



Procedimiento N°: A/00156/2016

RESOLUCIÓN: R/00871/2016

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **HIPER USERA, S.L.** con CIF n°: **B*******, en virtud de denuncia presentada por D^a **A.A.A.**, y de conformidad con lo establecido en el artículo 45.6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha de 18 de mayo de 2015 tiene entrada en esta Agencia escrito de D^a **A.A.A.** (en adelante la denunciante), comunicando una posible infracción a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), motivada por la existencia de un sistema de videovigilancia en las sedes de **HIPER USERA, S.L.** (en adelante el denunciado) situadas en el **Centro Comercial Las Acacias en la Avenida Principal, s/n, Polígono Las Acacias, Cubas de la Sagra (Madrid)**. La denunciante señala que las imágenes grabadas por el sistema de videovigilancia han sido utilizadas para el control de los trabajadores.

La denunciante manifiesta que HIPER USERA donde trabaja, presentó en el Juzgado de lo Social nº 14 de Madrid, procedimiento ****/2014, un CD con imágenes cedido por el local colindante AQUALUNA PERFUMERIAS para sancionarla. El día 31 de octubre de 2013 se encontraba en la zona de perfumería (Perfumería Aqualuna) junto al supermercado (Hiper Usera) sustituyendo a una compañera, cuando se produjo un robo que quedó grabado en las cámaras de seguridad, el fallo estima la demanda contra HIPER USERA revocando íntegramente la sanción impuesta a la denunciante.

Adjunta: copia de DNI, demanda de la denunciante a HIPER USERA presentada en el Juzgado de lo Social de Madrid el 24/01/2014, denuncia en la Inspección de Trabajo de 17/12/2013, comunicación de la Inspección a la empresa de 6/5/2015, solicitud de 5 y 15/5/2015 de la denunciante a AQUALUNA del CD de la grabación, respuesta de HIPER USERA de 8/5/2015 informando que la única copia del CD de la grabación es la aportada al procedimiento ****/2014 del Juzgado de lo Social nº 14 de Madrid.

Se solicita a la denunciante fotografías de las cámaras de la empresa denunciada y soporte informático de las grabaciones realizadas y con fecha 30 de julio tiene entrada en esta Agencia reportaje fotográfico de las cámaras y copia de sentencia nº ****/15 del Juzgado de lo Social nº 14 de Madrid de 7/5/2015 de la demanda de la denunciante a HIPER USERA donde prestaba sus servicios como cajera.

SEGUNDO: Con fecha 7 de septiembre de 2015 por los Servicios de Inspección de esta Agencia, se solicita información del sistema de videovigilancia denunciado a HIPER USERA y AQUALUNA, siendo esta última carta devuelta por el Servicio de Correos con la indicación “Desconocido”, y teniendo entrada en esta Agencia con fecha 24 de septiembre escrito del representante legal de HIPER USERA en el que pone de manifiesto lo siguiente:

- El responsable de la instalación es **HIPER USERA S.L.**, con CIF nº: **B*******.
- La instalación del sistema de videovigilancia situado en el Centro Comercial Las Acacias, en la (C/.....1) (Madrid) fue realizada por DIGITAL CCTV Control System, S.L. el 15 de diciembre de 2005, posteriormente se ha firmado contrato de mantenimiento de dicho sistema con la mercantil HELFEN SYSTEM S.L.
 - Se aporta copia de los Contratos suscritos entre DIGITAL CCTV Control System, S.L. e HIPER USERA S.L. como documentos núm. 1 y 2.
 - Se aporta copia del Contrato suscrito entre HELFEN SYSTEM S.L. e HIPER USERA S.L. como documento núm. 3.
- Por razones de seguridad de las instalaciones frente a actuaciones dolosas o mal intencionadas de terceros ajenos a HIPER USERA se adoptó la decisión de la instalación de un sistema de videovigilancia en sus instalaciones del Centro Comercial Las Acacias.
- Se adjunta como documentos núm. 4 y 5 fotografía de los carteles informativos de la existencia de cámaras de videovigilancia en los que consta la identificación de HIPER USERA S.L. como responsable del tratamiento, con indicación de la dirección del responsable y la posibilidad de ejercicio de los derechos de acceso, rectificación, cancelación y oposición. **Hay carteles expuestos en el supermercado Hiper Usera y en el local de Perfumerías Aqualuna, en ambos casos se identifica como responsable a la entidad Hiper Usera, S.L.**
- Se adjunta como documento núm. 6 copia del documento realizado por HIPER USERA S.L. para el cumplimiento del deber de información; documento que se encuentra a disposición de cualquier afectado en las sedes de HIPER USERA y PERPUMERIAS AQUALUNA en el Centro Comercial Las Acacias.
- El sistema de videovigilancia está compuesto de dieciséis cámaras. Aporta un listado con la descripción del tipo de cámaras.
- Se adjunta como documento núm. 7, detalle del número de cámaras y lugares donde se encuentran instaladas en el Centro Comercial Las Acacias, con indicación expresa del tipo de cámara y una captura en pantalla de la imagen captada por cada una de las cámaras instaladas, las cámaras son fijas, realizándose un visionado en tiempo real en aquellos supuestos o situaciones de producirse una acción dolosa o culpable de terceros ajenos a HIPER USERA o bien, un acceso a las imágenes grabadas en caso de solicitud de la autoridad policial competente.

