



Procedimiento N°: A/00064/2014

RESOLUCIÓN: R/01661/2014

En el procedimiento A/00064/2014, instruido por la Agencia Española de Protección de Datos a D. **E.E.E.** titular del establecimiento con denominación comercial “**RESTAURANTE MESÓN XXXXX**” situado en la calle **(C/.....1) de Madrid**, vista la denuncia presentada por D. **C.C.C.** y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 26 de abril de 2013, tiene entrada en esta Agencia escrito del D. **C.C.C.** (en lo sucesivo el denunciante), en el que pone de manifiesto una posible infracción a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) motivada por la instalación de videocámaras en el establecimiento con denominación comercial “**RESTAURANTE MESÓN XXXXX**” situado en la calle **(C/.....1) de Madrid**, cuyo titular es D. **E.E.E.** (en adelante el denunciado).

En el escrito, el denunciante informa de la instalación de un sistema de videovigilancia compuesto por dos cámaras, con capacidad de audio, ubicadas en el interior del establecimiento denunciado en el que prestaba sus servicios. Denuncia el uso y tratamiento de los datos captados por el sistema, dando lugar a su despido en la empresa.

Mediante escrito de 2 de julio de 2013, el denunciante aporta reportaje fotográfico de las cámaras denunciadas.

SEGUNDO: Con fecha 8 de octubre de 2013 se solicita información complementaria al denunciante en relación al motivo de su despido laboral y al sistema de videovigilancia denunciado.

Con fecha 8 de octubre de 2013 se solicita información al responsable del sistema del videovigilancia denunciado, teniendo entrada en esta Agencia escrito de fecha 28 de octubre de 2013 en el que se pone de manifiesto, lo siguiente:

- D. **E.E.E.** es el titular y responsable del sistema de videovigilancia instalado en el establecimiento de su propiedad, **RESTAURANTE MESÓN XXXXX**.
- La empresa que realizó la instalación del sistema fue la mercantil **SECURITAS DIRECT ESPAÑA S.A.U.** (en adelante la empresa de seguridad). En **ANEXO 1** se adjunta declaración descriptiva, emitida por la empresa de seguridad, en la que se detallan las siguientes características entre otras del sistema de seguridad instalados:

o Sistema de Seguridad homologado por el

Ministerio de Interior, que cuenta con elementos de protección electrónicos a través de Verificación por vídeo y número de contrato *****CONTRATO.1.**

- o Sistema de videovigilancia como elemento de captación y grabación de imágenes, en modo local, bajo exclusiva responsabilidad del cliente y número de contrato *****CONTRATO.2.** Se compone de dos cámaras ubicadas en las zonas descritas como “Entrada” y “Barra” del inmueble. Dicho sistema tiene la posibilidad de captar imágenes de manera ininterrumpida las 24 horas del día, mientras no se produzca ninguna verificación por salto de alarma. Cualquier captación y grabación de dichos dispositivos quedará almacenada en el equipo que haya destinado el cliente para dicha función, sin que exista intervención alguna en el tratamiento de las imágenes por parte de Securitas Direct.
- o Todos los elementos se encuentran instalados en ámbitos privados y privativos del inmueble, propiedad del titular del contrato de prestación de servicios de seguridad, protegiendo única y exclusivamente zonas privativas del mismo.

En **ANEXO 2** se acompaña copia del certificado de instalación y conexión del sistema de registro de imágenes, emitido por la empresa de seguridad con fecha 26 de febrero de 2013 y en **ANEXO 3**, se adjunta copia del certificado de instalación y conexión a través de Central de Alarmas emitido por la misma con fecha 28 de julio de 2005.

