GUÍA SOBRE TRATAMIENTOS DE CONTROL DE PRESENCIA MEDIANTE SISTEMAS BIOMÉTRICOS

v. noviembre de 2023

ÍNDICE

I. INTRODUCCIÓN 4

A. Sistemas y datos biométricos 4

B. La plantilla biométrica como dato personal 4

C. El tratamiento de control de presencia 6

Registro de jornada 6

Control de acceso con fines laborales 7

Control de acceso con otras finalidades 7

II. PRINCIPIO DE MINIMIZACIÓN DE DATOS Y PROTECCIÓN DE DATOS DESDE EL DISEÑO 7

A. Minimización en el tratamiento del control de presencia 8

B. Minimización en las técnicas de recogida de información biométrica. 8

III. BIOMETRÍA EN UN TRATAMIENTO DE CONTROL DE PRESENCIA 8

A. Biometría como uno de los medios para implementar el tratamiento 10

B. Identificación y autenticación biométricas 10

C. Finalidades adicionales en un tratamiento de control de presencia a partir de los datos biométricos 12

IV. DATOS BIOMÉTRICOS Y CATEGORÍAS ESPECIALES DE DATOS 12

A. Identificación y autenticación como categorías especiales de datos 12

B. Biometría y su vinculación con otras categorías especiales de datos 13

V. LEVANTAMIENTO DE LA PROHIBICIÓN DE TRATAR CATEGORÍAS ESPECIALES DE DATOS 14

A. Excepción del art. 9.2.b RGPD: control de presencia para el registro de jornada y control de acceso con fines laborales. 14

Art. 9.2.b RGPD: Existencia de una norma de rango legal 14

Art 9.2.b RGPD: Necesidad 16

Art. 9.2.b RGPD: Idoneidad 17

B. Excepción del art. 9.2.a del RGPD: control de presencia para registro de jornada, control de acceso (con fines laborales o no) 18

Registro de jornada y control de acceso con fines laborales. 19

Control de acceso con fines no laborales 21

VI. LICITUD DEL TRATAMIENTO 21

A. Tratamiento de registro de jornada 21

B. Control de acceso con fines laborales o con otras finalidades. 22

VII. DECISIONES AUTOMATIZADAS 22

VIII. GESTIÓN DEL RIESGO Y EVALUACIÓN DE IMPACTO PARA LA PROTECCIÓN DE DATOS (EIPD) 23
A. Alto riesgo 23
B. Realización y superación de una EIPD 24
C. Superación del análisis de idoneidad, necesidad y proporcionalidad 26
D. Implementación 27
E. Contexto del tratamiento 27
F. Medidas mínimas por defecto 27
G. Brechas de datos personales 28
IX. SUBCONTRATACIÓN DE TRABAJADORES 29
X. CONCLUSIONES 29

I. INTRODUCCIÓN

En el presente documento se van a determinar los criterios para el tratamiento de control de presencia 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 aumentan el detalle de la información recogida, permiten la posibilidad de recoger información sin cooperación de la persona, a veces sin ser consciente de ello. A través de información disponible a en la red y a mayores distancias es posible tratar información biométrica. El desarrollo de la Inteligencia Artificial permite inferir información adicional sobre el sujeto mediante incluso categorías de datos sensibles. Los datos biométricos se pueden recoger y usar de forma transversal entre múltiples servicios físicos y de Internet.

Como consecuencia de ello, se han producido cambios en el contexto normativo, social y tecnológico, incluso en un período corto y cercano, que hacen necesario plantearse los límites al tratamiento de datos biométricos y las medidas que han de establecerse para que un tratamiento de datos personales que decida utilizar sistemas biométricos garantice el cumplimiento del RGPD, o de otras normativas que incidan en estos sistemas, en el caso de basarse en técnicas de inteligencia artificial, como el futuro Reglamento Europeo sobre Inteligencia Artificial.

A. SISTEMAS Y DATOS BIOMÉTRICOS

Los sistemas de procesamiento de datos biométricos se basan en recoger y procesar datos personales relativos a las características físicas, fisiológicas o conductuales de las personas físicas, entre las que cabe incluir, como se ha puesto de manifiesto recientemente, las características neuronales de estas, mediante dispositivos o sensores, creando plantillas biométricas (también denominadas firmas o patrones) que posibilitan la identificación, seguimiento o perfilado de dichas personas (esto es, "tratar", art. 4.2 del RGPD).

El RGPD define el art.4 .14 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 son datos biométricos todos aquellos que permitan la identificación o autenticación de una persona.

B. LA PLANTILLA BIOMÉTRICA COMO DATO PERSONAL

El art. 4.1 del RGPD define por datos personales:

> *1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios*

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

elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

Identificar a una persona, como resulta de dicho precepto, es determinar la identidad, directa o indirectamente, de la persona. Asignar un identificador es, pues, un proceso que permite singularizar a un individuo y, por tanto, las acciones dirigidas a él. En particular, entre otros medios posibles, a través de "*elementos propios de la identidad física, fisiológica, genética, psíquica*". En ese sentido, un tratamiento que permite singularizar a una persona entre varias utilizando, por ejemplo, un proceso de análisis biométrico conductual que diferencia y señala unívocamente a una persona, es un tratamiento de identificación.

El considerando 51, con relación a los datos biométricos, explica:

El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física.

Una fotografía, cuando se captura y almacena en un sistema digital, se codifica en un formato estándar mediante ceros y unos. La forma de codificación utilizada está orientada a poder reproducir la imagen para que vuelva a ser interpretable por un humano. Así, el considerando 51 RGPD, cuando manifiesta que el tratamiento de fotografías *"… no debe considerarse* ***sistemáticamente*** *tratamiento de categorías especiales …*", lo que está poniendo de manifiesto es que el contenido de esa fotografía o un tratamiento adicional ***puede llegar a ser*** un tratamiento de categorías especiales de datos[2].

Un dato biométrico contenido en un sistema se almacena en forma de una plantilla o patrón biométrico. Una plantilla biométrica es una forma de escritura de una característica biométrica humana, como un rostro o una huella dactilar, de manera que sea interpretable por una máquina de forma eficiente y eficaz para un propósito o propósitos determinados. La plantilla biométrica no está orientada a ser interpretada por una persona, como una fotografía, sino que está orientada a ser tratada en un proceso automatizado, es decir, ser eficiente y eficazmente interpretable por una máquina. Esta forma de almacenamiento permitiría singularizar a un individuo y ejecutar acciones de forma automática, perfilar o inferir información sobre un sujeto como actitudes o patrones de comportamiento, etc.

En el caso de operaciones de identificación o autenticación, para que una plantilla biométrica sea eficaz es necesario que las plantillas generadas a partir de dos individuos distintos sean claramente distinguibles. En ese caso, la plantilla actúa como un identificador único de la persona. El hecho de que, a partir de una plantilla biométrica, por ejemplo, de reconocimiento facial, no se pueda reconstruir el rostro original carece de relevancia, pues es un identificador único que lo singulariza unívocamente, al menos, en el marco de un tratamiento automatizado. De igual forma, a partir de únicamente del número de DNI no se puede reconstruir un nombre o un rostro. A ambos identificadores únicos, plantilla biométrica o número del DNI, se les puede asociar datos personales y atributos adicionales en un fichero. A diferencia de un número de DNI, la plantilla biométrica no es asignada a una persona, sino que se genera directamente de la observación de características físicas únicas e inalterables del propio individuo, sin necesidad de recurrir a documentos, otros dispositivos o bases de datos de terceros.

[2] Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108+) Informe Explicativo, párrafo 60 "Processing images of persons with thick glasses, a broken leg, burnt skin or any other visible characteristics related to a person's health can only be considered as processing sensitive data when the processing is based on the health information that can be extracted from the pictures."

Por lo tanto, una plantilla biométrica con propósito de identificación o autenticación es un dato personal per se y un identificador único[3].

C. EL TRATAMIENTO DE CONTROL DE PRESENCIA

El control de presencia es un tratamiento que puede servir para la consecución de distintas finalidades, y está sometido al efectivo cumplimiento de la normativa de protección de datos y sin perjuicio de las especificidades previstas en la norma para cada uno de los supuestos, en atención a la normativa a aplicar en cada caso.

