



Expediente Nº: E/06984/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **CAL TRAPET SCP** en virtud de denuncia presentada por D^a. **A.A.A.** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fechas 1 y 6 de agosto de 2013 tienen entrada en esta Agencia escritos remitidos por Dña. **A.A.A.** (en adelante la denunciante) comunicando posible infracción a la Ley Orgánica 15/1999 motivada por la existencia de cámaras de videovigilancia en el establecimiento sito en C/ **(C/.....1) (BARCELONA)** y cuyo titular es la mercantil **CAL TRAPET S.C.P** con NIF *****NIF.1**(en adelante la denunciada).

En escrito la denunciante manifiesta el tratamiento y uso de las imágenes, captadas mediante la instalación de un sistema de videocámaras oculto en distintas zonas del establecimiento donde venía prestando sus servicios, las cuales motivan su despido disciplinario de la empresa. Una de las cámaras instaladas se encontraba enfocando hacia el armario ropero donde guardaba el bolso, el cual según la temporada podía ser usado como vestuario.

Se adjunta a la denuncia: (1) copia de la denuncia interpuesta ante los Mossos d'Esquadra con fecha 10 de mayo de 2013, (2) copia del documento de finiquito con fecha de firma 9 de mayo de 2013 y (3) copia de la carta de despido presentada a la denunciante, en la que se hace la siguiente mención expresa: *"... tras tener sospechas de usted ante la falta de productos en el establecimiento...., la Dirección procedió el pasado mes de marzo a realizar una investigación de lo que estaba ocurriendo mediante la instalación de dos cámaras de vídeo ocultas en el mismo, una en la zona de almacén junto a la salida y otra enfocando a donde se encuentra el armario ropero donde guarda su bolso, con el fin de aclarar qué era lo que estaba sucediendo con el material que desaparecía sin explicación alguna...Dichas filmaciones han sido realizadas por personal experto ajeno al establecimiento que nos han sido entregadas junto con un informe explicativo. En la carta de despido hacemos constar a qué cámara corresponde cada filmación...que muestran que usted se ha apropiado indebidamente de productos..."*

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 23 de diciembre de 2013 se solicita información al responsable del sistema, teniendo entrada en esta Agencia escrito de fecha 20 de enero de 2014 en el cual los Administradores mancomunados de la mercantil denunciada, manifiestan:

En relación con la instalación de cámaras de vigilancia en el

establecimiento, cabe distinguir entre:

- o **PROCESO I:** *La instalación de una cámara de vigilancia en la sala de ventas del local, cuyo objeto es evitar hurtos de clientes en dicha sala.*
- o **PROCESO II:** *La instalación de dos cámaras en dos espacios abiertos de paso, realizada por una empresa de detectives a principios del mes de marzo de 2013 durante cinco semanas, cuyo objeto era acreditar judicialmente las irregularidades detectadas de transgresión de la buena fe contractual mediante el hurto de productos del establecimiento por parte de un empleado (en adelante).*

Respecto al **PROCESO I**, informan:

- o *Se solicitaron varios presupuestos a la empresa INSTALACIONES RUFAT S.L, GRUPO SISTEMAS DE SEGURIDAD 8X8, sin monitor, que nos fueron remitidos con fecha 9 de enero de 2013. Finalmente se suscribe un contrato de instalación, con fecha 25 de enero de 2013.*

En documento **Doc.1** se acompañan copias de los mencionados presupuestos y en documento **Doc.2** copia del contrato de instalación, cuyo objeto viene definido, en su cláusula segunda, como: *“la instalación de aparatos, dispositivos o elementos de seguridad (servicio prestado por Seguridad 8X8); mantenimiento de tales instalaciones (servicio prestado por Seguridad 8X8) y conexión a la central receptora de alarmas (servicio prestado por la CRA).*

- o *Con fecha 25 de enero de 2013 se contrata con la empresa SERVICIOS TECNOLÓGICOS IBERCRA S.L el arrendamiento de la central receptora de alarmas.*

Se acompaña copia del contrato de arrendamiento (**Doc.3**).

