Expediente Nº: E/04936/2016

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante D. ***A.A.A. (B.B.B. ASOCIADOS, S.L.)*** **y** Dª**.** ***C.C.C.*** en virtud de denuncia presentada por Dª. ***D.D.D.*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 21 de junio y de 7 de julio de 2016 tiene entrada en la Agencia Española de Protección de Datos (AEPD) escrito de D. ***E.E.E.*** (en representación de Dña. ***D.D.D.*** (en adelante denunciante), comunicando posible infracción a la Ley Orgánica 15/1999 motivada por la instalación de cámaras de videovigilancia cuyos titulares son ***B.B.B. ASOCIADOS, S.L.*** (en adelante el denunciado1), ubicadas ***(C/...1),*** y Dª. ***C.C.C.*** (en adelante denunciado2)***,*** instaladas en ***(C/...2) de MADRID***, ambas con denominación comercial "XXXX", sin las debidas medidas de seguridad.

La denunciante manifiesta que fue empleada de los denunciados, si bien contratada por la entidad ***B.B.B. ASOCIADOS, S.L.,*** pero comparten los denunciados espacios físicos de trabajo e incluso trabajadores. Que la denunciante tenía libre acceso a las grabaciones de las cámaras de videovigilancia de ambos centros de trabajo, al igual que el resto de los trabajadores, habiendo descargado las imágenes grabadas, de varios días completos, para poderlas usar como prueba ante las demandas presentadas ante un tribunal competente en materia de legislación laboral.

Que los denunciados facilitan a sus empleados el nombre de usuario y la clave de acceso para que puedan analizar en las imágenes grabadas, cuando lo consideran oportuno, detalles del desarrollo laboral diario como entrega correcta de prendas, de dinero metálico, etc.

La denunciante manifiesta que dispone de ficheros de las cámaras de videovigilancia de los establecimientos:

(C/...1): de los días 4, 11, 13 y 16 de enero de 2016.

(C/...2): de los días 14, 15 y 18 de marzo de 2016.

Se aporta reportaje fotográfico con las siguientes características:

"4" fotografías del interior del establecimiento ubicado en (C/...1) de Madrid, en las que se observan a dos personas que según manifiesta una de ellas es la denunciante y la otra ***A.A.A.***.

"3" fotografías del interior del establecimiento ubicado en (C/...2) de Madrid en las que se observan a dos personas que según manifiesta una es la denunciante y la otra ***C.C.C..***

También, aporta la denunciante sendos dispositivos de almacenamiento de datos "pendrive" que contienen dos archivos con el siguiente contenido:

Cámaras videovigilancia. *A.A.A.*: con "8" videos de fecha 4, 11, 13 y 16 de

enero de 2016, en los que figuran grabaciones de imágenes del interior de un establecimiento.

Cámaras videovigilancia. *C.C.C.*: con "6" videos de fecha 14, 15 y 18 de marzo de 2016, en los que figuran grabaciones de imágenes del interior de un establecimiento.

En la Diligencia de fecha 3 de abril de 2017 se detallan dichas circunstancias.

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 relación con el sistema de videovigilancia instalado en el local de **(C*l*...1)** de Madrid en el que desarrollaba su actividad la compañía ***B.B.B. Asociados, S.L***. (denunciado1) como negocio de venta al por mayor de ropa, cuyo administrador único es ***A.A.A.***, ha manifestado lo siguiente:

En la actualidad el local se encuentra alquilado a una tercera persona, desde diciembre de 2016, no teniendo instaladas cámaras ni monitores, habiendo cesado la actividad en el mismo en abril de 2016. Se adjunta copia del *Contrato de arrendamiento de local de negocio*, de fecha 1 de enero de 2017.

La finalidad del sistema de videovigilancia era evitar los robos y hurtos en la tienda y la empresa que realizó la instalación fue Tecnologies Serviphal 2010, S.L.U., no se realizaban grabaciones del exterior, y las imágenes permanecían durante un periodo de quince días. Se adjunta *Contrato de mantenimiento de circuito cerrado de TV* nº ****, de fecha 1 de mayo de 2010.

Al sistema de videovigilancia la única persona que estaba autorizada para acceder a las grabaciones era el administrador de la sociedad y la denunciante, empleada y responsable del negocio en ausencia del administrador, persona de confianza, en el caso de que surgiera un incidente o robo y fuera preciso acceder a ellas por causa justificada. Que nunca se autorizó a otra persona el acceso a las imágenes y no le consta que otros trabajadores hubieran accedido a las mismas.

