Expediente Nº: E/03942/2015

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la ***OFICILIA MAYOR DEL MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS*** en virtud de denuncia presentada por D. ***B.B.B.*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 28 de abril de 2015, tuvo entrada en esta Agencia escrito de D. ***B.B.B.*** en el que denuncia que el citado Ministerio de Hacienda y Administraciones Públicas, a través de su Oficialía Mayor, ha establecido un sistema biométrico con lector de huella dactilar para acceder al centro de trabajo ubicado en la c/ María de Molina 50 en los accesos de la calle Castello ubicados en el número 115, 2ª y 3ª planta y número 117 3ª planta y para utilizar el citado sistema, que ha entrado en funcionamiento en fecha de 25/2/2015, se precisa que el trabajador aporte su huella dactilar que queda incorporada a un fichero.

Añade, que el personal afectado no ha recibido la información establecida en al artículo 5.1 de la LOPD y considera el denunciante que el mencionado sistema no es idóneo al no garantizar la seguridad y la integridad física del personal debido, a juicio de los denunciantes, a que los lectores de huellas se encuentran ubicados en zonas de libre acceso al público, como son las escaleras y los ascensores, además de que los empleados cuentan con una tarjeta de empleado que cuenta con firma digital con lo que se podría haber instalado un lector para dichas tarjetas.

Junto a la denuncia aporta la siguiente documentación:

Reportaje fotográfico en los que según los denunciantes se aprecia:

- El interior de dos ascensores que se encuentran ubicados en la calle Castello, 115 y en los que se observa lectores de huellas dactilares según los denunciantes para el acceso a la tercera planta.
- Puertas de acceso junto a las cuales se observa lectores de huellas según los denunciantes para el acceso a la segunda planta tanto a su parte izquierda como a su parte derecha.

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:

1.En fecha de 18/1/2016 se ha practicado inspección a las dependencias del Ministerio donde se ha implantado el sistema averiguándose lo siguiente:

1.1. Las dependencias que el Ministerio tiene en la calle María de Molina, 50 de Madrid, se ubican en diversas plantas del edificio que limita con las calles Maria

de Molina, Castelló, Núñez de Balboa y General Oráa. Dichas dependencias se conocen bajo en nombre de COMPLEJO EUROCIS

1.2. El edificio que alberga las citadas oficinas no es de uso exclusivo del Ministerio sino que es compartido con otras oficinas privadas y viviendas particulares, de tal forma que en los accesos a las citadas dependencias del Ministerio se da la siguiente casuística:

1.2.1. *Acceso por Maria de Molina, 50:* proporciona acceso exclusivo a las dependencias del Ministerio. Dicho acceso es utilizado tanto por el personal que trabaja en las dependencias como por público que acude a realizar determinadas gestiones administrativas ante el Ministerio.

1.2.2. *Acceso por la calle Castello, números 115 y 117*: Se trata de dos accesos a través de un portal compartido con otras oficinas y viviendas y donde las dependencias Ministeriales ocupan las plantas segunda y tercera planta.

La planta tercera es exclusiva del Ministerio tanto en el acceso por el portal 115 como por el 117.

La planta segunda es exclusiva del Ministerio en el acceso por el número 117. En el acceso por el número 115 la planta se comparte con una oficina privada por lo que en este caso el control de acceso no está ubicado en el interior del ascensor sino justo en las puertas de entradas a las dependencias del Ministerio. En todo caso dichos accesos a las dependencias del Ministerio se encuentran reservados en exclusiva al personal, ya sea propio o subcontratado, que presta servicios en las citadas dependencias del Ministerio, personal que puede realizar dicho acceso de dos formas:

1.2.2.1. A través de la escalera que conduce a las plantas segunda y tercera a sus respectivos descansos donde se ubican sus correspondientes puertas de entrada. La apertura de dichas puertas que dan acceso a las dependencias del Ministerio puede realizarse bien llamando a un video portero electrónico o bien accionando la apertura de la puerta mediante un lector de huella dactilar.