Por un lado, el registro de jornada es un tratamiento de control de presencia que se encontraría enmarcado dentro de una relación laboral, con la finalidad de controlar el desenvolvimiento de la misma. Por otro, el control de acceso es un tratamiento de control de presencia que se encontraría vinculado a la finalidad de supervisar la entrada y/o salida a determinados recintos. Este último puede realizarse o no, dentro del ámbito laboral y con finalidades laborales. Ambos, en cuanto tratamiento de datos personales, tiene que cumplir en todo caso con los principios, derechos y obligaciones establecidos en el RGPD. El hecho de implementarlos mediante un sistema biométrico implica, además, consideraciones adicionales para el cumplimiento del RGPD.

Registro de jornada

En relación al 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.*
>
> *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.

[3] Grupo del Artículo 29 Documento de trabajo sobre biometría WP80 de 1 de agosto de 2003 apartado 3.8 Identificador único

Control de acceso con fines laborales

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".

Control de acceso con otras finalidades

Con independencia de la obligatoriedad del registro de jornada o del control de acceso con fines laborales, existen casos en los que también resulta preciso realizar un control de presencia que no necesariamente tiene que ver con una relación laboral. En esta situación, lo que se pretende es la consecución de una finalidad distinta que consiste en una supervisión de acceso de usuarios o clientes a determinados recintos o espacios, o bien que sea necesario para la ejecución de un contrato de, por ejemplo, disfrute de determinados servicios.

II. PRINCIPIO DE MINIMIZACIÓN DE DATOS Y PROTECCIÓN DE DATOS DESDE EL DISEÑO

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»);"*

El considerando 39 explica muy claramente 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…"*

Los datos que se traten han de ser limitados a lo necesario para conseguir los fines del tratamiento. En el caso que nos ocupa, la finalidad de un tratamiento de control de presencia no es tratar datos biométricos[4].

La aplicación de este principio se extiende, tanto a la obligación tener en cuenta la condición de necesidad, como también la 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 apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de*

[4] Existen tratamientos en los que el uso de datos biométricos forme parte de su finalidad, como podría ser un tratamiento relativo a la investigación de técnicas biométricas, donde sí se cumpliría la condición de necesidad.

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.

A. MINIMIZACIÓN EN EL TRATAMIENTO DEL CONTROL DE PRESENCIA

Atendiendo a lo establecido en los artículos 5.1.c y 25.1, en un tratamiento de control de presencia deben tratarse exclusivamente los datos necesarios para la consecución de dichos fines y no más de los necesarios. Así mismo, hay que aplicar dicha minimización cuando el tratamiento, entre otros y como sucede cuando hay involucrados sistemas biométricos, implique un riesgo para los derechos y libertades de las personas físicas.

Por lo tanto, hay que justificar la necesidad de un tratamiento adicional de datos cuando las mismas finalidades se han estado alcanzando y se pueden alcanzar con otro tipo de implementación del tratamiento de registro de jornada equivalente y menos intrusivo.

No es obligatorio, ni recomendable, que la implementación de un tratamiento, se limite exclusivamente a la selección de recursos tecnológicos. En las opciones de implementar un tratamiento hay que considerar, entre otros, la utilización de recursos humanos, las garantías jurídicas y los procedimientos organizativos. Por lo tanto, en la evaluación de alternativas equivalentes y menos intrusivas se han de explorar opciones que no sean solo tecnológicas.

B. MINIMIZACIÓN EN LAS TÉCNICAS DE RECOGIDA DE INFORMACIÓN BIOMÉTRICA.

Los distintos productos disponibles en el mercado para la recogida de datos biométricos que registran dichos datos con una precisión, detalle o frecuencia que están muy por encima de las necesidades de un determinado tratamiento específico, vulneran el principio de minimización.

En muchos casos, simplemente porque la tecnología lo permite y es asequible, estos productos recogen mucha más información de la que es realmente necesaria para la finalidad del tratamiento, o con mucho más detalle. El hecho de que una tecnología permita extraer más información de la imprescindible para la finalidad del tratamiento no justifica su utilización. En la selección de las tecnologías para la implementación de las operaciones del tratamiento se habrá de seguir el principio de minimización de datos (art.5.1.c) RGPD), que determina que los datos personales habrán de ser sólo los adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados, de forma que los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios (considerando 39). Incluso si está plenamente justificado y legitimado el uso de operaciones biométricas y el levantamiento de la prohibición de tratar categorías especiales de datos (art. 9.1 RGPD), cuando el responsable elige una determinada tecnología biométrica para implementar el tratamiento de control de presencia, tiene que aplicar el principio de minimización de datos desde el diseño (art. 25.1 RGPD), para ello seleccionar y/o configurar el sistema para adecuarlo a las necesidades concretas del tratamiento, y evaluar o conseguir una evaluación de forma objetiva cuyo resultado sea que no hay recogida de datos innecesarios para cumplir el propósito del tratamiento, en particular, categorías especiales de datos (art. 35 RGPD).

Por lo tanto, en sistemas biométricos para el control de presencia hay que realizar una evaluación objetiva de si se están recogiendo datos excesivos para la finalidad del tratamiento (ver apartado IV.B de este documento).

III. BIOMETRÍA EN UN TRATAMIENTO DE CONTROL DE PRESENCIA

El art. 4.2 del RGPD define “tratamiento” como:

"cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjunto de datos personales ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;"

El RGPD tiene como objeto (art. 1) establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.

El Tribunal de Justicia de la Unión Europea (en adelante TJUE) ha establecido una interpretación amplia tanto del concepto de "dato personal" como del concepto de "tratamiento de datos", en aras al objetivo declarado del RGPD de garantizar un nivel uniforme y elevado de protección de las personas físicas dentro de la Unión y reforzar y especificar los derechos de los interesados (considerandos 10 y 11 RGPD, y apartado 55 de la sentencia del TJUE de 22 de junio de 2023, C-579/21, Pankki S).

Así, en sus apartados 42 a 46 en la sentencia C-579/21, Pankki S, citada, el TJUE establece:

42 El empleo de la expresión «toda información» en la definición del concepto de «datos personales», que figura en esa disposición [art. 4.1 RGPD], evidencia el objetivo del legislador de la Unión de atribuir a este concepto un significado muy ***amplio****, que puede abarcar todo género de información, tanto objetiva como subjetiva, en forma de opiniones o apreciaciones, siempre que sean «sobre» la persona en cuestión (sentencia de 4 de mayo de 2023, Österreichische Datenschutzbehörde y CRIF, C-487/21, EU:C:2023:369, apartado 23).*

43 A este respecto, se ha declarado que una información se refiere a una persona física identificada o identificable cuando, debido a su contenido, finalidad o efectos, la información está relacionada con una persona identificable (sentencia de 4 de mayo de 2023, Österreichische Datenschutzbehörde y CRIF, C-487/21, EU:C:2023:369, apartado 24).

44 En cuanto al carácter «identificable» de una persona, el considerando 26 del RGPD precisa que deben tenerse en cuenta «todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física».

45 De ello resulta que la definición amplia del concepto de «datos personales» no abarca únicamente los datos recabados y conservados por el responsable del tratamiento, sino que ***incluye también toda la información resultante de un tratamiento de datos personales*** *que se refiera a una persona identificada o identificable (véase, en este sentido, la sentencia de 4 de mayo de 2023, Österreichische Datenschutzbehörde y CRIF, C-487/21, EU:C:2023:369, apartado 26).*

46 En segundo lugar, por lo que respecta al ***concepto de «tratamiento»****, tal como se define en el artículo 4, punto 2, del RGPD, procede señalar que, al utilizar la expresión «cualquier operación», el legislador de la Unión quiso dar a este concepto un* ***alcance amplio****, al emplear una* ***enumeración no exhaustiva de operaciones aplicadas a datos personales*** *o conjuntos de datos personales, que comprenden, entre otras cosas, la recogida, el registro, la conservación o incluso la consulta (véase, en este sentido, la sentencia de 4 de mayo de 2023,*

Österreichische Datenschutzbehörde y CRIF, C-487/21, EU:C:2023:369, apartado 27).

A. BIOMETRÍA COMO UNO DE LOS MEDIOS PARA IMPLEMENTAR EL TRATAMIENTO

Las técnicas y tecnologías empleadas en la implementación de un tratamiento forman parte de la naturaleza de este. Las operaciones de un tratamiento se podrán implementar de diversas formas: ya sean tratamientos manuales o automatizados, y estos últimos a su vez se pueden materializar con tecnologías distintas. Debido a la complejidad de las tecnologías disponibles, estas pueden implicar que se amplíe la extensión del tratamiento en cuanto a las categorías de datos tratadas, como puede ser, por ejemplo, en caso de tratamientos implementados sobre un portal web, que implica la recogida de identificadores como direcciones IP, cookies, firma del dispositivo, etc.

