Expediente Nº: E/02116/2016

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas *[de oficio]* por la Agencia Española de Protección de Datos ante la ***UNIVERSIDAD AUTONOMA DE MADRID*** en virtud de denuncia presentada por D. ***B.B.B.*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha de 26 de febrero de 2016 tuvo entrada en esta Agencia un escrito de D. ***B.B.B.*** en el que denuncia a la **Universidad Autónoma de Madrid** (en lo sucesivo UAM), en base a que el Servicio Interdepartamental de Investigación –SIDI-, ha implantado un sistema de control de presencia basado en la huella digital., que no ha sido notificado a los representantes de los trabajadores de manera oficial ni se les ha facilitado información al respecto.

Según manifiesta, parece ser que los trabajadores han sido informados de manera indebida, dado que no se les ha informado de las repercusiones disciplinarias de la negativa al uso de dicho sistema de control.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

Con fecha 11 de mayo de 2016, la Universidad Autónoma de Madrid ha remitido a esta Agencia la siguiente información en relación con los hechos denunciados:

1. El Servicio Interdepartamental de Investigación –SIDI-, es una infraestructura de investigación de la Universidad Autónoma de Madrid (UAM) y dispone de unas instalaciones con acceso contralado situadas en la Facultad de Ciencias.
2. En relación con el procedimiento por el que se ha informado a los trabajadores de la implantación del sistema de control de presencia basado en la huella digital, se envió información por correo electrónico a los trabajadores y usuarios del SIDI, sobre la instalación del sistema, su uso y finalidad.

   Aportan copia del correo electrónico remitido por el Director del SIDI, con fecha **4 de diciembre de 2015**, a Lista del SIDI (....@uam.es) sobre la implantación del citado sistema desde el 15 de diciembre de 2015, en el que se informa, entre otros extremos, de que:

   > El sistema cumplirá la función de **Control de Acceso** a través de huella dactilar, que permitirá, además de la identificación inequívoca de cada uno, el registro de la hora de entrada y salida del personal contratado.

Además el control de usuarios se realizara mediante una tarjeta que permitirá: Control de Asistencia, Solicitudes de Permisos, Solicitudes de Moscosos y Vacaciones, Control de usuarios

3. Así mismo, aportan copia de los siguientes correos electrónicos remitidos, al igual que el anterior, por el Director de SIDI, a la Lista del SIDI:

   De fecha 16 de diciembre de 2015: En el que se recuerda que los trabajadores deben pasar por administración para el registro de la huella, ya que desde el viernes dejaran de tener validez las tarjetas que se usan para acceder al SIDII.

   De fecha 17 de septiembre de 2015: Informando de que por problemas técnicos, la fase de pruebas del nuevo sistema se pospone al 21 de diciembre.

   De fecha 21 de enero de 2016: En el que se informa de la implantación del nuevo sistema el 1 de febrero.

   De fecha 14 de marzo: Con el que se remite una carta con instrucciones sobre la utilización del sistema.

   Según manifiestan, entre los destinatarios de los correos, se encuentra un miembro del Comité de Empresa de la UAM y los cinco trabajadores del centro designados como representantes del resto ante la Junta de Facultad en la que se encuentra localizado el SIDI.

4. El sistema de control de acceso a las instalaciones tiene las siguientes finalidades:

   Incrementar la seguridad tanto del personal, usuarios externos y visitantes como de los recursos del SIDI.

   Mejorar la organización del centro.

   Disminuir la carga burocrática sobre el control de accesos, permanencia y permisos.

   Uniformidad en el tratamiento de las incidencias relacionadas con ausencias del personal contratado eventual.

   Mayor aprovechamiento de la jornada laboral por parte del personal contratado eventual.

   Aumentar el control de acceso de todo el personal externo.

5. El dato que se ha recogido de los trabajadores está constituido por varios puntos (3 o 4) de la huella de uno de sus dedos índice que se tratan por un algoritmo matemático mediante el que se asocia a dicho conjunto de puntos un número que identifica al trabajador en cuestión.

6. Respecto al fichero en el que se van a recoger los datos del nuevo sistema, según manifiestan, no se ha solicitado la inscripción del mismo a la Agencia, ya que consideran que no recogen ningún dato adicional a los ya recogidos en los ficheros declarados a la Agencia, entre los que se encuentran los denominados: Control de Presencia y Videovigilancia y Control de Acceso.

   Se ha verificado que los dos ficheros citados se encuentran inscritos en el Registro General de Protección de Datos, no obstante no se encuentra

declarado que ninguno de ellos contenga el dato de “Huella” ni “Otros datos biométricos”.

7. Por otra parte, según manifiestan, el sistema que debería estar en funcionamiento desde el 1 de abril de 2016, **aún se encuentra en fase experimental, dadas las incidencias que se han dado en su implantación, por lo que los datos recopilados aún no han pasado a la fase de explotación**.

