos y libertades de las personas, cuando existen alternativas igualmente eficaces que entrañan un menor riesgo, o cuando no es posible aplicar garantías y medidas de mitigación apropiadas para reducir el riesgo residual a un nivel aceptable.

3.2. CATEGORÍAS ESPECIALES DE DATOS

El art. 9, apartado 1, del RGPD establece una regla general consistente en prohibir el tratamiento de datos personales que revelen lo que denomina "categorías especiales de datos personales". Esta especial protección deriva del impacto que el tratamiento de estos datos puede tener en los derechos fundamentales y libertades de las personas.

Únicamente cabe excepcionar la prohibición de tratamiento de los datos de categoría especial cuando concurra alguna de las circunstancias que se especifican en el apartado 2 del art. 9 del RGPD. El responsable tiene la obligación de valorar muy seriamente y con diligencia si tiene una razón sólida para tratar categorías especiales que aparezca enumerada en dicho art. 9.2 del RGPD. Entre las circunstancias enumeradas no se encuentra el interés legítimo, la ejecución de un contrato o medidas precontractuales.

Los datos biométricos se consideran una categoría especial de datos cuando son tratados con la finalidad de identificar de manera única a una persona física. Éste es el caso de los tratamientos en el registro y control de acceso biométricos. Lo anterior aplica con independencia de que la operación de comparación sea uno-a-uno o uno-a-varios[5], de que se busque determinar la existencia o inexistencia de una referencia biométrica en una base de datos, y de que se recuperen o no existan referencias de identidad asociadas. No obstante, aunque desde el plano formal los usos anteriores pueden estar incluidos en el artículo 9 del RGPD, el impacto real sobre los derechos y la intensidad de las medidas de protección requeridas pueden variar sustancialmente, debiendo valorarse caso por caso en función del contexto, la escala, la tecnología empleada y el control efectivo[6] que conserve el interesado sobre sus datos biométricos (véase 2.4 y 4.2).

En el ámbito de esta guía, el levantamiento de la prohibición del artículo 9.1 del RGPD podrá fundarse, según los casos, en una norma que reúna los requisitos exigidos por el artículo 9.2 o en el consentimiento explícito de las personas interesadas. Ello no permite presumir, por sí solo, la necesidad de recurrir al tratamiento de datos biométricos en lugar de otros tipos de datos personales. Esta necesidad deberá justificarse separadamente en los términos expuestos en la presente guía.

No obstante, la graduación en la intensidad de las garantías comentada anteriormente también podrá reflejarse en los requisitos para el levantamiento de la prohibición, así como en la necesidad de contar con una base jurídica adecuada conforme al artículo 6 (véase 3.3). El principio de legalidad impone no sólo una base jurídica en abstracto, sino un grado suficiente de precisión y previsibilidad en función del riesgo y del impacto del tratamiento. Por ejemplo. no puede exigirse el mismo nivel de densidad normativa para una identificación masiva y automatizada sin conocimiento del afectado que para una autenticación puntual,

[5] Directrices 05/2022 del Comité Europeo de Protección de Datos (CEPD), sobre el uso de reconocimiento facial en el ámbito de las fuerzas de orden público (véase Versión 2.0, de 26 de abril de 2023), apartado 12 y Dictamen 11/2024, sobre el uso del reconocimiento facial para agilizar el flujo de pasajeros de los aeropuertos, apartado 21.

BORRADOR

localizada y consentida, donde los interesados conserven el control efectivo[6] sobre sus datos biométricos (véase sección 4 Gestión del riesgo y 4.5 Garantías y medidas).

3.2.1. EXCEPCIÓN BASADA EN EL CONSENTIMIENTO

El consentimiento puede levantar la prohibición y legitimar el tratamiento de datos biométricos realizado por el responsable. Ahora bien, tratándose datos especialmente protegidos es importante contar con las garantías del consentimiento (véanse las Directrices 5/2020 sobre el consentimiento del CEPD). En todo caso, el consentimiento deberá ser libre, específico, informado e inequívoco.

El responsable, teniendo en cuenta todas las circunstancias, deberá poder demostrar que el consentimiento ha sido otorgado libremente, sin presiones o influencias indebidas, y que existe una alternativa real y cierta. Esto puede traducirse en el establecimiento de un método razonable y alternativo al tratamiento de datos biométricos, que podrá implicar la coexistencia de dos mecanismos de control de acceso que obviamente no son iguales. No obstante, este método alternativo no deberá suponer una carga, penalidad o menoscabo evidente o pretendido para el interesado, ni representar un tratamiento claramente gravoso, como tiempos de espera más largos o costes adicionales, por ejemplo.

El consentimiento, en su caso, podrá darse en el contexto de un contrato. Sin embargo, al evaluar la validez del consentimiento, se deberá prestar especial atención cuando exista un desequilibrio de poder entre el interesado y el responsable del tratamiento. Éste puede ser el caso en las que intervienen autoridades y ciudadanos, empleadores y empleados, o instituciones educativas y estudiantes. En estos contextos también podrá darse el consentimiento, guardándose obviamente las garantías exigibles.