Si el tratamiento de datos personales consiste en el registro diario de la jornada, "registro de jornada", se requiere realizar un variado conjunto de operaciones, entre las que cabe incluir la identificación del empleado, la recogida de sus datos personales, su almacenamiento, la identificación y autenticación de este en el proceso de fichaje, el registro de tiempo y otros posibles datos (como localizaciones), su procesamiento para determinar excesos o faltas horarias, su conservación, la puesta a disposición de la Inspección de Trabajo, etc.

Algo similar ocurre cuando lo que se pretende es el control de acceso a determinados lugares con fines distintos a los laborales, dado que se requiere realizar un conjunto de operaciones, si bien en este caso no se trata de identificar a un empleado con el propósito de contabilizar sus horas laborales, sino simplemente identificar la entrada de una persona y, en ocasiones, también su salida.

Todas estas operaciones podrían ejecutarse empleando distintos medios humanos, técnicos y organizativos, bien mediante la exhibición de documentos, la comprobación de la integridad de estos, el contraste de información compartida, el uso de claves o certificados, el uso de tokens físicos, el análisis comportamental de la veracidad de sus afirmaciones, tratamientos mediante análisis automático del movimiento de un ratón u otro dispositivo de entrada/salida, análisis biométrico de la firma manuscrita, de huellas digitales, de manos, de voz, de reconocimiento facial, de iris, etc. Incluso con una combinación de varios de ellos, como, por ejemplo, empleando diferentes sistemas biométricos (multibiometría) con mayor o menor grado de intervención humana.

Un responsable de un tratamiento de control de presencia podría decidir, en principio y en detrimento de otras soluciones, el empleo de sistemas biométricos para implementar el tratamiento del control de presencia. En ese caso, el procesamiento biométrico no será un tratamiento con un fin en sí mismo, sino que es un medio para llevar a cabo operaciones dentro del tratamiento. Esta elección tomada por el responsable supone un tratamiento adicional de datos, en ese caso biométricos, para los que será necesario evaluar su conformidad con el RGPD.

B. IDENTIFICACIÓN Y AUTENTICACIÓN BIOMÉTRICAS

Identificación y autenticación son operaciones que no están definidas en el RGPD. Sin embargo, si se encuentran definidos en otra normativa de ámbito europeo como es el Reglamento 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS). En el art. 3 del Reglamento eIDAS se definen dichos términos de la siguiente manera:

1 «identificación electrónica», el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica;

5 «autenticación», un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico;[5]

Es decir, esta norma considera a la autenticación como un proceso electrónico que posibilita la identificación.

De una manera informal o intuitiva, cabe explicar el concepto de identificación como el proceso por el cual se reconoce a un individuo particular dentro de un grupo, comparándose los datos del individuo que se desea identificar con los datos de cada individuo en el grupo (uno-a-varios). La verificación o autenticación sería el proceso de probar que es cierta la identidad reclamada por un individuo, comparándose los datos del individuo únicamente con los datos asociados a la identidad reclamada (uno-a-uno).

Las primeras operaciones de identificación o autenticación biométrica en el tratamiento de control de presencia implementado biométricamente se realizan durante el alta o registro del empleado o durante el alta de una persona para poder acceder a un espacio o actividad. En este proceso es necesario identificar a la persona de forma correcta, pues de lo contrario todo el tratamiento de control de presencia podría estar viciado. Para ello se recogen una serie de atributos acreditables de su identidad. Así, podría identificarse al individuo con el DNI y, a continuación, recoger datos adicionales en el proceso de alta, en particular, sus datos biométricos. Pero también podría darse el caso de que se autentiquen los documentos presentados, por ejemplo, el DNI, mediante análisis biométrico de la correspondencia de la foto del DNI con la imagen de la persona presente, por lo que se tendría una operación de autenticación (uno-a-uno). O bien, se podrían recoger los datos biométricos en primer lugar para identificarlo contra una base de datos de almacenamiento de atributos (como nombre o número de DNI) en una búsqueda de uno entre muchos (uno-a-varios), por lo que tendríamos una operación de identificación.

A continuación, se realiza de forma regular un proceso de control de la persona con el objetivo de recoger sus datos de inicio/fin de la jornada laboral o de entrada y, en su caso, salida de un determinado lugar o espacio. En el caso de emplear sistemas biométricos, se puede hacer mediante un proceso de identificación, cuando se recoge el dato biométrico para compararlo con una base de datos en la que se almacenan los atributos de, por ejemplo, nombre o número de empleado (uno-a-varios). El proceso, para que fuese de autenticación se tendría que implementar a la inversa, se realizaría en primer lugar la identificación mediante, por ejemplo, una tarjeta de identidad, y posteriormente se autenticaría al individuo biométricamente contra los datos almacenados en el sistema asociados a los atributos de identidad.

Por lo tanto, en un tratamiento de control de presencia, ya sea para el registro de jornada como para el control de acceso (para finalidades laborales o para otras finalidades), que emplee sistemas biométricos, podrían existir diferentes alternativas de implementación: bien (i) basadas en dos operaciones de identificación, (ii) basadas en una de autenticación y otra de identificación, o (iii) basadas en una única operación de autenticación.

[5] En la última redacción de la propuesta de modificación del Reglamento eIDAS se estable “autenticación”, un proceso electrónico que permite confirmar la identificación electrónica de una persona física o jurídica, o el origen y la integridad de datos en forma electrónica;»

Sin embargo, la casuística podría ser incluso más compleja para tratamientos concretos y el responsable debe describir con detalle las operaciones biométricas que se ejecutan en el marco de un registro de jornada en cada caso.

C. FINALIDADES ADICIONALES EN UN TRATAMIENTO DE CONTROL DE PRESENCIA A PARTIR DE LOS DATOS BIOMÉTRICOS

Los datos biométricos recogidos en el marco del tratamiento de control de presencia son susceptibles de ser utilizados ("tratados") con otros propósitos o finalidades diferentes de los iniciales, ya que son tratamientos que, en definitiva, identifican de una manera u otra a una persona; por ejemplo, un registro de jornada podría utilizarse para otras cuestiones: seguridad física, control de acceso a ciertos espacios o recursos de la propia entidad, evaluación de rendimiento laboral, etc.

Todos estos propósitos, que muchas veces se presentan como ventajas adicionales a la decisión de implementar el tratamiento de registro de jornada o el control de acceso con operaciones biométricas, han de ser considerados tratamientos con finalidades distintas a los efectos de la normativa de protección de datos personales. Por lo tanto, la posibilidad de ejecutar dichos tratamientos depende del cumplimiento de todos los principios, derechos y obligaciones establecidos en el RGPD.

IV. DATOS BIOMÉTRICOS Y 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".

A. IDENTIFICACIÓN Y AUTENTICACIÓN COMO CATEGORÍAS ESPECIALES DE DATOS

En el art. 9, apartado 1, dentro de dichos datos de categorías especiales, se encuentran los *"datos biométricos dirigidos a identificar de manera unívoca a una persona física"*.

El considerando 51, al mencionar los datos biométricos, interpreta que en dicho concepto se encuentran comprendidos aquellos datos de tal carácter cuando su tratamiento con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física.

> *El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de* ***datos biométricos*** *cuando el hecho de ser tratadas con medios técnicos específicos* ***permita la identificación o la autenticación unívocas de una persona física****. Tales datos personales* ***no deben ser tratados****, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, …"*[6]

Las 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), determinan, en su apartado 12, que el concepto de dato biométrico abarca tanto la "autenticación" como la "identificación", y si bien son conceptos distintos, en ambos procedimientos se tratan datos dirigidos a identificar a una persona física, por lo que ambos se incluyen en el concepto de "tratamientos de datos", y más específicamente, son tratamientos de datos personales de categorías especiales. En

[6] El resaltado no está en el original

consecuencia, a ambos se extiende la prohibición general establecida en el art. 9.1 del RGPD, por lo que dicha prohibición ha de aplicar no sólo a los tratamientos dirigidos a la identificación sino también a los supuestos de tratamientos de datos biométricos dirigidos a la autenticación o verificación de la persona con respecto al patrón previamente establecido para la misma.

La Agencia Española de Protección de Datos publicó en mayo de 2021 la guía "La Protección de Datos en las Relaciones Laborales", en la que se abordaba en el apartado "Los datos biométricos" del capítulo 4.6 el empleo de biometría en la implementación de los tratamientos de registro de presencia. En el texto se interpretaba la autenticación biométrica fuera de las categorías especiales de datos. Sin embargo, esta interpretación ha sido superada por las Directrices antes citadas, por lo que la interpretación de esta AEPD ha de adaptarse a las Directrices del CEPD mencionadas de 26 de abril de 2023.