En el documento *Protocolo sobre uso de los datos de carácter personal: dirigido a trabajadores y colaboradores de B.B.B. Asociados, S.L.:* se detallan instrucciones sobre el uso de los medios informáticos, la correcta utilización de la información que garantice el deber de secreto y el respeto a la intimidad, se adjunta dicho documento, que supuestamente debía ser firmado por el trabajador según consta el pie de la última página. También, se aporta, modelo de *Compromiso de confidencialidad* que debían de suscribir los trabajadores.

En el Registro General de Protección de Datos figura inscrito el fichero denominado "VIDEOVIGILANCIA", con el código ******CÓD.1,*** siendo responsable la compañía ***B.B.B. ASOCIADOS, S.L.,*** con fecha de última modificación el 26 de noviembre de 2012. Dichas circunstancias constan en la Diligencia de fecha 25 de abril de 2017.

Los establecimientos ubicados de ***(C/...1) y (C/...2)***, están próximos y la relación la

tienen sus dueños (Dña. ***C.C.C.*** y D. ***A.A.A.***), además hasta abril de 2016 existía una relación comercial, pues ***C.C.C.*** era cliente de ***B.B.B. ASOCIADOS, S.L.,*** que era su proveedor de mercancía, ya que ambos se dedicaban a tiendas de moda.

Que la denunciante presentó una reclamación judicial para solicitar una indemnización, decidió denunciar ante la AEPD para aprovechar esta circunstancia ante el juzgado, pero se llegó a un acuerdo, según consta en el Decreto del Juzgado de lo Social nº ** de Madrid, de fecha DD de MM de AA..

2. En relación con el sistema de videovigilancia instalado en el local de (C/...2) de Madrid, tienda XXXX, cuyo responsable es ***C.C.C.*** (denunciado2), ha manifestado lo siguiente:

La finalidad del sistema de videovigilancia es evitar robos y hurtos en la tienda y la empresa que realizó la instalación fue Tecnologies Serviphal 2010, S.L.U., no se realizan grabaciones del exterior, y las imágenes permanecen durante un periodo de quince días. Se adjunta *Contrato de mantenimiento de circuito cerrado de TV* nº ****, de fecha 1 de junio de 2011. En el que se detalla los componentes del sistema: grabador digital, monitores TFT, cámaras en carcasa, cámaras tipo compactas con leds y cámaras tipo mini domo con leds y anti-vandálicas.

El sistema de videovigilancia se compone de "5" cámaras y dos monitores, instaladas en planta principal y planta -1, se adjunta plano de situación de las cámaras, fotografías de cada una de las cámaras y de los dos monitores, ubicados en el interior de un establecimiento. También, se adjunta cartel informativo de la existencia de cámaras de videovigilancia.

Al sistema de videovigilancia únicamente están autorizados los responsables, nunca se autorizó el acceso a la denunciante, que trabajaba únicamente para ***B.B.B. ASOCIADOS, S.L.,*** que dicha persona aprovechando la confianza y la relación laboral entre ambas empresas, la cercanía de los establecimientos, abuso de la confianza, con el fin de preparar su defensa en la reclamación laboral, ya que denunció a ***C.C.C.*** de lo que finalmente desistió.

En el documento *Protocolo sobre uso de los datos de carácter personal: dirigido a trabajadores y colaboradores de* ***C.C.C.*** se detallan instrucciones sobre el uso de los medios informáticos, la correcta utilización de la información que garantice el deber de secreto y el respeto a la intimidad, se adjunta dicho documento, que supuestamente debe ser firmado por el trabajador según consta el pie de la última página. También, se aporta, modelo de *Compromiso de confidencialidad* que deben suscribir los trabajadores.

En el Registro General de Protección de Datos figura inscrito el fichero denominado "VIDEOVIGILANCIA", con el código ******CÓD.1,*** siendo responsable ***C.C.C.***, con fecha de última modificación el 28 de noviembre de 2012. Dichas circunstancias constan en la Diligencia de fecha 25 de abril de 2017.

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).

El artículo 126.1, apartado segundo, 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 establece:

Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.

II

Con carácter previo, procede situar la materia de videovigilancia en su contexto normativo.

