Expediente Nº: E/00793/2016

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad ***KONECTA SERVICIOS ADMINISTRATIVOS Y TECNOLÓGICOS S.L.*** – **KONECTA SAT SL**- en virtud de denuncia presentada por D. ***A.A.A.*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 15 de diciembre de 2015, tuvo entrada en esta Agencia un escrito de D. ***A.A.A.,*** miembro del Comité de empresa de la mercantil Konecta SAT SL , en el que denuncia que, desde el día 11/12/2015, la empresa comenzó a utilizar la huella dactilar de los trabajadores como control de acceso y salida del centro de trabajo sito en la calle (C/...1), no habiendo informado previamente a los trabajadores sobre la finalidad de la toma de huella dactilar ni han solicitado consentimiento,
Asimismo, manifiesta no existir ningún fichero registrado en la Agencia relativo a las huellas digitales.

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. Con fecha 15 de febrero de 2016, se realiza una búsqueda en el Registro General de Protección de Datos, verificando la existencia de un fichero titularidad de KONECTA SERVICIOS ADMINISTRATIVOS Y TECNOLÓGICOS, S.L., denominado Seguridad y Control de Accesos a Edificios, con el código de inscripción: ***CÓD.1.
2. Con fecha 1 de agosto de 2016, se recibe información de la entidad KONECTA SAT, poniendo de manifiesto que:
    2.1. El sistema de huella digital implantado en el centro ubicado en la calle del (C/...1) (Madrid), no es un sistema de control de presencia, únicamente es un sistema de "seguridad" que pretende garantizar que aquellas personas que acceden al edificio cuenten con la preceptiva autorización y sean trabajadores de KONECTA SAT SL.
    2.2. Con fecha **2 de junio de 2015**, por primera vez desde el Departamento de Relaciones Laborales de la compañía, se procedió a informar a la Representación Legal de los trabajadores de KONECTA SAT, SL de la futura implantación de este control de acceso a la plataforma, comunicación que fue reiterada el día 7 de diciembre de 2015, según copia de los correos electrónicos remitidos con fechas 2 de junio y 7 de diciembre de 2015.
    2.3. Con fecha 16 de octubre de 2015 se colocaron carteles informativos en la plataforma informando a todos los trabajadores de la implantación del citado

sistema de acceso y adjuntan copia de la Nota informativa colocada.

2.4. Se anexa copia del correo electrónico enviado por el Departamento de Recursos Laborales de KONECTA SAT SL a los responsables de Servicio para que procedieran a su inmediata colocación de la Notas Informativas preparadas al efecto.

2.5. En **paralelo** a estas acciones, se informó por escrito y de forma individualizada a los trabajadores del referido centro de trabajo, de la implantación del control de acceso a las instalaciones como medida para garantizar la seguridad del centro y adjuntan copia del modelo de la referida ´comunicación.

2.6. La implantación del citado sistema de acceso en la calle del (C/...1) (Madrid), tuvo lugar la última semana del mes de enero de 2016

3. Con fecha 30 de agosto de 2016, se persona en esta Agencia, D.ª ***B.B.B.,*** en calidad de representante legal de la entidad KONECTA SAT S.L., haciendo entrega de un pen-drive que contiene aproximadamente 150 hojas informativas a trabajadores de la entidad, en la que comunican la implantación del nuevo sistema de control de acceso al centro de trabajo sito (C/...1) (Madrid), todos ellos suscritos por los propios trabajadores,

Así mismo, manifiesta que dichos comunicados fueron ofrecidos a la firma con fecha 16 de diciembre de 2015, a los trabajadores que en ese momento trabajaban en la Plataforma, pero en los nuevos contratos se incluirá una cláusula informativa del sistema de control de acceso a dicho centro.

No obstante, manifiesta que únicamente se trata de un control de acceso al centro, para comprobar que son personas autorizadas, pero en ningún caso se trata de un control de presencia, ya que para salir no es preciso poner la huella, es un acceso libre.

Se adjuntan a estas Actuaciones 14 ejemplares (de los 150 visualizados en el pen drive) de comunicaciones de implantación del sistema de huella dactilar, firmadas por 14 trabajadores de la Plataforma con fecha 16 de diciembre de 2015.

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

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, según el cual, a efectos de dicha Directiva, 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 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal 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; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

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."

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.

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 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."

VI

En el presente caso, el representante del Comité de Empresa de KONECTA denuncia comenzó la utilización de la huella dactilar de los trabajadores como control de acceso y salida del centro de trabajo sito en la calle (C/...1), a lo que se ha de señalar que consultado el Registro General de Protección de datos se acredita que la mercantil KONECTA SAT, SL tiene inscrito el fichero denominado "control de accesos" con la finalidad de gestión de los accesos en los edificios mediante lectura dactilar y previsto el dato identificativo de "otros datos biométricos"

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.

Pues bien, de las diligencias preliminares llevadas a cabo en KONECTA SAT SL en las que informa que el sistema der acceso implementado únicamente se trata de un control al centro para comprobar que son personas autorizadas ya que para salir no es preciso poner la huella, respecto al derecho de información ha quedado acreditan :

- Que con fecha 2/06/2015, por primera vez, desde el departamento de Relaciones Laborales de la compañía se procedió a informar a la Representación Legal de los trabajadores de la futura implantación de este control de acceso a la plataforma, comunicación que fue reiterada el día 7/12/2015, según copia de los correos electrónicos remitidos con fechas 2/6 y 7/12/2015.

- Que con fecha 16/10/2015 se colocaron "carteles informativos" informando a todos los trabajadores de la implantación del citado sistema de acceso y adjuntan copia de la Nota informativa colocada.

- Que en paralelo a dichas acciones, se informó por escrito y de forma individualizada a los trabajadores, de la implantación del control de acceso a las instalaciones como medida para garantizar la seguridad del centro , implantación del citado sistema de acceso que en la calle del (C/...1) (Madrid), tuvo lugar la última semana del mes de enero de 2016

- Y que el 30/08/2016, la entidad KONECTA SAT S.L., hizo entrega en la Agencia de un pen-drive que contiene aproximadamente 150 hojas informativas a trabajadores de la entidad, en la que comunican la implantación del nuevo sistema de control de acceso al centro de trabajo sito C/ (C/...1) (Madrid), todos ellos suscritos por los propios trabajadores y manifiestan que dichos comunicados fueron ofrecidos a la firma con fecha 16/12/2015 a los trabajadores que en ese momento trabajaban en la Plataforma, pero en los nuevos contratos se incluirá una cláusula informativa del sistema de control de acceso a dicho centro.

Por lo que, desde el punto de vista de protección de datos el empresario cumplió con la obligación de informar "previamente y de buena fe" sobre el tratamiento del dato personal de la huella dactilar para, en su caso, pudiese ser utilizada para el control horario de los trabajadores de la empresa., procediendo el archivo en base a dicho motivo laboral.

VII

No obstante, KONECTA alega que el tratamiento del dato de la huella dactilar únicamente se trata al acceder las personas a las instalaciones pero no a la salida, siendo la finalidad motivos de "seguridad" interna de la empresa, por lo que constatado que los trabajadores fueron informados "previamente y de buena fe" del tratamiento de la huella dactilar dichas medidas no corresponde enjuiciarlas a esta Agencia si,

como ha quedado, acreditado, la empresa informó previamente a sus trabajadores, por lo que procede, igualmente, al Archivo en base a dicho motivo.

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

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.

2. **NOTIFICAR** la presente Resolución a ***KONECTA SERVICIOS ADMINISTRATIVOS Y TECNOLÓGICOS S.L..***

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.

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