Del mismo modo, la interpretación que de estos tipos de tratamientos hacía esta AEPD en su Informe Jurídico 036/2020, basándose, entre otros documentos, en el Dictamen 3/2012 del Grupo de Trabajo del Artículo 29 (GT29), sobre la evolución de las tecnologías biométricas, - publicado en un momento, 2012, en que ni unos ni otros datos biométricos tenían la consideración de categoría especial (sólo a partir de la entrada en vigor del GDPR en 2016)-, ha de considerarse igualmente superada por la nueva posición del CEPD, expuesta en dichas Directrices 05/2022.

En definitiva, se ha de considerar que, al igual que en el caso de identificación, la autenticación biométrica es un proceso que implica el tratamiento de categorías especiales de datos personales.

B. BIOMETRÍA Y SU VINCULACIÓN CON OTRAS CATEGORÍAS ESPECIALES DE DATOS

La consideración de categoría especial de datos debe interpretarse de manera amplia. El art. 9.1 del RGPD establece que categorías especiales de datos son aquellos que "***revelen***" cierto tipo de información. El término "revelen" debe entenderse en el sentido que, además de los datos que por su naturaleza contienen información sensible, también son categorías especiales los datos de los que puede deducirse información sensible relativa a una persona[7]. En el mismo sentido se manifiestan las conclusiones del TJUE "*con relación al propósito de la Directiva, la expresión "datos relativos a la salud" usada en el artículo 8(1) del mismo modo de darse una interpretación amplia para incluir la información concerniente a todos los aspectos, físicos y mentales, de la salud de un individuo*"[8].

En ese sentido, la interpretación de los datos biométricos como categorías especiales de datos debe tener en cuenta la posibilidad de que, mediante el análisis biométrico, se puedan inferir y recoger otras categorías especiales de datos y, en particular, datos relativos a la salud o datos que revelen el origen racial o étnico entre otros.

El desarrollo tecnológico está permitiendo extraer cada vez más detalles de los rasgos biométricos de una persona. Por ejemplo, un análisis biométrico de la voz humana puede recoger más de cien parámetros distintos que permiten extraer información de salud, problemas físicos o sicológicos, entre otros. En sistemas biométricos basados en el reconocimiento facial se pueden tratar datos que revelan el origen racial o étnico[9], y también se puede extraer información de salud, problemas físicos o sicológicos como en el caso de

[7] Página 6 del documento del Grupo de Trabajo del Artículo 29 Advice paper on special categories of data ("sensitive data").

[8] TJUE, 6 noviembre 2003, Bodil Lindqvist, C-101/01, párrafo 50

[9] Grupo del Artículo 29 Documento de trabajo sobre biometría WP80 de 1 de agosto de 2003 apartado 3.7 Datos sensibles

la voz, incluso algunos sistemas de identificación mediante huella dactilar permiten el registro de parámetros como la temperatura o la presión sanguínea.

V. LEVANTAMIENTO DE LA PROHIBICIÓN DE TRATAR CATEGORÍAS ESPECIALES DE DATOS

La especial protección que establece el RGPD en su art. 9 a determinadas categorías de datos 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.

A. EXCEPCIÓN DEL ART. 9.2.B RGPD: CONTROL DE PRESENCIA PARA EL REGISTRO DE JORNADA Y CONTROL DE ACCESO CON FINES LABORALES.

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"*[10]

A su vez, cabe indicar que la mención a la autorización por el Derecho de los Estados miembros de la UE debe entenderse referida, en el caso del Estado Español, a la existencia de una norma previsora de rango legal en consonancia con lo dispuesto en el art. 53.1 de la Constitución Española, por tratarse del desarrollo de un derecho, el de la protección de datos personales, reconocido como fundamental. Abundando al respecto, la sentencia del **Tribunal Constitucional 76/2019**, de 22 de mayo, precisa que la norma legal debe reunir todas las características indispensables como garantía de la seguridad jurídica, **expresando todos y cada uno de los presupuestos y condiciones de la intervención**, de forma que las limitaciones del derecho fundamental establecidas por una ley pueden vulnerar la Constitución si adolecen de falta de certeza y previsibilidad.

En concreto, el Tribunal Constitucional, en la citada STC 76/2019, de 22 de mayo, tras citar, entre otras, a su anterior STC 292/2000, de 30 de noviembre, señala:

> *- En segundo lugar, por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas ora incida directamente sobre su desarrollo (art. 81.1 CE), ora limite o condicione su ejercicio (art. 53.1 CE), precisa una habilitación legal (por todas, STC 49/1999, de 5 de abril,*

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

FJ 4). En la STC 49/1999, FJ 4, definimos la función constitucional de esa reserva de ley en los siguientes términos:

Esa reserva de ley a que, con carácter general, somete la Constitución española la regulación de los derechos fundamentales y libertades públicas reconocidos en su Título I, desempeña una doble función, a saber: de una parte, asegura que los derechos que la Constitución atribuye a los ciudadanos no se vean afectados por ninguna injerencia estatal no autorizada por sus representantes; y, de otra, en un Ordenamiento jurídico como el nuestro en el que los Jueces y Magistrados se hallan sometidos "únicamente al imperio de la Ley" y no existe, en puridad, la vinculación al precedente (SSTC 8/1981, 34/1995, 47/1995 y 96/1996) constituye, en definitiva, el único modo efectivo de garantizar las exigencias de seguridad jurídica en el ámbito de los derechos fundamentales y las libertades públicas. Por eso, en lo que a nuestro Ordenamiento se refiere, hemos caracterizado la seguridad jurídica como una suma de legalidad y certeza del Derecho (STC 27/1981, fundamento jurídico 10).”

Esta doble función de la reserva de ley se traduce en una doble exigencia: por un lado, la necesaria intervención de la ley para habilitar la injerencia; y, por otro lado, esa norma legal “ha de reunir todas aquellas características indispensables como garantía de la seguridad jurídica”, esto es, “ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención” (STC 49/1999, FJ 4). En otras palabras, “no sólo excluye apoderamientos a favor de las normas reglamentarias […], sino que también implica otras exigencias respecto al contenido de la Ley que establece tales límites” (STC 292/2000, FJ 15).

La segunda exigencia mencionada constituye la dimensión cualitativa de la reserva de ley, y se concreta en las ***exigencias de previsibilidad y certeza de las medidas restrictivas en el ámbito de los derechos fundamentales****. En la STC 292/2000, FJ 15, señalamos que, aun teniendo un fundamento constitucional, las limitaciones del derecho fundamental establecidas por una ley «pueden vulnerar la Constitución si adolecen de falta de certeza y previsibilidad en los propios límites que imponen y su modo de aplicación», pues «****la falta de precisión de la ley en los presupuestos materiales de la limitación de un derecho fundamental es susceptible de generar una indeterminación sobre los casos a los que se aplica tal restricción»;*** *«al producirse este resultado, más allá de toda interpretación razonable, la ley ya no cumple su función de garantía del propio derecho fundamental que restringe, pues deja que en su lugar opere simplemente la voluntad de quien ha de aplicarla». En la misma sentencia y fundamento jurídico precisamos también el tipo de vulneración que acarrea la falta de certeza y previsibilidad en los propios límites: «no sólo lesionaría el principio de seguridad jurídica (artículo 9.3 CE), concebida como certeza sobre el ordenamiento aplicable y expectativa razonablemente fundada de la persona sobre cuál ha de ser la actuación del poder aplicando el Derecho (STC 104/2000, FJ 7, por todas), sino que al mismo tiempo dicha ley estaría lesionando el contenido esencial del derecho fundamental así restringido, dado que la forma en que se han fijado sus límites lo hacen irreconocible e imposibilitan, en la práctica, su ejercicio (SSTC 11/1981, FJ 15; 142/1993, de 22 de abril, FJ 4, y 341/1993, de 18 de noviembre, FJ 7)»*[11]*.*

Y en el apartado 16 de la STC 292/2000, citada de nuevo por la STC 76/2019, se especifica:

[11] El resaltado no está en el orignal

(…) Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante ***reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias****. Pues en otro caso el legislador habría trasladado a la administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del artículo 53.1 CE, esto es, establecer claramente el límite y su regulación.*

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, 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 cumplimento 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 Decreto Legislativo 5/2015, de 30 de octubre.

