



Expediente Nº: E/02119/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **EISMANN S.A** en virtud de denuncia presentada por D. **A.A.A. Y OTROS**, y por D^a. **B.B.B.** teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 18 de marzo de 2014, y 7 de abril de 2014 tiene entrada en esta Agencia sendos escritos remitidos por la Autoridad Catalana de Protección de Datos, de D. **A.A.A.**, D. **C.C.C.**, D^a. **D.D.D.** y D. **E.E.E.** y de D^a. **B.B.B.** respectivamente (en adelante los denunciantes) comunicando posible infracción a la Ley Orgánica 15/1999 motivada por seguimientos realizadas a sus personas con cámaras por Agencia de detectives para sustentar despidos disciplinarios realizados por la entidad **EISMANN S.A** (en adelante el denunciado) ubicada en **(C/.....1) - BARCELONA**.

D^a. **B.B.B.**, se reitera en los hechos relatados por los primeros denunciantes.

Con fecha 8 y 21 de abril de 2014 se solicita, respectivamente, a los denunciantes D. **A.A.A.** y D^a. **B.B.B.** acreditar el sistema de videovigilancia utilizado para sustentar el despido disciplinario.

Con fecha 22 de abril de 2014 tiene entrada en esta Agencia escrito firmado por D. **A.A.A.** en el que manifiesta desconocer el sistema de videovigilancia utilizado, si bien aporta, copia de expedientes de despido de D^a **D.D.D.** referido a seguimientos realizados en fechas de 28 de junio y 1 y 2 de julio de 2013, de D. **E.E.E.** referido a seguimientos realizados en fechas 25, 26, 27 de septiembre de 2013, de D. **A.A.A.**, de seguimientos realizados en fechas 16, 17, 18, 19 de julio de 2013 y demanda de impugnación de carta de despido disciplinario realizada por D. **C.C.C.**, formulada ante el Juzgado de los Social en Barcelona.

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 13 de mayo, 25 de junio y 27 de julio de 2014 se solicita información a la entidad denunciada **EISMANN, S.A.**, sobre el sistema de videovigilancia teniendo entrada en esta Agencia con fecha 28 de mayo, 9 de julio y 28 de julio de 2014 escritos de la denunciada en los que manifiesta:

*El responsable del sistema es **EISMANN, S.A.**, domiciliada en*

(C/.....1) DE BARCELONA.

*La empresa que realizó la instalación de las alarmas y que se encarga del servicio de vigilancia es la empresa **CHUBB PARSİ S.L. ((C/.....2)-BARCELONA)**, inscrita en el Registro de empresas de seguridad en la Dirección General de la Policía con el número **3016** como empresa de seguridad privada para las actividades de instalación y mantenimiento de aparatos, dispositivos, sistemas de seguridad y explotación de central de alarmas.*

Se adjunta contrato de prestación de servicios con la empresa de seguridad, acreditación por el Ministerio del Interior como empresa de seguridad y notificación de la instalación a la autoridad competente y copia del contrato de acceso a datos personales por cuenta de terceros.

Las causas que han motivado la instalación de las alarmas son proporcionar protección frente a intrusiones, robos o atracos en nuestras oficinas, con la finalidad de que la empresa de seguridad, una vez conectado el sistema de seguridad pueda recibir la señal de activación de alarma, para que ésta ponga en marcha los mecanismos establecidos, y si es de robo o atraco avisar a la policía.

Adjuntan copia del cartel informativo de zona videovigilada con indicación del responsable del fichero **EİSMANN, S.A.**

Aportan copia de formulario informativo con indicación de que el destinatario de los datos personales es la empresa de seguridad **CHUBB PARSİ S.L.** y que se pueden ejercitar los derechos ARCO ante el responsable del fichero **EİSMANN, S.A.**

Respecto de los lugares donde se encuentran ubicadas las cámaras de videovigilancia:

- o *Las oficinas constan de dos dependencias separadas, en una se encuentran las “oficinas” y en la otra se encuentra la “cocina - office”. Las alarmas con cámara se encuentran situadas en la entrada de cada una de las dependencias enfocando a la puerta.*
- o *El sistema de alarmas disponen de dos detectores de infrarrojos con cámara que solo se activa al saltar la alarma por intrusión. No dispone de zoom, ni posibilidad de movimiento.*
- o *Aportan croquis de los lugares donde se ubican las cámaras citadas y fotos de las cámaras e imagen captada del interior de la empresa.*

Respecto de la información facilitada a terceros sobre la existencia de monitores que permitan visualizar las imágenes captadas por las videocámaras, manifiestan que:

- o *El sistema de alarma no dispone de monitores desde donde se*

puedan visualizar las imágenes. Las imágenes son visualizadas exclusivamente por la empresa de seguridad en la central de alarmas, con la particularidad de que la cámara se activa solamente cuando salta la alarma. Es simplemente un sistema de detección de intrusión que realiza una filmación de 10 segundos al saltar la alarma.

- o *El sistema no permite la visualización ni la “inspección” remota fuera del estado de alarma, por lo que es técnicamente imposible que el sistema de alarmas haya servido como base para el seguimiento ni para el despido de ningún trabajador.*
- o *Únicamente tiene acceso a las imágenes la empresa de seguridad **CHUBB PARSI S.L.**, que controla la central receptora de alarmas.*
- o *Adjuntan contrato de prestación de servicios con esta empresa como encargado del tratamiento.*

Respecto del procedimiento empleado para informar a los trabajadores de la finalidad por la cual se han instalado cámaras de videovigilancia

- o *Al tratarse de un sistema de alarma de detección de intrusos, se informó a cada responsable de área sobre el uso y la instalación de la alarma, y para que advirtiera a las personas de su departamento de la activación de las alarmas fuera del horario de trabajo. Se adjunta documento.*

Respecto a las imágenes se adjunta *copia extracto del documento de seguridad* Estos documentos se encuentran firmados por todos y cada uno de los empleados, para que conozcan sus funciones y obligaciones respecto a la LOPD.