Aporta croquis con la ubicación de las 16 cámaras interiores que se reparten en el espacio del supermercado (dos plantas) y la perfumería Aqualuna (**cámaras 15 y 16**). Las cámaras únicamente captan zonas interiores.

- Se aporta foto del monitor ubicado en el interior de un despacho. En este monitor que se encuentra en las dependencias del supermercado se visionan todas las



cámaras del sistema de videovigilancia, incluidas las cámaras 15 y 16 que se encuentran situadas en el local de Perfumería Aqualuna.

- Se adjunta relación de las personas autorizadas dentro de HIPER USERA con autorización para acceder a las grabaciones de seguridad.
- El sistema de almacenamiento de imágenes es en archivos informáticos, grabándose en discos duros de los servidores de HIPER USERA siendo conservadas las imágenes de grabación por un plazo máximo de 30 días. El acceso a las imágenes se encuentra protegido mediante un código de usuario y una clave asociada al mismo y para su visionado se requiere una herramienta específica.
- Se adjunta como documento núm. 8 copia del procedimiento de información a la denunciante de la existencia y finalidad de las cámaras con el siguiente tenor: *“Asimismo, le informamos que existen cámaras de video vigilancia que graban en las zonas de acceso a los locales, común e interiores con la finalidad de preservar la seguridad de los locales y control de personal.”*
- HIPER USERA, S.L. es responsable del Fichero denominado “Videovigilancia”, inscrito ante el Registro General de Protección de Datos con el código de inscripción núm. ***CÓD.1.

Mediante una diligencia de Inspección se comprueba la inscripción en el Registro General de Protección de Datos de los ficheros:

- VIDEO VIGILANCIA con nº ***CÓD.1 y cuyo responsable es HIPER USERA, S.L. y su finalidad SEGURIDAD Y CONTROL DE ACCESO A EDIFICIOS.
- VIDEO VIGILANCIA con nº ***CÓD.2, cuyo responsable es PERFUMERIA AQUALUNA y su finalidad SEGURIDAD Y CONTROL DE ACCESO A EDIFICIOS.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 37. g) en relación con el artículo 36 de la LOPD.

II

Antes de entrar de lleno en el análisis de la cuestión que aquí nos ocupa, es conveniente hacer hincapié en los requisitos que debe cumplir un sistema de videovigilancia para ser acorde con la normativa de protección de datos. Así pues hay que tener en cuenta lo siguiente:

- Respetar el principio de proporcionalidad.

- Las videocámaras no podrán captar imágenes de las personas que se encuentren fuera del espacio privado ya que el tratamiento de imágenes en lugares públicos sólo puede ser realizado, salvo que concurra autorización gubernativa, por las Fuerzas y Cuerpos de Seguridad.

- Se deberá cumplir el deber de informar a los afectados en el modo previsto en el artículo 3 de la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el Tratamiento de Datos Personales con Fines de Vigilancia a través de Sistemas de Cámaras o Videocámaras (Instrucción 1/2006). En concreto:

“a) Colocar, en las zonas video vigiladas, 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.”

Hay que tener en cuenta que el distintivo del apartado a) debe por un lado avisar de la existencia de una zona videovigilada y por otro debe identificar al responsable del tratamiento o, en caso de grabar imágenes, al responsable del fichero ante el que los interesados podrán ejercitar los derechos de acceso, rectificación, cancelación y oposición reconocidos en la LOPD.

- Salvo en el caso de que el tratamiento consista exclusivamente en la reproducción o emisión de imágenes en tiempo real, cuando se graben imágenes se deberá notificar previamente a esta Agencia la creación del fichero que contenga las imágenes para su inscripción en el Registro General de Protección de Datos.

III

El artículo 3.a) de la LOPD define **datos de carácter personal** como *“cualquier información concerniente a personas físicas identificadas o identificables.”* Se completa dicha definición con lo establecido en el artículo 5.1 f) del Reglamento de desarrollo de la LOPD aprobado por Real Decreto 1720/2007, de 21 diciembre (RLOPD) que señala que son datos de carácter personal *“cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables”*.

El apartado c) del artículo 3 de la LOPD recoge la definición de **tratamiento de datos**, entendiendo por tal *“... 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.”*

Para que un tratamiento de datos de carácter personal sea legítimo deberá contar con el **consentimiento del afectado**, siendo este uno de los principios básicos en la protección de datos de carácter personal, recogido en el artículo 6.1 de la LOPD:

“el tratamiento de los datos de carácter personal requerirá el consentimiento

inequívoco del afectado, salvo que la ley disponga otra cosa.”

Este es el principio que también informa al artículo 11 de la LOPD que regula la **cesión de datos** con el siguiente tenor:

“1. Los datos de carácter personal objeto del 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 está autorizada en una ley.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros.

En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

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. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica...”

En el caso que nos ocupa, la denunciante afirma que ha habido una cesión de datos desde el sistema de videovigilancia de la Perfumería Aqualuna a la entidad Hiper Usera, S.L. sin su consentimiento y que estas imágenes fueron utilizadas por esta última entidad para sancionarla disciplinaria ya que presta sus servicios en Hiper Usera, S.L.

Del análisis de la documentación obrante en el expediente, se desprende que hay un único sistema de videovigilancia cuyo responsable y titular es la entidad Hiper Usera, S.L. Este sistema se compone de 16 cámaras, de las cuales las número 15 y 16 se encuentran instaladas en el local Perfumería Aqualuna. Las imágenes que graban estas cámaras son visualizadas y grabadas directamente por el sistema de Hiper Usera, por lo que esta entidad no tiene necesidad de solicitar las imágenes a Perfumería Aqualuna ya que desde el primer momento las tenía en su poder. De hecho el cartel que hay expuesto en el local de Perfumería Aqualuna que avisa de la existencia de una zona videovigilada identifica como responsable del fichero a la entidad Hiper Usera, S.L. Así pues, no puede afirmarse que se haya dado una cesión de imágenes incontestada por la denunciante, porque la cesión material de las mismas no era posible ya que como se ha indicado las imágenes siempre han estado en poder de la entidad Hiper Usera, S.L. pues se han generado en sus sistema de videovigilancia.

IV

Seguidamente, debe analizarse si la entidad Hiper Usera, S.L. ha vulnerado la LOPD a la hora de utilizar imágenes grabadas en su sistema de videovigilancia para el control laboral y en concreto si ha infringido el artículo 5 de la LOPD que regula el deber de información que compete al responsable del fichero o tratamiento.

El artículo 5 de la LOPD dispone, en su apartado 1, lo siguiente:

“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”.*

La obligación que impone el artículo 5 al responsable del fichero sirve para garantizar el derecho de información en la recogida de datos que reconoce la LOPD a favor del afectado.

El uso de sistemas de videovigilancia en el entorno laboral está amparado por el artículo 20.3 del Estatuto de Trabajadores, cuyo tenor literal expresa:

“3. 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.”

Este artículo permite al empresario la instalación de sistemas de videovigilancia para verificar el cumplimiento por los trabajadores de sus obligaciones y deberes laborales. La grabación y visualización de las imágenes deberán respetar su derecho a la intimidad, quedando limitadas a las finalidades legítimas reconocidas por el Estatuto de los Trabajadores y por la normativa vigente: LOPD e Instrucción 1/2006, debiendo cumplir en este último caso adicionalmente las previsiones específicas que sean de aplicación.

El responsable del fichero deberá garantizar el derecho a la información en la recogida de las imágenes por medio de información específica que deberá ser previa al tratamiento de los datos y tendrá que incluir todos los extremos contenidos en el artículo 5.1 anteriormente expuesto. Cuando la finalidad del sistema de videovigilancia sea no sólo la de conseguir la seguridad en general del establecimiento sino también la de control laboral de los trabajadores, la información del artículo 5.1 de la LOPD deberá

darse a la representación sindical de los trabajadores (en este caso al tratarse de un establecimiento pequeño dicho requisito no se aplicaría), a través de dispositivos informativos (carteles) que avisen de la existencia de una zona videovigilada e identifiquen a los responsables del tratamiento (consta que hay carteles expuestos en ambos locales) y mediante información personalizada a los trabajadores. La entidad Hiper Usera, S.L. ha aportado al procedimiento copia de una carta dirigida a la denunciante fechada el 1 de diciembre de 2011 en la que aparece la firma de la trabajadora y en la que entre otras cosas le informa de “...*que existen cámaras de video vigilancia que graban en las zonas de acceso a los locales, común e interiores con la finalidad de preservar la seguridad de los locales y el control de personal...*”

Así pues, consta que la entidad denunciada ha cumplido con la obligación establecida en el artículo 5 de la LOPD.

V

Teniendo en cuenta lo anterior, cabe señalar que no son necesarias medidas correctoras adicionales por lo que se debe proceder a resolver el **archivo de las actuaciones**, sin practicar apercibimiento o requerimiento alguno a la entidad denunciada, en aplicación del artículo 45.6 de la LOPD, atendida su interpretación sistemática y teleológica.

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 la entidad **HIPER USERA, S.L.**
3. **NOTIFICAR** la presente Resolución a D^a **A.A.A.**

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

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