- **Procedimiento Nº: E/05310/2020**

940-0419

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: La reclamación interpuesta por ***A.A.A.*** (en adelante, la reclamante) tiene entrada en la Agencia Española de Protección de Datos el 18/12/2019 y se dirige contra la **ASOCIACIÓN DEL COLEGIO ALEMAN DE BILBAO,** con NIF ***G48064836*** (en adelante, la reclamada).

La reclamante manifiesta que en el Colegio que dirige la reclamada en Bilbao se ha implantado el sistema de la huella dactilar como método de fichaje horario a la entrada y salida para los empleados (añade que no se aplica a todas las categorías de empleados).

Considera que son datos desproporcionados, no necesarios para el cumplimiento de la obligación, indicando que fallan las medidas de seguridad dando lugar a la identificación de otro trabajador, si bien no aporta acreditación, y desproporcionados pues existen medidas menos intrusivas como la implantación de una tarjeta.

Finaliza indicando que dos empleados han sido sancionados por negarse a fichar con este sistema y uno de ellos lo ha llevado a sede social.

Aporta un artículo que habla sobre la legalidad del sistema de registro digital de huella. No se contiene fecha de referencia del escrito, y ofrece sus sistemas de relojes especiales, constando "*JPG RELOJERIA INDUSTRIAL*".

En el artículo, se informa que "*no utilizan Imágenes de huellas sino descripciones de puntos denominados minucias. Aporta como ejemplo dos huellas- distintas para explicar que: "Cuando se registra una persona en un reloj de fichar lo que se realiza desde la detección de ciertas características del dibujo de la huella, conocidas como minucias, y qué pueden ser de varios tipos: bifurcaciones terminaciones, bucles, etcétera*." Continúa informando que: "*En la base de datos del sistema no se guarda la imagen original de la huella, sino un patrón que contiene la posición y tipo de las minucias. Cuando se registra una persona en un reloj de fichar, lo que se realiza es la detección de ciertas características del dibujo de la huella conocidas como minucias y que pueden ser de varios tipos: bifurcaciones, terminaciones bucles, etcétera ".* En la imagen del ejemplo con dibujos de huellas*, "se muestran los patrones con algunas de las minucias detectadas en cada huella, y el sistema no guarda la imagen original de la huella sino un patrón que contiene la posición y tipo de las minucias. Se observa que es imposible reconstruir el dibujo original de las huellas a partir de las minucias y que las personas podrían llegar a tener el mismo patrón aunque la probabilidad es baja."*

Indica que "*los datos están codificados en formato no estándar y que es imposible su utilización fuera del ámbito de los sistemas de control horario*".

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5/12, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), en escrito de 18/02/2020 se dio traslado de dicha reclamación a la reclamada, para que procediese a su análisis e informase a esta Agencia, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

La reclamada informó el 1/06/2020, en relación con la reclamación:

A-Según el escrito de la reclamada y que también firma el Delegado de Protección de Datos (IKAL ASESORES S.L.) de 13/03/2020, se indica que el sistema de fichaje a través de huella digital implantado en el colegio tiene:

-Como base legitimadora el cumplimiento de una obligación legal como es la que se prevé del control horario de empleados en el artículo 10 del Real decreto ley 8/2019, de 8/03, medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo, BOE 12 de marzo 2019: "*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 jornada.

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.»

-Se recogen datos parciales de la huella dactilar que tienen almacenados en cuatro terminales, encriptados. El acceso al sistema se efectúa mediante asignación a persona autorizada.

-Identifica el nombre de una empleada que señala: "*no ha prestado el consentimiento a este tipo de tratamiento y de la que no se usan este tipo de datos*", manifestando: "*con la cual existe un contencioso judicial en vía de lo social*".

Indica que no consta trabajador que haya ejercido el derecho de oposición.

-El software y el hardware se contrataron con la empresa *JPG RELOJERIA INDUSTRIAL,* con la que suscribieron un contrato de encargo de tratamiento.

- En mayo del 2019, se empezó a informar a los trabajadores con vistas a la implantación del sistema, que fue efectivo en junio 2019, afectando a unos 100 trabajadores, y figurando cuatro personas con acceso a esos datos para su gestión y control. – Aporta copia del documento de confidencialidad y seguridad del tratamiento e información que se entrega a empleados que tratan los datos de gestión del colegio con acceso a datos.

-Tienen establecido un registro de actividad de tratamiento.

-Manifiesta que existe un protocolo o manual de seguridad en el que se relacionan las medidas técnicas aplicables a la seguridad, las copias de seguridad y la gestión de incidencias en la seguridad de los datos personales; Indica que hasta el momento no ha habido ningún incidente. Señala que "*los datos personales disponibles en los terminales-datos parciales de huella dactilar-están totalmente cifrados y nadie los puede leer".* Aporta como anexo, copia parcial de documento, conteniéndose el nombre de DOCUMENTO DE SEGURIDAD, abarcando epígrafes de 1 "*Ciclo de vida de la actividad del tratamiento*", 2 "*Descripción de la actividad del tratamiento"*, 3 "*Evaluación necesidad de EIPD"*, y 4 "*Análisis básico de riesgos"*, *ver EIPD*.

-Aporta copia de documento de EVALUACIÓN DE IMPACTO (29 folios) aprobado en mayo del 2019, limitado a la sede del Colegio en Bilbao, desconociendo si en otras ciudades se utiliza el mismo sistema. En el documento no se señala nada al respecto de otras sedes. Figuran los datos del responsable de seguridad y como delegado de protección de datos IKAL ASESORES SL.

Se indica que el tratamiento de parte de la huella no entraña alto riesgo, que "*no está incluido entre los que requieren evaluación de impacto de protección de datos en el artículo 35.3 del RGPD* ""*por lo que se evalúa la necesidad según la directriz 248 del Grupo de trabajo* 29, de 4/04/2017 revisada el 4/10/2017", **"***en este caso se seguirá el criterio para determinar si existe un elevado riesgo inherente a las actividades de tratamiento y qué se deben evaluar y pueden determinar la necesidad de realizar una EIPD, considerando de manera genérica, que aquellos tratamientos que cumplen dos o más de los presentes criterios deben disponer de una EIPD*." Y aquí *como tratamiento relacionado con datos confidenciales o de naturaleza altamente personal, relativos a personas vulnerables y su uso es innovador o aplica nuevas tecnologías*."

Se mencionan los principios básicos de gestión de riesgos, se indica que la gestión del dato del fichaje se conecta con la gestión de nóminas de personal y recursos humanos y se contienen menciones a los riesgos específicos a la integridad, y la disponibilidad, ciclo de vida de los datos, y a la necesidad y la proporcionalidad del sistema.

"*Sistema de tratamiento: datos alojados en los terminales lectores de huella dactilar*".

Plazos previstos para la supresión: "*Los datos parciales de la huella dactilar son conservados únicamente en el periodo en el que se mantiene la relación laboral con el trabajador suprimiéndose a la finalización de dicha relación laboral. Los datos que constituyen el registro de jornada forman parte de la actividad de tratamiento para la gestión de nóminas personal y recursos humanos y son conservados por el tiempo legal de 4 años* ".

A partir del punto 3 desarrolla:

-Análisis de la necesidad de evaluación*, considerando que su tratamiento cumple dos o más de los presentes criterios deben disponer de una EIPD*."

Acompaña un cuadro de gestión con casillas a marcar, en un bloque, denominado "*características de las actividades de los tratamientos*" y figura una marca x en "*datos confidenciales o de naturaleza altamente personal",* otra en "*datos relativos a las personas vulne-*

rables" y otra en "*uso innovador de aplicación de nuevas soluciones tecnológicas u organizativas"*. En el apartado *número de tratamientos:* 3 y una marca x en requiere EIP: SI.

A continuación detalla en estudio previo los apartados de:

-ciclo de vida de tratamiento, con:

- La *captura de los datos:* reiterando que "*tras el consentimiento informado del trabajador* "se toman los datos, "*que son alojados en todas las terminales lectoras*".

-*Clasificación almacenamiento:* Indica que se almacena un patrón, que contiene ciertas *minucias* de la huella, encriptado y alojado en la base de datos de cada terminal lectora. "*Esa Información procedente de la terminal lectora, nombre, apellidos, hora de inicio o fin de jornada laboral se traslada a una herramienta de gestión con la finalidad de realizar el tratamiento de datos de nóminas personal y recursos humanos. Esa herramienta de gestión se encuentra alojada en el servidor de administración y únicamente tiene acceso a personal con privilegios para ello", 4 personas*.

-*Uso-tratamiento*: Control de la jornada laboral que exige el Real decreto ley 8/2019.

-Sobre la necesidad y proporcionalidad del sistema implantado: Lo relaciona con la limitación de finalidad y la minimización de datos y plazo de conservación.

Finaliza la evaluación con un cuadro "*riesgo inherente*", "*riego residual con valores y referencias* " y probabilidad/impacto.

-Aporta copia de documento de consentimiento a cada empleado en el que se indica que es para el cumplimiento de la relación laboral que vincula a ambas partes y para dar cumplimiento a la obligación establecida del real decreto ley 8-2019 de 8/03/2019. Se informa de los derechos a ejercer, solicitando el consentimiento expreso a través de la firma del escrito sobre el dato huella dactilar, de conformidad con el artículo 9 del RGPD, dato con categoría especial.

TERCERO**:** Con fecha 9/06/2020, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por el reclamante.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

Hay que señalar que los datos biométricos están estrechamente vinculados a una persona, dado que pueden utilizar una determinada propiedad única de un individuo para su identificación o autenticación.

Según el Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, "*Los datos biométricos cambian irrevocablemente la relación entre el cuerpo y la identidad, ya que hacen que las características del cuerpo humano sean legibles mediante máquinas y estén sujetas a un uso posterior*."

En relación con ellos, el Dictamen precisa que cabe distinguir diversos tipos de tratamientos al señalar que "*Los datos biométricos pueden tratarse y almacenarse de diferentes formas. A veces, la información biométrica capturada de una persona se almacena y se trata en bruto, lo que permite reconocer la fuente de la que procede sin conocimientos especiales; por ejemplo, la fotografía de una cara, la fotografía de una huella dactilar o una grabación de voz. Otras veces, la información biométrica bruta capturada es tratada de manera que solo se extraen ciertas características o rasgos y se salvan como una plantilla biométrica*."

Los datos biométricos los define el artículo 4.14 del RGPD:

«datos biométricos»: 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;

Hay que señalar que el RGPD no parece considerar a todo tratamiento de datos biométricos como tratamiento de categorías especiales de datos, ya que el artículo 9.1. se refiere a los *"datos biométricos dirigidos a identificar* de manera unívoca a una persona física". En el original en versión inglesa se señala: "*biometric data for the purpose of uniquely identifying a natural person*".

Una interpretación conjunta de ambos preceptos parece dar a entender que los datos biométricos solo constituirían una categoría especial de datos en el caso de que se sometan a un tratamiento técnico específico dirigido a identificar de manera unívoca a una persona física.

En este sentido, parece que igualmente se pronuncia el Considerando 51 al señalar que "*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".*

Si bien el original en ingles, señala: "The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person."

Con igual criterio, el Protocolo de enmienda al Convenio para la Protección de Individuos con respecto al procesamiento de datos personales, aprobada por el Comité de Ministros en su 128º período de sesiones en Elsinore el 18/05/2018 (Convenio 108) incluye únicamente como categorías especiales de datos, en su artículo 6.1 a los datos biométricos dirigidos a la identificación unívoca de una persona ("*biometric data uniquely identifying a person*"), sin incluir la referencia a la autenticación.

El Grupo del artículo 29 (GT 29, WP en inglés), fue hasta la entrada en vigor del RGPD un órgano consultivo independiente de la Unión Europea en materia de protección de datos e intimidad creado en virtud de lo previsto en el citado artículo de la Directiva 95/46/CE del Parlamento y del Consejo, de 24/10/1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Sus funciones se describían en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE. Con la entrada en vigor del artículo 94.2 del RGPD que deroga la directiva 95/46 se indica expresamente "*Toda referencia a la Directiva derogada se entenderá hecha al presente Reglamento. Toda referencia al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales establecido por el artículo 29 de la Directiva 95/46/CE se entenderá hecha al Comité Europeo de Protección de Datos (*CEPD*) establecido por el presente Reglamento*."

El CEPD tiene como objetivo garantizar la aplicación coherente del Reglamento General de Protección de Datos**.** Puede entre otras competencias, adoptar directrices generales para clarificar los términos de la legislación europea de protección de datos, proporcionando a todas las partes interesadas una interpretación coherente de sus derechos y obligaciones. Al objeto de aclarar las dudas interpretativas que surgen respecto a la consideración de los datos biométricos como categorías especiales de datos puede acudirse a la distinción entre identificación biométrica y verificación/autenticación biométrica que establecía GT 29, en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas:

> "*Identificación biométrica: la identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias* uno-a-varios*).*
>
> *Verificación/autenticación biométrica: la verificación de un individuo por un sistema biométrico es normalmente el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (es decir,* un proceso de búsqueda de correspondencias uno-a-uno)."

Esta misma diferenciación se recoge en el Libro blanco sobre la inteligencia artificial de la Comisión Europea:

> *"En lo que se refiere al reconocimiento facial, por «identificación» se entiende que la plantilla de la imagen facial de una persona se compara con otras muchas plantillas almacenadas en una base de datos para averiguar si su imagen está almacenada en ella. La «autenticación» (o «verificación»), por su parte, se refiere habitualmente a la búsqueda de correspondencias entre dos plantillas concretas.*

Permite la comparación de dos plantillas biométricas que, en principio, se supone que pertenecen a la misma persona; así, las dos plantillas se comparan para determinar si la persona de las dos imágenes es la misma. Este procedimiento se emplea, por ejemplo, en las puertas de control automatizado de fronteras empleadas en los controles fronterizos de los aeropuertos".

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

En el presente supuesto, inicialmente se trataría de una *identificación uno-varios* pues se introduce la huella que confronta con los datos almacenados en una base de datos, donde figuran las del resto de empleados, sin que conste una modalidad adicional extra de autenticación. Por poner un ejemplo similar comprensible, la extracción de efectivo de un cajero con una tarjeta, al introducir la tarjeta sería la identificación, que pone en marcha el sistema y reconoce al usuario. Al pedir e introducir el PIN, sería la verificación o autenticación a través de la cual el sistema reconoce que el usuario es quien dice ser y da el permiso para efectuar la operación. En este supuesto se produce cada vez que se ficha de entrada o salida en el Colegio, una identificación con la confrontación entre la huella que pone el empleado y la que guarda la base de datos, contrastando la introducida a cada momento, contra el resto de las huellas que guarda sistema-en este caso las de todos los trabajadores, y en este caso algoritmos de la huella.

El tratamiento de estos datos está expresamente permitido por el RGPD cuando el empresario cuenta con una base jurídica. A este respecto, la STS, sala de lo contencioso administrativo, sección 7, de 2/07/2007 (Recurso 5017/2003), sobre sistema de control horario en una administración pública, analiza que ha entendido legitimo el tratamiento de los datos biométricos que realiza la Administración para el control horario de sus empleados públicos, sin que sea preciso el consentimiento previo de los trabajadores. indicando en su fundamento de derecho séptimo: "*Desde luego, la finalidad perseguida mediante su utilización es plenamente legítima: el control del cumplimiento del horario de trabajo al que vienen obligados los empleados públicos. Y, en tanto esa obligación es inherente a la relación que une a estos con la Administración Autonómica, no es necesario obtener previamente su consentimiento ya que el artículo 6.2 de la Ley Orgánica 15/1999 lo excluye en estos casos. Además, no parece que la toma, en las condiciones expuestas, de una imagen de la mano incumpla las exigencias de su artículo 4.1. Por el contrario, puede considerarse adecuada, pertinente y no excesiva*."

Sin embargo, debe tenerse en cuenta lo siguiente:

- El trabajador debe ser informado sobre estos tratamientos.

- Deben respetarse los principios de limitación de la finalidad, necesidad, proporcionalidad y minimización de datos.

En todo caso, el tratamiento también deberá ser adecuado, pertinente y no excesivo en relación con dicha finalidad. Por tanto, los datos biométricos que no sean necesarios para esa finalidad deben suprimirse y no siempre se justificará la creación de una base de datos biométricos (Dictamen 3/2012 del GT 29).

- Uso de plantillas biométricas: Los datos biométricos deberán almacenarse como plantillas biométricas siempre que sea posible. La plantilla deberá extraerse de una manera que sea específica para el sistema biométrico en cuestión y no utilizada por otros responsables del tratamiento de sistemas similares a fin de garantizar que una persona solo pueda ser identificada en los sistemas biométricos que cuenten con una base jurídica para esta operación.

- El sistema biométrico utilizado y las medidas de seguridad elegidas deberán asegurarse de que no es posible la reutilización de los datos biométricos en cuestión para otra finalidad.

- Deberán utilizarse mecanismos basados en tecnologías de cifrado, a fin de evitar la lectura, copia, modificación o supresión no autorizadas de datos biométricos.

- Los sistemas biométricos deberán diseñarse de modo que se pueda revocar el vínculo de identidad.

- Deberá optarse por utilizar formatos de datos o tecnologías específicas que imposibiliten la interconexión de bases de datos biométricos y la divulgación de datos no comprobada.

- Los datos biométricos deben ser suprimidos cuando no se vinculen a la finalidad que motivó su tratamiento y, si fuera posible, deben implementarse mecanismos automatizados de supresión de datos.

III

En el presente caso, la reclamada ha implantado un sistema de gestión para registro de jornada laboral de sus trabajadores mediante huella dactilar.

Hay que señalar que la legitimación para el tratamiento de la huella para el acceso y control horario de los trabajadores por parte del empleador debemos buscarlo en el artículo 9 y 6 del RGPD.

El artículo 9 del RGPD establece en sus apartados 1 y 2.b) lo siguiente:

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

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

(…)

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

(…)"

El artículo 6.1.b) y c) del RGPD indica:

"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;"

El reclamado tiene legitimación, fundamentada en la normativa señalada, para efectuar el control de registro de horario en acceso y fin de jornada en el Colegio para su registro por tener relación contractual con los empleados y verificar el cumplimiento de la jornada que dimana del contrato, así como el registro de la misma que está previsto en norma con rango de Ley.

Así pues, no es necesario que se solicite el consentimiento a los trabajadores, ya que la causa que legitima el tratamiento revisado son las señaladas del artículo 9 del RGPD, que levanta la prohibición de tratamiento de los datos biométricos y el 6.1.b) y c) que lo legitima.

IV

En el Dictamen 3/2012 del Grupo de Trabajo del artículo sobre evolución de las tecnologías biométricas, adoptado el 27/04/2012, se expresa que "*los datos biométricos se utilizan con éxito y eficacia en la investigación científica, son un elemento clave de la ciencia forense y un valioso elemento de los sistemas de control de acceso*".

Refiriéndose a la proporcionalidad, se establece en el dictamen que:

"*Puesto que los datos biométricos solo pueden utilizarse si son adecuados, pertinentes y no excesivos, ello implica una evaluación estricta de la necesidad y la proporcionalidad de los datos tratados y de si la finalidad prevista podría alcanzarse de manera menos intrusiva*.

Al analizar la proporcionalidad de un sistema biométrico propuesto, 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 solo el más adecuado o rentable. Un segundo factor que deber 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. Un tercer aspecto para 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. El cuarto aspecto para evaluar la adecuación de un sistema biométrico es considerar si un medio menos invasivo de la intimidad alcanzaría el fin deseado". (Por ejemplo, tarjetas inteligentes y otros métodos que no recojan o centralicen datos biométricos para fines de autenticación).

El Grupo de Trabajo advierte de los riesgos que conlleva la utilización de datos biométricos para fines de identificación en grandes bases de datos centralizadas, dadas las consecuencias potencialmente perjudiciales para las personas afectadas.

Debe tenerse en cuenta el importante impacto de la dignidad humana de los interesados y las implicaciones en cuestión de derechos fundamentales de tales sistemas. A la luz del Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales y de la jurisprudencia del Tribunal Europeo de Derechos Humanos sobre el artículo 8 del Convenio, el Grupo de Trabajo subraya que cualquier interferencia con el derecho a la protección de datos solo podrá autorizarse si es conforme a la ley y si es necesaria, en una sociedad democrática, para proteger un interés público importante.»

A la hora de valorar si en el supuesto planteado se cumplirían los presupuestos necesarios para apreciar la existencia de proporcionalidad en el tratamiento, es preciso recordar que la citada proporcionalidad exige, según la doctrina del Tribunal Constitucional, siguiendo a tal efecto la sentada por el Tribunal Europeo de Derechos Humanos, la superación de un triple juicio, en el sentido de determinar si la medida adoptada 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), es decir, si la injerencia producida en el titular del derecho objeto de restricción por la medida es la mínima en aras al logro del fin legítimo perseguido con aquélla.

Para la realización de la valoración a la que acaba de hacerse referencia, se pone de manifiesto que el sistema cuya implantación se pretende es idóneo para el cumplimiento de la finalidad de control de asistencia que se persigue, indicándose que el mismo sirve a tal finalidad, considerándose además que prevista legalmente la conservación del formato de los datos en la norma legal de registro de jornada, resulta adecuado.

En cuanto a la injerencia en el derecho de los afectados para analizar la proporcionalidad, se tiene en cuenta que se han adoptado medidas reforzadas para garantizar la confidencialidad de los datos, tales como la utilización de un algoritmo para registrar determinadas partes de la huella, el cifrado de la información, o la limitación de los protocolos de acceso a los datos. La agrupación de estos elementos permite considerar proporcional la instauración del sistema en el Colegio.

V

En cuanto a los deberes de información de la implantación del sistema, establece el artículo 13 del RGPD, la información que debe ser facilitada al interesado en el momento de la recogida de sus datos, estableciendo lo siguiente:

"Artículo 13. Información que deberá facilitarse cuando los datos personales se ob-

tengan del interesado.

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento; 4.5.2016 L 119/40 Diario Oficial de la Unión Europea ES
d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
d) el derecho a presentar una reclamación ante una autoridad de control;
e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;
f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información".

La reclamada ha acompañado la cláusula informativa que ha facilitado a sus empleados informándoles del sistema de control mediante huella dactilar**.**

VI

El artículo 30 del RGPD establece lo siguiente en relación con el Registro de las actividades de tratamiento:

<<1. Cada responsable y, en su caso, su representante, llevarán *un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:*

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
b) los fines del tratamiento;
c) una descripción de las categorías de interesados y de las categorías de datos personales;
d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

2. Cada encargado y, en su caso, el representante del encargado llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;
b) las categorías de tratamientos efectuados por cuenta de cada responsable;
c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.

3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.

4. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que

lo solicite.

5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.>>

La reclamada ha aportado documento de registro de actividades de tratamiento realizado, que se adecua a lo establecido en el artículo referido.

VII

Por último, sobre la Evaluación de Impacto de protección de datos (EIPD), el artículo 35 del RGPD establece lo siguiente:

"*1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.*

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) *tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o*

c) observación sistemática a gran escala de una zona de acceso público.

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.>>

El RGPD no requiere que se realice una EIPD para cada operación de tratamiento que pueda entrañar riesgos para los derechos y libertades de las personas físicas. La realización de una EIPD es únicamente obligatoria cuando el tratamiento «*entrañe probablemente un alto riesgo para los derechos y libertades de las personas físicas*» (artículo 35, apartado 1, ilustrado en el artículo 35, apartado 3 y complementado por el artículo 35, apartado 4),

y especialmente pertinente cuando se introduce una nueva tecnología de tratamiento de datos.

Las palabras «*en particular*» indicadas en la frase introductoria del artículo 35, apartado 3 del RGPD se refieren a una lista no exhaustiva. Pueden existir operaciones de tratamiento de «*alto riesgo*» que no estén incluidas en esta lista pero que supongan unos riesgos similarmente elevados.

En cumplimiento del artículo 35.4 del RGPD, para facilitar a los responsables de los tratamientos la identificación de aquellos que requieren una EIPD, la Agencia Española de Protección de Datos ha publicado la "*lista de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos*". La lista se basa en los criterios establecidas por el GT 29, WP248 "*Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del RGPD*", los complementa y debe entenderse como una lista no exhaustiva, y orientativo. Comprende once supuestos, y en el caso de darse dos o más de ellos, el responsable estará obligado a realizar una EIPD.

Concretamente, para el caso que nos ocupa, y que motivan que se deba efectuar una EIPD, se cumplen los siguientes:

- Se tratan categorías especiales de datos,
- Se tratan datos biométricos para identificar a personas físicas;

Otras recomendaciones de valor que se contienen en la directriz son el examen o valoración de la nueva tecnología empleada y su relación con los riesgos y derechos de los afectados, así como la participación o mención al tratamiento llevado a cabo por el encargado de tratamiento, junto con las revisiones y análisis periódicos del documento para corregir y adaptar mejoras con la finalidad de acreditar el correcto tratamiento de datos.

Se acredita que la actuación de la reclamada, como entidad responsable del tratamiento, ha sido acorde con la normativa sobre protección de datos personales analizada en los párrafos anteriores.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución al reclamante y reclamado.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1/10, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1/10, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13/07, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Mar España Martí
Directora de la Agencia Española de Protección de Datos