3.2.2. EXCEPCIÓN AUTORIZADA POR LEY

En el ámbito del control de acceso de esta guía, un tratamiento con datos biométricos puede traer causa de una ley en el ámbito del Derecho laboral y de la seguridad y protección social (art. 9.2.b), o por razones de interés público, ya sea esencial (art. 9.2.g) o en el ámbito de la salud pública (art. 9.2.i).

Dicha autorización legal puede derivarse del Derecho de la Unión o del Derecho de los Estados miembros. Adicionalmente, en el ámbito laboral, también puede derivarse de un convenio colectivo conforme al Derecho de los Estados miembros.

De la legislación habilitante debe derivarse claramente la finalidad del tratamiento. También podrá especificar los tipos de datos, las limitaciones de finalidad, los interesados afectados y otras condiciones. La legislación habilitante debe ser proporcional al objetivo perseguido y establecer garantías adecuadas para el respeto de los derechos fundamentales y los intereses del interesado. Esto es sin perjuicio de las garantías más específicas que otras leyes o convenios puedan establecer en el ámbito laboral, tal y como se prevé en el art. 88 del RGPD y en el art. 91 de la LOPDGDD. En la sección 4.3 de esta guía se aportan algunos ejemplos de posibles garantías.

[6] En esta línea, la propuesta Ómnibus de la Comisión Europea para la modificación del RGPD, contempla una nueva excepción a la prohibición (artículo 9.2.l) donde los datos biométricos o los medios necesarios para la autenticación se encuentren bajo el control exclusivo del interesado.

BORRADOR

3.3. LICITUD DEL TRATAMIENTO

En tanto en cuanto el tratamiento de datos biométricos se considere que es un tratamiento de datos especialmente protegidos del artículo 9 RGPD, como se ha señalado, debe darse un levantamiento de la prohibición mediante el consentimiento o legislación suficiente.

A partir de lo anterior, cabe analizar si dicho tratamiento cuenta con -al menos- una de las condiciones enumeradas el art. 6.1 del RGPD. Cabe advertir que muy posiblemente la ubicación de un levantamiento de la prohibición y la búsqueda de una base de legitimación en el tratamiento es una acción conjunta e indistinta.

En el caso de que el responsable decida basar la licitud de tratar datos biométricos en el art. 6.1.a) del RGPD se trasladan las conclusiones alcanzadas en la sección 3.2.1 de este texto, referentes a la validez del consentimiento.

En el caso de fundamentar la licitud del tratamiento de datos biométricos en el control de acceso en alguna de las bases previstas en las letras b) a f) del artículo 6.1 del RGPD, deberá acreditarse que el tratamiento es necesario para la concreta finalidad o presupuesto definido en la base jurídica invocada. Además, en los supuestos de las letras c) y e), deberá concurrir la base normativa exigida por el artículo 6.3 y, cuando se invoque la letra f), deberá realizarse la ponderación entre los intereses legítimos perseguidos por el responsable y los intereses o los derechos y libertades fundamentales de la persona interesada que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

3.4. DECISIONES AUTOMATIZADAS

El art. 22 del RGPD establece restricciones y garantías cuando una decisión basada únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, produce efectos jurídicos sobre el interesado o le afecte significativamente de modo similar.

Un tratamiento en el control de acceso se podría implementar por parte del responsable mediante un sistema biométrico que dé lugar, sin intervención humana, a una decisión que produzca efectos jurídicos sobre el interesado o le afecte significativamente de modo similar. Por ejemplo, cuando un sistema que controle el acceso al lugar deniegue dicho acceso por motivos técnicos y esa denegación produzca automáticamente consecuencias sobre la persona, como efectos sobre el salario o el empleo de una persona trabajadora. Otro ejemplo es que impida a un interesado el acceso a una determinada actividad o servicio previamente contratado o que limite su libertad de movimientos.

A estos efectos, una intervención humana meramente formal no será suficiente para excluir que la decisión se considere basada únicamente en un tratamiento automatizado. Dicha intervención deberá ser realizada por una persona con autoridad y competencia para valorar los elementos pertinentes y modificar o dejar sin efecto la decisión.

Cuando el responsable configure un tratamiento en el control de acceso de esta forma, deberá tener en cuenta que, conforme al artículo 22.4 del RGPD, las decisiones contempladas en el artículo 22.2 no podrán basarse en categorías especiales de datos, salvo que:

- La excepción para tratar datos biométricos esté basada en el consentimiento del interesado (artículo 9.2.a del RGPD, véase 3.2.1) o esté autorizada por una ley por razones de interés público esencial (artículo 9.2.g del RGPD, véase 3.2.2);
- y se hayan adoptado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos de la persona interesada. Entre dichas medidas deberán figurar, como mínimo, en los supuestos previstos en el artículo 22.3 del RGPD:
    - el derecho a obtener intervención humana por parte del responsable;

BORRADOR

- el derecho a expresar su punto de vista; y
- el derecho a impugnar la decisión.

4. GESTIÓN DEL RIESGO

El levantamiento de la prohibición de tratar categorías especiales de datos y la existencia de una legitimación para el tratamiento no concluye con el conjunto de requisitos que son de obligado cumplimiento para determinar que el tratamiento es conforme al RGPD, y por tanto que se puede llevar a cabo.