- o *En el citado documento figura un fichero de videovigilancia con nº ***CÓD.1 junto con la copia de la solicitud de inscripción del fichero.*

Por una diligencia se ha comprobado que en el Registro de la Agencia figura un fichero denominado **VIDEOVIGILANCIA** inscrito con el código nº ***CÓD.2, cuyo responsable es **EISMANN S.A.**

Respecto del método empleado para realizar el seguimiento de los trabajadores, objeto de denuncia del presente expediente:

- o *El seguimiento lo realizó la Agencia de Detectives WINTERMAN SOLVIMAR, S.L.P. habilitada por la DGP para obtener información y pruebas sobre conductas enmarcadas en el ámbito laboral.*

Aportan copia del contrato de acceso a datos personales por cuenta de terceros por parte de la Agencia de Detectives.

- o *El encargo se limitó exclusivamente a la obtención de información y*

pruebas sobre el desempeño de la actividad de los empleados: C.C.C., D.D.D., A.A.A., E.E.E., durante su jornada laboral

- o *Las investigaciones fueron encargadas en base a la relación contractual con los investigados, siendo necesaria la información que se pretendía recabar para el mantenimiento de los contratos concertados con ellos, de conformidad con lo previsto en el apartado f) del número 1 del artículo 2 de la Ley 8/1 980, de 10 de marzo, del Estatuto de los Trabajadores y el RD 1438/1985, de 1 de agosto, por el que se regula la relación laboral de carácter especial de las personas que intervengan en operaciones mercantiles por cuenta de un empresario, sin asumir el riesgo y ventura de aquéllas.*
- o *La conducta de los mencionados empleados provocaba un perjuicio importante para EISMANN, por la merma importante en las contrataciones manteniendo sus zonas sin actividad, no sólo por la no contratación de nuevos clientes, sino por la paralización de la actividad de los clientes recurrentes, con el consiguiente coste añadido para **EISMANN** de la cotización por estos empleados en el Régimen General Colectivo de Representantes de Comercio (TC1/3).*
- o *Las imágenes se tomaron con la finalidad de aportarlas como prueba en los consiguientes procedimientos de despido. Se aportan cuatro DVD y un CD con las grabaciones.*

D.D.D. — Procedimiento de despido ******/2013** - Juzgado Social 21 de Barcelona

E.E.E. — Procedimiento de despido *****1/2013**- Juzgado Social 16 de Barcelona

C.C.C. — Procedimiento de despido *****2/2013** Secc. D- Juzgado Social 28 de Barcelona.

A.A.A. - Procedimiento de despido *****3/2013**- Juzgado Social 21 de Barcelona

B.B.B.

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

En el presente expediente, se denuncia la captación de la imagen de los denunciados, mediante cámaras, por una Agencia de detectives contratada por la entidad denunciada **EISMANN S.A.** con la finalidad de aportarlas como prueba en los consiguientes procedimientos de despido de los denunciados.

A la solicitud de información realizada por la Inspección de datos de esta Agencia, a la entidad denunciada, ésta expone la existencia de un sistema de videovigilancia en el interior de la entidad denunciada cuya finalidad es la protección frente a intrusiones, robos o atracos, contratado con una empresa de seguridad. El sistema de alarma dispone de detectores de infrarrojos con cámara que se activa al saltar la alarma por intrusión, transmitiendo la imagen a la empresa de seguridad contratada al efecto. El sistema no permite la visualización ni la “inspección” remota fuera del estado de alarma, por lo que es técnicamente imposible que el sistema de alarmas haya servido como base para el seguimiento ni para el despido de ningún trabajador. Únicamente tiene acceso a las imágenes la empresa de seguridad CHUBB PARISI S.L., que controla la central receptora de alarmas.

Por tanto, en primer lugar debe clarificarse que las cámaras con las que se realizan las captaciones de los denunciados, no es una instalación de seguridad propiamente dicha, sino un seguimiento temporal con cámaras encomendada por la entidad denunciada a una Agencia de detectives, para obtener información y pruebas sobre el desempeño de la actividad de los empleados denunciados durante su jornada laboral. Por lo tanto las grabaciones fueron efectuadas por la Agencia de detectives por encargo de la entidad denunciada para comprobar el cumplimiento de sus tareas profesionales.

Así, la captación de imágenes con fines de control laboral, a través de un sistema de videovigilancia propiamente dicho, se encuentra condicionada a una información precisa según la Sentencia del Tribunal Constitucional de fecha 29 de enero de 2013: *“No contrarresta esa conclusión que existieran distintivos anunciando la instalación de cámaras y captación de imágenes en el recinto universitario, ni que se hubiera notificado la creación del fichero a la Agencia Española de Protección de Datos; era necesaria además la 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. Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, 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 (...).”*

A este respecto, debe señalarse que las imágenes se tomaron con la finalidad de aportarlas como prueba en los consiguientes procedimientos de despido contra los denunciados, siendo aportadas por tanto en el seno de un procedimiento judicial. Por tanto, 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, será el órgano judicial correspondiente quien se manifestará sobre la legitimidad de la prueba aportada, por lo que cualquier resolución por parte de esta Agencia al contexto de un procedimiento sancionador supondría una predeterminación indebida de una resolución jurisdiccional.

A la vista de lo expuesto se procede al archivo del presente expediente de actuaciones previas.

Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a **EISMANN S.A** y a D. **A.A.A. Y OTROS** 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 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