- Procedimiento Nº: E/07273/2020

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 ASOCIACIÓN DE MÉDICOS Y TITULADOS SUPERIORES DE MADRID (en adelante, el reclamante) tiene entrada con fecha 07/02/2020 en la Agencia Española de Protección de Datos. La reclamación se dirige contra IDCQ HOSPITALES Y SANIDAD, S.L.U., con NIF B87324844 (en adelante, el reclamado). Los motivos en que basa la reclamación son, en síntesis: el reclamante manifiesta que el Hospital Universitario Rey Juan Carlos, el Hospital Universitario Fundación Jiménez Díaz y Quirón Salud han implantado un sistema de control de horario mediante huella dactilar sin previamente informar a los trabajadores y sin cumplir los parámetros establecidos en la normativa de protección de datos.

SEGUNDO: Tras la recepción de la reclamación, la Subdirección General de Inspección de Datos procedió a realizar las siguientes actuaciones:

El 27/03/2020 fue trasladada al reclamado la reclamación presentada para su análisis y decisión adoptada al respecto. Igualmente, se le requería para que en el plazo de un mes remitiera a la Agencia determinada información:

- Copia de las comunicaciones, de la decisión adoptada que haya remitido al reclamante a propósito del traslado de esta reclamación, y acreditación de que el reclamante ha recibido la comunicación de esa decisión.

- Informe sobre las causas que han motivado la incidencia que ha originado la reclamación.

- Informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares.

- Cualquier otra que considere relevante.

El 04/07/2020 el reclamado manifestaba que con carácter general y para la implementación del registro de jornada no se precisa el consentimiento del trabajador, siendo base suficiente de legitimación la propia norma laboral, que en el artículo 34.9 del ET que establece la obligación de las empresas de realizar el registro de la jornada con carácter individual de cada trabajador y que, de acuerdo con lo previsto en el artículo 6.1.c) del 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 (en adelante RGPD), el tratamiento de datos personales de los trabajadores derivado de la implantación del registro de jornada es

necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.
Que, en todo momento, QUIRÓNSALUD ha cumplido los parámetros de la normativa de protección de datos, considerando que los datos recogidos y tratados son adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados, de conformidad con lo dispuesto en el principio de minimización regulado en el artículo 5.1.c) del RGPD.

Por último, de acuerdo con lo solicitado por la AEPD, se adjuntaban las evaluaciones de impacto de la actividad del tratamiento *"Huella - Registro de Jornada"* realizadas y, considerando que eran muchos hospitales y las evaluaciones de impacto realizadas, aportaban la evaluación de impacto de la actividad de tratamiento *"Huella - Registro de Jornada"* del Hospital Fundación Jiménez Díaz.

Asimismo se adjunta documento con formato de cuestionario en el que se responde afirmativa o negativamente y los apartados de *"justificación"* están cumplimentados en muy pocos casos. Sobre la seguridad, apartado 9 brechas, señala que se pueden producir pero el riesgo es bajo porque no se puede revertir el proceso para volver a la *"huella digital".* En el apartado 1.3 como medidas técnicas de seguridad: encriptación, listas control acceso y autentificación de red; justificación: ninguno. 1.4 medidas de seguridad organizativa.

Adjuntan también constancia de la información a los sindicatos y empleados.

TERCERO: El 02/09/2020, de conformidad con el artículo 65 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por el reclamante contra el reclamado.

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

En el presente caso, como consta en el hecho primero el reclamante manifiesta que los hospitales citados han implantado un sistema de control de horario mediante huella dactilar sin previamente informar a los trabajadores y sin cumplir los parámetros establecidos en la normativa de protección de datos.

En relación con la cuestión planteada en el caso presente, habría que señalar que la implantación de un sistema de control horario basado en la huella dactilar ha de ser informado a todos los afectados de manera completa, clara, concisa y, además, la

citada información debe ser adicionada con referencia tanto a las bases legales que den cobertura a dicho tipo de control como a la información básica a la que hace referencia el artículo 13 del RGPD.

La instalación de un sistema de control basado en la recogida y tratamiento de la huella dactilar de los empleados implica el tratamiento de sus datos personales puesto que dato personal es toda aquella información sobre una persona física identificada o identificable de conformidad con el artículo 4.1 del RGPD.

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;

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",* por lo que, de 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".*

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 de mayo de 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.

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 el Grupo del Artículo 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".

El tratamiento de datos biométricos requerirá, además de la concurrencia de una de las bases jurídicas establecidas en el artículo 6 del RGPD, alguna de las excepciones previstas en el artículo 9.2 del RGPD.

El análisis de la base legal de legitimación para realizar este tratamiento viene del artículo 6 del RGPD, relativo a la licitud del tratamiento, que en su apartado 1, letra b) señala: *"El tratamiento 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 éste de medidas precontractuales (…)".*

En virtud de este precepto, el tratamiento sería lícito y no requeriría el consentimiento, cuando el tratamiento de datos se realice para el cumplimiento de relaciones contractuales de carácter laboral.

Este precepto daría cobertura también al tratamiento de datos de los empleados públicos, aunque su relación no sea contractual en sentido estricto. Hay que señalar que en ocasiones, para el cumplimiento de sus obligaciones en relación con los empleados públicos, la Administración ha de realizar tratamientos de determinados datos a los que se refiere el RGPD, en su artículo 9, como *"categorías especiales de datos".*

En este punto hay que hacer especial mención de la letra b) del artículo 9.2 del RGPD, según la cual la prohibición general de tratamiento de datos biométricos no será de aplicación 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".*

En el ordenamiento español, el artículo 20 del Texto refundido del Estatuto de los trabajadores (TE), aprobado por el Real decreto legislativo 2/2015, de 23 de octubre, prevé la posibilidad de que el empresario adopte medidas de vigilancia y control para verificar el cumplimiento de las obligaciones laborales de sus trabajadores:

"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".

Y en el Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, en su artículo 54 en relación con los principios de conducta de los empleados públicos señala: *"El desempeño de las tareas correspondientes a su puesto de trabajo se realizará de forma diligente y cumpliendo la jornada y el horario establecidos"*

Es innegable la posibilidad de utilización de sistemas basados en datos biométricos para llevar a cabo el control de acceso y horario, aunque tampoco parece que sea o deba ser el único sistema que puede ser usado: el uso de tarjetas personales, la utilización de códigos personales, la visualización directa del punto de marcaje, etc., que pueden constituir, por sí mismos o en combinación con alguno de los otros sistemas disponibles, medidas igualmente eficaces para llevar a cabo el control.

En cualquier caso, con carácter previo a la decisión sobre la puesta en marcha de un sistema de control de este tipo y teniendo en cuenta sus implicaciones, el

tratamiento de datos biométricos dirigidos a identificar de manera unívoca a una persona física sería preceptivo establecer el Registro de Actividades de Tratamiento y llevar a cabo una Evaluación de Impacto relativa a la protección de datos de carácter personal para evaluar tanto la legitimidad del tratamiento y su proporcionalidad como la determinación de los riesgos existentes y las medidas para mitigarlos de conformidad con lo señalado en el artículo 35 RGPD.

III

También en relación la necesidad de información a los interesados 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.

El tratamiento de estos datos está expresamente permitido por el RGPD cuando el empresario cuenta con una base jurídica, que de ordinario es el propio contrato de trabajo. A este respecto, la STS de 2 de julio de 2007 (Rec. 5017/2003), 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.

Sin embargo, debe tenerse en cuenta lo siguiente:

1. El empleado debe ser informado sobre estos tratamientos en los términos del artículo 13 del RGPD.

2. 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 Grupo de Trabajo del art. 29).

3. 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.

4. 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.

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

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

7. 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.

8. 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.

.

IV

Por lo tanto, se ha acreditado que la actuación del reclamado 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 a la ASOCIACIÓN DE MÉDICOS Y TITULADOS SUPERIORES DE MADRID y a IDCQ HOSPITALES Y SANIDAD, S.L.U., con NIF B87324844.

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 de octubre, 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 de octubre, 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 de julio, 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