- o *Adjuntan reportaje fotográfico que acredita la existencia de cartel informativo de zona videovigilada, con la indicación del responsable ante quien poder ejercitar los derechos ARCO, ubicado según se manifiesta en la fachada del establecimiento (**Doc.4**).*

Aportan copia del modelo de cláusula informativa debidamente cumplimentada (**Doc.5.1**).

- o *En documento gráfico **Doc.5.2** se anexan fotografías de la cámara, instalada según se observa en un área interior del local.*

No aportan fotografía del monitor, ya que manifiestan *“no existe monitor en las instalaciones”*.

- o *El trámite de instalación finaliza a finales de mayo de 2013, fecha en la que no existían trabajadores en la empresa, dado que la única trabajadora Dña. **A.A.A.** había sido despedida con fecha 9 de mayo de 2013.*

Se presenta copia de la notificación telemática de fichero de videovigilancia

realizada ante la Agencia Española de Protección de Datos, con fecha 31 de mayo de 2013, (documento **Doc.4.2**).

Respecto al **PROCESO II**, comunican:

- o *Al tratarse de un establecimiento pequeño en el que únicamente en el mes de marzo de 2013, trabajaban los dos titulares y administradores de la empresa y la empleada Dña. **A.A.A.** (en adelante la empleada), ya que la otra trabajadora se encontraba de baja médica, se observó una serie de actuaciones irregulares por parte de la empleada, tales como entradas con productos a un pequeño almacén y salida sin los mismos. Ante tal circunstancia y con la finalidad de esclarecer los hechos, se contactó con la empresa de Detectives INDAGA XXXXX (en adelante la empresa de detectives), la cual procedió a instalar dos cámaras ocultas de mínimo tamaño orientadas: hacia un armario sin llave situado en un pasillo de acceso al único cuarto de baño del establecimiento, en el que la empleada venía dejando el bolso y el abrigo; y hacia un pequeño almacén situado junto a la puerta de salida de los empleados.*

El sistema de cámaras estuvo grabando durante el período de tiempo comprendido desde el 14 de marzo al 9 de abril de 2013, exactamente durante cinco semanas.

- o En documento **Doc.5.3** se adjunta:
 - (1) Certificación de la empresa de detectives en base a la prestación del servicio contratado por la mercantil denunciada, con fecha 10 de marzo de 2013, para la instalación de un sistema de videovigilancia sin monitor con la finalidad de investigar posibles hurtos en el establecimiento. En dicho escrito se manifiesta: “...que la instalación se desmontó en su totalidad el día 10 de abril de 2013...se visualizan las imágenes y se seleccionan los clips en los que se aprecia claramente el robo de productos por parte de la trabajadora...Se elaboró un informe por parte de esta agencia, donde se adjuntan las instantáneas de las grabaciones y los vídeos ya editados...”
 - (2) Copia de la notificación de la inscripción del fichero denominado INFORMES en el que figura como responsable D. **B.B.B.** en calidad de detective privado de la empresa **INDAGA XXXXX**.

Asimismo aporta copia del informe de las actuaciones realizadas por la empresa de detectives que contiene la grabación de las imágenes efectuada (Doc.6).

- o En relación al proceso de despido disciplinario de la empleada, incorporan la siguiente documentación acreditativa:

- Copia de la carta de despido (Doc.7), de fecha 9 de mayo de 2013, en la cual se describe el procedimiento llevado a cabo en la investigación de hurtos en el establecimiento.
 - Copias de las declaraciones (Doc.8) realizadas por los titulares de la empresa, con fechas 15 de mayo de 2013, ante los Mossos d'Esquadra y en base a los hechos descritos.
 - Manuscrito de la empleada, en el que reconoce los hechos que se le imputan en la carta de despido (Doc.9).
 - Copia de la demanda judicial por despido (Doc.10) interpuesta por la empleada ante el Juzgado de lo Social de Terrassa con fecha 19 de junio de 2013; actualmente pendiente de celebración en vista oral y en la cual según manifiestan *"...aportarán las imágenes grabadas por la empresa de detectives"*.
2. Con fecha 20 de marzo de 2014, tiene entrada en esta Agencia escrito remitido por los administradores mancomunados de la entidad denunciada en el que comunican :
- Que la trabajadora ha desistido de la demanda por despido. Adjuntan fotocopia del Acta de conciliación de fecha 10 de marzo de 2014 del Juzgado Social 1 de Terrassa.
 - Que el Juzgado de Instrucción 2 de Terrassa ha sobreseído provisionalmente la denuncia que la trabajadora realizó contra la empresa por la instalación de las cámaras, revelación de secretos y coacciones. Adjunta fotocopia del Auto de fecha 21 de febrero de 2014.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director 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

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 lo 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.” (el subrayado es de la Agencia Española de Protección de Datos).

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 caso que nos ocupa es necesario distinguir el sistema de videovigilancia que ha sido instalado en la entidad denunciada con posterioridad a la denuncia efectuada por la denunciante; de la instalación efectuada por una empresa de detectives que es la que ha dado lugar a la denuncia efectuada.

En primer lugar, respecto a la instalación por parte de la empresa de detectives **INDAGA XXXXX**, de dos cámaras ocultas por encargo de la entidad denunciada con el fin de esclarecer la falta de productos que se venían produciendo y aportar por parte de



la entidad denunciada las grabaciones si fueran necesarias a un procedimiento judicial, hemos de estudiar las implicaciones que lo denunciado presenta al respecto del derecho a la protección de datos en relación con el derecho a la tutela judicial efectiva de los protagonistas, por lo que partiremos de un análisis general relativo a la conexión de dichos derechos. Así, al respecto del derecho a la tutela judicial efectiva, nuestra norma suprema en el artículo 24 de la Constitución Española, en sus apartados 1 y 2, dispone lo siguiente:

“1. Todas las personas tienen derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que en ningún caso, pueda producirse indefensión.

2. Asimismo, todos tienen derecho a utilizar los medios de prueba pertinentes para su defensa.”

Así, constitucionalmente se consagra el derecho de los ciudadanos, ya sean personas físicas o jurídicas, a la tutela judicial efectiva y al derecho a utilizar los medios de prueba que consideren adecuados para el sostenimiento de su pretensión. Sin embargo, de dicha previsión, surge una colisión entre el derecho a la protección de datos de carácter personal y el derecho a la tutela judicial efectiva de los jueces y tribunales referida, contenido en el artículo 24 de la Constitución, anteriormente transcrito, dadas a los bienes jurídicos afectados en su aplicación.

Por ello, ante tales situaciones, el Legislador ha creado un sistema en que el derecho a la protección de datos de carácter personal cede en aquellos supuestos en que el propio Legislador (constitucional u ordinario) haya considerado la existencia de motivos razonados y fundados que justifiquen la necesidad del tratamiento de los datos, incorporando dichos supuestos a normas de, al menos, el mismo rango que la que regula la materia protegida.

En efecto, la exigibilidad del consentimiento del titular de los datos que pudieran ser objeto de un tratamiento en un procedimiento judicial, para dicho tratamiento de sus datos supondría dejar a disposición de aquél el almacenamiento de la información necesaria para que una persona pueda ejercer, en plenitud, su derecho a la tutela judicial efectiva. Así, la falta de estos datos o la dependencia en su aplicación a quien manejara la titularidad del dato, implicaría, lógicamente, una merma en la posibilidad de aportación por el interesado de “los medios de prueba pertinentes para su defensa”, vulnerándose otra de las garantías derivadas del citado derecho a la tutela efectiva y coartándose la posibilidad de obtener el pleno desenvolvimiento de este derecho.