1.2.2.2. A través de los ascensores ubicados en dichos portales (dos en cada uno de ellos) que tanto en la planta segunda como en la tercera, conducen directamente al interior de las oficinas del Ministerio por lo que para poder seleccionar dichas plantas en los ascensores se ha dispuesto del control basado en huella dactilar cuyo sensores se encuentran en la botoneras de los citados ascensores. Lo anterior es con excepción en el acceso a la segunda planta por el número 115 donde al estar compartido con la oficina privada el control de acceso para dicha planta se encuentra fuera del ascensor. Estos ascensores cuentan también con video-portero como mecanismo alternativo a la huella dactilar para realizar dicho control de acceso.

1.3. El sistema de huella dactilar presenta las siguientes características:

1.3.1. Tiene como finalidad exclusiva la de control de acceso. De hecho el mencionado sistema no se encuentra conectado a ningún otro sistema, por lo que no se utiliza para control laboral ni se encuentra conectado al sistema de fichaje para el control horario de los empleados. Los datos de accesos recabados por dicho sistema son almacenados en el mismo por un periodo de 30 días tras los cuales son borrados.

1.3.2. El sistema de huella da lugar un fichero automatizado que contiene datos de carácter personal y cuyo fichero fue aprobado mediante la Orden HAP 2478/2013 de 20 de diciembre (BOE 1/1/2014), modificada por la Orden HAP 2503/2015 de 25/11/2015 (BOE 26/11/2015) donde en su página 10 se recoge las características de dicho fichero. El mencionado fichero figura inscrito en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos con el código ****CÓD.1* bajo el nombre de *CONTROL DE ACCESO* recogiendo en su estructura de datos de carácter identificativo el *NIF/DNI, Nombre y apellidos, Dirección, Teléfono y Huella* y como finalidades las de *Seguridad y Control de Acceso a Edificios,* figurando como descripción detallada de la finalidad y usos previstos la de *Gestión del control de entradas a los edificios de la Secretaría de Estado de Administraciones Públicas y dependencias del Ministerio de Hacienda y Administraciones Públicas ubicadas en el Complejo Eurocis.* Constan en las actuaciones copias de las citadas Órdenes.

1.3.3. La utilización del sistema de control de acceso basado en huella dactilar se realiza de forma voluntaria. Es decir, únicamente se aplica a aquellos empleados que así lo solicitan, ya que existen mecanismos de control de acceso alternativos (el uso del video-portero en los accesos por la calle Castelló para las plantas segunda y tercera, y el uso de la entrada general de la calle Maria de Molina 50 para la planta tercera). El sistema es utilizado por cerca de 500 personas de un total de aproximadamente 2000.

1.3.4. Los empleados que solicitan dicho acceso rellenan una ficha, de la que consta copia en las actuaciones, donde se recaban sus datos identificativos. Dicho formulario incluye como información relativa al artículo 5.1 de la LOPD y como paso previo a captura de los datos de huella para su incorporación al sistema la siguiente:

> *"Accedo voluntariamente a la captura de mi huella dactilar, con el fin de poder utilizar el sistema biométrico de control de accesos, establecido para acceder a las zonas restringidas del edificio a las que estoy autorizado por el Área de Seguridad, no utilizando mi autorización de acceso para facilitar la entrada de personas no autorizadas por el Área de Seguridad. Estos datos formarán parte del fichero denominado 'Control de Accesos', dado de alta en la Agencia Española de Protección de Datos, con código de inscripción número ***CÓD.1, cuyo responsable es la Oficial Mayor del Ministerio de Hacienda y Administraciones Públicas. Los derechos de acceso, consulta, oposición y cancelación recogidos en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de Datos de Carácter Personal, podrán ser ejercitados ante la Oficialía Mayor del citado Ministerio en la siguiente dirección: (C/.....1)".*

1.3.5. Desde la Oficialía Mayor se procedió a D.D.D. a los empleados mediante el documento del que se adjunta copia y que se remitió a la Junta de Personal y a la Subdirectora General de Organización, Planificación y Gestión de Recursos de la IGAE y al Subdirector General de Asuntos Generales y Coordinación de la Secretaria de Estado de Administración Públicas, ambas subdirecciones por ser las competentes en materia de recursos humanos con personal en las dependencias afectadas por el mecanismo de control de acceso basado en huella y con el fin de que difundieran la información entre su personal, realizándose dicha difusión mediante los tablones de información al personal existentes en dichas dependencias.