Art 9.2.b RGPD: Necesidad

El art. 9.2.b) del RGPD, con relación al tratamiento en el ámbito del Derecho laboral y de la seguridad y protección social, no solo exige que exista una habilitación legal -o convenio colectivo-, sino que impone en primer término el requisito de que el tratamiento sea "necesario".

Los sistemas automáticos de control de jornada existen desde 1890[12], y el registro de presencia se ha realizado durante varios siglos a través de medios no biométricos. Por poner un ejemplo, en los años 80 del siglo XX existían más de doce millones de trabajadores en España[13] sometidos a control de jornada. La mayor factoría de vehículos en España tenía en esa época más de 30.000 trabajadores[14], cifra que actualmente no llega a la mitad[15]. En definitiva, en el marco de grandes volúmenes de trabajadores, el empleador disponía de potestad y capacidad para establecer un control de jornada.

[12] https://en.wikipedia.org/wiki/Time_clock

[13] https://elpais.com/diario/1981/03/12/economia/353199602_850215.html

[14] https://infogram.com/evolucion-empleados-seat-1g4qpz7vxgd8m1y

[15]https://www.seat-mediacenter.es/smc/seat-sa/facilitiespage/martorell-production-facility#:~:text=En%20sus%2015%20edificios%20trabajan,por%20carretera%2C%20mar%20y%20tren.

El responsable de dichos tratamientos, a la hora de proponer operaciones biométricas, debe justificar las circunstancias por las que *ya no es posible* utilizar los sistemas de registro de presencia que se estaban empleando en el mismo centro hasta ese momento, o que se están empleando en entidades equivalentes. Además, debe justificar que el empleo de otros sistemas existentes como tarjetas, certificados, claves, sistemas *contact-less*, etc. que evitan el tratamiento de categorías especiales de datos no son adecuados. También, hay que tener en cuenta que un tratamiento de datos personales también puede contar en sus operaciones con intervención humana, es decir, no existe una obligación a que se implementen exclusivamente con medios tecnológicos. Dicha intervención humana puede ser el adecuado complemento para otras opciones.

En el mismo sentido, el proceso de información biométrica ha de ser *esencial* para satisfacer el cumplimiento de la finalidad de registro de presencia, como establece el Dictamen 3/2012 del Grupo de Trabajo del Artículo 29, sobre la evolución de tecnologías biométricas:

> *"… es preciso considerar previamente si el sistema es necesario para responder a la necesidad identificada, es decir, si es esencial para satisfacer esa necesidad, y no sólo lo más adecuado o rentable. Un segundo factor que debe tenerse en cuenta es la probabilidad de que el sistema sea eficaz para responder a la necesidad en cuestión a la luz de las características específicas de la tecnología biométrica que se va a utilizar."*

Por lo tanto, la evaluación de la necesidad ha de superarse mediante evidencias objetivas, con una visión amplia del contexto y evitando guiarse sólo por tendencias tecnológicas. Cuando en la evaluación intervengan elementos distintos a la finalidad del tratamiento o a la protección de derechos, como por ejemplo condicionantes económicos, de empleo, de técnicas de mercado (como la compra impulsiva), o la posibilidad de conseguir el consentimiento para tratamientos adicionales, se ha de realizar una evaluación rigurosa de la proporcionalidad del tratamiento.

En conclusión, tal y como se ha indicado anteriormente, debe tenerse en cuenta el art. 5.1.c y el considerando 39 del RGPD que indica que los datos personales sólo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Nuevamente, se señala que debe realizarse un análisis previo sobre la necesidad de dicho tratamiento para la consecución de la finalidad pretendida por el responsable del tratamiento, en el sentido de que no haya otro medio igual de eficaz y menos intrusivo, antes de la implantación de cualquier sistema; y todo ello debe de ser evaluado desde el Principio de protección de datos desde el diseño, focalizando el análisis en los derechos y libertades de las personas cuyos datos se van a tratar, dentro de ese primer paso. Para ello debería realizarse el correspondiente análisis de riesgos y superarse la evaluación de impacto y tener en cuenta el triple juicio de idoneidad, necesidad y proporcionalidad.

Art. 9.2.b RGPD: Idoneidad

En todo caso, dicha ley -o convenio colectivo- que establece el tratamiento deberá respetar el principio de proporcionalidad, tal y 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).”

Como establece el Dictamen 3/2012 del Grupo de Trabajo del Artículo 29, sobre la evolución de tecnologías biométricas:

“… Un segundo factor que debe tenerse en cuenta es la probabilidad de que el sistema sea eficaz para responder a la necesidad en cuestión a la luz de las características específicas de la tecnología biométrica que se va a utilizar.”

Para que un tratamiento se pueda considerar idóneo, 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 ello, es necesario que estén definidas métricas, no solo sobre el rendimiento de los sistemas biométricos, sino también sobre los objetivos de rendimiento necesarios en el tratamiento para el registro de jornada. Es preciso realizar un análisis objetivo sobre la adecuación de las distintas opciones técnicas para el registro de presencia, 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.

B. EXCEPCIÓN DEL ART. 9.2.A DEL RGPD: CONTROL DE PRESENCIA PARA REGISTRO DE JORNADA, CONTROL DE ACCESO (CON FINES LABORALES O NO)

Cabría considerar el levantamiento de la prohibición del tratamiento de datos biométricos por concurrencia de la prestación del consentimiento *explícito* por parte del interesado para el tratamiento de dichos datos personales con uno o más de los fines especificados (salvo establecimiento expreso contrario a tal sentido por parte del derecho de la Unión o de sus estados miembros), según se establece en el art. 9.2.a) del RGPD.

El art. 4.11 del RGPD se refiere al consentimiento del interesado como “*toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*”. La información proporcionada al interesado a de, entre otros, hacer consciente a los interesados de los riesgos de dicho tratamiento (considerando 39 del RGPD), especialmente cuando afecta a personas se encuentre en situación de vulnerabilidad[16].

[16] “They should also be informed on how the collection, use or sharing of facial recognition data is likely to affect them, especially when they concern persons in vulnerable situations. The information provided also has to state which rights and legal remedies the data subjects are entitled to.” Guidelines on Facial Recognition. Consultative Committee of The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data - Convention 108

Existen tratamientos que implican el uso de sistemas biométricos, distintos a los de control de acceso como puede ser el participar voluntariamente en una investigación sobre técnicas biométricas de identificación, en los que el interesado podría otorgar el consentimiento de tratar sus datos biométricos libremente con el objeto de participar como sujeto de prueba en dicha investigación. En la finalidad de dicho tratamiento está el tratar datos biométricos y participar como sujeto de prueba de forma libre implica el tratar los datos biométricos.

Registro de jornada y control de acceso con fines laborales.

En el tratamiento de registro de jornada, el empleado tiene la obligación de participar en el tratamiento cuya finalidad es dicho registro y no el de tratar datos biométricos. En este caso, el consentimiento no aplica sobre el tratamiento de registro de jornada en sí, donde no cabe oponerse, sino sobre el tratamiento adicional que suponen los datos biométricos.

De esta forma, en el tratamiento del registro de jornada y con relación a la libertad del consentimiento para ese tratamiento adicional de datos, el considerando 43 del RGPD establece que:

> *"para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular".*

Las condiciones para la consideración del consentimiento se prevén en el art. 4.11 y 7 del RGPD, pudiendo acudirse también a las Directrices 5/2020 del CEPD, sobre el consentimiento en el sentido del RGPD. En particular, estas interpretan que en el contexto de las relaciones laborales, de forma general, se produce un desequilibrio de poder entre empleado y empleador que hace que este consentimiento no se proporcione libremente por lo que no debe ser la base jurídica. A mayor abundamiento, en dicho contexto, el consentimiento del interesado no puede servir en ningún caso como circunstancia del levantamiento de una prohibición de tratar categorías especiales de datos. Así, dichas Directrices 5/2020 establecen

> *21. También en el contexto del empleo se produce un desequilibrio de poder. Dada la dependencia que resulta de la relación entre el empleador y el empleado, no es probable que el interesado pueda negar a su empleador el consentimiento para el tratamiento de datos sin experimentar temor o riesgo real de que su negativa produzca efectos perjudiciales. Parece poco probable que un empleado pudiera responder libremente a una solicitud de consentimiento de su empleador para, por ejemplo, activar sistemas de vigilancia por cámara en el lugar de trabajo o para rellenar impresos de evaluación, sin sentirse presionado a dar su consentimiento. Por tanto, el CEPD considera problemático que los empleadores realicen el tratamiento de datos personales de empleados actuales o futuros sobre la base del consentimiento, ya que no es probable que este se otorgue libremente. En el caso de la mayoría de estos tratamientos de datos en el trabajo, la base jurídica no puede y no debe ser el consentimiento de los trabajadores [art. 6, apartado 1, letra a)] debido a la naturaleza de la relación entre empleador y empleado.*

Una limitación al uso del consentimiento se hace expresa en las mismas Directrices con relación al recurso al consentimiento en el marco de las AA.PP.:

> *16. El considerando 43 indica claramente que no es probable que las autoridades públicas puedan basarse en el consentimiento para realizar el tratamiento de datos*

ya que cuando el responsable del tratamiento es una autoridad pública, siempre hay un claro desequilibrio de poder en la relación entre el responsable del tratamiento y el interesado. Queda también claro en la mayoría de los casos que el interesado no dispondrá de alternativas realistas para aceptar el tratamiento (las condiciones de tratamiento) de dicho responsable. El CEPD considera que hay otras bases jurídicas que son, en principio, más adecuadas para el tratamiento de datos por las autoridades públicas.