Así 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"*

En cuanto al ámbito de aplicación de la LOPD, el artículo 2.1 de la misma 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".*

El artículo 3 de la LOPD define en su letra c) el tratamiento de datos como aquellas "*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*".

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, 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.

La Exposición de Motivos de la Instrucción 1/2006, de 8 de noviembre, de esta Agencia Española de Protección de Datos, relativa al tratamiento de los datos con fines de videovigilancia señala que: *"La seguridad y la vigilancia, elementos presentes en la sociedad actual, no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos, para de esta manera mantener la confianza de la ciudadanía en el sistema democrático"*. Sigue señalando: *"Las imágenes se consideran un dato de carácter personal, en virtud de los establecido en el artículo 3 de la Ley Orgánica 15/1999…".*

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.

Por su parte, la citada Instrucción 1/2006, dispone en su artículo 1.1 lo siguiente:

"1. La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras.

El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas.

Se considerará identificable una persona cuando su identidad pueda determinarse mediante los tratamientos a los que se refiere la presente instrucción, sin que ello requiera plazos o actividades desproporcionados.

Las referencias contenidas en esta Instrucción a videocámaras y cámaras se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita los tratamientos previstos en la misma."

La Instrucción 1/2006 en su artículo 2 establece lo siguiente:

"1. Sólo será posible el tratamiento de los datos objeto de la presente instrucción,

cuando se encuentre amparado por lo dispuesto en el artículo 6.1 y 2 y el artículo 11.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Sin perjuicio de lo establecido en el apartado anterior la instalación de cámaras y videocámaras deberá respetar en todo caso los requisitos exigidos por la legislación vigente en la materia."

De lo anteriormente expuesto se desprende que el concepto de dato personal, según la definición de la LOPD, requiere la concurrencia de un doble elemento: por una parte, la existencia de una información o dato y, por otra, que dicho dato pueda vincularse a una persona física identificada o identificable, por lo que la imagen de una persona física identificada o identificable constituye un dato de carácter personal.

III

En el presente expediente ***Dª D.D.D.,*** a través de su representante D. ***E.E.E.,*** denuncia la posible infracción a la Ley Orgánica 15/1999 motivada por la instalación de cámaras de videovigilancia cuyos titulares son ***B.B.B. ASOCIADOS, S.L.*** ubicadas en ***(C/...1),*** y Dª. ***C.C.C.*** instaladas en ***(C/...2) de MADRID***, ambas con denominación comercial "XXXX", sin las debidas medidas de seguridad, teniendo la denunciante libre acceso a las grabaciones de las cámaras de videovigilancia de ambos centros de trabajo, al igual que el resto de los trabajadores.

En primer lugar, debe entrarse a valorar el cumplimiento del deber de información e inscripción de ficheros, por parte del sistema de videovigilancia, en los establecimientos denunciados***.***

El tratamiento de las imágenes por parte del responsable, obliga a que se cumpla con el deber de informar a los afectados, en los términos establecidos en el artículo 5.1 de la LOPD el cual reza 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".

En cuanto al modo en que hay de facilitarse la información recogida en el artículo

5 de la LOPD, debe tenerse en cuenta el artículo 3 de la Instrucción 1/2006, que establece lo siguiente:

"Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán:

a) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y

b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999.

El contenido y el diseño del distintivo informativo se ajustará a lo previsto en el Anexo de esta Instrucción."

"ANEXO-

1. El distintivo informativo a que se refiere el artículo 3.a) de la presente Instrucción deberá de incluir una referencia a la «LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS», incluirá una mención a la finalidad para la que se tratan los datos («ZONA VIDEOVIGILADA»), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal."

En el caso que nos ocupa, en relación con el sistema de videovigilancia instalado en el local de **(C*l*...1) *de Madrid*** en el que desarrollaba su actividad la compañía ***B.B.B. Asociados, S.L.*** (denunciado1), cuyo administrador único es ***A.A.A.***, manifiesta que en la actualidad el local se encuentra alquilado a una tercera persona, desde diciembre de 2016, no teniendo instaladas cámaras ni monitores, habiendo cesado la actividad en el mismo en abril de 2016. Se adjunta copia del *Contrato de arrendamiento de local de negocio*, de fecha 1 de enero de 2017.

