



**Procedimiento Nº PS/00143/2008**

**RESOLUCIÓN: R/01208/2008**

En el procedimiento sancionador PS/00143/2008, instruido por la Agencia Española de Protección de Datos a la entidad Café Iruña S.A., vista la denuncia presentada por D. O.O.O. Y D. Z.Z.Z. y en base a los siguientes,

**ANTECEDENTES**

**PRIMERO:** Con fecha de 28 de febrero de 2007, tiene entrada en esta Agencia un escrito de D. O.O.O. y D. Z.Z.Z. en el que declaran, en calidad de miembros de CCOO en el comité de empresa de la entidad Café Iruña S.A. (en adelante IRUÑA), que en el interior del “Café Iruña” de (.....) se han instalado varias cámaras de videovigilancia, tanto en el área de atención al público, como en el área de utilización exclusiva de los empleados. Manifiestan que tienen conocimiento de que las imágenes obtenidas tienen un tratamiento posterior, sin que se haya creado ningún fichero ni se informe adecuadamente a los usuarios ni a los trabajadores.

**SEGUNDO:** Tras la recepción de la denuncia, el Director de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

1. RESPECTO DE CAFÉ IRUÑA S.A.

1.1. IRUÑA manifiesta que el 23 de marzo de 2007 se firmó un contrato con la entidad SERCOIN NAVARRA S.L., del que adjuntan copia, para la instalación y mantenimiento de un sistema de videovigilancia. El motivo fundamental de ésta instalación fue la prevención de los delitos que se pudieran cometer en el local, así como el control de los accesos al local.

1.2. La instalación se compone de un total de 13 cámaras de videovigilancia, todas ellas de instalación fija, y un videograbador. La distribución de las cámaras es la siguiente:

2 para control del comedor principal

1 para control de la caja registradora del establecimiento anexo, denominado “El rincón de Hemingway”.

2 para control de acceso al local por la barra y la caja registradora.

1 para control de accesos desde la cocina.

1 para control de los accesos al comedor del personal.



1 para control de acceso y 1 en el interior de la cámara frigorífica.

4 para control del establecimiento denominado "Sub-suelo", regentado por IRUÑA.

1.3. Todas las imágenes se centralizan en el dispositivo videograbador desde el que se pueden visualizar y que las almacena, por un periodo no superior a 4 días, mediante un disco duro interno. Existe la posibilidad de realizar copias de las imágenes y extraerlas del dispositivo. Las imágenes fueron en alguna ocasión solicitadas por la Policía Judicial para el esclarecimiento de algún delito.

1.4. La entidad SERCOIN NAVARRA S.L. es la encargada de las gestiones legales y administrativas en cuanto a permisos y licencias, habiendo instalado en las puertas de entrada al local sendos carteles informativos de la operación del sistema de videovigilancia. IRUÑA no tiene constancia de las gestiones realizadas o licencias obtenidas a favor de IRUÑA por SERCOIN NAVARRA S.L.

1.5. Iruña manifiesta que todos los empleados y el comité de empresa están informados de la existencia de las videocámaras y del tratamiento que se da a las imágenes obtenidas, mediante instrucciones verbales proporcionadas por la dirección. A principios de junio de 2007 el Comité de Empresa le solicitó información sobre el sistema de videovigilancia, por lo que se les proporcionó la información reflejada en el contrato antes mencionado.

1.6. IRUÑA no tiene constancia de la existencia de ninguna reclamación de ningún empleado o cliente sobre la existencia de las cámaras. Así mismo, manifiesta que el sistema de videovigilancia sólo es accedido y gestionado por el gestor de IRUÑA, sin que ninguna otra persona tenga acceso a las imágenes ni se hayan proporcionado a terceras personas excepto a las Fuerzas y Cuerpos de Seguridad del Estado y para la resolución de conflictos judiciales.

1.7. Durante la inspección realizada se verificó que en la puerta de acceso al local se encuentra una pegatina con la siguiente leyenda: "PARA SU TRANQUILIDAD, ESTA PROPIEDAD ESTÁ PROTEGIDA POR SISTEMAS DE SEGURIDAD Y GRABACION PERMANENTE DE IMÁGENES POR CCTV. LA DIRECCIÓN. SERCOIN. TELF. #####".