Entre otros requisitos, es indispensable que, con carácter previo a cualquier decisión de implantación de un sistema de control de acceso a través de sistemas biométricos, se realice una gestión del riesgo (art. 24.1 RGPD) y, como consecuencia de dicha gestión del riesgo, se elaboren medidas de diseño y por defecto (art. 25 RGPD), técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD. En particular, cuando sea probable que un tipo de tratamiento entrañe un alto riesgo, se deberá realizar una Evaluación de Impacto para la Protección de Datos (EIPD) antes del inicio del tratamiento y documentar en ella la identificación y evaluación de los riesgos para los derechos y libertades, las medidas previstas para afrontarlos y el riesgo residual resultante. La EIPD deberá evaluar la necesidad y proporcionalidad de las operaciones del tratamiento con respecto a su finalidad en los términos del artículo 35.7.b) del RGPD y acreditar, conforme a la doctrina constitucional y del TJUE, que la medida es idónea, necesaria y proporcionada en sentido estricto.

A su vez, hay que tener en cuenta que una gestión del riesgo para los derechos y libertades no excluye la obligación previa de que exista una circunstancia que permita el levantamiento de la prohibición de tratar categorías especiales, una condición que legitime el tratamiento, cumplir con las condiciones del art. 22 sobre decisiones automatizadas, con el principio de minimización de datos y el cumplimiento de los principios, derechos y otras obligaciones establecidas en el RGPD.

4.1. EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS

La obligación de realizar una EIPD la establece el RGPD para los tratamientos donde exista la probabilidad de un alto riesgo inherente o inicial[7], con independencia de que este alto riesgo se confirme o no durante la realización de la EIPD. Con carácter previo al inicio del tratamiento, los responsables deben evaluar el nivel de riesgo inherente de las operaciones del tratamiento previstas, teniendo en cuenta la naturaleza, el alcance y el contexto del sistema biométrico utilizado para el control del acceso físico, así como cualquier decisión de diseño relevante.

La EIPD es un proceso que debe abarcar el ciclo de vida completo del tratamiento de datos personales. Permite gestionar desde el diseño los riesgos específicos del tratamiento, con el objetivo de determinar que, o bien el riesgo inherente no es alto o que, de serlo, con la aplicación de medidas técnicas y organizativas, estos riesgos se mitigan a un nivel residual aceptable. Además, la EIPD también constituye un instrumento donde expresar el análisis y la superación del triple juicio de idoneidad, necesidad y proporcionalidad del tratamiento.

[7] Una de las obligaciones de los responsables es la de evaluar el riesgo de sus tratamientos. Ya desde la norma, se establece una relación no exhaustiva de tipos de tratamiento con probabilidad de entrañar un alto riesgo para los derechos y libertades de las personas físicas. En concreto, en desarrollo de la previsión contemplada en el apartado cuarto del art. 35 del RGPD se establece la obligación de la AEPD de publicar las "Listas de tipos de tratamiento de datos que requieren evaluación de impacto relativa a protección de datos", tras su aprobación por el Comité Europeo de Protección de Datos. En dichas listas fueron incluidos, entre otros, aquellos tipos de tratamiento que "impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física".

BORRADOR

De acuerdo con el principio de responsabilidad proactiva (art. 5.2 del RGPD) el responsable del tratamiento debe ser capaz no sólo de demostrar la superación de la EIPD, sino también de aportar toda la documentación elaborada con ocasión de la realización de la EIPD y justificativa de los resultados obtenidos en la EIPD y de las medidas, organizativas, jurídicas y técnicas, adoptadas al respecto. También se ha de incluir la documentación relativa a la participación del Delegado de Protección de Datos (DPD), en caso en que estuviera nombrado, entre otros. Además, será obligatoria la consulta previa a la autoridad de control cuando la EIPD muestre que, pese a las medidas previstas por el responsable, el tratamiento entrañaría un alto riesgo residual para los derechos y libertades de las personas afectadas, de conformidad con el artículo 36 y el considerando 94 del RGPD.

La concreción sobre cómo cumplir con el art. 35 y 36 del RGPD la ha desarrollado la AEPD en las siguientes orientaciones, que indican cómo se ha de ejecutar y superar una EIPD, cómo hay que documentarla y cómo se ha de realizar la consulta previa:

- Gestión del riesgo y evaluación de impacto en tratamientos de datos personales
- Lista de verificación para determinar la adecuación formal de una EIPD y la presentación de consulta previa
- Instrucción 1/2021 de la AEPD de directrices respecto de la función consultiva de la Agencia. Capitulo V: Consultas Previas
- Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para Administraciones Públicas
- Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para el Sector Privado
- Guía de Privacidad desde el Diseño
- Guía de Protección de Datos por Defecto
- Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial
- Requisitos para Auditorías de Tratamientos que incluyan IA

4.2. ALTO RIESGO

Las operaciones biométricas en los tratamientos para el control de acceso pueden requerir el uso de distintos sistemas, algunos de forma simultánea. A su vez, una misma técnica biométrica se puede implementar de distintas formas en un sistema. Dado un tratamiento concreto, las operaciones con datos biométricos podrán tener un grado distinto de intrusión e impacto en la privacidad de los individuos, que dependerá no sólo de la técnica empleada sino también de la propia definición del tratamiento, su naturaleza, el ámbito o alcance en el que se va a desarrollar, su contexto y, en particular, si el tratamiento se configura como una decisión automatizada.

Los responsables del tratamiento deben evaluar cuidadosamente los siguientes elementos de diseño, entre otros, para determinar si el tratamiento puede suponer un alto riesgo inherente para los derechos y libertades de las personas físicas:

- Datos biométricos bajo el control exclusivo del responsable
- Referencias biométricas reversibles, vinculables o irrevocables
- Registro biométrico remoto o sin supervisión
- Carácter masivo del tratamiento
- Participación de terceros

Los sistemas donde los datos biométricos están bajo el control exclusivo del responsable plantean un mayor riesgo inherente para los derechos y libertades de todas las personas registradas. Con independencia de si están destinados a la verificación o identificación biométrica, las bases de datos de dichos sistemas podrían usarse para identificar a estas

BORRADOR

personas sin su participación activa, o con fines distintos de los originalmente previstos o consentidos. Estos riesgos se mitigan cuando los datos biométricos están bajo control compartido y, más aún, se evitan cuando están bajo el control exclusivo del interesado y con protección basada en secreto y son revocables (véase 2.3 y 2.4).

Las referencias biométricas reversibles[8] conllevan un mayor riesgo inherente de suplantación de identidad u otras formas de uso indebido. Dado que las características biométricas representan algo que los interesados son, no pueden modificarse fácilmente como otros factores de autenticación.

Las referencias biométricas vinculables[9] plantean el riesgo de poder vincular a los interesados entre diferentes aplicaciones dentro de la misma base de datos, o entre múltiples bases de datos de referencias biométricas.

Las referencias biométricas irrevocables[10] aumentan el riesgo inherente en caso de brechas de datos e imposibilitan el establecimiento de períodos de validez o políticas de caducidad.

En la práctica, las tecnologías biométricas ofrecen distintos grados de irreversibilidad, no vinculación y revocabilidad, lo que puede dar lugar a riesgos residuales que no puedan mitigarse hasta un nivel aceptable.

El registro biométrico puede realizarse de forma remota o en persona, ya sea en las instalaciones del responsable del tratamiento o directamente en el punto de control durante el primer acceso. El registro biométrico remoto o sin supervisión conlleva un mayor riesgo inherente, como el riesgo de suplantación de identidad, fraude, o de brecha de datos durante la transmisión, por ejemplo, debido a la mayor complejidad de una verificación fiable de la identidad del interesado.

La participación de terceros aumenta significativamente los riesgos inherentes, entre otros, el de acceso no autorizado o de brecha de datos.

4.3. SUPERACIÓN DEL ANÁLISIS DE IDONEIDAD, NECESIDAD Y PROPORCIONALIDAD

El artículo 35.7.b) del RGPD exige que la EIPD incluya una evaluación de la necesidad y proporcionalidad de las operaciones de tratamiento con respecto a su finalidad. Dicha evaluación deberá incorporar, de acuerdo con la doctrina del Tribunal Constitucional y del Tribunal de Justicia de la Unión Europea, el triple juicio de idoneidad, necesidad y proporcionalidad en sentido estricto.

Los requisitos para superar este análisis son los ya expuestos anteriormente en la Sección 3.1.

4.4. IMPLEMENTACIÓN Y CONTEXTO DEL TRATAMIENTO

[8] (véase 2.3) Una referencia biométrica es reversible si a partir de ella se puede reconstruir la muestra biométrica original, como la captura del rostro de una persona, por ejemplo.

[9] (véase 2.3) Dos o más referencias biométricas son vinculables si se puede determinar una asociación entre ellas o con la persona de la que se obtuvieron. Esto posibilita vincular a las personas entre diferentes aplicaciones.

[10] (véase 2.3) Una referencia biométrica es revocable si es posible prevenir futuras operaciones de identificación o autenticación basadas en dicha referencia biométrica.

BORRADOR

Hay una gran diferencia entre el concepto de operación biométrica y su implementación. La implementación concreta implica selección de sensores, protocolos de comunicaciones, bibliotecas de código, dispositivos en los que se integran (móviles o cajeros automáticos, por ejemplo), almacenamiento (en la nube, por ejemplo), etc. Cada uno de ellos, tendrá distintos grados de calidad, certificación, auditoría, seguridad, implicación de terceros, etc.

En la implementación concreta de un tratamiento para el control de acceso mediante operaciones de tratamiento biométricas pueden surgir riesgos adicionales de protección de datos, además de que también pueden surgir potenciales incumplimientos, como podrían ser transferencias internacionales de datos sin las garantías adecuadas, por ejemplo. Incluso aunque inicialmente se hubieran solventado estas situaciones, éstas podrían sobrevenir como consecuencia de una renovación o actualización de sus componentes una vez que el sistema hubiera sido puesto en producción.

Por tanto, se recomienda que el riesgo de las operaciones biométricas, así como del tratamiento en su conjunto, sea revisado periódicamente o siempre que haya cambios significativos, ya sean normativos, técnicos u organizativos que afecten al tratamiento, sus fines, su naturaleza, ámbito o contexto.

4.5. GARANTÍAS Y MEDIDAS

En el planteamiento de un control de acceso con operaciones biométricas, tal y como se ha ido exponiendo, se dan unas exigencias y garantías. Así, se necesita una base jurídica del tratamiento del art. 6.1 RGPD y, por tratarse de categorías especiales de datos, de una circunstancia que levante la prohibición de tratar categorías especiales de datos (art. 9.2 RGPD). Asimismo, se requiere el cumplimiento de las condiciones del art. 22 del RGPD. Además, es necesario establecer desde el diseño medidas técnicas y organizativas apropiadas, a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD. Estas medidas, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, deben ser las adecuadas para gestionar el riesgo (arts. 24 y 25.1 del RGPD) e, independientemente del nivel de riesgo, deben implementar protección de datos por defecto (art. 25.2 RGPD).

La intensidad de las medidas y garantías deberá ser proporcional a la sensibilidad de los datos tratados y, especialmente, al nivel de riesgo que tenga el tratamiento concreto.

Dada una implementación concreta de un control de acceso con técnicas biométricas, las medidas aquí expuestas no son exhaustivas, ni agotan el conjunto de las que se pueden o deben implementar para gestionar los riesgos que pueden surgir. Igualmente, se deberán respetar aquellas medidas y garantías ya establecidas en las normas que autoricen determinados tratamientos. Además, la validación de los sistemas biométricos empleados en un tratamiento debe de asegurarse “desde el diseño” como exige el art. 25.1 del RGPD y con las recomendaciones que establece en la Guía de Privacidad desde el Diseño.

4.5.1. ORGANIZATIVAS

Cuando el tratamiento esté autorizado por ley, esta ley podría obligar a los responsables del tratamiento a realizar una EIPD, a consultar a la autoridad de control y obtener su autorización previa, o ambas cosas. Aun existiendo una autorización legal para el tratamiento biométrico, los responsables deben garantizar la disponibilidad de métodos alternativos de control de acceso, por ejemplo, cuando los interesados no puedan operar el sistema debido a una discapacidad temporal o permanente, o en casos de caída, interrupción, o mal funcionamiento del sistema, o ante incidencias en la interacción entre el usuario y el sistema.

Cuando el tratamiento esté basado en el consentimiento del interesado, dichos métodos alternativos de control de acceso deben estar disponibles de forma inherente, ya que el uso de datos biométricos debe ser realmente opcional.

BORRADOR

Los interesados deben estar informados sobre el tratamiento. Esto implica, como señala el considerando 39 del RGPD que "*Las personas físicas deben tener conocimiento de los riesgos*" con relación a los tratamientos, en este caso biométrico. Una medida recomendada es que la toma de los datos se realice de forma consciente por el individuo, e incluso con la exigencia de una acción positiva para iniciar el procesamiento de datos biométricos que, como se ha indicado, implicaría que la persona afectada disponga de la información previa y suficiente, para que sea consciente del riesgo que supone el tratamiento de sus datos biométricos, especialmente si se encuentra en una situación de vulnerabilidad.

Los sistemas de control de acceso físico no deben recopilar, ni procesar de ninguna otra forma, los datos biométricos de las personas que no estén sujetas al proceso de control de acceso. Esto se puede garantizar, por ejemplo, utilizando puntos de control biométricos específicos que estén claramente indicados y, cuando sea necesario, separados físicamente.

Los períodos de conservación y validez de las referencias biométricas deben estar basados en la naturaleza del tratamiento, la frecuencia de las operaciones de acceso y los requisitos de seguridad aplicables. Las referencias biométricas almacenadas durante el registro biométrico deben eliminarse de forma segura una vez que hayan caducado, hayan sido revocadas o ya no sean necesarias. Las referencias biométricas creadas durante la verificación o identificación biométrica sólo deben usarse durante el tiempo mínimo estrictamente necesario para completar la operación de comparación, tras la cual deben eliminarse de forma segura.

En todo caso, se deberán suprimir los datos biométricos cuando no se vinculen a la finalidad que motivó su tratamiento.

4.5.2. **TÉCNICAS**

El uso de identificadores adicionales conlleva un mayor riesgo de combinación con otras fuentes de información. Por lo tanto, cuando sea necesario el uso de referencias de identidad, se aconseja su almacenamiento por separado de las referencias biométricas. Igualmente, se recomienda habilitar la posibilidad de revocar el vínculo entre ambas referencias, así como utilizar formatos de datos o tecnologías específicas que dificulten la interconexión de bases de datos biométricos y la divulgación de datos no comprobada.

Se debe considerar la implementación de medios técnicos para asegurar la imposibilidad de utilizar las plantillas para otros propósitos distintos al del tratamiento.

Se recomienda el cifrado de los datos biométricos tanto en su almacenamiento como en su transmisión, para proteger de esta forma su confidencialidad, disponibilidad e integridad. Este cifrado global es complementario a la protección basada en secreto a nivel de referencia biométrica.

Las operaciones de los tratamientos deben realizarse en dispositivos específicos, certificados y seguros. Debe garantizarse la integridad y la configuración de dichos dispositivos, y cualquier operación no autorizada o intento de manipulación debe activar alertas a los administradores. Los dispositivos personales deben almacenar los datos biométricos en un enclave seguro y procesarlos en un entorno de ejecución confiable.