Tal y como sostiene reiterada jurisprudencia del Tribunal Constitucional (por todas, STC 186/2000, de 10 de julio, con cita de otras muchas) *“el derecho a la intimidad no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto,*

proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho".

Por otro lado, junto a lo dispuesto en el artículo 6.2 de la LOPD, el artículo 11 de la LOPD, recoge otras excepciones, a la exigencia del consentimiento:

"1.- Los datos de carácter personal objeto de tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2.-El consentimiento exigido en el apartado anterior no será preciso:

a.-Cuando la cesión esté autorizada en una ley.(...)

d.-Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas.(...)"(el subrayado es de la Agencia Española de Protección de Datos).

En este sentido, entraría en liza lo dispuesto en el artículo 299 de la Ley 1/2000, de 7 de enero de Enjuiciamiento Civil, que admite la aportación como medio de prueba, de medios de reproducción de imágenes que sean relevantes para el proceso. Así establece, el precitado artículo:

"1. Los medios de prueba de que se podrá hacer uso en juicio son:

1. Interrogatorio de las partes.
2. Documentos públicos.
3. Documentos privados.
4. Dictamen de peritos.
5. Reconocimiento judicial.
6. Interrogatorio de testigos.

2. También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso..

3. Cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias".

Por lo tanto, en cuanto a lo aportado en un juicio, dicho cuerpo legal admite la aportación como medio de prueba de los medios de reproducción de la palabra, el sonido y la imagen, lo cual implica la posibilidad de tratamiento de datos dentro de dichas propuestas de prueba, debiendo ser el correspondiente órgano jurisdiccional quien se manifestara sobre la legitimidad de lo presentado. Además, hemos de tener en cuenta que, la Audiencia Nacional en sentencia de 22 de octubre de 2010 (rec. 409/2009) nos dice, en cuanto a la obtención de medios probatorios y su validez en el procedimiento, pese a no ser solicitadas ni obtenidas por vía judicial, lo siguiente:

“De un lado ha de tenerse en cuenta que una de las causas que excluye la necesidad de consentimiento para la cesión de datos personales es que la comunicación que deba efectuarse tenga por destinatarios a los Jueces o Tribunales (Art. 11.2.d) LOPD).

Excepción en la que no es descabellado incluir aquellos supuestos en que se trata de pruebas que, si bien inicialmente no han sido solicitadas por el Juez o Tribunal, sino aportadas por las partes, con posterioridad no consta que las mismas hayan sido rechazadas, sino incorporada por el Juez a las actuaciones, tal y como, parecer ser, y así se desprende del acta de juicio, ocurrió en el presente supuesto.

Por otra parte, y si bien es cierto que los procedimientos judiciales tampoco son ajenos a la normativa de protección de datos, tal y como indicamos en la SAN 9-10-2009 (Rec. 37/2009) dado que el derecho de protección de datos, en cuanto derecho fundamental y autónomo previsto en el artículo 18.4 CE , vincula a todos los poderes públicos (Art. 53 CE) y entre ellos al Poder Judicial, tal y como igualmente indica la STS 18-9-2006 Rec. 274/2002 . Sin embargo dicha LOPD debe ser aplicada con gran cautela, y en la medida en que resulte compatible con las funciones propias (jurisdiccionales y no jurisdiccionales) de los referidos órganos judiciales, pues la singularidad de la actividad jurisdiccional y los intereses que en ella subyacen, exigen en ocasiones una limitación o modulación de los derechos y garantías de los ciudadanos.

Además de que el sometimiento de los ficheros judiciales a la LOPD ha de entenderse (según la misma SAN 9-10-2009 Rec. 37/2009) sin menoscabo de la función jurisdiccional y, por tanto, atinente a lo que debe considerarse como "aspecto accesorio" o administrativo de la función jurisdiccional, centrándonos concretamente en el procedimiento judicial, existen también en él una serie de intereses y garantías que ostentan un trascendente valor en dicho proceso, tales como el del verdadero esclarecimiento de los hechos o el legítimo ejercicio del derecho de defensa de las partes, que han de ser ponderados en aquellos casos en que dichos intereses y garantías confluyen con el derecho contemplado en el artículo 18.4 CE , hasta el punto de que pueden llegar a implicar una importante limitación de tal derecho de protección de datos personales.”