1.8. También se verificó que la instalación consta de un total de 9 cámaras de videovigilancia con instalación fija en los lugares detallados anteriormente. Las imágenes captadas por las mencionadas videocámaras se muestran en una pantalla ubicada en el despacho del "Cargo 1" de IRUÑA. El representante de la entidad manifiesta que el acceso al referido despacho está limitado a él mismo y a sus acompañantes. Conectado a la misma se encuentra un equipo de control y grabación de imágenes marca "Air Space CCTV". Se comprueba así mismo que existe un dispositivo de control remoto del sistema de visualización y que dispone de una unidad de grabación de DVD.

Al acceder al dispositivo de grabación y almacenamiento de imágenes, se verificó que no requería la introducción de ninguna contraseña ni para el acceso a las funciones de configuración, ni para la visión y recuperación de las imágenes



almacenadas. En el menú de configuración del dispositivo se comprobó que el mismo está programado para grabar durante las 24 horas del día, sin interrupción. El sistema está configurado para la sobreescritura de las imágenes una vez se haya alcanzado el límite de capacidad de almacenamiento del disco duro.

Se realizaron varias pruebas de acceso a imágenes almacenadas, comprobándose que las más antiguas correspondían a cinco días antes. Las imágenes tomadas durante el día corresponden a las distintas ubicaciones de las cámaras, sin que se aprecien cambios en el campo de visión. Durante la reproducción de las imágenes se pudo observar el tránsito de varias personas en el establecimiento y en los locales interiores de uso del personal, en algunas de las cuales es posible la identificación de los sujetos grabados.

Se comprobó que sobre las imágenes almacenadas se puede seleccionar una zona del campo de visión registrado y realizar un acercamiento.

IRUÑA manifiesta que se puede acceder a las imágenes almacenadas utilizando la red INTERNET mediante la instalación de un programa especial y la habilitación de algunos puertos de comunicación, y tras identificarse como usuario mediante contraseña.

## 1. RESPECTO DEL REGISTRO GENERAL DE PROTECCIÓN DE DATOS

En el Registro General de Protección de Datos no consta ningún fichero inscrito a nombre de Café Iruña S.A. ni al NIF \*\*\*\*\*.

**TERCERO:** En fecha 28 de abril de 2008 el Director de la Agencia Española de Protección de Datos, acordó iniciar procedimiento sancionador a la entidad Café Iruña S.A., por la posible infracción del artículo 5.1 y 26.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en los sucesivos LOPD), tipificadas como leves en los artículos 44.2.d) y 44.2. c) respectivamente de dicha norma, pudiendo ser sancionada con multa de 601,01 € a 60.101,21 €, por cada una de las infracciones, a tenor del artículo 45.1 de la citada Ley Orgánica.

**CUARTO:** En fecha 19 de mayo de 2008 se recibe escrito en esta Agencia en el que, los denunciados D. O.O.O. y D. Z.Z.Z. se personan como interesados y realizan en síntesis, las siguientes alegaciones al acuerdo de inicio:

- Que no es cierto, que en fecha 23 de marzo de 2007, se firmara un acuerdo de instalación y mantenimiento del sistema de videovigilancia, ya que las cámaras estaban instaladas meses antes, habiendo presentado la primera denuncia en esta Agencia el 28 de febrero de 2007.
- Que han tenido conocimiento de la instalación de una cámara adicional a las ya instaladas, en la cocina del establecimiento denunciado, con posterioridad a la inspección realizada por esta Agencia. También han constatado el cambio de ubicación y características técnicas de algunas de las cámaras ya instaladas.



- En ningún momento, el Comité de Empresa ni los trabajadores han recibido comunicación o consulta alguna a cerca de la instalación de las cámaras de vigilancia, ni del propósito que la dirección de la empresa perseguía con la instalación de las mismas. No habiendo recibido ningún tipo de explicación, por parte de la dirección de la empresa, pese a haber sido requerida a ésta para proporcionarles información a cerca de la instalación de las cámaras de videovigilancia.

**QUINTO:** En fecha 20 de mayo de 2008, D. A.A.A. en representación de Café Iruña S.A., formuló en síntesis, las siguientes alegaciones al acuerdo de inicio:

- Que las imágenes obtenidas no han tenido un tratamiento posterior, salvo en una ocasión que fueron requeridas por la Unidad de Delitos contra el Patrimonio de la Policía Nacional.
- Solicitar que los denunciante aporten prueba de la creación de ficheros por parte del denunciado en el que se almacenen imágenes de personas que no hayan sido advertidas de la creación del mismo.
- Inexistencia de la creación de ficheros de carácter personal no habiendo solicitado inscripción alguna.

**SEXTO:** Transcurrido el plazo de alegaciones, por parte de la instructora del procedimiento se inició el período de práctica de pruebas, dando por reproducidas las actuaciones previas de investigación E/00378/2007, desarrolladas por los Servicios de Inspección de esta Agencia Española de Protección de Datos, así como las alegaciones presentadas por el denunciado y denunciante.

En cuanto a las pruebas solicitadas por el representante del denunciado se procedió a denegar la solicitud a los denunciante de aportación de prueba de creación de ficheros por parte de la empresa, al no considerarse necesaria para el esclarecimiento de los hechos imputados que son por una parte, la infracción del artículo 5 de la LOPD, relativo a la obligación de informar previamente al tratamiento de datos y por otra parte, la infracción del artículo 26 de la LOPD, relativo a la notificación e inscripción de los ficheros de carácter personal en la Agencia Española de Protección de Datos.

**SEPTIMO:** En fecha 22 de julio de 2008, el Instructor del Procedimiento emitió Propuesta de Resolución, en la que se propone que por el Director de la Agencia Española de Protección de Datos, se sancione a Café Iruña S.A. con multa de 601,01 euros (seiscientos un euro con un céntimo de euro) por la infracción del artículo 5 de la LOPD, tipificada como leve en el artículo 44.2.d) de dicha norma, y con multa de 601,01(seiscientos un euro con un céntimo de euro), por la infracción del artículo 26 de la LOPD, tipificada como leve en el artículo 44.2. c) de dicha norma, dándose traslado a ésta para que en el plazo máximo de quince días hábiles presentara alegaciones.



**OCTAVO:** En fecha 10 de septiembre de 2008, el representante de la entidad denunciada formula, en síntesis, las siguientes alegaciones a la Propuesta de Resolución:

- Adjunta una serie de firmas que, manifiesta ser de personal de la empresa Iruña S.A., según las cuales se puso en conocimiento del personal la instalación de cámaras de videovigilancia.

**NOVENO:** De las actuaciones llevadas a cabo en el presente procedimiento, han quedado acreditados los siguientes

### HECHOS PROBADOS

**PRIMERO:** Café Iruña S.A., tiene suscrito un contrato de instalación y mantenimiento del sistema de videovigilancia con la empresa SERCOIN NAVARRA S.L., desde el 23 de marzo de 2007.(Folios 64, 65).

**SEGUNDO:** Café Iruña tiene instaladas un total de 13 cámaras de videovigilancia, de instalación fija y un videograbador. La distribución de las cámaras es la siguiente:(Folio 61)

2 para control del comedor principal

1 para control de la caja registradora del establecimiento anexo, denominado "El rincón de Hemingway".

2 para control de acceso al local por la barra y la caja registradora.

1 para control de accesos desde la cocina.

1 para control de los accesos al comedor del personal.

1 para control de acceso y 1 en el interior de la cámara frigorífica.

4 para control del establecimiento denominado "Sub-suelo", regentado por IRUÑA.

**TERCERO:** Las imágenes captadas por las mencionadas videocámaras se centralizan en una pantalla ubicada en el despacho del "Cargo 1" de Iruña, desde el que se pueden visualizar dichas imágenes. Conectado a la misma se encuentra un equipo de control y grabación de imágenes marca "Air Space CCTV". Existe un dispositivo de control remoto del sistema de visualización y que dispone de una unidad de grabación de DVD.(Folios 62 y 68).



**CUARTO:** Al acceder al dispositivo de grabación y almacenamiento de imágenes, se verificó que no requería la introducción de ninguna contraseña ni para el acceso a las funciones de configuración, ni para la visión y recuperación de las imágenes almacenadas. En el menú de configuración del dispositivo se comprobó que el mismo está programado para grabar durante las 24 horas del día, sin interrupción. El sistema está configurado para la sobreescritura de las imágenes una vez se haya alcanzado el límite de capacidad de almacenamiento del disco duro. (Folios 62 y 68).

**QUINTO:** Al realizar varias pruebas de acceso a imágenes almacenadas, se comprobó que las más antiguas correspondían a cinco días antes. Durante la reproducción de las imágenes se pudo observar el tránsito de varias personas en el establecimiento y en los locales interiores de uso del personal, en algunas de las cuales es posible la identificación de los sujetos grabados. (Folios 62 y 68)

**SEXTO:** Se verifica por los inspectores de esta Agencia la posibilidad de uso del sistema de videovigilancia de forma remota, utilizando un programa instalado al efecto, sin necesidad de identificación previa. Se realizan pruebas de control de movimiento y acercamiento de imágenes, no siendo posible el control remoto de las cámaras. (Folio 63)

**SEPTIMO:** Durante la inspección realizada se verificó que en la puerta de acceso al local se encuentra una pegatina con la siguiente leyenda: "PARA SU TRANQUILIDAD, ESTA PROPIEDAD ESTÁ PROTEGIDA POR SISTEMAS DE SEGURIDAD Y GRABACION PERMANENTE DE IMÁGENES POR CCTV. LA DIRECCIÓN. SERCOIN. TELF. #####". (Folio 62).

**OCTAVO:** En fecha 7 de agosto de 2007, en el Registro General de Protección de Datos no consta ningún fichero inscrito a nombre de Café Iruña S.A. ni al NIF \*\*\*\*\*. (Folio 70,71)

## **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**

Con carácter previo, hay que señalar que 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".



La LOPD, viene a regular el derecho fundamental a la protección de datos de las personas físicas, esto es, el derecho a disponer de sus propios datos sin que puedan ser utilizados, tratados o cedidos sin su consentimiento, con la salvedad de las excepciones legalmente previstas.

En cuanto al ámbito de aplicación de la citada norma, 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”*. 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.

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 Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, 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.

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.



Por tanto, la captación de imágenes con fines de vigilancia y control, como es el caso que nos ocupa, se encuentra plenamente sometida a lo dispuesto en la LOPD, ya que constituye un tratamiento de datos de carácter personal.

De acuerdo con los preceptos transcritos, la videocámara 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 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.

En el supuesto en cuestión las cámaras instaladas en el local denunciado, cuyo responsable es Café Iruña S.A., graba imágenes de todas las personas que se encuentran en el local ya sean empleados como clientes, siendo éstas perfectamente identificables por cuanto ésta es la finalidad de la instalación de la cámara, prevenir los delitos que se pudieran cometer en el local y controlar el acceso al mismo.

### III

En primer lugar es necesario realizar varias aclaraciones respecto a las alegaciones presentadas por el “Cargo 1” de Iruña S.A., relativas al concepto de responsable del fichero.

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.

En el caso que nos ocupa, Café Iruña es el que ha decidido la instalación del sistema de videovigilancia, lo que en definitiva le convierte en responsable del fichero dado que decide sobre la finalidad, contenido y uso del tratamiento derivado de las imágenes, requisitos necesarios para considerarte responsable del fichero, al amparo del artículo 3 d) de la LOPD.

Además, el responsable del fichero, en este caso Café Iruña, tiene una serie de obligaciones, que se empiezan a producir incluso con anterioridad a ser responsable. Una vez que se disponga a recabar datos personales, que haya decidido la finalidad del tratamiento y que deba crear un fichero de datos, comienza su obligación de inscribirlo en el Registro General de Protección de Datos.

Además, el responsable del fichero debe tener en cuenta otros aspectos, como el principio de calidad de los datos, los principios del consentimiento, los derechos de los afectados y su obligación de deber de secreto.

De acuerdo con lo anterior, el concepto de fichero, a los efectos de lo establecido en la LOPD, parte esencialmente de que exista un conjunto organizado de datos de carácter personal empleados por el responsable del fichero para el cumplimiento de una finalidad específica.

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.

En el caso concreto, Café Iruña en fecha 7 de agosto de 2007, no tenía inscrito en esta Agencia el fichero de videovigilancia del que es responsable.

#### IV

Respecto a las alegaciones realizadas por los denunciantes, relativa a la instalación de las cámaras de videovigilancia con anterioridad a la firma del contrato de instalación y mantenimiento del sistema de videovigilancia y la falta de información a los trabajadores de la entidad sobre la instalación de las cámaras de seguridad, hay que decir que la inspección por parte de esta Agencia se realizó en fecha 20 de junio de 2007 y esa fecha es la que consta como el hecho objetivo acreditado en virtud del cual se inicia el presente procedimiento y precisamente en dicha fecha se pudo constatar la existencia de una contrato de instalación y mantenimiento del sistema de videovigilancia firmado con la empresa Sercoin Navarra S.L. en fecha 23 de marzo de 2007.

Respecto a la legitimación en el tratamiento de las imágenes, por parte de Café Iruña, el artículo 6.1 de la LOPD establece que *“el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa”* y así lo dispone el artículo 2 de la Instrucción 1/2006: *“ 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.”*

En el caso analizado, las imágenes captadas por las cámaras son datos de carácter personal conforme al artículo 3.a) de la LOPD y al artículo 5.1. f) del citado Real Decreto 1720/2007, toda vez que las cámaras captan imágenes de las personas que circulan por la vía pública. Asimismo, tales imágenes constituyen, en sí mismas consideradas, un tratamiento de datos en los términos de la LOPD.

Son pues elementos característicos del derecho fundamental a la protección de datos personales, los derechos del afectado a consentir sobre la recogida y tratamiento de sus datos personales y a saber de los mismos.

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

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

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

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

b) Específico, es decir referido a un determinado tratamiento o serie de tratamientos concretos y en el ámbito de las finalidades determinadas, explícitas y legítimas del responsable del tratamiento, tal y como impone el artículo 4.2 de la LOPD.

c) Informado, es decir que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce.



Precisamente por ello el artículo 5.1 de la LOPD impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen.

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

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

El artículo 20.3 del Estatuto de los Trabajadores (ET) dispone que *“El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso”*.

Por otra parte, no se puede obviar la doctrina del Tribunal Supremo, en Sentencia de 18 de junio de 2006, en virtud de la cual dichas medidas (como las relacionadas con la utilización de Internet y correo electrónico) deben haber sido hechas constar expresamente al trabajador, pasando así a formar parte de la propia relación laboral y siendo el tratamiento de los datos necesario para su adecuado desenvolvimiento.

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

## V

Respecto a la alegación de la entidad denunciada a la propuesta de resolución aportando una lista de firmas de personas, que manifiesta ser trabajadores de la empresa, y que afirma fueron informados del sistema de videovigilancia hay que señalar que como se ha establecido *“ut supra”*, la aplicación del artículo 20.3 del ET no legitima por sí solo el tratamiento de las imágenes, si bien este será posible, aún sin contar con el consentimiento del afectado en caso de que el trabajador haya sido debidamente informado de la existencia de esta medida, debiendo además ser claro



que, conforme a lo exigido por el artículo 4.2 de la LOPD, los datos no podrán ser utilizados para fines distintos.

Respecto a la forma en que se debe llevar a cabo el deber de información, el artículo 5 de la LOPD señala que debe ser expresa, aunque rige el principio de libertad de forma. Ahora bien en el caso de una mera información verbal, como es el caso que se plantea, el problema es cómo se puede probar que se ha producido dicha información.

Los artículos 18 y 19 del Reglamento de desarrollo de la LOPD (aprobado por RD 1720/2007, de 21 de diciembre) establecen una regulación complementaria a la del propio artículo 5 de la LOPD. Así el artículo 18 del citado Real Decreto 1720/2007 establece:” 1. *El deber de información al que se refiere el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado. 2. El responsable del fichero o tratamiento deberá conservar el soporte en el que conste el cumplimiento del deber de informar. Para el almacenamiento de los soportes, el responsable del fichero o tratamiento podrá utilizar medios informáticos o telemáticos. En particular podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales.*”

A este respecto la SAN, Sección 1ª., de fecha 27 de abril de 2005 (rec. 305/2003) establece. <<Es cierto que el artículo 5 de la LO 15/1999 no impone formalidades específicas para que se facilite información en el momento de la recogida de datos, pero eso no es incompatible con la necesidad de que se pueda acreditar que se ha producido esa información y para ello no es suficiente con que se produzca una simple información verbal sino que se necesita alguna forma de constancia de la que no dispone el recurrente. La garantía del artículo 5 de la Ley Orgánica 15/1999 no puede hacerse efectiva si no fuera sobre la base de que se informe a aquellas personas a las que se soliciten datos personales de que se va a proceder al tratamiento de dichos datos, por lo que es necesario que dicha información pueda ser acreditada para lo que es imprescindible que conste de algún modo no siendo suficiente la información oral que pretender haber realizado la parte recurrente. No se olvide que el artículo 6.1 de la LO 15/1999 establece que el “tratamiento automatizado de los datos personales de carácter personal requerirá del consentimiento del afectado, salvo que la Ley disponga otra cosa”; por lo tanto, corresponde a quien realiza el tratamiento estar en condiciones de acreditar que ha obtenido el consentimiento del afectado pues, salvo las excepciones establecidas en la Ley, sólo el consentimiento justifica o legitima el tratamiento y dicha acreditación exige que la información a que se refiere el artículo 5 se realice de algún modo del que quede constancia por escrito>>.

Por lo tanto, en el caso que nos ocupa, Café Iruña S.A. no ha probado que los denunciantes fueran informados previamente a la instalación del sistema de videovigilancia de un modo expreso, claro e inequívoco, de conformidad con el artículo 5 de la LOPD.



## VI

Ahora bien, respecto del deber de informar de la existencia de una videocámara, la cámara recoge imágenes, lo que en definitiva supone un tratamiento de datos, según lo dispuesto en el artículo 3.c) de la LOPD, donde se define el tratamiento de datos como “operaciones y procedimientos técnicos de carácter automatizado o no, que, permiten la recogida, grabación, conservación, elaboración, modificación, bloque y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias”. Este criterio se complementa con lo dispuesto en el artículo 1 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 (en lo sucesivo Instrucción 1/2006), en sus artículos 1.1 y 2 señala lo siguiente:

*“Artículo 1.1. 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.”*

*“Artículo 2.*

*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.”*

Por ello, 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.*

*Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de tránsito, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento”.*

La obligación que impone este artículo 5 es, por tanto, la de informar al afectado en la recogida de datos, pues sólo así queda garantizado el derecho del afectado a tener una apropiada información y a consentir o no el tratamiento, en función de aquélla.

La Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, que delimita el contenido esencial del derecho fundamental a la protección de los datos personales, ha destacado la importancia del derecho de información en la recogida de datos, como un elemento indispensable de este derecho, en los siguientes términos: *“De suerte que, sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales (art. 5 LOPD) quedaría sin duda frustrado el derecho del interesado a controlar y disponer de sus datos personales, pues es claro que le impedirían ejercer otras facultades que se integran en el contenido del derecho fundamental al que estamos haciendo referencia”.*

Y añade la citada Sentencia que *“el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.*

*En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del*



*derecho a ser informado de quién posee sus datos personales y con qué fin, y, el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que rectifique o los cancele”.*

De ello cabe concluir que la vigente LOPD ha acentuado las garantías precisas para el tratamiento de los datos personales, vinculando el consentimiento del afectado a la información previa que reciba.

## VII

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.”*

Respecto a los clientes que acceden al local, el denunciado si consta que tiene instalado en la puerta de acceso al mismo un cartel informativo que indica la existencia de un sistema de videovigilancia con la siguiente leyenda: PARA SU TRANQUILIDAD, ESTA PROPIEDAD ESTÁ PROTEGIDA POR SISTEMAS DE SEGURIDAD Y GRABACION PERMANENTE DE IMÁGENES POR CCTV. LA DIRECCIÓN. SERCOIN. TELF. #####”. Si bien es recomendable la instalación del previsto en la Instrucción 1/2006, debiendo además instalar dentro del local dichos carteles informativos y tener a disposición de los clientes los impresos en los que se detalla la información prevista en el artículo 5. 1 de la LOPD.