Dichas comunicaciones se efectuaron desde la Oficialía Mayor mediante correos electrónicos entre el 2 y el 18 de febrero de 2015 de los que también se ha recabado copia. Dicha difusión ha sido adicional a la información personalizada que a cada empleado se le facilita en el momento de recoger su huella como se detalla en el punto anterior.

1.3.6. Se ha recaba copia del documento que contiene una memoria justificativa del sistema.

1.3.7. Técnicamente la lectura de la huella dactilar se realiza de tal manera que al capturar la huella se obtienen una serie de parámetros o resumen de la huella de origen de forma que es posible distinguirla de otras pero no reproducir, a partir del resumen obtenido, la imagen origen de la huella.

Se recaba copia del certificado emitido por la empresa instaladora del sistema en el que se recoge que en ningún caso se almacena ni en la base de datos ni en los terminales una imagen de la huella, así como que técnicamente es imposible reproducir la imagen exacta de la huella a partir de patrón de huella captado con el sensor.

2. Durante la inspección se han visitado las distintas dependencias del complejo en general y en particular:

2.1. A la sala de control donde se centraliza el control de accesos tanto mediante la utilización del mecanismo de huella dactilar como del video-portero.

2.2. Al puesto desde el que se realiza el alta en el sistema de huella comprobándose que el procedimiento de captura de huella se corresponde con el descrito en el presente acta.

2.3. A los ascensores y escaleras de accesos ubicadas en los portales de la Calle Castelló 115 y 117, en sus plantas segunda y tercera.

Se ha recaba reportaje fotográfico de las dependencias visitadas obrante a las actuaciones.

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

Se denuncia que el Ministerio de Hacienda y Administraciones Públicas, a través de su Oficialía Mayor, ha establecido un sistema biométrico con lector de huella dactilar para acceder al centro de trabajo ubicado en la c/ María de Molina 50 en los accesos y para utilizar el citado sistema, que ha entrado en funcionamiento en fecha de 25/2/2015, se precisa que el trabajador aporte su huella dactilar que queda incorporada a un fichero, considerando el denunciante que el personal afectado no ha recibido la información establecida en al artículo 5.1 de la LOPD y que el sistema no es idóneo al no garantizar la seguridad y la integridad física del personal debido a que los lectores de huellas se encuentran ubicados en zonas de libre acceso al público, como son las escaleras y los ascensores, además de que los empleados cuentan con una tarjeta de empleado que cuenta con firma digital con lo que se podría haber instalado un lector para dichas tarjetas.

La LOPD en su artículo 6, recoge:

"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 competencias; 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";

En el presente caso, está probada la relación administrativa del denunciante con el Ministerio de Hacienda y Administraciones Públicas que la permite tratar los datos personales del denunciante para las finalidades laborales que tiene encomendadas como el seguimiento de las obligaciones profesionales.

Por otra parte, son "datos biométricos" 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.

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."

III

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 al declarar que: "...*el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.*

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y, el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que rectifique o los cancele."

La información sobre la finalidad del sistema implantado, sus usos, y el establecimiento del procedimiento para el ejercicio de derechos a los mismos datos constituyen parte esencial no solo del marco de protección de datos de carácter personal sino también relevante en el ámbito de los derechos y deberes laborales relacionados con los derechos a la intimidad personal y a la propia imagen, en relación con su derecho a la tutela judicial efectiva por admitirse por ejemplo como prueba de cargo en un hipotético proceso por despido los datos obtenidos.

Así, el establecimiento del sistema en la Administración General de Estado al tener la competencia para la ordenación del tiempo de trabajo del personal a su servicio, de acuerdo con el artículo 47 de la Ley 7/2007, de 12 de abril que aprueba el Estatuto Básico del Empleado Público, no precisa para la implantación y recogida de datos del consentimiento de los empleados para su funcionamiento, si bien sí que se debe adecuar a los principios básicos de la LOPD: proporcionalidad, calidad de datos y que se contenga una adecuada información sobre dicha recogida de datos, pues la no necesidad de obtención del consentimiento no supone la no información sobre el mecanismo de información y uso de la recogida de los mismos que tiene lugar a través del mismo. Esta información se constituye en garantía de la autodeterminación informativa o la "*libertad informática*", reconocido expresamente por la jurisprudencia de nuestro Tribunal Constitucional, a partir de su Sentencia 254/1993, de 20/07 que constituyen parte del derecho fundamental a la protección de datos que se concreta jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos

posibles, por un tercero, sea el Estado o un particular.

En cuanto a la legitimación para la instalación de dicho medio de control laboral hay que remitirse al Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores -ET- que atribuye 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, 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.

4. El empresario podrá verificar el estado de enfermedad o accidente del trabajador que sea alegado por éste para justificar sus faltas de asistencia al trabajo, mediante reconocimiento a cargo de personal médico. La negativa del trabajador a dichos reconocimientos podrá determinar la suspensión de los derechos económicos que pudieran existir a cargo del empresario por dichas situaciones. (Art. 20.3 y 4 Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores).

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. Pueden citarse entre otros, 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.

En la mayor parte de estos supuestos existen tratamientos de datos personales y, en consecuencia es necesario cumplir con los principios de protección de datos.

La Agencia Española de Protección de Datos y la jurisprudencia de los tribunales han venido indicando distintos supuestos en los que tales tratamientos son admisibles y las condiciones para su realización.

Por otro lado, el uso de tecnologías de la información multiplica las posibilidades de control empresarial y obliga a tener en cuenta el respeto a los derechos fundamentales de los trabajadores, a adoptar medidas de control que sean proporcionales y respeten su dignidad, su derecho a la protección de datos y su vida privada.

Existe por tanto, un conjunto de principios cuyo respeto resulta recomendable cuando no prácticamente ineludible.

La legitimación para el tratamiento deriva de la existencia de la relación laboral y, por tanto, de acuerdo con el trascrito artículo 6.2 LOPD, no se requiere del

"consentimiento" .

A la hora de decidir adoptar una medida de control de acceso que comporte un tratamiento de datos personales debe aplicarse el principio de **"proporcionalidad"** así puede ser perfectamente razonable dotar de un sistema mediante el tratamiento de la "huella dactilar" como, en el presente caso, para el control laboral por el empresario del cumplimiento de las obligaciones de los trabajadores y de la seguridad en las instalaciones del Ministerio dado que el mismo edificio ciertas plantas es compartido con empresas privadas y viviendas.

Debe existir una **"finalidad"** que, en este caso, no puede ser otra que la establecida por el trascrito artículo 20.3 ET de *«verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales»*.

«En cuanto a la posibilidad de que las huellas sean tratadas sin consentimiento del interesado, (...) será posible el tratamiento inconsentido, ya que el artículo 6.2 de la LOPD prevé que no será preciso el consentimiento cuando los datos "se refieran a las partes de un contrato o precontrato de una relación laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento" (Informe sobre Tratamiento de la huella digital de los trabajadores)»

Los datos que se obtengan y almacenen deberán ser **"exactos y puestos al día"** y no podrán conservarse más tiempo del necesario. Se recomienda a los empleadores fijar un plazo de conservación.

Y también, debe cumplirse con el deber de **"información"** a los trabajadores. Este deber resulta particularmente relevante, no solo sobre el uso de Internet y/o del correo electrónico, sino cuando se trate de controles a través del tratamiento de la huella dactilar máxime cuando puedan ser objeto de utilización posterior a efectos disciplinarios. En este caso, es muy recomendable que la información a los trabajadores sea clara en lo que respecta a la política de la empresa en cuanto al uso de la huella dactilar a efectos del control horario y la seguridad de las instalaciones, describiendo de forma pormenorizada en qué medida los trabajadores pueden quedar afectados por la información obtenida del tratamiento de dicho dato biométrico.

Por otra parte, en la medida en la que este tipo de controles inciden sobre el conjunto de la empresa puede ser muy recomendable informar también a los representantes de los trabajadores de las políticas adoptadas en esta materia. No se trata en absoluto de que el trabajador conozca el detalle de políticas de seguridad que pueden afectar a ámbitos que la empresa necesita proteger. La **información previa** y su prueba es esencial, ya que estos tratamientos no requieren el consentimiento del trabajador y son manifestación de los poderes de control del empresario.