Sin embargo, se deja la puerta abierta a que el responsable demuestre que no tendrá consecuencias adversas para el interesado denegar el consentimiento:

22. No obstante, esto no significa que los empleadores no puedan basarse nunca en el consentimiento como base jurídica para el tratamiento de datos. Puede haber situaciones en las que el empleador pueda demostrar que el consentimiento se ha dado libremente. Dado el desequilibrio de poder entre un empleador y los miembros de su personal, los trabajadores únicamente pueden dar su libre consentimiento en circunstancias excepcionales, cuando el hecho de que otorguen o no dicho consentimiento no tenga consecuencias adversas.

En el caso del registro de jornada, como el interesado tiene la obligación de registrar su jornada, únicamente podría considerarse la existencia de un consentimiento libre a un tratamiento adicional de datos, en este caso biométricos, si el interesado dispone de una alternativa de libre elección para cumplir con dicha obligación. En este sentido, las mismas Directrices interpretan:

37. El responsable del tratamiento podría argumentar que su organización ofrece a los interesados una elección real si estos pudieran escoger entre un servicio que incluya el consentimiento para el uso de datos personales con fines adicionales, y un servicio equivalente ofrecido por el mismo responsable que no implicara prestar el consentimiento para el uso de datos con fines adicionales. Siempre que exista una posibilidad de que dicho responsable del tratamiento ejecute el contrato o preste los servicios contratados sin el consentimiento para el otro uso o el uso adicional de los datos en cuestión, significará que ya no hay condicionalidad con respecto al servicio. No obstante, ambos servicios deben ser realmente equivalentes.

Cuando existan opciones realmente equivalentes y disponibles para todos los trabajadores, se podría estudiar si el consentimiento fuese válido, cumpliendo con los requisitos del art. 4.11 del RGPD y el resto de las condiciones del art. 7 del RGPD.

Sin embargo, y respecto de este requisito de la posible "equivalencia de los tratamientos" hay que tener en cuenta que, si existen alternativas disponibles al tratamiento de datos biométricos que impliquen menor riesgo para los derechos y libertades de las personas cuyos datos personales se van a tratar, que permitan que en un momento dado todos los trabajadores opten por otras alternativas, el procesamiento de datos biométricos deja de ser *necesario* para la implementación del tratamiento.

Al no ser necesario el tratamiento de datos biométricos, no se estaría cumpliendo con lo establecido en el art. 5.1.c del RGPD, y como se explicará más adelante en el capítulo VIII de este documento, al ser un tratamiento de alto riesgo, no cumpliría por tanto el requisito de "*necesidad*" que le impone el art. 5.1 y 35.7.b. Si el tratamiento es de alto riesgo, además de ser necesario, tiene que demostrarse la evaluación positiva de *necesidad* (art. 35.7.b del RGPD); que en este caso no se cumpliría, precisamente por esa falta de necesidad.

Por lo tanto, en un tratamiento de registro de jornada implementado con técnicas biométricas el consentimiento del interesado no levanta la prohibición del tratamiento, con

carácter general, al existir una situación en la que existe un desequilibrio con el responsable del tratamiento, como ocurre en el ámbito de una relación laboral (o administrativa/funcionarial), y no superaría la evaluación de necesidad, requisito para tratamientos de alto riesgo (ver apartado VIII.A).

Control de acceso con fines no laborales

Un análisis similar podría establecerse para el control de acceso con finalidades diferentes a las laborales. El consentimiento debe ser libre, específico, informado e inequívoco. Entre otros, el responsable del tratamiento debe establecer un método alternativo para poder realizar el control de acceso, sin tener ninguna consecuencia para la persona que no quiera utilizar el control de acceso mediante un tratamiento de datos biométricos.

De igual forma que en el caso anterior, debe demostrarse la necesidad objetiva (requisito para tratamientos de alto riesgo ver apartado VIII.A) y las posibles alternativas, de tal manera que para poder tratar esos datos biométricos no exista otra alternativa que sirva para satisfacer la necesidad identificada y que implique un riesgo menor en los derechos y libertades de las personas físicas.

VI. LICITUD DEL TRATAMIENTO

Si no se ha levantado la prohibición del tratamiento de categorías especiales de datos personales, en este caso biométricos, es indiferente que se cuente con una base jurídica de las previstas en el art. 6.1 del RGPD, puesto que ya hay una condición que invalida el tratamiento.

Una vez que se ha levantado la prohibición, cabe analizar si dicho tratamiento se pretende desplegar en el marco de al menos una de las condiciones enumeradas el art. 6.1 del RGPD. Es decir, no se debería proponer un tratamiento y, a continuación, buscar una condición de licitud. Al contrario, debería existir una condición (la causa) definida en el art. 6.1 del RGPD para que un responsable decida realizar un tratamiento (el efecto).

A. TRATAMIENTO DE REGISTRO DE JORNADA

El registro de jornada es una obligación legal impuesta al empresario y al trabajador (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 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.

En este caso, si el levantamiento de la prohibición de un tratamiento adicional de datos biométricos se ha realizado en base a lo establecido en el art. 9.2.b) de RGPD, debe existir una norma con rango de ley que ampare dicha excepción y, por lo tanto, dicha norma englobará la licitud del tratamiento de acuerdo con el art. 6.1.c).

Ya se ha indicado anteriormente que, a los efectos de levantar la prohibición del art. 9.2.b) del RGPD, la normativa actual precitada no es suficiente en los términos previstos en el RGPD.

Por otro lado, en vez del art. 9.2.b) del RGPD, se ha podido considerar levantar la prohibición de un tratamiento adicional de datos biométricos teniendo en cuenta lo previsto en el art. 9.2.a) RGPD. En ese caso, para poder considerar el consentimiento libre han de existir, como se ha expuesto, la posibilidad de implementar opciones equivalentes. Si estas existen en el propio tratamiento, o es factible implementarlas, y son menos intrusivas en

relación con los derechos y libertades de los interesados, no se cumpliría, como ya se desarrollado en el apartado anterior, el requisito de la "necesidad" establecido en el art. 6.1.c) del RGPD.

Si el levantamiento de la prohibición de tratar datos biométricos se ha basado en otras previsiones distintas al art. 9.2.a) y al art. 9.2.b), también hay que preguntarse si existen esas otras opciones equivalentes y menos intrusivas para implementar el registro de jornada.

La realidad es que, en la argumentación de muchos responsables al fundamentar el levantamiento de la prohibición en el consentimiento libre al proporcionar alternativas a los interesados, han hecho evidente la posibilidad y la viabilidad de dichas alternativas. Por lo tanto, aunque el levantamiento de la prohibición se haya basado en otras previsiones distintas de las del art. 9.2.a), eso no implica de forma automática que no existan esas alternativas. Puede ocurrir que el responsable ha decidido no implementar las alternativas, en ese caso, el responsable tendrá que justificar de forma objetiva que en su caso concreto sí son necesarias.

El mismo razonamiento aplicaría a cualquiera de las bases jurídicas previstas en el art. 6.1. del RGPD, del 6.1.b al 6.1.f, pues siempre se debe cumplir con el requisito de necesidad para la consecución de la finalidad, que esta enunciado en cada una de dichas bases jurídicas.

B. CONTROL DE ACCESO CON FINES LABORALES O CON OTRAS FINALIDADES.

En el caso que el responsable decida basar la licitud de tratar datos biométricos en el art. 6.1.a) del RGPD en un tratamiento de control de acceso con fines laborales o con otras finalidades distintas a las laborales, se trasladan las conclusiones alcanzadas en el apartado V.B de este texto.

