

Expediente Nº: E/04860/2015

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **CENTRE MEDIC DE PREVENCIO, DIAGNOSTIC I TRACTAMENT, S.L.P.**, en virtud de denuncia presentada por D^a. **B.B.B.** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha de 25 de junio de 2015 tiene entrada en esta Agencia un escrito de D^a. **B.B.B.** en el que declara que a principios de 2015 tuvo conocimiento de la instalación de cámaras de video vigilancia en el Centre Medic de Prevencio, Diagnostic i tractament S.L.P., concretamente en la recepción, lugar de paso y sala de espera de los pacientes.

No se informa a los trabajadores ni pacientes de la existencia de las cámaras.

Las fotografías aportadas por la reclamante son de una única cámara que parece estar desconectada.

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:

A mediados de 2014, comenzaron a desaparecer fichas de pacientes de Oftalmología; estos expedientes se encuentran en un archivo de acceso restringido a las Secretarías del centro -que son las personas que se encargan de preparar las fichas de los pacientes que van a ser visitados, y facilitarlos al Médico en cuestión-, así como de los Doctores. Las secretarías solicitaron que se activara una cámara en el archivo, para saber el motivo de dichas desapariciones, ya que las mismas entorpecían su trabajo y creaban una situación insostenible en el Centro.

Prevía información a las Secretarías, se conectó una única cámara de forma temporal, que enfocaba únicamente a la zona donde sólo se visualiza el archivo de las fichas de los pacientes en el archivo con acceso restringido.

A juicio de los responsables de la clínica, era una medida justificada, idónea para la finalidad pretendida (verificar por qué desaparecían fichas de pacientes); necesaria (ya que la grabación serviría de prueba de tales irregularidades); y equilibrada (pues la grabación de imágenes se limitó a la zona del archivo de acceso restringido y a una duración temporal limitada).

De las imágenes obtenidas se observa que una Doctora del centro está cogiendo fichas del Servicio de Oftalmología, las destruye y las guarda en su bolsillo de la bata. Una vez visualizadas estas imágenes, se desconectó esta cámara y se procedió a interponer denuncia ante la Comisaría de los Mossos d'Esquadra, entregándoles a los mismos un CD con dichas grabaciones.

Esta denuncia fue proveída y tramitada ante el Juzgado de Instrucción;

inicialmente lo calificaron como faltas, pero Su Señoría convirtió la falta como un delito por destrucción de documentos y se señaló juicio de lo penal. La prueba del CD fue admitida a trámite como prueba en el procedimiento penal.

Actualmente la cámara se encuentra apagada y sin equipo de grabación, estando a la espera de instalar un sistema compatible para ser conectado con centralita de alarmas y adecuado a la normativa vigente de Protección de Datos.

Aportan copia de la notificación de inscripción ante el Registro General de Protección de Datos de un fichero de videovigilancia con fecha de alta 18/02/2016

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

En primer lugar procede situar el contexto normativo en materia de videovigilancia. 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 Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por 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.

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."

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.

De acuerdo con los preceptos transcritos, la cámara reproduce la imagen de los afectados por este tipo de tratamientos y, a efectos de la LOPD, la imagen de una persona constituye un dato de carácter personal, toda vez que la información que capta concierne a personas que las hacen identificadas o identificables y suministra información sobre la imagen personal de éstas, el lugar de su captación y la actividad desarrollada por el individuo al que la imagen se refiere.

III

En el presente expediente se denuncia por parte de D^a. **B.B.B.** la instalación de cámaras de videovigilancia en el Centre Medic de Prevencio, Diagnostic i tractament S.L.P., donde la denunciante presta sus servicios, concretamente en la recepción, lugar de paso y sala de espera de los pacientes, sin informar ni a trabajadores ni pacientes de la existencia de las cámaras.

En primer lugar, se plantea por el denunciante el incumplimiento del deber de información a los trabajadores de la existencia de las citadas cámaras de videovigilancia.

Ahora bien, en esta cuestión, en primer lugar se plantea si es necesario el consentimiento inequívoco de los trabajadores cuando se instalan cámaras de videovigilancia en el centro de trabajo, al amparo del artículo 6.1 de la LOPD.

A este respecto es necesario realizar varias aclaraciones respecto al consentimiento en el ámbito laboral. Así, el consentimiento, elemento base en el tratamiento de los datos, entraña cierta complejidad, especialmente cuando nos referimos al ámbito laboral, dado que resulta de difícil cumplimiento que en ese ámbito concurren los requisitos legalmente previstos para considerar que se ha obtenido libremente el consentimiento. El artículo 3 h) de la LOPD lo define como *“Toda manifestación de voluntad libre, inequívoca, específica e informada mediante la que el interesado consienta el tratamiento de datos personales que el conciernen”*.

Del concepto de consentimiento se desprende la necesaria concurrencia para que el mismo pueda ser considerado conforme a derecho de los cuatro requisitos enumerados en dicho precepto. Un adecuado análisis del concepto exigirá poner de manifiesto cuál es la interpretación que ha de darse a estas cuatro notas características del consentimiento, tal y como la misma ha indicado en numerosas Resoluciones de la AEPD, siguiendo a tal efecto los criterios sentados en las diversas recomendaciones emitidas por el Comité de Ministros del Consejo de Europa en relación con la materia que nos ocupa. A la luz de dichas recomendaciones, el consentimiento habrá de ser:

a) Libre, lo que supone que el mismo deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil.

b) Específico, es decir referido a un determinado tratamiento o serie de

tratamientos concretos y en el ámbito de las finalidades determinadas, explícitas y legítimas del responsable del tratamiento, tal y como impone el artículo 4.2 de la LOPD.

c) Informado, es decir que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce. Precisamente por ello el artículo 5.1 de la LOPD impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen.

d) Inequívoco, lo que implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado (consentimiento presunto), siendo preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento.

La concurrencia de estos requisitos resulta de difícil cumplimiento en el ámbito laboral. En consecuencia, vista la dificultad que entraña obtener el consentimiento, la Agencia Española de Protección de Datos, ha entendido que lo procedente es acudir a las normas que legitimen el tratamiento de los datos. Por tanto, en el ámbito laboral, el Ordenamiento Jurídico Español, regula en el Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo de 24 de Octubre de 1995, los poderes de Dirección del empresario y es en éste articulado donde hallamos la oportuna legitimación.

El artículo 20.3 del Estatuto de los Trabajadores (ET) dispone que *“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”*.

De todo ello se desprende que el empresario, en este caso la entidad denunciada, está legitimada para tratar las imágenes de los trabajadores en el ámbito laboral, al amparo del artículo 20.3 del ET. Ahora bien, esta legitimación no es absoluta y exige por parte del empresario la obligación de informar de dicho tratamiento a los trabajadores(cumpliendo así con el deber de informar previsto tanto en el artículo 10 de la Directiva 95/46/CE como en el artículo 5 de la LOPD).

Es necesario en este punto diferenciar si la instalación de la cámara en el centro de trabajo es como medida de vigilancia y control del empresario, para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales o si es una medida de seguridad para proteger la instalación y sus empleados.

En el primer caso, es decir cuando el objetivo de la instalación de las cámaras va dirigido al cumplimiento por los trabajadores de sus deberes laborales, sería necesario por parte del empresario, garantizar el derecho de información en la recogida de las imágenes, mediante información a los trabajadores del alcance específico que se va a dar a las mismas para el control laboral, como establece la Sentencia del Tribunal Constitucional 29/2013, de 11 de febrero de 2013, debe ir precedido de *“una información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida”*.

En el segundo caso, es decir cuando la finalidad es de vigilancia y protección de las instalaciones y personal de la empresa, es necesario el cumplimiento de la LOPD, el Reglamento de Desarrollo de la LOPD y la Instrucción 1/2006. Por lo tanto, debería cumplirse, entre otros, el deber de información recogido en el artículo 5 de la LOPD,

disponiendo de distintivos informativos de zona de videovigilancia acordes a la Instrucción 1/2006 e impresos informativos.

A este respecto, la entidad denunciada manifiesta que a mediados de 2014, comenzaron a desaparecer fichas de pacientes de oftalmología; estos expedientes se encuentran en un archivo de acceso restringido a las Secretarías del centro -que son las personas que se encargan de preparar las fichas de los pacientes que van a ser visitados, y facilitarlos al Médico en cuestión-, así como de los Doctores. Las secretarías solicitaron que se activara una cámara en el archivo, para saber el motivo de dichas desapariciones, ya que las mismas entorpecían su trabajo y creaban una situación insostenible en el Centro.

Prevía información a las Secretarías, se conectó una única cámara de forma temporal, que enfocaba únicamente a la zona donde sólo se visualiza el archivo de las fichas de los pacientes en el archivo con acceso restringido. La grabación se limitaba por tanto, a la zona del archivo de acceso restringido.

De las imágenes obtenidas se observó que una Doctora del centro estaba cogiendo fichas del Servicio de oftalmología, las destruía y las guardaba en su bolsillo de la bata. Una vez visualizadas estas imágenes, se desconectó esta cámara y se procedió a interponer denuncia ante la Comisaría de los Mossos d'Esquadra, entregándoles a los mismos un CD con dichas grabaciones.

Según manifiesta la entidad denunciada, esta denuncia fue tramitada ante el Juzgado de Instrucción; inicialmente lo calificaron como faltas, pero Su Señoría convirtió la falta como un delito por destrucción de documentos y se señaló juicio de lo penal. La prueba del CD fue admitida a trámite como prueba en el procedimiento penal.

En el presente caso, las sentencias que se han venido pronunciando en este tipo de casos (cámaras de videovigilancia en centros de trabajo) lo han hecho de forma radicalmente distinta dependiendo de si se trata de cámaras permanentes y visibles (que además de cumplir con los requisitos de la LOPD y de la Instrucción 1/2006, requerirá comunicación previa sobre el uso y finalidad a los trabajadores); de si se trata de cámaras ocultas que debían ser limitadas a un corto espacio temporal y la mayor prevalencia del derecho a la tutela judicial efectiva debía ser justificado con el consiguiente juicio de idoneidad, necesidad y proporcionalidad.

A este respecto, en lo que respecta al control laboral por parte de cámaras fijas está la [Sentencia 29/2013 del Tribunal Constitucional de 11 de febrero](#), **que declaró nulo un despido disciplinario utilizando como prueba imágenes de cámaras instaladas, a priori, con finalidad de seguridad y no de control laboral**; y en esa misma línea, resolvió el Tribunal Supremo en la Sentencia 2618/2014 de 13 de mayo de 2014 al declarar igualmente nulo el despido de una cajera de supermercado basado en imágenes captadas por las cámaras ubicadas en el mismo, que probaban que la cajera, en beneficio de un cliente, no pasaba todos los productos por el lector de la caja.

Por otra parte, en cuanto a las sentencias dictadas respecto a cámaras no permanentes sino instaladas “ad hoc” para descubrir determinados sucesos acaecidos tenemos, la Sentencia 186/2000 del Tribunal Constitucional de 10 de julio en la que se desestima el recurso de amparo de un trabajador que fue captado por cámaras instaladas al efecto en el economato de su empresa como consecuencia de diversos descuadres ocurridos, e igualmente la [Sentencia 84/2015 del Tribunal Superior de](#)

[Justicia de Madrid de 9 de febrero de 2015](#), que desestima el recurso de suplicación interpuesto contra la sentencia del juzgado de lo Social número 2 de Madrid que declaró procedente el despido del trabajador, considerando que se trata de una grabación episódica y de breve duración al existir sospechas fundadas de que la falta de prendas y otros objetos del establecimiento mercantil obedecía a su sustracción por algún trabajador.

Esta última sentencia ha establecido su pronunciamiento respecto a las cámaras temporales resolviendo en su texto las diferencias existentes entre las sentencias del TC y TS.

El TSJ de Madrid entiende que al tratarse de cámaras temporales, *"el presente supuesto tiene mayor conexión con el resuelto en la STC 186/00 que con los examinados en la STC 29/13 y en la STS 13-5-14 rec. 1685/2013"*, por lo que entraría en juego el artículo 18.1 CE (al tratarse de una grabación episódica) y no el 18.4 CE (al tratarse de una grabación con carácter preventiva). Recuerda el TSJM que *"En el supuesto de la STC 186/00 también se trata de la instalación ocasional y temporal de una cámara de grabación en el puesto de trabajo - las cajas registradoras - tras acreditadas sospechas razonables de incumplimientos contractuales que fueron acreditados de esta manera"*. Existen en ambos casos ilícitos laborales previos cuya averiguación es necesaria para cortar de raíz estas prácticas y sancionar a los culpables.

Al tratarse por ello de un supuesto episódico y de corta duración entiende el TSJM que *"sería absurdo exigir a la empresa una comunicación a los trabajadores de la instalación de unas cámaras de grabación advirtiéndoles "en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo", así como la colocación de carteles de publicidad ,pues de esta forma se arruinaría con toda seguridad la finalidad buscada"*.

Además entiende el TSJM que el derecho del trabajador a ser informado conforme al 18.4 CE tiene que ser ponderado con el derecho al empresario a la tutela judicial efectiva del 24.1 CE entendiendo que *"La actuación de la empresa en este caso en cuanto medida restrictiva de un derecho fundamental, el del art. 18.4 de la Constitución , supera el juicio de proporcionalidad, pues cumple los tres requisitos o condiciones siguientes (STC 186/00): 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 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). La idoneidad no es cuestionable pues la grabación demostró en el juicio la conducta del trabajador que se le atribuía en la carta de despido e hizo posible la extinción del contrato de trabajo mediante despido disciplinario procedente por haber incurrido en un comportamiento muy grave. La necesidad es negada por el recurrente aduciendo que podría haberse utilizado un registro, pero no explica por qué un registro en la persona del trabajador es menos invasivo que una grabación de imágenes, aparte de que esta medida de control es menos idónea, ya que si resulta fallido un primer registro es claro que el trabajador culpable ya queda alertado. Y en cuanto a la proporcionalidad en sentido estricto el interés general de evitar la impunidad de conductas como la sancionada resulta superior*

al leve menoscabo relativo al tratamiento de datos, sobre todo teniendo en cuenta que las imágenes ni siquiera fueron tomadas por la demandada sino por una empresa del sector de vigilancia, se informó previamente al presidente del comité de empresa y no consta que hayan sido utilizadas para otra finalidad que su presentación en juicio".

El presente caso, la instalación de la cámara respondió a la continua desaparición de fichas de pacientes, de un archivo de acceso restringido a las secretarías del centro y a los doctores. Con el conocimiento e información a dichas secretarías se procedió a instalar una única cámara puntual que enfocaba únicamente a la zona donde se encontraba el citado archivo. Por lo tanto las grabaciones, objeto de denuncia, no proceden de un sistema de videovigilancia instalado permanente y previamente (como en las sentencias 29/2013 ni 2618/2014 citadas) a que ocurrieran los sucesos que dieron lugar a la instalación de la citada cámara, sino que la cámara, en el presente caso, se instaló de forma puntual para descubrir lo que estaba ocurriendo con la desaparición de las fichas de pacientes y una vez obtenidas las pruebas se desconectó la cámara entregándose las grabaciones a los Mossos d'e Esquadra y dando lugar esta denuncia a su tramitación en la correspondiente sede judicial, por lo que se entiende en base a las sentencias descritas, legítima la actuación de la entidad denunciada.

IV

A este respecto, 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.”

En el caso que nos ocupa, la prueba obtenida con la cámara se aporta junto a denuncia a los Mossos dando lugar, según manifiesta la entidad al inicio de procedimiento judicial.

Así, la entidad denunciada estaba legitimada para presentar, ante el Juzgado la citada prueba videográfica, al existir una habilitación legal para ello, a tenor del artículo 11.2.d). Así la aportación de la prueba videográfica, tuvo como finalidad la defensa de los derechos e intereses legítimos de la denunciada.

A este respecto, se debe traer a colocación la Sentencia del TS67/2014 de 28 enero, que recoge *“la STS 485/2013, de 5 de junio, considera que el material fotográfico y videográfico obtenido en el ámbito público y sin intromisión indebida en la intimidad personal o familiar tiene un valor probatorio innegable. La doctrina jurisprudencial de esta Sala en sentencias de 6 de mayo de 1993, 7 de febrero, 6 de abril, 31 de mayo de 1994, 18 de diciembre de 1995, 27 de febrero de 1996, 5 de mayo de 1997, 968/1998 de 17 de julio, 188/1999, de 15 de febrero, 1207/1999, de 23 de julio, 387/2001, de 13 de marzo, 27 de septiembre de 2002, 180/2012 de 14 de marzo, entre otras muchas) ha considerado legítima y no vulneradora de derechos fundamentales los espacios o vías públicas, estimando que la captación de imágenes de actividades que pueden ser constitutivas de acciones delictivas se encuentra autorizada por la ley en el curso de una investigación criminal, siempre que se limiten la grabación de lo que ocurre en espacios públicos fuera del recinto inviolable del domicilio o de lugares específicos donde tiene lugar el ejercicio de la intimidad. (...).*

Así las cosas, es el órgano judicial correspondiente quien se debe manifestar sobre la legitimidad de la prueba aportada, y en el caso que nos ocupa no consta pronunciamiento en contra en este sentido.

V

Por último, respecto al artículo 4 de la LOPD, los datos obtenidos se consideran adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas y explícitas para la que fueron obtenidos, no siendo otro su objetivo que el constituir un elemento probatorio en un procedimiento judicial.

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, cabe decir que en el presente caso, la medida adoptada era idónea para la finalidad pretendida que no era otra que descubrir cómo estaban desapareciendo las fichas de pacientes; era necesaria, dado que la grabación serviría de prueba de tales irregularidades; y equilibrada, pues la grabación de imágenes se limitó a la zona del archivo de acceso restringido y a un intervalo de tiempo limitado.

De conformidad con la normativa expuesta, la captación de imágenes a través de videocámaras constituye un tratamiento de datos personales. Sin embargo, en el supuesto que nos ocupa, la captación de las imágenes objeto de denuncia, fueron utilizadas como medio de prueba en un procedimiento judicial, y cumpliendo los requisitos de finalidad y proporcionalidad exigidos por la normativa en materia de protección de datos y jurisprudencia existente al respecto, por lo que se procede al a archivo del presente expediente de actuaciones previas.

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 **CENTRE MEDIC DE PREVENCIO, DIAGNOSTIC I TRACTAMENT, S.L.P..** y a D^a. **B.B.B..**

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

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.



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