- Las causas que fundamentan la instalación del sistema son esencialmente la seguridad y naturaleza preventiva ante la proliferación de robos en el área urbana donde radica el establecimiento.
- Se aporta copia del cartel informativo de zona videovigilada (**ANEXO 4**) en el que se identifica como responsable del fichero y del sistema a D. **E.E.E.**

Asimismo en documento **ANEXO 5**, se adjunta copia del modelo de formulario informativo debidamente cumplimentado, el cual y según manifiesta el titular del sistema: “... se encuentra in situ a disposición de los ciudadanos o afectados que lo soliciten siguiendo el procedimiento recogido en el Documento de Seguridad (secciones IX y XII), a saber: *“el impreso estará disponible en una carpeta física especial, denominada e identificada...El responsable del fichero tendrá en su poder y a disposición de los afectados una carpeta digital... a fin de tener la posibilidad de imprimirlo a petición de los afectados...”*”.

- Las cámaras instaladas en el interior del local, tienen capacidad de movimiento, zoom y la función de audio.

Según se indica en el plano de situación adjunto (**ANEXO 6**) existen dos cámaras interiores, ubicadas respectivamente en la zona de barra (Cámara 1) y la Sala (Cámara 2).

- Se acompaña documento gráfico de las cámaras (**ANEXO 7**) y de las imágenes captadas por cada una de ellas (**ANEXO 8**) tal y como se visualizan a través de tecnología IP de acceso seguro (requiere nombre de usuario y password).

Del análisis de las imágenes aportadas, se constata que las cámaras graban espacios interiores del establecimiento.

- El sistema de videovigilancia tiene el acceso restringido al titular del contrato y la empresa de seguridad.

Se acompaña copia del contrato de tratamiento de datos personales (versión sistema de seguridad con conexión a central de alarmas) suscrito por ambas partes con fecha 22 de octubre de 2013 (**ANEXO 9**).

- El registro y almacenamiento de las imágenes videograbadas se realiza mediante alojamiento en los servidores de la empresa de seguridad y pudiendo tener acceso a ellas mediante tecnología IP de acceso seguro. Las imágenes grabadas se conservan por un período no superior a los siete días desde el momento de su registro.

No existen por tanto monitores propiamente de visualización ni sistema de videograbación propio. En documento **ANEXO 10** se acompaña copia del Documento de Seguridad. El sistema conserva las imágenes por un período no superior a 7 días desde el momento de su registro.

- Se aporta documento acreditativo (**ANEXO 11**) de la existencia de fichero de videovigilancia inscrito en el Registro General de Protección de Datos con el código *****COD.1** y en el que figura como responsable el denunciado y como finalidad la videovigilancia de las instalaciones.
- Se acompaña documentación justificativa del registro, por parte de la empresa de seguridad, en la aplicación de Seguridad Privada SEGURPRI del Ministerio del Interior con los siguientes contratos y números de validación:
 - o Contrato *****CONTRATO.1** con número de validación *****NÚMERO.1 (ANEXO 12)**.
 - o Contrato *****CONTRATO.2** con número de validación *****NÚMERO.2(ANEXO 13)**.

- Se adjunta copias de comunicaciones informativas en materia de protección de datos personales a la plantilla que integra actualmente la empresa, en las que constan las firmas de los empleados como prueba de recepción de dicha comunicación (**ANEXO 14**).

En documento **ANEXO 15** acredita la información llevada a cabo por la empresa, a los actuales empleados y en distintas fechas, sobre la implementación de medidas de vigilancia y control que incorpora referencia al deber de secreto.

En los citados documentos no figura notificación personalizada a D. **C.C.C.**, en calidad de antiguo empleado, sobre las medidas de vigilancia y control adoptadas por la empresa.

Con fecha 31 de enero de 2013 y previa diligencia telefónica de inspección, se solicita al responsable del sistema información complementara en relación al procedimiento empleado para informar al denunciante, en calidad de trabajador de la empresa, sobre la finalidad por la cual se ha instalado el sistema de videovigilancia.