«..es necesario recordar lo que ya se dijo sobre la existencia de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores. Esa tolerancia crea una expectativa también general de confidencialidad en esos usos; expectativa que no puede ser desconocida, aunque tampoco convertirse en un impedimento permanente del control empresarial, porque, aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza un

medio proporcionado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio. Por ello, lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer ***previamente*** *las reglas de uso de esos medios –con aplicación de prohibiciones absolutas o parciales- e* ***informar*** *a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones. De esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado "una expectativa razonable de intimidad" en los términos que establecen las sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (caso Halford) y 3 de abril de 2007 (caso Copland) para valorar la existencia de una lesión del artículo 8 del Convenio Europeo par la protección de los derechos humanos. (Sentencia de la Sala de lo Social del Tribunal Supremo de 26 de septiembre de 2007)».*

En síntesis, el Tribunal Supremo en la Sentencia de fecha 26 de septiembre de 2007 sobre el *"control empresarial del correo electrónico",* concluye la posibilidad de que el empresario pueda acceder al control del ordenador, del correo electrónico, los accesos a Internet de los trabajadores, a controles de geolocalización y al control horario a través de la huella dactilar, 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.

IV

Pues bien, de las diligencias preliminares llevadas a cabo por la Inspección "in situ" se desprende que la Oficialía Mayor del Ministerio estableció el sistema de control horario por la huella dactilar con carácter "voluntario" adoptándose por cerca de 500 trabajadores de un total de aproximadamente 2000 y previamente al funcionamiento informó a los trabajadores, conducta que observa las prescripciones previstas en la normativa sobre protección de datos y jurisprudencia consolidada.

El Hecho Segundo de la presente resolución es concluyente respecto a que la Oficialía Mayor del Ministerio de Hacienda y Administraciones Publicas informó a los trabajadores previamente de la instalación del control de presencia mediante huella dactilar dado que los empleados que lo solicitaron rellenaron una ficha, en la que se recaban sus datos identificativos e incluye información relativa al artículo 5.1 de la LOPD como paso previo a captura de los datos de huella para su incorporación al sistema del siguiente tenor : *"Accedo voluntariamente a la captura de mi huella dactilar, con el fin de poder utilizar el sistema biométrico de control de accesos, establecido para acceder a las zonas restringidas del edificio a las que estoy autorizado por el Área de Seguridad, no utilizando mi autorización de acceso para facilitar la entrada de personas no autorizadas por el Área de Seguridad. Estos datos formarán parte del fichero denominado 'Control de Accesos', dado de alta en la Agencia Española de Protección de Datos, con código de inscripción número ***CÓD.1, cuyo responsable es la Oficial Mayor del Ministerio de Hacienda y Administraciones Públicas. Los derechos de acceso,*

consulta, oposición y cancelación recogidos en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de Datos de Carácter Personal, podrán ser ejercitados ante la Oficialía Mayor del citado Ministerio en la siguiente dirección: (C/.....1)".

A mayor abundamiento, desde la Oficialía Mayor se procedió a informar a los empleados según obra a las actuaciones y que se remitió a la Junta de Personal y a la Subdirectora General de Organización, Planificación y Gestión de Recursos de la IGAE y al Subdirector General de Asuntos Generales y Coordinación de la Secretaria de Estado de Administración Públicas, ambas por ser las competentes en materia de recursos humanos con personal en las dependencias afectadas por el mecanismo de control de acceso basado en la huella y con el fin de que difundieran la información entre su personal, realizándose dicha difusión mediante los tablones de información al personal existentes en dichas dependencias y de electrónicos entre el 2 y el 18 de febrero de 2015, siendo dicha difusión ha sido adicional a la información personalizada que a cada empleado se le facilita en el momento de recoger su huella.

Por lo que, está acreditado que los trabajadores que "voluntariamente" adoptaron el sistema de control horario mediante la "huella dactilar" en el Ministerio de Hacienda y AA.PP con anterioridad a su establecimiento se informó a los afectados, por lo que procede declarar el archivo de las actuaciones

Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

3. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
4. **NOTIFICAR** la presente Resolución a la ***OFICILIA MAYOR DEL MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS*** y a D ***B.B.B..***

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 Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, 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