8. Aportan copia del informe realizado por la empresa SOPORTE TECNICO DIGITAL S.L. en base al emitido por el Gabinete Jurídico de la Agencia en el año 2009, dando respuesta a una consulta realizada sobre la posibilidad de implantar un sistema de control horario de los trabajadores basado en la huella digital. En éste informe se indica que aunque no es necesario el consentimiento del interesado para el tratamiento de su huella digital, deberá darse cumplimiento a lo dispuesto en el artículo 5 de la LOPD, especialmente de las consecuencias disciplinarias que podría acarrear la negativa del trabajador al tratamiento de su huella digital.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

Cuestión similar a la ahora planteada ha sido resuelta por resoluciones de esta Agencia, las más reciente la dictada en el procedimiento, E/00793/2016, declarando el Archivo de las actuaciones al no desprenderse la comisión de infracción en el establecimiento de un control de presencia mediante la huella dactilar, al acreditársela la información previa y de buena fe a los afectados.

El artículo 3 de la LOPD, establece: “A los efectos de la presente Ley Orgánica se entenderá por:

a) Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables.

b) Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

d) Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza

pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento…"

El artículo 1 de la LOPD dispone: *"La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".*

El artículo 2.1 de la LOPD señala: "*La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado";* definiéndose el concepto de dato de carácter personal en el apartado a) del artículo 3 de la LOPD, como *"Cualquier información concerniente a personas físicas identificadas o identificables".*

La garantía del derecho a la protección de datos, conferida por la normativa de referencia, requiere que exista una actuación que constituya un tratamiento de datos personales en el sentido expresado. En otro caso las mencionadas disposiciones no serán de aplicación.

El artículo 5.1.f) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en lo sucesivo Real Decreto 1720/2007, de 21 de diciembre), define datos de carácter personal como: *"Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables".*

En este mismo sentido se pronuncia el artículo 2.a) de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 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, se entiende por dato personal *"toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social"*. Asimismo, el Considerando 26 de esta Directiva se refiere a esta cuestión señalando que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a aquélla.

III

El artículo 6 de la LOPD, dispone:

"*1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.*

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencia; cuando se refieran a las partes de un contrato o precontrato

de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento…;".

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuya efectos retroactivos."

Pues bien, el denunciante mantiene una relación laboral con la UAM que la habilita el tratamiento de sus datos para las finalidades que tiene encomendadas como es control horario/presencial de sus trabajadores.

Dentro de los datos a tratar incluyen los "datos biométricos" que son aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto de aquellos de forma que resulta imposible la coincidencia de tales aspectos en dos individuos. Una vez procesados, permiten servir para identificar al individuo en cuestión. Así, se emplean para tales fines las huellas digitales, el iris del ojo o la voz, entre otros.

IV

El tratamiento de datos biométricos han sido objeto de estudio por el Grupo de Protección de Datos que se creó en virtud del artículo 29 de la Directiva 95/46/ CE del Parlamento y del Consejo Europeo, de 24 de octubre de 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.

El citado Grupo en el Documento de trabajo sobre biometría adoptado el 1 de agosto de 2003 establece entre sus conclusiones que:

"El Grupo opina que la mayor parte de los datos biométricos implican el tratamiento de datos personales. Por consiguiente, es necesario respetar plenamente los principios de la protección de datos que aparecen en la Directiva 95/46/CE teniendo en consideración, al desarrollar los sistemas biométricos, la especial naturaleza de la biometría, y entre otras cosas su capacidad de recopilar datos biométricos sin el conocimiento del interesado y la casi seguridad del vínculo con la persona.

El cumplimiento del principio de proporcionalidad, que constituye el núcleo de la protección garantizada por la Directiva 95/46/CE impone, especialmente en el contexto de la autenticación/comprobación, una clara preferencia por las aplicaciones biométricas que no tratan datos obtenidos a partir de rastros físicos dejados por personas sin darse cuenta o que no se almacenan en un sistema centralizado. Ello permite al interesado ejercer un mejor control sobre los datos personales tratados que le afectan."

V

El artículo 5.1 de la LOPD dispone lo siguiente:

"1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante".

El citado artículo 5 de la LOPD se constituye en la premisa necesaria para que el responsable del fichero pueda tratar los datos de carácter personal. Para ello se informa al titular de los datos de modo preciso, expreso e inequívoco de la existencia del fichero así como de su finalidad y de los destinatarios de la información, de la identidad del responsable, del carácter obligatorio o voluntario de las preguntas que les sean formuladas, de las consecuencias de la negativa a suministrar los datos, y de los derechos que reconoce la LOPD al titular de los datos. Por tanto, el principio de información en la recogida de los datos es el presupuesto necesario para que el responsable del fichero pueda tratar los mismos. La razón de esta exigencia viene basada en el principio del consentimiento que es el fundamento básico de la normativa de protección de datos.

La Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, al delimitar el contenido esencial del derecho fundamental a la protección de los datos personales, ha considerado el *"principio de información"* como un elemento indispensable del derecho fundamental a la protección de datos según recoge y desarrolla el cuerpo del citado fallo

VI

Desde el punto de vista laboral por parte del empresario, el Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el Texto Refundido del Estatuto de los Trabajadores -ET- ha atribuido facultades específicas a la empresa que posibilitan el control del desarrollo de la prestación laboral y el ejercicio de estas facultades comporta en muchas ocasiones tratamientos de datos personales.