En el caso de fundamentar la licitud de emplear datos biométricos en tratamientos de control de acceso en otros supuestos del art. 6.1 del RGPD distintos del consentimiento, se tendrán que atender los requisitos de necesidad, presente en todos ellos, además de los de reserva de ley en las letras c) y d) y también en el caso de la letra f) la superación del análisis de prevalencia entre los intereses legítimos del responsable y los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

VII. DECISIONES AUTOMATIZADAS

El art. 22 del RGPD establece restricciones y garantías cuando un proceso automatizado sin intervención humana produce efectos jurídicos sobre el interesado o le afecte significativamente de modo similar.

Un tratamiento de control de presencia se podría implementar por parte del responsable como un proceso automatizado basado en un sistema biométrico sin intervención humana 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, al impedir el acceso, y sin posibilidad de intervención humana, tenga un impacto de forma automática sobre la persona, ya sea sobre el trabajador en su salario o en su empleo, entre otros. 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.

Cuando el responsable configure el tratamiento de control de presencia de esta forma, hay que tener en cuenta que, según el art. 22. del RGPD, no pueden basarse en las categorías especiales de datos salvo que:

- Se base el levantamiento de la prohibición en el consentimiento (9.2.a) o el interés público esencial (9.2.g) ambos del RGPD.
- Y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado. Entre dichas medidas, como mínimo (art. 22.3 RGPD) deberán figurar las de:
    - El derecho a obtener intervención humana por parte del responsable,
    - A expresar su punto de vista y
    - A impugnar la decisión.

Al no aplicar el art. 9.2.a del RGPD como ya se ha explicado, ni el art. 9.2.g del RGPD, en el caso de que se plantee el control de presencia como un tratamiento en el que hay decisiones automatizadas sin una intervención humana con la competencia para revertir la decisión no se podrá utilizar un proceso de identificación o autenticación biométrica.

VIII. GESTIÓN DEL RIESGO Y EVALUACIÓN DE IMPACTO PARA LA PROTECCIÓN DE DATOS (EIPD)

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 presencia a través de sistemas biométricos, se realice una gestión del riesgo (art. 24.1 RGPD) y desde el diseño y por defecto (art. 25 RGPD) se apliquen las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD. En particular, en caso de alto riesgo, deberá superar favorablemente una Evaluación de Impacto para la Protección de Datos (EIPD) que incluya y también supere el triple juicio de idoneidad, necesidad y proporcionalidad estricta establecido en el art. 35.7.b y también previsto por la doctrina del Tribunal Constitucional.

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, con el principio de minimización de datos y el cumplimiento de los principios, derechos y otras obligaciones establecidas en el RGPD.

A. ALTO RIESGO

Un tratamiento de alto riesgo es todo aquel que sea probable que, por su naturaleza, alcance, contexto o fines, en particular si utiliza nuevas tecnologías, entrañe un alto riesgo para los derechos y libertades de las personas físicas.

Una de las obligaciones de los responsables es la de evaluar el riesgo de sus tratamientos. Ya desde la norma se establece el alto riesgo de algunos tratamientos, siendo una relación no exhaustiva. 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 de una serie de criterios no exhaustivos para determinar el alto riesgo de un tratamiento.

Un tratamiento de registro de presencia que incluya procesos biométricos se considerará de alto riesgo por, al menos, del cumplimiento de los criterios correspondientes a los números 4, 5 y 10 de la lista antes citada. Dicha lista no es exhaustiva para la evaluación de tratamientos de alto riesgo. Otras características con relación al ámbito, contexto o naturaleza concreta de la implementación del tratamiento (p.ej. uso de multibiometría, condiciones de vulnerabilidad de los interesados, situaciones sociales, etc.), podrían abundar aún más en la condición de alto riesgo para los interesados. Por ello, según los criterios establecidos en la guía "La Protección de Datos en las Relaciones Laborales" de la AEPD, también se considera de alto riesgo el tratamiento control de presencia mediante técnicas biométricas.

En las Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de vídeo, Versión 2.0 Adoptado el 29 de enero de 2020, por el Comité Europeo de Protección de Datos, en el apartado 5.1 "Consideraciones generales con respecto al tratamiento de datos biométricos" manifiesta la importancia la evaluación del riesgo, de un análisis de la necesidad, de la proporcionalidad y la aplicación de la minimización de datos. Estas condiciones, que son directamente aplicables para las operaciones biométricas mediante reconocimiento facial en tratamientos de control de presencia, se pueden extender al empleo de otros sistemas biométricos para implementar dicho tratamiento:

> *73. El uso de datos biométricos y, en particular, del reconocimiento facial conllevan elevados riesgos para los derechos de los interesados. Es fundamental que el recurso a dichas tecnologías tenga lugar respetando debidamente los principios de licitud, necesidad, proporcionalidad y minimización de datos tal y como establece el RGPD. Aunque la utilización de estas tecnologías se pueda percibir como particularmente eficaz, los responsables del tratamiento deben en primer lugar evaluar el impacto en los derechos y libertades fundamentales y considerar medios menos intrusivos de lograr su fin legítimo del tratamiento.*

En cuanto a los sistemas biométricos que sean implementados con técnicas de inteligencia artificial, habrá que tenerse en consideración la clasificación de dichos sistemas como de alto riesgo según el Anexo III de la propuesta de Regulación de Inteligencia Artificial y del cumplimiento de los requisitos que dichos sistemas tendrán que cumplir para poder ser integrados en un tratamiento de registro de presencia.

Un tratamiento de alto riesgo requerirá del responsable la superación, previa al inicio de tratamiento, de la evaluación de impacto relativa a la protección de datos establecida en el art. 35 del RGPD.

B. REALIZACIÓN Y SUPERACIÓN DE UNA EIPD

La superación de una EIPD exige demostrar la idoneidad, necesidad y proporcionalidad del tratamiento y gestionar desde el diseño los riesgos específicos del tratamiento, con la aplicación práctica de medidas orientadas específicamente a minimizar dichos riesgos, de forma que se garantice un umbral de riesgo aceptable durante todo el ciclo de vida del tratamiento, tal como se establece en el art. 35 del RGPD. Esto implicaría que, 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 en caso en que estuviera nombrado,

entre otros. Además, será obligatoria la consulta previa a la autoridad de control en caso de que el responsable no haya tomado medidas que permitan mitigar el riesgo tal y como se exige en el art. 36 del RGPD.

Hay que tener en cuenta que una gestión del riesgo para los derechos y libertades no resuelve la inexistencia de una circunstancia de levantamiento de la prohibición de tratar categorías especiales, la inexistencia de una condición de licitud, el no cumplimiento de las condiciones del art. 22, del principio de minimización de datos y de la aplicación de los principios, derechos y otras obligaciones establecidas en el 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

Con relación a las operaciones biométricas en un tratamiento de control de presencia, estas pueden emplear distintos sistemas, algunos de forma simultánea, y, a su vez, una misma técnica biométrica se puede implementar de distintas formas. 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, en particular, si el tratamiento se configura como una decisión automatizada.

La Agencia Española de Protección de Datos, en la guía “La Protección de Datos en las Relaciones Laborales”, en el apartado “Los datos biométricos” del capítulo 4.6, recomienda algunas medidas para tratamientos generales de registro de presencia mediante sistemas biométricos para gestionar el riesgo, que se pueden extender al control de presencia en general:

- La utilización de tecnologías biométricas debería basarse en utilizar dispositivos bajo el control exclusivo de los usuarios.
- Preferentemente no debería emplearse un almacenamiento centralizado de las plantillas biométricas.
- Deberían implementarse mecanismos automatizados de supresión de datos.
- En el caso de registro de presencia, se deben recoger en los convenios colectivos el conjunto de garantías con relación a estos tratamientos en el sentido dispuesto en el art. 91 de la LOPDGDD.

Otra 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.

Las medidas aquí expuestas no son exhaustivas ni agotan el conjunto de las que se pueden o se deben implementar para gestionar los riesgos que pueden surgir de una implementación concreta del registro de jornada con técnicas biométricas. 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.

C. SUPERACIÓN DEL ANÁLISIS DE IDONEIDAD, NECESIDAD Y PROPORCIONALIDAD

El RGPD exige en el art. 35.7.b que, en un tratamiento de alto riesgo, con carácter previo a cualquier decisión de implementación, se supere el triple juicio de idoneidad, necesidad y proporcionalidad estricta, también previsto por la doctrina del Tribunal Constitucional.