Así las cosas, debiera ser el órgano judicial correspondiente quien se manifestara sobre la legitimidad de la prueba aportada, no constando pronunciamiento en este sentido, por lo que no cabría inicio de actuaciones encaminadas a la apertura de un

procedimiento administrativo del tipo sancionador en materia de protección de datos de carácter personal.

III

Una vez analizado las cuestiones relativas a la posible aportación de las grabaciones a un procedimiento judicial, debemos entrar en el análisis de las captaciones realizadas por la Agencia de detectives de la persona de la denunciante.

En cuanto a la legitimación de la actuación llevada por la correspondiente Agencia de Detectives, en su procedimiento de investigación con la finalidad de acreditar la autoría de la desaparición de productos, como regla general, la ley 23/1992, de 30 de julio, de Seguridad Privada, en su redacción dada por el Real Decreto-Ley 2/1999, de 29 de enero y por la Ley 14/2000, de 29 de diciembre, ha dado carta de naturaleza a la actividad realizada por las empresas de seguridad privada, del tipo de detectives privados, por lo que no estaríamos ante una actuación ilegítima, aún más si tenemos en cuenta lo establecido en el artículo 19 .1 de dicha ley 23/1992, que nos dice:

‘Artículo 19

- 1. Los detectives privados, a solicitud de personas físicas o jurídicas, se encargarán:*
 - a) De obtener y aportar información y pruebas sobre conductas o hechos privados.*
 - b) De la investigación de delitos perseguibles sólo a instancia de parte por encargo de los legitimados en el proceso penal.*
 - c) De la vigilancia en ferias, hoteles, exposiciones o ámbitos análogos.*
- 2. Salvo lo dispuesto en el párrafo c) del apartado anterior, no podrán prestar servicios propios de las empresas de seguridad ni ejercer funciones atribuidas al personal a que se refieren las Secciones anteriores del presente Capítulo.*
- 3. Tampoco podrán realizar investigaciones sobre delitos perseguibles de oficio, debiendo denunciar inmediatamente ante la autoridad competente cualquier hecho de esta naturaleza que llegara a su conocimiento y poniendo a su disposición toda la información y los instrumentos que pudieran haber obtenido.*
- 4. En ningún caso podrán utilizar para sus investigaciones medios materiales o técnicos que atenten contra el derecho al honor, a la intimidad personal o familiar o a la propia imagen o al secreto de las comunicaciones.*

De la citada norma, se desprende que los detectives privados se encuentran habilitados por Ley para obtener información de personas, siempre que no se utilicen

para ello *“medios materiales o técnicos que atenten contra el derecho al honor, la intimidad personal o familiar”*. En el caso en que el denunciante interpretara que las actuaciones realizadas al respecto atentaron contra sus derechos, de la forma enumerada en el artículo 23.c de la ley 23/1992 visto, debe señalarse que no corresponde a la Agencia Española de Protección de Datos dirimir si se ha utilizado medios ilícitos en la obtención del informe, al estar fuera de su ámbito competencial, por lo que en tal caso, habría de acudir a los órganos jurisdiccionales competentes para dirimir dicha cuestión.