Las operaciones de la verificación biométrica deben ser realizadas de forma local, por ejemplo, en el dispositivo personal o junto con un terminal o quiosco biométrico dedicado, minimizando así la necesidad de transmitir datos biométricos a sistemas remotos.

Los sistemas de control de acceso físico disponibles para uso público, como los quioscos biométricos, deben instalarse en lugares que ofrezcan la privacidad y seguridad adecuadas. No deben estar conectados a Internet. El acceso a las funciones de administración y

BORRADOR

configuración debe estar restringido al personal autorizado responsable de la seguridad y el mantenimiento del sistema.

Las muestras biométricas (como la huella dactilar o una fotografía) sólo deben almacenarse durante el tiempo mínimo estrictamente necesario para completar las operaciones de creación de referencias biométricas, tras la cual deben eliminarse de forma segura.

4.6. BRECHAS DE DATOS PERSONALES

La realidad de la tecnología es que cada día aparecen nuevas formas, técnicas o de ingeniería social, de explotar vulnerabilidades de seguridad. En el marco del tratamiento donde se encuentra la operación biométrica el responsable tiene que plantear posibles escenarios de brechas de datos personales, para, como resultado de su análisis, implementar garantías para minimizar no solo la probabilidad de que se produzca, sino de minimizar el impacto sobre los derechos y libertades de los ciudadanos en caso de que se materialicen.

En la gestión del riesgo hay que determinar medidas y garantías para minimizar el impacto que el uso de sistemas biométricos puede ocasionar en los derechos y libertades de las personas interesadas, contemplando la posibilidad de que, pese a las medidas preventivas adoptadas, pueda producirse una brecha de datos personales.

Los escenarios que se deben plantear son, al menos, el filtrado o pérdida de patrones biométricos, uso malicioso de patrones almacenados, intrusión en el sistema de análisis biométrico y en sus resultados, intercepción de la comunicación entre sistemas, ataques de denegación de servicio, discontinuidad de servicios propios o de terceros, etc. Todos los escenarios hay que analizarlos para medir el grado de impacto que puede ocasionar en los derechos y libertades.

Asimismo, hay que conocer qué brechas se están produciendo actualmente y que podrían determinar la falta de adecuación de una técnica biométrica concreta, de la biometría en general o de las garantías implementadas. Esto supone el realizar una evaluación continua del tratamiento en función de los eventos que se estén produciendo en el contexto del social y tecnológico.

5. ACCESO AL ENTORNO LABORAL. REGISTRO DE JORNADA

En el ámbito laboral, el control de acceso puede limitarse a una finalidad básica en materia de seguridad o también servir para la finalidad de registro de jornada.

En relación con el registro de jornada, el Real Decreto-Ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo establece en su Capítulo III “Medidas de lucha contra la precariedad laboral en la jornada de trabajo”, y en su art. 10 regula el registro de jornada como forma de combatir la precariedad laboral, mediante una modificación del art. 34 del texto refundido de la Ley del Estatuto de los Trabajadores (en adelante ET), aprobado por Real Decreto Legislativo 2/2015, de 23 de octubre, añadiendo un nuevo apartado 9, con la siguiente redacción:

«9. La empresa garantizará el registro diario de jornada, que deberá incluir el horario concreto de inicio y finalización de la jornada de trabajo de cada persona trabajadora, sin perjuicio de la flexibilidad horaria que se establece en este artículo.

Mediante negociación colectiva o acuerdo de empresa o, en su defecto, decisión del empresario previa consulta con los representantes legales de los trabajadores en la empresa, se organizará y documentará este registro de presencia.

BORRADOR

La empresa conservará los registros a que se refiere este precepto durante cuatro años y permanecerán a disposición de las personas trabajadoras, de sus representantes legales y de la Inspección de Trabajo y Seguridad Social.»

Como se especifica en el apartado V de la Exposición de motivos del citado Real Decreto Ley 8/2019, el propósito de la obligación establecida tiene como objetivo garantizar el cumplimiento de los límites en materia de jornada, crear un marco de seguridad jurídica tanto para las personas trabajadoras como para las empresas y posibilitar el control por parte de la Inspección de Trabajo y Seguridad Social, como medio para corregir la situación de precariedad, bajos salarios y pobreza que afecta a muchos de los trabajadores que sufren los abusos en su jornada laboral.

En relación con el control de acceso con fines laborales, éste se suele fundamentar en la previsión contenida en el art. 20.3 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores, que establece que:

"3. El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad".

5.1. EXCEPCIÓN DEL ART. 9.2.B RGPD: EXISTENCIA DE UNA NORMA DE RANGO LEGAL

En el art. 9 del RGPD, apartado 2, letra b), se levanta la prohibición del tratamiento de categorías especiales de datos cuando

> *"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"*[11]

Ello supone, como bien apunta el Dictamen 2/2022, de la Autoridad Catalana de Protección de Datos, que "la afectación por el derecho a la protección de datos que se derive de la norma debe ser previsible" y que "no se puede considerar previsible la norma si no concreta la posibilidad de utilizar datos biométricos con el fin de realizar el control horario".