En relación con el sistema de videovigilancia instalado en el local de ***(C/...2) de Madrid,*** tienda XXXX, cuyo responsable es ***C.C.C.*** (denunciado2), ha aportado fotografía del cartel informativo de la existencia de las cámaras, ubicado en el establecimiento, acorde al que hace referencia el citado artículo 3.a) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD.

Por lo tanto el citado establecimiento, cumple el deber de información, en cuanto al sistema de videovigilancia, recogido en el artículo 5 de la LOPD, anteriormente trascrito.

Por otro lado, respecto al cumplimiento de la inscripción de ficheros, el artículo

26.1 de la LOPD, recoge lo siguiente:

"1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos"

El responsable del fichero es el titular del fichero que contiene datos de carácter personal. Sobre él van a recaer las obligaciones que establece la LOPD. . El responsable del fichero, antes de disponerse a someter datos personales a tratamiento, deberá cumplir con los requisitos de la normativa de protección de datos, teniendo en cuenta su naturaleza y la naturaleza de los datos que va a someter a tratamiento.

El apartado d) del artículo 3 de la LOPD define al responsable del fichero o tratamiento como aquella persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento. El artículo 43 de la LOPD sujeta a su régimen sancionador precisamente al responsable del fichero o tratamiento.

El reglamento de desarrollo de la LOPD, aprobado por RD 1720/2007, de 21 de diciembre, complementa esta definición en el apartado q) del artículo 5, en el que señala lo siguiente:

"q) Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados".

El responsable del fichero es, en suma, quien debe garantizar el derecho fundamental de protección de datos personales de todas las personas cuyos datos almacena. Por ello, va a estar obligado a llevar a cabo una serie de actuaciones dirigidas a la protección de los datos, a su integridad y a su seguridad.

El responsable debe notificar su fichero a la Agencia Española de Protección de Datos, que dispondrá inscribirlo en el Registro General de Protección de Datos. La notificación de inscripción del fichero facilitará que terceros puedan conocer que se está produciendo un tratamiento con una finalidad determinada y los afectados tendrán la oportunidad de ejercitar sus derechos ante el responsable.

Además este es el criterio que se hace constar en la Instrucción 1/2006 , al señalar en su artículo 7 que *"1-La persona o entidad que prevea la creación de ficheros de videovigilancia deberá notificarlo previamente a la Agencia Española de Protección de Datos, para su inscripción en el Registro General de la misma.*

Tratándose de ficheros de titularidad pública deberá estarse a lo establecido en el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal.

2.-A estos efectos, no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real."

En el caso que nos ocupa, en relación con el sistema de videovigilancia que estaba instalado en el local de **(C/...1)** de Madrid en el que desarrollaba su actividad la compañía B.B.B. Asociados, S.L. (denunciado1), constaba inscrito el fichero denominado "VIDEOVIGILANCIA", en el Registro General de Protección de Datos cuyo responsable era ***B.B.B. ASOCIADOS, S.L***., con fecha de inscripción el 26 de noviembre de 2012.

En relación con el sistema de videovigilancia instalado en el local de ***(C/...2) de Madrid***, tienda XXXX, cuyo responsable es ***C.C.C.*** (denunciado2), consta en el Registro General de Protección de Datos inscrito el fichero denominado "VIDEOVIGILANCIA", siendo responsable ***C.C.C.***, con fecha de inscripción el 28 de noviembre de 2012.

Por lo tanto ambos sistemas de videovigilancia cumplían el deber de inscripción de ficheros, recogido en el artículo 26 de la LOPD.

IV

Una vez analizado el deber de información e inscripción de ficheros, procede entrar en el fondo de la denuncia planteada relativa a la falta de medidas de seguridad de los sistemas de videogilancia, manifestando la denunciante que tenía libre acceso a las grabaciones de las cámaras de videovigilancia de ambos centros de trabajo, al igual que el resto de los trabajadores.

A este respecto, solicitada información al respomsable del local de la **(C/...1)**, D. ***A.A.A.***, este manifiesta que al sistema de videovigilancia la única persona que estaba autorizada para acceder a las grabaciones era el administrador de la sociedad y la denunciante, empleada y responsable del negocio en ausencia del administrador, persona de confianza, en el caso de que surgiera un incidente o robo y fuera preciso acceder a ellas por causa justificada. Que nunca se autorizó a otra persona el acceso a las imágenes y no le consta que otros trabajadores hubieran accedido a las mismas.