Asimismo la Ley de Enjuiciamiento Civil en sus artículos 335 y 336 se refiere a los *“dictámenes de perito”*, recogiendo éste último lo siguiente:

“Aportación con la demanda y la contestación de dictámenes elaborados por peritos designados por la partes: 1. Los dictámenes de que los litigantes dispongan, elaborados por peritos por ellos designados, y que estimen necesarios o convenientes para la defensa de sus derechos, habrán de aportarlos con la demanda o con la contestación...,”

La Sentencia de la Audiencia Nacional de 19/10/2005, recurso nº 1139/2003, en su Fundamento de Derecho tercero, es del tenor siguiente: *“Asimismo, la comunicación realizada por .. a su abogado y al perito imparcial se haya autorizada por la Ley de Protección de Datos a tenor del artículo 11.2 de la misma, al ser preceptiva la intervención de abogado y procurador en el procedimiento judicial, y dado que el artículo 335 de la Ley de Enjuiciamiento Civil exige que los dictámenes periciales se acompañen con la demanda. Además tal comunicación tendría igualmente amparo en el artículo 12 de la LOPD que permite el acceso y comunicación de datos para la prestación de un servicio al responsable del tratamiento”*.

Por otro lado sobre el ámbito de consideración de si los datos obtenidos por las grabaciones incluidas en el procedimiento se consideran adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas y explícitas para la que fueron obtenidos, hemos de tener en cuenta que el objetivo de la grabación no es otro que el de constituir un elemento probatorio para acreditar las actuaciones irregulares que se venían produciendo. De conformidad con la doctrina del Tribunal Constitucional, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan, basta recordar que (como sintetizan las SSTC 66/1995, de 8 de mayo [RTC 1995\66], F.5; 55/1996, de 28 de marzo [RTC 1996\55], FF. 6, 7, 8 y 9; 207/1996, de 16 de diciembre [RTC1996\207], F.4.e) y 37/1998, de 17 de febrero [RTC 1998\37], F.8) para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es

ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

En primer lugar, debemos analizar si la medida adoptada es adecuada y, en efecto, concluimos que así era pues su objetivo no era otro que acreditar las desviaciones de productos que se venían produciendo; resultaba idónea y necesaria ya que se trataba de recabar exclusivamente pruebas a los efectos de los eventuales conflictos que se pudieran sustanciar y es equilibrada pues la grabación se limita a determinadas zonas limitadas y durante un periodo corto de tiempo.

A este respecto, la denunciada manifiesta que una de las cámaras ocultas estaba instalada en la zona donde se encuentra el armario ropero donde guardaba su bolso la denunciante, si bien según manifiesta ésta, también lo utilizaba de vestuario, lo que supondría una vulneración a su intimidad y honor. A este respecto, cabe decir que el citado armario ropero estaba situado en un pasillo de acceso al único cuarto de baño del establecimiento, sin que se haya aportado prueba alguna que acredite que dicha zona se tratase de un vestidor propiamente dicho, ni que se desarrollaran en él actividades privadas como las llevadas a cabo en una zona de dicha naturaleza.

IV

Una vez, desarrollado en los Fundamentos de Derecho anteriores, el objeto principal de la denuncia, debemos entrar a analizar el sistema de videovigilancia instalado en fecha posterior al despido de la denunciante, consistente en una cámara en la sala de ventas del local cuyo objetivo es evitar hurtos de clientes.

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, se ha aportado por parte de la entidad denunciada, fotografías de la existencia de cartel informativo de la existencia de la cámara, ubicado en la fachada del establecimiento, con la indicación del responsable ante quien ejercer los derechos ARCO. Asimismo se aporta modelo de cláusula informativa a disposición de los clientes, de conformidad con el artículo 3.b) de la citada Instrucción

Por lo tanto la citada entidad, cumple el deber de información, en cuanto al sistema de videovigilancia, recogido en el artículo 5 de la LOPD, anteriormente transcrito.

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, consta la existencia de dos ficheros inscritos, en el Registro General de la Agencia Española de Protección de Datos, denominados “VIDEOVIGILANCIA”, cuyo responsable es **CAL TRAPET S.C.P.**

De conformidad con lo expuesto se procede al archivo del presente expediente de actuaciones previas, al no apreciarse vulneración a la actual normativa en materia de protección de datos.

Por lo tanto, de acuerdo con lo señalado,

Por el Director de la Agencia Española de Protección de Datos,

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a **CAL TRAPET SCP** y a D^a. **A.A.A.**.

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 el Director 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.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos