

Expediente Nº: E/04173/2017

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **CUALTIS, S.L.** en virtud de sentencia remitida por el **JUZGADO DE LO SOCIAL Nº X.X.** y teniendo como base los siguientes

HECHOS

PRIMERO: Fecha de entrada de la denuncia: 2 de junio de 2017

Denunciante: **JUZGADO DE LO SOCIAL Nº X.X.**

En sentencia *****SENTENCIA.1**, sobre despido, se acuerda remitir copia de dicha sentencia a la Agencia Española de Protección de Datos.

Denunciado: **CUALTIS, S.L.U.**

Por los siguientes hechos según manifestaciones del denunciante: Captación de imágenes de terceros sin consentimiento

Que según el denunciante tuvieron lugar a fecha de: Entre el 15 de mayo de 2016 y el 13 de julio de 2016

Y anexa la siguiente documentación:

*Copia de la Sentencia *****SENTENCIA.1** del Juzgado de los Social Nº X.X.de Madrid*

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:

Con fecha 14 de julio de 2017 y número de salida 207239/2017 se solicita información a la sociedad investigada teniendo entrada en esta Agencia con fecha 2 de agosto de 2017 y número de registro 258039/2017 escrito del investigado en el que manifiesta:

1. El Responsable del sistema de videovigilancia es la sociedad CUALTIS S.L.U.
2. La instalación de las cámaras que conforman el sistema de videovigilancia la realizó la empresa PROYECTA TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN, S.L., la cual ha suscrito dos contratos con la sociedad investigada: uno de ellos para la instalación y mantenimiento del sistema de videovigilancia de las instalaciones, compuesto por 26 cámaras, y que regula la relación entre las partes desde la perspectiva de protección de datos, teniendo la empresa instaladora consideración de encargado del tratamiento, y un segundo contrato en el que se le encarga a PROYECTA la instalación y posterior desinstalación de dos cámaras

ocultas en el período comprendido entre el 15 de mayo de 2016 y el 15 de julio de 2016, sin acceso, en este caso, a los datos registrados por las cámaras por parte del instalador.

3. Respecto de la finalidad por la cual se han instalado las cámaras, el denunciado indica que el sistema de videovigilancia integrado por las 26 cámaras instaladas inicialmente tiene por finalidad comprobar el estado de las instalaciones y los bienes de la empresa así como el control de accesos.

En lo que respecta a las dos cámaras ocultas a las que alude la Sentencia ***SENTENCIA.1 e instaladas de forma temporal en el periodo comprendido entre el 15 de mayo de 2016 y el 13 de julio de 2016, el investigado manifiesta que se instalaron con el objetivo de investigar ilícitos que se estaban cometiendo en las instalaciones de la sociedad, esclarecer los hechos e identificar a los posibles responsables de los mismos. Los hechos consistían en la desaparición continuada de unas tarjetas precargadas con un importe monetario que se facilitaban a los trabajadores de las empresas clientes de la sociedad investigada tanto para controlar la entrada y salida a las instalaciones como para que estos pudieran adquirir productos de las máquinas de vending ubicadas en la planta 1 y 2 del edificio. La utilización de estas tarjetas, según indica el investigado, es exclusivo de clientes y está prohibido su uso a los trabajadores de la sociedad; se entregan al visitante al acceder al edificio y se recogen cuando la persona abandona las instalaciones. Mediante la instalación de las cámaras ocultas, el investigado manifiesta que se pretendía averiguar si la desaparición de las tarjetas estaba fundamentada en un uso defraudatorio e irregular de las mismas por parte de los empleados o por el contrario se había producido una vulneración de los controles de seguridad en la entrada y salida del edificio. Para justificar este modo de proceder, el investigado alega la aplicación de la doctrina y jurisprudencia de la STC 186/2000, entre otras, que establece, en el punto 7 de los Fundamentos jurídicos

“Pues bien, del razonamiento contenido en las Sentencias recurridas se desprende que, en el caso que nos ocupa, la medida de instalación de un circuito cerrado de televisión que controlaba la zona donde el demandante de amparo desempeñaba su actividad laboral era una medida justificada (ya que existían razonables sospechas de la comisión por parte del recurrente de graves irregularidades en su puesto de trabajo); idónea para la finalidad pretendida por la empresa (verificar si el trabajador cometía efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias correspondientes); necesaria (ya que la grabación serviría de prueba de tales irregularidades); y equilibrada (pues la grabación de imágenes se limitó a la zona de la caja y a una duración temporal limitada, la suficiente para comprobar que no se trataba de un hecho aislado o de una confusión, sino de una conducta ilícita reiterada), por lo que debe descartarse que se haya producido lesión alguna del derecho a la intimidad personal consagrado en el art. 18.1 CE.”

4. En relación con la información facilitada sobre la existencia de cámaras, el investigado manifiesta que existen varios carteles que señalizan la existencia de las mismas y que responden al modelo de cartel de zona videovigilada. En ellos se identifica al responsable del sistema y se indica la dirección dónde ejercitar los derechos ARCO. También facilita copia del formulario informativo al que se refiere la instrucción 1/2006 de la Agencia indicando que los interesados pueden solicitarlo en la recepción del edificio. Los carteles están situados en la entrada a los ascensores de las

dos plantas sótano del parking, a la entrada del edificio por la planta baja, en la recepción principal, en la recepción de las plantas 1ª y 2ª, en las que se desarrollan los reconocimientos médicos y están ubicadas las máquinas expendedoras utilizadas por los trabajadores de las empresas clientes de la sociedad, así como en la planta 4ª destinada a la Dirección. En la planta 3ª, donde se encuentra la sala de descanso del personal propio de la empresa, no existe señalización al no existir tampoco cámaras instaladas.

5. En relación a los lugares en los que se encuentran ubicadas las cámaras de videovigilancia del sistema general empleado para garantizar la seguridad de las instalaciones, la sociedad investigada aporta plano de situación en el que se marca el emplazamiento concreto de las cámaras así como fotografía de todas y cada una de ellas y muestra de la imagen capturada. Asimismo manifiesta que ninguna de las cámaras, ni las de la instalación general ni las cámaras ocultas instaladas de forma temporal, disponen de zoom ni de posibilidad de movimiento. Las 26 cámaras están distribuidas por todo el edificio (dos plantas de sótano, planta baja, primera, segunda y cuarta planta) con la excepción indicada anteriormente de la tercera planta. De las 26 cámaras, 23 son interiores y por su ubicación y enfoque captan imágenes de las plazas de garaje, la rampa de acceso al mismo, las zonas de recepción, de acceso a los ascensores, tránsito por los pasillos, salas de espera y algunas zonas de la planta de dirección. Las tres instaladas en el exterior captan imágenes del aparcamiento descubierto, la zona de Unidades Móviles y de un pasillo externo perimetral al edificio.

Las dos cámaras ocultas, ya desinstaladas, a las que se refiere la citada Sentencia, estaban instaladas en el área de descanso de las plantas 1ª y 2ª, enfocando a las máquinas de vending en las que las personas que asistían a realizarse el reconocimiento médico en ayunas podían, tras este, adquirir bebidas y alimentos con las tarjetas facilitadas a la entrada, captando ambas cámaras imágenes globales de dichas áreas de descanso.

6. En lo que respecta al sistema de monitorización, el investigado manifiesta que la visualización de las imágenes registradas se realiza a través de una aplicación web a la que sólo accede la persona encargada de la gestión y control de los sistemas de información, estando protegido el acceso a esta aplicación mediante usuario y contraseña. Asimismo manifiesta que, sin perjuicio de lo anterior, las imágenes registradas por la cámara que enfoca la rampa de acceso al garaje también pueden verse en un monitor instalado en la recepción principal del edificio y de acceso exclusivo al personal habilitado en este puesto, con el objetivo de poder detectar y solucionar cualquier incidencia que se produzca en la entrada y salida de vehículos a través de esta rampa. En relación a la visualización de las imágenes registradas por las cámaras ocultas, el investigado refiere que, a efectos de garantizar al máximo los derechos de las personas implicadas en las grabaciones, la seguridad, la viabilidad probatoria y la legitimidad de las pruebas, se definió un protocolo en base al cual las imágenes se registraban en un espacio protegido del servidor de la sociedad, sin posibilidad de acceso por parte de terceros hasta la desinstalación de las cámaras; siendo visionadas las grabaciones ante notario y depositando el

disco duro notarialmente para garantizar la custodia de las pruebas obtenidas hasta la terminación del procedimiento que pudiera incoarse contra los empleados responsables de los ilícitos esclarecidos.

7. El sistema de videovigilancia general integrado por las 26 cámaras instaladas en el edificio de la sociedad están configuradas para activar la grabación por detección de movimiento, variando la duración de cada grabación individual. No obstante, el investigado refiere que, en todo caso, las grabaciones registradas se cancelan en el plazo de un mes computado desde su captación. Aporta código de inscripción del fichero en el Registro General de Protección de Datos con número *****COD.1**, comprobándose, tal y como figura en Diligencia incorporada a las actuaciones de inspección, que este se corresponde con el fichero "Videovigilancia".
8. Respecto a posibles cámaras ubicadas en el exterior el investigado refiere que no existen cámaras exteriores que tomen imágenes de la vía pública. Del análisis de la información facilitada como respuesta al requerimiento practicado por esta Agencia, se constata que, las tres cámaras instaladas en el exterior del edificio de la sociedad están enfocadas al aparcamiento exterior y sólo una de ellas, la que enfoca el pasillo exterior perimetral al edificio registra, a lo lejos, la imagen de un edificio situado enfrente de las instalaciones de la sociedad.

La sociedad manifiesta que, no conforme con la sentencia recaída, ha presentado recurso de súplica ante la Sala de lo Social del Tribunal Superior de Justicia de la Comunidad de Madrid. Con fecha 6 de septiembre de 2017 y número de salida *****SALIDA.1** se solicita a la sociedad investigada que aporte copia del Recurso de Suplicación presentado así como copia de la sentencia que, en su caso, se haya dictado. Con fecha 19 de septiembre de 2017 y número de registro *****REGISTRO.1** se recibe copia del referido Recurso así como los justificantes de presentación y admisión, refiriendo la sociedad que está pendiente de que recaiga Sentencia relativa al mismo. Asimismo solicitan, tal y como queda incorporado al expediente mediante Diligencia, que se garantice el derecho de la tutela judicial efectiva en relación a toda la información aportada, dado que hay un expediente judicial en curso.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

El artículo 126.1, apartado segundo, 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 (RLOPD) 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.”

III

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.

IV

En el presente expediente el **JUZGADO DE LO SOCIAL Nº X.X.** de Madrid remite sentencia *****SENTENCIA.1**, de fecha 23 de mayo 2017, sobre captación de imágenes de terceros sin consentimiento realizado por la entidad CUALTIS, S.L. con el sistema de videovigilancia instalado en la misma, por si vulnerase la normativa de protección de datos.

De la sentencia aportada y de las manifestaciones realizadas por la entidad denunciada, a requerimiento de esta Agencia, se desprende que la dos cámaras ocultas instaladas de forma temporal en el periodo comprendido entre el 15 de mayo de 2016 y el 13 de julio de 2016, tenían el objetivo de investigar ilícitos que se estaban cometiendo en las instalaciones de la sociedad, esclarecer los hechos e identificar a los posibles responsables de los mismos. Los hechos consistían en la desaparición continuada de unas tarjetas precargadas con un importe monetario que se facilitaban a los trabajadores de las empresas clientes de la sociedad investigada tanto para controlar la entrada y salida a las instalaciones como para que estos pudieran adquirir productos de las máquinas de vending ubicadas en la planta 1 y 2 del edificio. La utilización de estas tarjetas, según indica el investigado, es exclusivo de clientes y está prohibido su uso a los trabajadores de la sociedad; se entregan al visitante al acceder al edificio y se recogen cuando la persona abandona las instalaciones. Mediante la instalación de las cámaras ocultas, el investigado manifiesta que se pretendía averiguar si la desaparición de las tarjetas estaba fundamentada en un uso defraudatorio e irregular de las mismas por parte de los empleados o por el contrario se había producido una vulneración de los controles de seguridad en la entrada y salida del edificio.

La sentencia *****SENTENCIA.1** recoge en su Fundamento de Derecho II que: (...) *“En reciente sentencia de 1 de febrero de 2017, RJ 2017/2015, se aborda la cuestión recordando que conforme al TC no se vulnera el derecho a la protección de datos en el ámbito de la relación laboral aunque no se contara con el consentimiento individual del trabajador o que el mismo no hubiera sido expresamente informado de la utilización con finalidad disciplinaria quedando cumplida esa obligación con la colocación de distintivos avisando de la existencia de los dispositivos que registran imágenes o sonido. El consentimiento del afectado salvo cuando se trata de fines ajenos al contrato de trabajo se entiende implícito.*

La duda surge respecto a la existencia de cámaras ocultas en las áreas donde se utilizaban y consumían los productos de las máquinas expendedoras (destinadas a los clientes o usuarios) no existiendo advertencia en esos recintos y sin que tampoco conste el consentimiento de los terceros cuyas imágenes han sido registradas que al menos han sido visualizadas por las personas responsables del protocolo y que se mantienen en un disco duro así como una copia en la notaría con expresa (...).

Puede considerarse en relación al demandante que los avisos que todos los testigos coinciden pueden visualizarse en las zonas de aparcamiento y en la entrada y salida principal (no hay coincidencia sobre si se ubicaban en todas las plantas) y aunque no los hubiera donde se instalaron las cámaras ocultas, sirve a los efectos señalados por el TC pero surge incidencia con la falta de consentimiento de terceros, respecto a las que se ha grabado sin advertencia expresa en una zona de acceso restringido sin su consentimiento y con mantenimiento de esos ficheros”.

Por lo tanto, la sentencia establece que no es necesario el consentimiento del

trabajador para la adopción de una medida de control de la actividad laboral, dada la existencia de relación laboral entre las partes, y que existían distintivos informativos de la existencia de un sistema de videovigilancia.

En relación a esta cuestión, existen al respecto, sentencias dictadas respecto a cámaras no permanentes sino instaladas “ad hoc”, como es el caso que nos ocupa, como 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.

El TSJ en su Sentencia 84/2015 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 era necesaria.

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".

Más recientemente la Sentencia del TC 39/2016, de 3 de marzo, dictada con relación a un conflicto entre el uso de cámaras ocultas y los derechos de los trabajadores, ha dado un giro a los criterios y efectos de la sentencia del TC 29/2013. La sentencia TC 39/2016 tiene origen en el despido de una trabajadora por apropiarse de dinero de caja del comercio en que prestaba sus servicios, conducta captada con cámaras instaladas ocultas por la empresa, no habiendo comunicado a los trabajadores dicha instalación pero sí habiéndose colocado en el escaparate del establecimiento, en lugar visible, el distintivo informativo de que el centro estaba vigilado. En esta sentencia se recoge: "(...) Se ha cumplido en este caso con la obligación de información previa pues basta a estos efectos con el cumplimiento de los requisitos estos efectos con el cumplimiento de los requisitos específicos de información a través del distintivo de acuerdo con la Instrucción 1/2006. El trabajador conocía que en la empresa se había instalado un sistema de control por videovigilancia, sin que haya que especificar, más allá de la mera vigilancia, la finalidad exacta que se le ha asignado a ese control. Lo importante será determinar si el dato obtenido se ha utilizado para la finalidad de control de la relación laboral o para una finalidad ajena al cumplimiento del contrato, porque sólo si la finalidad del tratamiento de datos no guarda relación directa con el mantenimiento, desarrollo o control de la relación contractual el empresario está obligado a solicitar el consentimiento de los trabajadores afectados. (...)

En consecuencia, teniendo la trabajadora información previa de la instalación de la cámaras de videovigilancia, a través del correspondiente distintivo informativo, y habiendo sido tratadas las imágenes captadas para el control de la relación laboral, no puede entenderse vulnerado el artículo 18.4 CE."

En consecuencia esta sentencia del TC estima que no se ha violado el derecho de protección de datos porque, dada la existencia de relación laboral entre las partes, no era preciso el consentimiento individual de los trabajadores, ni el colectivo, para la adopción de una medida de control de la actividad laboral y que la obligación de informar previamente del dispositivo instalado quedaba cumplida con la colocación del correspondiente distintivo avisando de su existencia, razón por la que acaba concluyendo que el proceder de la empresa supera el juicio de proporcionalidad.

La doctrina de esta sentencia ya la ha aplicado la Sala IV del Tribunal Supremo en sentencia de 7 de julio de 2016 (R. 3233/2010) en la que el Tribunal declara la validez de una prueba videográfica que motivó el despido disciplinario de una trabajadora, que había sido grabada hurtando productos de la empresa. Pues bien, el Tribunal declara la validez de la prueba utilizada, y concluye que en este caso existió un uso apropiado de la videovigilancia implantada, por los siguientes motivos: existían carteles que anunciaban la existencia de cámaras de videovigilancia; La trabajadora conocía en qué

lugar se encontraban; Las cámaras estaban instaladas en zonas comunes de trabajo; la grabación de conductas tuvo como detonante las múltiples pérdidas sufridas por la empresa. Por todo ello, el TS considera que la medida adoptada por la empresa superó el juicio de proporcionalidad, al ser idónea, necesaria y equilibrada.

Ahora bien, la cuestión que se plantea en la sentencia *****SENTENCIA.1**, según recoge: *“Respecto a los terceros no se puede entender implícito el consentimiento por el hecho de la advertencia de acceder a zona videovigilada”*, por lo que se remite a esta Agencia la sentencia por si fuera constitutiva de vulneración de la normativa de protección de datos.

A este respecto, según consta en la propia sentencia, la citada entidad dispone de carteles informativos de la existencia de las cámaras, ubicados al menos en las zonas de aparcamiento y en la entrada y salida principal, (no existiendo coincidencia sobre si se ubicaban en todas las plantas,) pero no en la zona donde se encontraban las cámaras ocultas donde se utilizaban y consumían los productos de las máquinas expendedoras (destinadas a los clientes o usuarios).

A este respecto, se puede afirmar, tal y como tiene sentado consolidada jurisprudencia del Tribunal Supremo - por todas las Sentencias de 8 de febrero de 1.964, 26 de mayo de 1.986 y 11 de junio de 1.991 - en interpretación del artículo 1.253 del Código Civil, que existen tres modos o formas básicas del consentimiento: expreso, manifestado mediante un acto positivo y declarativo de la voluntad; tácito, cuando pudiendo manifestar un acto de voluntad contrario, éste no se lleva a cabo, es decir, cuando el silencio se presume o se presupone como un acto de aquiescencia o aceptación; y presunto, que no se deduce ni de una declaración ni de un acto de silencio positivo, sino de un comportamiento o conducta que implica aceptación de un determinado compromiso u obligación. A efectos de la Ley Orgánica 15/1999 y con carácter general, son admisibles las dos primeras formas de prestar el consentimiento.

En este sentido la Sentencia de la Audiencia Nacional de 21 de noviembre de 2007 (Rec 356/2006) en su Fundamento de Derecho Quinto señala que: *“ por lo demás, en cuanto a los requisitos del consentimiento, debemos señalar que estos se agotan en la necesidad de que este sea “inequívoco”, es decir, que no exista duda alguna sobre la prestación de dicho consentimiento, de manera que en esta materia el legislador, mediante el artículo 6.1 de la LO de tanta cita, acude a un criterio sustantivo, esto es, nos indica que cualquiera que sea ,la forma que revista el consentimiento éste ha de aparecer como evidente, inequívoco – que no admite duda o equivocación- , pues éste y no otro es el significado del adjetivo utilizado para calificar al consentimiento.”*

En el presente caso, los terceros (clientes) que acceden a la entidad denunciada, prestan su consentimiento tácito a ser captados o grabados por el sistema de videovigilancia instalado, al acceder a la entidad, siendo debidamente informados de la existencia del sistema mediante los carteles informativos que están instalados al menos, en las zonas de aparcamiento y en la entrada y salida principal, según sentencia. Dichos carteles, según documentación aportada por la entidad CUALTIS, son acordes al establecido en el artículo 3 a) de la Instrucción 1/2006. Aportando CUALTIS fotografías

de su ubicación en zona ascensores parking-1 y -2; en planta baja entrada; en planta 1ª (recepción); en planta 2ª (recepción) y en 4ª planta. Asimismo, se han aportado al expediente, por la citada entidad, los impresos informativos a disposición de los interesados de conformidad con el artículo 3 b) de la citada Instrucción.

Así, 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 cuanto a la ubicación del cartel informativo, no es necesario que se coloque debajo de cada cámara, siendo suficiente conforme a lo dispuesto en el artículo 3 a) de la Instrucción 1/2006, *“Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados”*

Por lo tanto, la entidad denunciada cumple con el deber de información recogido en el artículo 3.a) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD, informando tanto a las personas que acceden a las instalaciones de la entidad como a sus trabajadores de la existencia y finalidad del sistema de videovigilancia instalado.

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 inscripción en el Registro General de la Agencia Española de Protección de Datos, por parte de la entidad denunciada, del fichero denominado “VIDEOVIGILANCIA”, cuyo responsable es CLOQUER, S.A.

Por último, 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 inscripción en el Registro General de la Agencia Española de Protección de Datos, del fichero denominado “VIDEOVIGILANCIA”, cuyo responsable es CUALTIS, S.L.U., con fecha inicial el 21/05/2007 y modificado el 22/01/2015.

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 **CUALTIS, S.L.** y **JUZGADO DE LO SOCIAL Nº X.X..**

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.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la citada LJCA, sólo podrá interponer directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la LJCA, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

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