Su artículo 20 *"Dirección y Control de la Actividad Laboral"* , apartado 3 y 4 , disponen:

«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 humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso.

Cuando para el desarrollo de la función empresarial de control se utilizan las tecnologías de la información, las posibilidades de repercusión en los derechos del trabajador se multiplican y se manifiestan de muy diversos modos, siendo ello aplicable tanto a la utilización de herramientas puestas a disposición por el empresario como, por

analogía, a la utilización del teléfono móvil particular por el trabajador siempre que la limitación impuesta sea necesaria para lograr un *"fin legítimo*" , sea "*proporcionada"* para alcanzarlo y *"respetuosa"* con el contenido del derecho., pudiéndose citar entre otros medios de control, los controles biométricos como la huella digital, la videovigilancia, los controles sobre el ordenador -como las revisiones, el análisis o la monitorización remota, la indexación de la navegación por Internet, o la revisión y monitorización del correo electrónico y/o del uso de ordenadores- o los controles sobre la ubicación física del trabajador mediante geolocalización, junto a la restricción en el uso del teléfono móvil .

Pues bien, el tema planteado ha sido tratado en numerosas sentencia de los tribunales por todas ellas la del Tribunal Supremo de fecha 26/09/2007 sobre el *"control empresarial del correo electrónico",* que concluye la posibilidad de que el empresario pueda establecer sistemas de control del ordenador, del correo electrónico, los accesos a Internet de los trabajadores a controles de geolocalización, siempre que la empresa de *"buena fe"* haya establecido *"previamente"* las reglas de uso de esos medios con aplicación de prohibiciones absolutas o parciales e informado de que va existir un control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos. Doctrina del Tribunal Supremo que es extensible sistemas de control m por da5tos biométricos siempre que se haya informado de buena fe.

En el presente caso, las diligencias preliminares llevadas a cabo en UAM respecto al derecho de información a los trabajadores acreditan lo siguiente:

- Que la UAM informó por correo electrónico de 4 de diciembre de 2015 remitido por el Director del SIDI a la lista del SIDI (....@uam.es) de la implantación del citado sistema desde el 15 de diciembre de 2015 y, entre otros extremos, que sistema tenía por finalidad el "Control de Acceso" a través de huella dactilar que permitía, además de la identificación inequívoca de cada uno, el registro de la hora de entrada y salida del personal así como que el control se realizaría a través de una tarjeta que permitiría: el Control de Asistencia, de Solicitudes de Permisos, de Solicitudes de moscosos , de Vacaciones y el Control de usuarios

Asimismo, aportó copias de los subsiguientes correos electrónicos remitidos, al igual que el anterior, por el Director a la lista del SIDI:

> De fecha 16 de diciembre de 2015: En el que se recuerda que los trabajadores deben pasar por administración para el registro de la huella, ya que desde el viernes dejaran de tener validez las tarjetas que se usan para acceder al SIDII.
>
> De fecha 17 de septiembre de 2015: Informando de que por problemas técnicos, la fase de pruebas del nuevo sistema se pospone al 21 de diciembre.
>
> De fecha 21 de enero de 2016: En el que se informa de la implantación del nuevo sistema el 1 de febrero.
>
> De fecha 14 de marzo: Con el que se remite una carta con instrucciones sobre la utilización del sistema.
>
> Y según manifiestan, entre los destinatarios de los correos, se encuentra un miembro del Comité de Empresa de la UAM y los cinco trabajadores del centro designados como representantes del resto ante la Junta de Facultad

en la que se encuentra localizado el SIDI.

Por ello, desde el punto de vista de protección de datos el empresario cumplió con la obligación de informar "previamente y de buena fe" previamente al tratamiento del dato de la huella dactilar para que pudiese ser utilizada para el control horario de los trabajadores de la UAM, procediendo el archivo .

VII

Respecto al hecho constatado de que no se ha solicitado la inscripción de los datos biométricos en los ficheros declarados a la Agencia como el de Control de Presencia, de Videovigilancia o de Control de Acceso, alegan que el sistema debería haber estado en funcionamiento desde el 1 de abril de 2016, no obstante dadas las incidencias que se han dado en la implantación se encuentra en **fase experimental**, por lo que los datos recopilados aún no han pasado a la fase de explotación.

Por ello, se observa a la UAM que una vez implantado definitivamente el sistema, deberá actualizar el fichero de "control de accesos" incluyendo el tratamiento del dato biométrico de la "huella dactilar" y en su caso, actualizar las finalidades del mismo.

Por lo tanto, de acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

La UNIVERSIDAD AUTONOMA DE MADRID, implementado el sistema de control de accesos a través de la huella dactilar deberá incluir dicho dato entre los datos utilizados en el tratamiento.

NOTIFICAR la presente Resolución a la ***UNIVERSIDAD AUTONOMA DE MADRID.***

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, 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 del referido texto legal.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la citada LJCA, sólo podrá interponer 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 LJCA, 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 del referido texto legal.

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