Tiene entrada en esta Agencia escrito de fecha 6 de febrero de 2013 por el que se incorpora:

- Copia de la carta de despido dirigida y firmada por D. **C.C.C.** (en adelante el trabajador) mediante la cual se le notifica: *“por la presente... que a tenor de lo establecido en la cláusula segunda de su contrato de trabajo indefinido... y dentro del período de prueba establecido en dicha cláusula, se da por finalizada la relación laboral que le unía a esta empresa con efectos del día de hoy 20 de marzo de 2013, ...”* (**ANEXO 1.1**).
- Copia de la comunicación informativa en materia de protección de datos personales dirigida al trabajador y en la que consta su firma como prueba de su recepción (**ANEXO 2.1**). Esta comunicación está firmada el 20 de marzo de 2013, el mismo día de la carta de despido.
- Copia de la comunicación informativa y compromiso de confidencialidad dirigida al trabajador, mediante la cual se le comunica entre otros aspectos la implementación de medidas de vigilancia y control por parte de la empresa. En el citado escrito consta la firma del trabajador (**ANEXO 3.1**). Esta comunicación está firmada el 20 de marzo de 2013, el mismo día de la carta de despido.

TERCERO: Con fecha 23 de abril de 2014, el Director de la Agencia Española de Protección de Datos acordó otorgar audiencia previa al procedimiento de apercibimiento a D. **E.E.E.**, por presunta infracción del artículo 4.1 de la LOPD, tipificada como **grave** en el artículo 44.3.c) de dicha norma.

CUARTO: En fecha 30 de abril de 2014, se notificó el citado acuerdo de audiencia

previa al procedimiento de apercibimiento al denunciado, tal y como figura en la copia de acuse de recibo expedido por el Servicio de Correos y que forma parte de este expediente.

QUINTO: Transcurrido el plazo concedido para formular alegaciones al acuerdo de audiencia previa al apercibimiento, no consta que se hayan recibido las mismas.

SEXTO: De las actuaciones practicadas en el presente procedimiento, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO: En el establecimiento con denominación comercial “**RESTAURANTE MESÓN XXXXX**” situado en la calle (**C/.....1**) de **Madrid** hay instalado un sistema de videovigilancia compuesto de dos cámaras interiores que graban **imágenes y sonido**.

SEGUNDO: El titular de este establecimiento es D. **E.E.E.**, es el responsable del sistema de videovigilancia.

TERCERO: El sistema fue instalado por la empresa SECURITAS DIRECT ESPAÑA S.A.U., la entidad tiene acceso a las imágenes grabadas y está contratada como central receptora de alarmas. Han aportado documentación justificativa del registro, por parte de la empresa de seguridad, en la aplicación de Seguridad Privada SEGURPRI del Ministerio del Interior con los siguientes contratos y números de validación:

- o Contrato *****CONTRATO.1** con número de validación *****NÚMERO.1.**
- o Contrato *****CONTRATO.2** con número de validación *****NÚMERO.2.**

CUARTO: Las cámaras graban imágenes del interior del establecimiento, las mismas se conservan por un período de tiempo de 7 días. El fichero está inscrito en el Registro General de Protección de Datos con el código nº: *****COD.1**, en la descripción detallada de la finalidad y usos previstos aparece “*videovigilancia de las instalaciones*”. Y así se comprueba por medio de diligencia de consulta al Registro llevada a cabo el 31 de enero de 2014.

QUINTO: El denunciado ha aportado copia de los carteles informativos que avisan de la existencia de una zona videovigilada y que identifican al responsable del fichero. También ha facilitado copia del formulario informativo que debe estar a disposición de los interesados.

SEXTO: El denunciado ha facilitado copia de la “*comunicación informativa para empleados de la empresa protección de datos de carácter personal*” y de la “*comunicación informativa y compromiso de confidencialidad para empleados de la empresa*” firmadas por los actuales trabajadores (4 personas). Estos escritos recogen las firmas de los empleados en distintas fechas: **D.D.D.** (4 de febrero de 2013), **F.F.F.** (27 de junio de 2013), **G.G.G.** (20 de diciembre de 2012) y **H.H.H.** (1 de mayo de 2013).