En cuanto al análisis de idoneidad y necesidad, nos remitimos a lo manifestado en el Apartado V.A de este documento con relación a ambos requisitos. 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.

En cuanto a superar el análisis de estricta necesidad, hay que demostrar que resuelve un problema que debe ser real, presente o inminente, y crítico para el funcionamiento del tratamiento. En ese sentido, el TEDH[17] estableció que «*necesario*» «*…no era sinónimo de indispensable…y tampoco tiene la flexibilidad de expresiones como 'admisible', 'ordinario', 'útil', 'razonable' o 'deseable'*». No basta la mera conveniencia o rentabilidad[18]. Además, hay que evaluar el alcance, la extensión y la intensidad de las interferencias en términos de impacto sobre los derechos fundamentales, explicando con pruebas por qué otras alternativas posibles no son suficientes para satisfacer esta necesidad de forma suficiente. Incluso, a la hora de evaluar las opciones, hay que tener en cuenta la posibilidad de emplear una combinación de medidas, tanto automatizadas como no automatizadas, organizativas, legales o técnicas.

En el caso del registro de jornada, el interesado tiene la obligación de participar en el tratamiento de registro de jornada y no hay levantamiento de la prohibición basándose en los artículos del 9.2.b al 9.2.g. Entonces, si el tratamiento adicional de datos biométricos se pretende basar en el consentimiento este ha de ser libre, para que sea libre el responsable ha de disponer de opciones equivalentes al tratamiento biométrico. Entonces, si esas opciones equivalentes existen, el tratamiento biométrico no es necesario. Por lo tanto, un tratamiento de registro de jornada implementado con técnicas biométricas, y que levante la prohibición del 9.1 del RGPD basándose en un consentimiento libre del interesado, no supera un análisis de necesidad en el marco de una EIPD.

Con relación a la superación de la evaluación de la proporcionalidad en sentido estricto, hay que 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 intrusismo en los derechos y libertades del interesado, estimando entre otros: la

[17] Handyside contra Reino Unido asunto nº 5493/72 (TEDH, 7 de diciembre de 1976), apartado 48.

[18] Grupo de Trabajo del Artículo 29, Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, WP 193, 27.04.2012, p. 8.

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; si pueden aparecer «intrusiones colaterales», incluso injerencias en la intimidad de personas distintas a los sujetos sujetos directamente afectados por la medida.

Con relación a todo ello, el Dictamen 3/2012 del Grupo de Trabajo del Artículo 29, sobre la evolución de tecnologías biométricas, afirma que hay que ponderar objetivamente la pérdida de intimidad con respecto a los beneficios esperados. En particular, el **que el tratamiento biométrico suponga un ahorro que no sea significativo, no es justificación suficiente** para llevar a cabo el tratamiento.

> *"Al analizar la proporcionalidad de un sistema biométrico propuesto…. Un tercer aspecto a ponderar es si la pérdida de intimidad resultante es proporcional a los beneficios esperados. Si el beneficio es relativamente menor, como una mayor comodidad o un ligero ahorro, entonces la pérdida de intimidad no es apropiada."*

D. IMPLEMENTACIÓN

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

En la implementación concreta de un tratamiento de control de presencia con técnicas 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. 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.

E. CONTEXTO DEL TRATAMIENTO

Con relación a lo anterior, al igual que la operación biométrica se ha de evaluar en el marco del tratamiento, todo el tratamiento en su conjunto se ha de evaluar teniendo en cuenta el contexto social y los efectos colaterales e imprevistos sobre los derechos y libertades que, al incorporar operaciones biométricas, se han producido o se están produciendo en el entorno (desvío de finalidades, impactos sociales, cambios normativos, cambios religiosos o culturales, conflictos, etc.).

F. MEDIDAS MÍNIMAS POR DEFECTO

En el planteamiento de un control de presencia con operaciones biométricas, además de una base jurídica del tratamiento del art. 6.1 RGPD, de una circunstancia que levante la prohibición de tratar categorías especiales de datos (art. 9.2 RGPD), y el cumplimiento de las condiciones del art. 22 del RGPD, 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 presente Reglamento. 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).

Entre las medidas mínimas por defecto, la Agencia Española de Protección de Datos, en la guía "La Protección de Datos en las Relaciones Laborales", en el apartado "Los datos biométricos" del capítulo 4.6, ya estableció el siguiente conjunto de garantías, que se pueden extender a todo tratamiento de control de presencia:

- Informar a los sujetos de los datos sobre el tratamiento biométrico. 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.
- 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.
- Implementar la protección de datos desde el diseño.
- Realizar previamente al inicio del tratamiento una Evaluación de Impacto para la Protección de Datos.

Todas estas exigencias son condiciones necesarias, pero no suficientes, que han de ejecutarse, evaluarse objetivamente y documentarse, para que el control de acceso basado en procesos biométricos cumpla con los requisitos de proporcionalidad del tratamiento.

G. 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 derivado que el uso de sistemas biométricos puede ocasionar en los derechos y libertades de los interesados, asumiendo que sea inevitable que produzca 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.

IX. SUBCONTRATACIÓN DE TRABAJADORES

En el caso de subcontratación de trabajadores, si el contratante exige por contrato sistemas biométricos para el registro de jornada o control de acceso en el ámbito laboral, dicha exigencia ha de cumplir con lo establecido en este documento.

La empresa contratada, como 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, si no se cumplen las condiciones de cumplimiento de las disposiciones del RGPD, la empresa contratada no tiene la obligación de realizar el registro de jornada o control de acceso en el ámbito laboral implementando técnicas biométricas.

X. CONCLUSIONES

Con relación al tratamiento de control de presencia mediante técnicas biométricas de identificación o autenticación, los responsables del tratamiento han de tener en cuenta que:

- La utilización de tecnologías biométricas de identificación y autenticación en el control de presencia supone un tratamiento de alto riesgo que incluye categorías especiales de datos.
- En la implementación del tratamiento de control de presencia hay que cumplir los principios de minimización y de protección de datos desde el diseño y por defecto, utilizando las medidas alternativas equivalentes, 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.
    - En el caso de registro de jornada y control de acceso con fines laborales, si el levantamiento de la prohibición se basa en el 9.2.b), el responsable debe contar con una norma con rango de ley que concrete la posibilidad de utilizar datos biométricos para dicha finalidad, que no se encuentra en la actual normativa legal española.
    - En el caso de registro de jornada o control de acceso en el ámbito laboral, el consentimiento no puede levantar la prohibición del tratamiento, ni ser una base para determinar la licitud, al existir de forma general una situación de desequilibrio entre el interesado y el responsable del tratamiento.
    - Para el caso del control de acceso fuera del ámbito laboral, la ejecución de un contrato no es una circunstancia que levanta la prohibición según el art.9.2 del RGPD. El consentimiento tampoco lo podrá ser, al resultar un tratamiento de alto riesgo, y que tendría que superar el requisito de necesidad establecido para dichos tratamientos.
- Cualquier utilización de los datos biométricos con finalidades adicionales a la de control de presencia deberá tener sus propias circunstancias de levantamiento de la prohibición y de condiciones que lo legitimen.
- En el tratamiento de control de presencia, no se pueden tomar decisiones automatizadas sin intervención humana que tengan efectos jurídicos sobre el interesado o le afecten significativamente de modo similar basadas en el proceso

biométrico, si no se cumple la circunstancia de un interés público esencial basado en una norma con rango de ley, proporcional al objetivo perseguido, que respete en lo esencial el derecho a la protección de datos y estableciendo 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.
- En cualquier caso, será obligatoria la superación favorable, previamente al inicio del tratamiento, 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.
- Superados todos los requisitos de cumplimiento de los principios generales del RGPD, en la implementación práctica del tratamiento de control de presencia con técnicas biométricas de identificación o autenticación, deben implementarse garantías organizativas, técnicas y jurídicas. En particular, al menos han de estar presentes las siguientes medidas por defecto:
    - Informar a los trabajadores, o personas si no se está en un entorno laboral, sobre el tratamiento biométrico y los riesgos elevados 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, se deben recoger en los convenios colectivos 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 debería basarse en utilizar dispositivos bajo el control exclusivo de los usuarios.
    - Es recomendable 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
    - Preferentemente no debería emplearse un almacenamiento centralizado de las plantillas biométricas.

- Deberían implementarse mecanismos automatizados de supresión de datos.

- Finalmente, todas las acciones y las medidas implementadas se revisarán y actualizarán cuando sea necesario.