Adjunta el documento *Protocolo sobre uso de los datos de carácter personal: dirigido a trabajadores y colaboradores de B.B.B. Asociados, S.L.: en el que* se detallan instrucciones sobre el uso de los medios informáticos, la correcta utilización de la información que garantice el deber de secreto y el respeto a la intimidad, y que supuestamente debía ser firmado por el trabajador según consta el pie de la última página. También, se aporta, modelo de *Compromiso de confidencialidad* que debían de suscribir los trabajadores.

Respecto al establecimiento sito en ***(C/...2) de Madrid,*** , cuyo responsable es ***C.C.C.*** manifiesta que al sistema de videovigilancia únicamente están autorizados los

responsables, nunca se autorizó el acceso a la denunciante, que trabajaba únicamente para ***B.B.B. ASOCIADOS, S.L.*** Aporta documento *Protocolo sobre uso de los datos de carácter personal: dirigido a trabajadores y colaboradores de* ***C.C.C.*** , donde se detallan instrucciones sobre el uso de los medios informáticos, la correcta utilización de la información que garantice el deber de secreto y el respeto a la intimidad, que supuestamente debe ser firmado por el trabajador según consta el pie de la última página. También, se aporta, modelo de *Compromiso de confidencialidad* que deben suscribir los trabajadores.

A este respecto el artículo 9 de la Ley Orgánica 15/1999, regula la Seguridad de los datos, concretando lo siguiente:

"1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley".

El citado artículo 9 de la LOPD establece el *"principio de seguridad de los datos"* imponiendo la obligación de adoptar las medidas de índole técnica y organizativa que garanticen aquella, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el *"acceso no autorizado"* por parte de terceros.

El responsable deberá informar a las personas con acceso a los datos sobre sus obligaciones de seguridad y su deber de secreto en los términos del artículo 8 de la Instrucción que recoge: *"El responsable deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado.*

Asimismo cualquier persona que por razón del ejercicio de sus funciones tenga acceso a los datos deberá de observar la debida reserva, confidencialidad y sigilo en relación con las mismas.

El responsable deberá informar a las personas con acceso a los datos del deber de secreto a que se refiere el apartado anterior":

Ahora bien, y para el caso que nos ocupa, hay que tener en cuenta que en el

ámbito administrativo sancionador son de aplicación, con alguna matización pero sin excepciones, los principios inspiradores del orden penal, resultando clara la plena virtualidad del principio de presunción de inocencia.

En tal sentido, el Tribunal Constitucional, en Sentencia 76/1990 considera que el derecho a la presunción de inocencia comporta *"que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas ,libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio"*. De acuerdo con este planteamiento, la hoy vigente Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en su artículo 53 relativo a Derechos del interesado en el procedimiento administrativo, donde en su apartado segundo establece *:"Además de los derechos previstos en el apartado anterior, en el caso de procedimientos administrativos de naturaleza sancionadora, los presuntos responsables tendrán los siguientes derechos: b) A la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario".*

En definitiva, la aplicación del principio de presunción de inocencia impide imputar una infracción administrativa cuando no se hayan obtenido evidencias o indicios de los que se derive la existencia de infracción, como es en el presente caso, donde la denunciante no aporta pruebas fehacientes que avalen sus declaraciones, y las de la Sra. ***F.F.F.***.

A la vista de lo expuesto, en las actuaciones previas de investigación realizadas por los Servicios de Inspección de esta Agencia, no se han obtenido pruebas que corroboren y acrediten que los denunciados han vulnerado la normativa de protección de datos, por lo que procede el archivo del presente expediente de actuaciones previas.

Asimismo debe recordarse a la denunciante que los empleados, incluso los ex–empleados, están obligados al deber de secreto recogido en el artículo 10 de la LOPD, que establece: *"El responsable del fichero y quienes intervengan en cualquier fase deltratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo."*

A su vez, el artículo 44.3.d) de la de la precitada Ley califica como infracción grave *"La vulneración del deber de guardar secreto sobre los datos de carácter personal al que se refiere el artículo 10 de la LOPD."*

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.

NOTIFICAR la presente Resolución a D. **A.A.A., (B.B.B. ASOCIADOS, S.L.),** a Dª. **C.C.C.** y a Dª ***D.D.D. (representada por D. E.E.E.).***

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