La “comunicación informativa y compromiso de confidencialidad para empleados de la empresa” en su apartado a) expresamente señala: “informarle de la implementación de medidas de vigilancia y control por parte de la empresa, de conformidad con lo establecido en el artículo 20 del R.D. Legislativo 1/1995 (texto refundido de la Ley del Estatuto de los Trabajadores)” sin especificar el tipo de medidas que se van a implementar.

SÉPTIMO: El denunciado ha aportado copia de la “comunicación informativa para empleados de la empresa protección de datos de carácter personal” y de la “comunicación informativa y compromiso de confidencialidad para empleados de la empresa” firmadas por el denunciante (antiguo trabajador). Estos escritos recogen las firmas del denunciante el día 20 de marzo de 2013.

La “comunicación informativa y compromiso de confidencialidad para empleados de la empresa” en su apartado a) expresamente señala: “informarle de la implementación de medidas de vigilancia y control por parte de la empresa, de conformidad con lo establecido en el artículo 20 del R.D. Legislativo 1/1995 (texto refundido de la Ley del Estatuto de los Trabajadores)” sin especificar el tipo de medidas que se van a implementar.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento el Director 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 ya que la presencia del mismo puede suponer una vulneración del requisito de consentimiento de los afectados. Así pues hay que tener en cuenta lo siguiente:

- Respetar el principio de proporcionalidad.
- Cuando el sistema esté conectado a una central de alarma, únicamente podrá ser instalado por una empresa de seguridad privada que reúna los requisitos contemplados en el artículo 7 de la Ley 23/92 de Seguridad Privada.
- 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. 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."

- Salvo en el caso de que el tratamiento consista exclusivamente en la reproducción o emisión de imágenes en tiempo real, 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

En primer lugar, hay que analizar las circunstancias relacionadas con el posible control empresarial de los trabajadores por medio del sistema de videovigilancia instalado en el establecimiento donde desarrollan su trabajo, ambas cámaras se encuentran en el interior del local, una de ellas sobre la barra, son cámaras móviles con dispositivo zoom y grabación de imágenes y sonido.

Durante la fase de actuaciones previas, el denunciado ha presentado como anexo nº 15, copias de la *"comunicación informativa y compromiso de confidencialidad para empleados de la empresa"* firmadas por los cuatro trabajadores actuales y por el denunciante. El tenor literal de dicha comunicación en cuanto a la información que facilita a sus trabajadores es el siguiente: *"En cumplimiento de las políticas de seguridad de la información de la empresa, se ha redactado el presente documento, a fin de: a) Informarle de la implementación de medidas de vigilancia y control por parte de la empresa, de conformidad con lo establecido en el artículo 20 del R.D. Legislativo 1/1995 (texto refundido de la Ley del Estatuto de los Trabajadores)."* Esta es toda la información que se da a los empleados, no se concreta el tipo de medidas que se van a utilizar y no se menciona que una de ellas sea el control a través del sistema de videovigilancia instalado en el local.

Los sistemas de videovigilancia pueden utilizarse para el control laboral de los empleados, en virtud del artículo 20.3 del Estatuto de los Trabajadores:

"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.

En relación con esta materia, es de suma importancia la sentencia 029/2013 del Tribunal Constitucional, que en relación con el derecho de información que debe cumplir el empresario, señala:

"...En aplicación de esa doctrina, concluimos que no hay una habilitación legal

*expresa para esa omisión del derecho a la información sobre el tratamiento de datos personales en el ámbito de las relaciones laborales, y que tampoco podría situarse su fundamento en el interés empresarial de controlar la actividad laboral a través de sistemas sorpresivos o no informados de tratamiento de datos que aseguren la máxima eficacia en el propósito de vigilancia. Esa lógica fundada en la utilidad o conveniencia empresarial haría quebrar la efectividad del derecho fundamental, en su núcleo esencial. En efecto, se confundiría la legitimidad del fin (en este caso, la verificación del cumplimiento de las obligaciones laborales a través del tratamiento de datos, art. 20.3 LET en relación con el art. 6.2 LOPD) con la constitucionalidad del acto (**B.B.B.**), cuando lo cierto es que cabe proclamar la legitimidad de aquel propósito (incluso sin consentimiento del trabajador, art. 6.2 LOPD) pero, del mismo modo, declarar que lesiona el art. 18.4 CE la utilización para llevarlo a cabo de medios encubiertos que niegan al trabajador la información exigible.*

En conclusión, no debe olvidarse que hemos establecido de forma invariable y constante que las facultades empresariales se encuentran limitadas por los derechos fundamentales (entre otras muchas, SSTC 98/2000, de 10 de abril, FJ 7, o 308/2000, de 18 de diciembre, FJ 4). Por ello, al igual que el interés público en sancionar infracciones administrativas resulta insuficiente para que la Administración pueda sustraer al interesado información relativa al fichero y sus datos, según dispone el art. 5.1 y 2 LOPD (STC 292/2000, de 30 de noviembre, FJ 18), tampoco el interés privado del empresario podrá justificar que el tratamiento de datos sea empleado en contra del trabajador sin una información previa sobre el control laboral puesto en práctica. No hay en el ámbito laboral, por expresarlo en otros términos, una razón que tolere la limitación del derecho de información que integra la cobertura ordinaria del derecho fundamental del art. 18.4 CE. Por tanto, no será suficiente que el tratamiento de datos resulte en principio lícito, por estar amparado por la Ley (arts. 6.2 LOPD y 20 LET), o que pueda resultar eventualmente, en el caso concreto de que se trate, proporcionado al fin perseguido; el control empresarial por esa vía, antes bien, aunque podrá producirse, deberá asegurar también la debida información previa.

*...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.A.A.** 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."*

En el caso de que las cámaras se utilicen para el control empresarial, el responsable del fichero deberá garantizar el derecho a la información en la recogida de las imágenes por medio de información específica a la representación sindical (en los negocios y empresas que la tengan), a través del cartel anunciador e informativo y mediante información personalizada a los trabajadores. Esta información debe ser **previa, expresa, precisa, clara e inequívoca**, es decir, debe informar al trabajador de qué medidas o medios se van a utilizar para el control de sus obligaciones laborales, cómo

se va a realizar ese control y para qué finalidad. Si faltara alguno de estos requisitos se vulneraría el **artículo 5.1** de la LOPD, según el cual:

“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 vulneración del artículo 5.1 citado está tipificada como **leve** en el artículo 44.2.c) de la LOPD, que establece:

“Son infracciones leves: ...c) El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado.”

En el supuesto que nos ocupa, no ha quedado acreditado que el empresario utilice el sistema de videovigilancia para el control empresarial ni que el despido del denunciante esté relacionado con un control de ese tipo. En el fichero de videovigilancia inscrito en el Registro General de Protección de Datos a nombre del denunciado, se describe como finalidad del sistema, la videovigilancia de las instalaciones. Esta circunstancia unida a que el denunciado no ha informado a sus trabajadores (cumpliendo con los requisitos anteriormente descritos) de la utilización del sistema de videovigilancia para el control empresarial, conllevaría que el denunciado no pueda utilizar las cámaras que tiene instaladas en el interior de su local para el control empresarial sin vulnerar la normativa de protección de datos.

IV

Se imputa asimismo, a D. **E.E.E.**, como responsable del sistema de videovigilancia instalado en el establecimiento con denominación comercial **“RESTAURANTE MESÓN XXXXX”** situado en la calle **(C/.....1) de Madrid**, la comisión de una infracción del artículo 4.1 de la LOPD.

La LOPD regula en su artículo 4 el principio de calidad de datos, que contiene a su vez el principio de **proporcionalidad**, aplicable al supuesto de hecho que nos ocupa, en lo relativo a la captación y grabación de sonido por parte de las cámaras que componen el sistema de videovigilancia denunciado.

El artículo 3 de la LOPD, define en su apartado a) lo que se entiende por datos de carácter personal: *“cualquier información concerniente a personas físicas identificadas o identificables.”*

El artículo 5.1.f) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (RLOPD), completa la anterior definición, entendiendo por datos de carácter personal: *“cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.”*

De ambas definiciones se deriva que tanto la imagen de una persona (información gráfica o fotográfica) como su voz (información acústica) son datos de carácter personal a cuyo tratamiento habrá que aplicar la LOPD.

La LOPD garantiza el cumplimiento del principio de proporcionalidad en todo tratamiento de datos personales, cuando señala en su artículo 4 que:

- “1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.*
- 2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos”.*

Este artículo consagra entre otros, el principio de proporcionalidad en el tratamiento de los datos de carácter personal que supone que el tratamiento de los datos sea ajustado y proporcionado a la finalidad a la que se dirige el tratamiento, debiendo restringirse el tratamiento de los datos excesivos o bien procederse a la supresión de los mismos.

Este principio se encuentra recogido también, en el artículo 6 de la Directiva 95/46/CE del Parlamento Europeo 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, y aparece también reflejado en el Convenio 108, cuyo artículo 5 c) indica que *“los datos de carácter personal que sean objeto de un tratamiento automatizado (...) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado”.*

La pertinencia en el tratamiento de los datos no sólo debe producirse en el ámbito de la recogida de los datos, sino que habrá asimismo de respetarse en el posterior tratamiento que se realice de los mismos. Además hay que tener en cuenta que la finalidad del tratamiento debe presidir el mismo, de tal forma que no es aceptable que se traten datos excesivos, que rebasan o que no son proporcionados y adecuados en relación con la finalidad perseguida (teniendo en cuenta que la misma debe ser legítima).

La Instrucción 1/2006, regula en su artículo 4, el **principio de proporcionalidad** en el tratamiento de los datos en el ámbito de la videovigilancia, en los siguientes términos:

- “1. De conformidad con el artículo 4 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.*
- 2. Sólo se considerará admisible la instalación de cámaras o videocámaras*

cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

3. Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida.”

La **sentencia del Tribunal Constitucional 98/2000**, trata el tema de la instalación de aparatos de captación y grabación del sonido en relación con la protección de derechos fundamentales y el incumplimiento de los requisitos derivados del principio de proporcionalidad, entre otros, en esta sentencia se indica:

“.....el uso de un sistema que permite la audición continuada e indiscriminada de todo tipo de conversaciones, tanto de los propios trabajadores, como de los clientes del casino, constituye una actuación que rebasa ampliamente las facultades que al empresario otorga el art. 20.3 L.E.T. y supone, en definitiva, una intromisión ilegítima en el derecho a la intimidad consagrado en el art. 18.1 C.E. En resumen, la implantación del sistema de audición y grabación no ha sido en este caso conforme con los principios de proporcionalidad e intervención mínima que rigen la modulación de los derechos fundamentales por los requerimientos propios del interés de la organización empresarial pues la finalidad que se persigue (dar un plus de seguridad...) resulta desproporcionada para el sacrificio que implica del derecho a la intimidad de los trabajadores (e incluso de los clientes del casino). Este sistema permite captar comentarios privados, tanto de los clientes como de los trabajadores del casino, comentarios ajenos por completo al interés empresarial...”

Los fines disuasorios que se persiguen con la instalación de un sistema de videovigilancia para evitar hurtos y actos vandálicos, y en relación con la seguridad en general del establecimiento donde se encuentran las cámaras, se consigue sin necesidad de incluir la grabación de sonido, tal y como ocurre en el caso que nos ocupa, en el que las dos cámaras graban imágenes y sonido. Así se denuncia en este procedimiento y **así lo reconoce el denunciado a la hora de facilitar información sobre el sistema de videovigilancia que tiene instalado en el establecimiento del que es titular.**

Así pues, en este supuesto concreto, se está realizando un tratamiento de datos excesivos (imágenes y voces) resultando desproporcionado para el fin de seguridad que se persigue. Este fin puede realizarse plenamente con la sola grabación de imágenes sin que sea necesario para el mismo incluir las voces de las personas que se encuentren en el local, ya sea como clientes o como trabajadores.

La infracción al artículo 4 de la LOPD, aparece tipificada como grave en el **artículo 44.3.c)** de la LOPD, que considera como tal:

“Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy

grave”.

Dicha infracción podría ser sancionada con multa de 40.001 a 300.000 euros, de acuerdo con el artículo 45.2 de la LOPD.

V

La disposición final quincuagésima sexta de la Ley 2/2011 de 4 de marzo de Economía Sostenible (BOE 5-3-2011) (LES), ha añadido un nuevo apartado 6 al artículo 45 de la LOPD en lugar del existente hasta su promulgación del siguiente tenor:

“Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador, y en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurren los siguientes presupuestos:

- a) que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.*
- b) que el infractor no hubiese sido sancionado o apercibido con anterioridad.*

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento”.

Los criterios a los que alude el nuevo artículo 45.6 de la LOPD, vienen recogidos en el apartado 5 de este mismo artículo, que también ha sido modificado por la Disposición Final Quincuagésima Sexta de la LES, quedando redactado del siguiente modo:

“El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:

- a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado 4 de este artículo.*
- b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.*
- c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.*
- d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.*
- e) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente.”*

En el presente supuesto se cumplen los requisitos recogidos en los apartados a) y b) del citado artículo 45.6 de la LOPD. Junto a ello se constata una disminución de la



culpabilidad del imputado teniendo en cuenta que no consta que existan beneficios obtenidos como consecuencia de la comisión de la infracción.

De acuerdo con lo señalado,

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

SE ACUERDA:

1. APERCIBIR (A/00064/2014) a D. **E.E.E.A**, como titular del establecimiento con denominación comercial **"RESTAURANTE MESÓN XXXXX"** situado en la calle **(C/.....1) de Madrid**, con arreglo a lo dispuesto en el artículo 45.6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, con relación a la denuncia por la infracción del **artículo 4.1** de la LOPD, tipificada como **grave** en el artículo 44.3.c) de la citada Ley Orgánica.

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 esta acto, según lo previsto en el artículo 46.1 del referido texto legal.

2.- REQUERIR a D. **E.E.E.**, de acuerdo con lo establecido en el apartado 6 del artículo 45 de la Ley 15/1999 para que acredite en el **plazo de un mes** desde este acto de notificación lo siguiente, (abriéndose expediente de actuaciones previas):

- ✓ **cumpla lo previsto en el artículo 4.1 de la LOPD.** En concreto se insta al denunciado a justificar que las cámaras que tiene instaladas no graban ni captan sonido. Puede acreditar la adopción de esta medida, a través del medio que crea más adecuado, entre otros, con una certificación de la empresa de seguridad que tiene contratada o cambiando los dispositivos por otros que únicamente graben imágenes.
- ✓ **informe a la Agencia Española de Protección de Datos del cumplimiento de lo requerido** en el punto anterior, acreditando dicho cumplimiento.

En caso de no cumplir el presente requerimiento, se procederá a acordar la apertura de un **procedimiento sancionador** pudiendo llegar a imponerse una sanción de 40.001 a 300.000 euros.

3.- NOTIFICAR el presente Acuerdo a D. **E.E.E.**

4.- NOTIFICAR el presente Acuerdo a D. **C.C.C.**

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.

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

En cumplimiento del artículo 5 de la Ley Orgánica 15/1999, se le informa de que los datos de carácter personal se incluyen en el fichero denominado "Expedientes de la Inspección de Datos", creado por Resolución de 27 de julio de 2001. La finalidad del fichero es la gestión y tramitación de expedientes de la Inspección de Datos. Pueden ser destinatarios de la información los interesados en los procedimientos, los órganos jurisdiccionales, el Ministerio Fiscal, el Defensor del Pueblo, otras Autoridades de Control, las Administraciones Públicas y las Cortes Generales. El afectado podrá ejercitar los derechos de acceso, rectificación, cancelación y oposición ante el responsable del tratamiento, la Agencia Española de Protección de Datos, calle Jorge Juan nº 6, 28001 Madrid.