Esto obliga a reconsiderar la interpretación realizada por esta AEPD en el apartado "Los datos biométricos" del capítulo 4.6 de la Guía "La Protección de Datos en las Relaciones Laborales" de mayo de 2021; y, como también concluye el Consejo de Transparencia y Protección de Datos de Andalucía, en su Dictamen 1/2023, "Relativo al tratamiento de categorías especiales de datos biométricos mediante el uso de dispositivos de reconocimiento facial y/o huella dactilar para el control horario del personal de un Ayuntamiento", en la actual normativa legal española no se contiene autorización suficientemente específica alguna para considerar necesario el tratamiento de datos biométricos con la finalidad de un control horario de la jornada de trabajo. La autorización suficientemente específica no se encuentra para el personal laboral, puesto que los artículos 20.3 y 34.9 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores, no contienen tal autorización. Tampoco para el personal sometido a una relación jurídica administrativa, al no constituirse en necesaria habilitación la previsión relacionada con el cumplimiento de jornada y horario a la que alude el art. 54.2 del texto refundido de la Ley del Estatuto Básico del Empleado Público (EBEP), aprobado por Real

[11] El resaltado no está presente en el original.

BORRADOR

Decreto Legislativo 5/2015, de 30 de octubre. Sería deseable, por tanto, disponer de un marco normativo que regulara específicamente, y con las garantías adecuadas, el posible tratamiento de datos biométricos en el contexto laboral.

En el ámbito laboral deberá atenderse asimismo a lo previsto en el artículo 88 RGPD y a su interpretación jurisprudencial y, en particular, al papel que pueden desempeñar los convenios colectivos en el establecimiento de normas más específicas y de garantías adecuadas para la protección de los derechos y libertades de las personas trabajadoras.

5.2. LICITUD DEL TRATAMIENTO Y CONSENTIMIENTO LIBRE DE LA PERSONA TRABAJADORA

El registro de jornada es una obligación legal impuesta al empresario (art. 34.9 ET), por lo que la base jurídica del tratamiento de registro de jornada se adecua a lo establecido en el art. 6.1.c): *"el tratamiento es **necesario** para el cumplimiento de una obligación legal aplicable al responsable del tratamiento"*, en conexión con el reiterado art. 34.9 del ET que dispone la obligación para la empresa de garantizar un registro diario de jornada que deberá incluir el horario concreto de inicio y finalización de jornada de cada persona trabajadora.

Cuando la excepción a la prohibición de tratar datos biométricos se fundamente en el artículo 9.2.b) del RGPD, deberá existir una norma con rango de ley o un convenio colectivo que autorice dicho tratamiento en los términos previstos en ese precepto. Asimismo, deberá concurrir una base jurídica de las previstas en el artículo 6.1 del RGPD que legitime el tratamiento, como la establecida en su letra c) cuando este sea necesario para el cumplimiento de una obligación legal aplicable al responsable.

Sin perjuicio de la existencia, en su caso, de una norma que permita el tratamiento, no cabe excluir que la excepción a la prohibición de tratar datos biométricos pueda fundarse en el consentimiento explícito previsto en el artículo 9.2.a) del RGPD, siempre que concurran todos los requisitos exigidos para su validez. En particular, para que el consentimiento pueda considerarse libre, deberá existir una posibilidad real de optar por medios alternativos para el control de acceso o de presencia que no impliquen el tratamiento de datos biométricos.

En el contexto laboral, el desequilibrio de poder entre empleador y persona trabajadora exige un examen especialmente riguroso de la libertad del consentimiento. El responsable deberá poder acreditar que la elección entre el sistema biométrico y la alternativa no biométrica es real y efectiva, y que esta última no comporta cargas, costes, penalizaciones, desventajas o menoscabos. La negativa o retirada del consentimiento tampoco podrá producir consecuencias adversas para la persona trabajadora.

Si la excepción a la prohibición de tratar datos biométricos se fundamentara en alguna de las restantes circunstancias previstas en el artículo 9.2 del RGPD, deberán concurrir igualmente los requisitos aplicables al tratamiento analizados con carácter general en esta guía.

5.3. SUBCONTRATACIÓN DE TRABAJADORES

La distribución de responsabilidades entre entidades contratantes y contratadas se determina por las funciones efectivamente desempeñadas, con independencia de la denominación que las partes atribuyan a su relación contractual. Deberá determinarse qué entidad decide los fines y los medios esenciales del tratamiento biométrico, así como si las distintas entidades actúan como responsables independientes, corresponsables o, respecto de operaciones concretas, como responsables y encargadas del tratamiento.

BORRADOR

En el caso de subcontratación de trabajadores, si el contratante exige por contrato sistemas biométricos para el establecimiento de un posible control de acceso, dicha exigencia ha de cumplir con lo establecido en este documento.

La entidad contratada, si además tuviera el rol de encargado del tratamiento, también tiene la obligación, como establece el art. 28.3 RGPD de: *"el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros"*.

Por lo tanto, cuando no se cumplan las condiciones establecidas en el RGPD, la entidad contratada no podrá implementar lícitamente el registro de jornada o el control de acceso mediante técnicas biométricas por el mero hecho de que dicha utilización haya sido exigida contractualmente por la empresa contratante.

6. CONCLUSIONES

Con relación a los tratamientos en el control de acceso mediante técnicas biométricas, los responsables del tratamiento han de tener en cuenta que:

- La utilización de tecnologías biométricas de identificación y autenticación en el control de acceso supone un tratamiento con probabilidad de entrañar un alto riesgo que incluye categorías especiales de datos.
- En cada caso, teniendo en cuenta la naturaleza, el alcance y el contexto del sistema biométrico utilizado, los responsables evaluarán el nivel de riesgo del tratamiento para los derechos y libertades de las personas físicas.
- En cualquier caso, previamente al inicio del tratamiento, será obligatoria la realización de una Evaluación de Impacto para la Protección de Datos en la que, entre otros, se encuentre documentada la acreditación de la superación del triple análisis de idoneidad, necesidad y proporcionalidad del tratamiento de datos biométricos.
- En la implementación de un tratamiento en el control de acceso hay que cumplir los principios de minimización y de protección de datos desde el diseño y por defecto, utilizando de entre las medidas igualmente eficaces las menos intrusivas y que traten los menos datos adicionales.
- Es necesario que exista una circunstancia para levantar la prohibición de tratar las categorías especiales de datos y, además, una condición que legitime el tratamiento.
    - El consentimiento puede levantar la prohibición y legitimar el tratamiento de datos biométricos. El responsable, teniendo en cuenta todas las circunstancias, deberá poder demostrar que el consentimiento ha sido otorgado libremente y que existe una alternativa real y cierta. Esto puede traducirse en el establecimiento de un método razonable y alternativo al tratamiento de datos biométricos, que podrá implicar la coexistencia de dos mecanismos de control de acceso que obviamente no son iguales. No obstante, este método alternativo no deberá suponer una carga, penalidad o menoscabo evidente para el interesado, ni representar un tratamiento claramente gravoso.
    - En el ámbito laboral, así como en otros contextos en los que pueda haber una asimetría de posiciones entre el responsable y el interesado, también podrá darse el consentimiento, guardándose obviamente las garantías exigibles.
    - En el caso del registro de jornada o del control de acceso con fines laborales, la excepción del artículo 9.2.b) del RGPD exige que el tratamiento biométrico sea necesario para el cumplimiento de obligaciones o el ejercicio de derechos específicos en el ámbito laboral y esté autorizado por una norma con rango de ley o, en los términos previstos por el Derecho nacional, por un convenio

BORRADOR

colectivo que establezca garantías adecuadas.
    - Cualquier utilización de los datos biométricos con finalidades adicionales a la de control de acceso deberá tener sus propias circunstancias de levantamiento de la prohibición y de condiciones que lo legitimen.
- En los tratamientos en el control de acceso, los responsables deben valorar si se toman decisiones automatizadas sin intervención humana basadas en el proceso biométrico. Cuando estas decisiones tengan efectos jurídicos sobre el interesado, o le afecten significativamente de modo similar, sólo podrán darse si se cumple la circunstancia de un interés público esencial. Este último deberá estar basado en una norma con rango de ley, ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.
- En el caso de que el sistema biométrico se implemente con técnicas de inteligencia artificial, para poder incluirlos en un tratamiento se deberán tener en cuenta las prohibiciones, limitaciones y exigencias establecidas en la normativa de inteligencia artificial.
- Superados todos los requisitos de cumplimiento de los principios generales del RGPD, en la implementación práctica del tratamiento en el control de acceso con técnicas biométricas de identificación o autenticación, deben implementarse garantías organizativas, técnicas y jurídicas. En particular, se recomiendan las siguientes medidas por defecto:
    - Informar a los interesados acerca del tratamiento biométrico y los riesgos asociados al mismo.
    - Implementar en el sistema biométrico la posibilidad de revocar el vínculo de identidad entre la plantilla biométrica y la persona física.
    - Implementar medios técnicos para asegurarse la imposibilidad de utilizar las plantillas para cualquier otro propósito.
    - Utilizar cifrado para proteger la confidencialidad, disponibilidad e integridad de la plantilla biométrica.
    - Utilizar formatos de datos o tecnologías específicas que imposibiliten la interconexión de bases de datos biométricos y la divulgación de datos no comprobada.
    - Suprimir los datos biométricos cuando no se vinculen a la finalidad que motivó su tratamiento.
    - Aplicar la minimización de los datos biométricos recogidos, con una evaluación objetiva de que no ha posibilidad de revelar categorías especiales de datos adicionales.
    - En el caso de registro de presencia o control de acceso en el ámbito laboral autorizado por convenio colectivo, éstos deben recoger el conjunto de garantías con relación a estos tratamientos en el sentido dispuesto en el art. 91 de la LOPDGDD.
- Entre las medidas recomendables para minimizar el riesgo se encuentran:
    - La utilización de tecnologías biométricas basadas en utilizar dispositivos bajo el control exclusivo de los usuarios y evitar el almacenamiento centralizado de las plantillas biométricas.
    - La toma de datos realizada de forma consciente por el individuo, e incluso con la exigencia de una acción positiva para iniciar el procesamiento de datos biométricos
    - La implementación de mecanismos automatizados de supresión de datos.
- Finalmente, todas las acciones y las medidas implementadas se revisarán, y en su

BORRADOR

caso se actualizarán, periódicamente o siempre que haya cambios significativos, ya sean normativos, técnicos u organizativos que afecten al tratamiento, sus fines, su naturaleza, ámbito o contexto.

BORRADOR