Respecto a sus trabajadores, el denunciado, Café Iruña S.A., procedió a la instalación, a través de la entidad Sercoin Navarra S.L., de un sistema de videovigilancia en el interior del local sin poder acreditar que hubiera proporcionado a sus trabajadores, previamente a la instalación del sistema de seguridad, información expresa, clara, inequívoca del sistema de seguridad, al resultar aquellos, afectados por este tipo de tratamiento. El representante de dicha entidad no ha podido acreditar que haya informado a los denunciados, trabajadores de su empresa, previamente a la instalación de dicho sistema de videovigilancia por lo que cabe estimar cometida la infracción del artículo 5 de la LOPD, por la que se ha instruido el presente procedimiento.

A este respecto el artículo 18.1 del Real Decreto 1720/2007 ya citado establece que, el deber de información al que se refiere el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado.

## VIII

El artículo 44.2.d) de la citada LOPD, tipifica como infracción leve:

*“d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley”.*

En función de todo lo expuesto cabe apreciar la existencia de la infracción denunciada por cuanto el motivo de la instalación de las videocámaras era la grabación de imágenes de personas, que, tal y como anteriormente se ha referido, constituyen datos de carácter personal, no acreditándose que se informara de su existencia y finalidad, tal y como establece el artículo 5 de la LOPD y la Instrucción 1/2006.

## IX

En segundo lugar, se imputa a Café Iruña S.A., una infracción del artículo 26.1 de la LOPD, que 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”*

En el caso analizado, ha quedado acreditado que Café Iruña S.A., grababa las imágenes tanto de las personas que trabajaban en dicho establecimiento como de sus clientes, almacenándolas por un periodo no superior a 4 días.



Dado que Café Iruña S.A., recababa datos personales, a través del sistema de videovigilancia, debió notificar a esta Agencia la creación del fichero antes de iniciar la recogida de datos.

Sin embargo, en fecha 7 de agosto de 2007, Café Iruña S.A., no había procedido a la notificación e inscripción del fichero de videovigilancia, del que es responsable, en el Registro General de Protección de Datos de esta Agencia. Por tanto tales hechos suponen una vulneración del citado artículo 26.1 de la LOPD.

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.”*

Ahora bien, hay que hacer constar que en fecha 28 de mayo de 2008, se ha podido constatar la inscripción, por parte de Café Iruña, en el Registro General de Protección de Datos de esta Agencia del fichero denominado “Grabador Digital de Imágenes”, figurando como fecha de alta en el mismo el día 7 de septiembre de 2007.

## X

El artículo 44.2.c) de la LOPD califica de infracción leve la conducta siguiente:

*“c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave”.*

La citada infracción del artículo 26.1 de la LOPD encuentra su tipificación en el precepto transcrito.

## XI

En relación a los criterios de graduación de la sanción, el artículo 45.1, 4 de la LOPD, dispone:



*“1. Las infracciones leves serán sancionadas con multa de 601,01 a 60.101,21 euros.”*

*“4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora”.*

En el presente caso, ha quedado acreditado que la entidad Café Iruña tiene instaladas 13 cámaras de videovigilancia distribuidas por el interior del local. Dicha entidad tiene suscrito un contrato de instalación y mantenimiento de dicho sistema de videovigilancia desde el 23 de marzo de 2007, si bien fueron puestas en funcionamiento sin haberse acreditado por parte del denunciado que hubiera informado a los denunciados, trabajadores de su empresa, de una forma expresa, clara e inequívocamente de la existencia y finalidad de las mismas. Por lo tanto se ha producido una omisión del deber de información a los trabajadores de dicho establecimiento. Por otro lado cabe apreciar, respecto a la vulneración del artículo 26 de la LOPD, que el denunciado ha procedido a la inscripción del fichero en el Registro General de Protección de Datos de esta Agencia lo que denota una diligencia en su actuación.

En relación con la infracciones imputadas, en base a los criterios de graduación establecidos en el artículo 45.4 de la LOPD, y en especial, en función a la ausencia de beneficios obtenidos y de intencionalidad observadas en el presente procedimiento, así como la pronta actuación en la inscripción de los ficheros resultantes de la videovigilancia, procede la imposición de las sanciones en su cuantías mínimas.

Vistos los preceptos citados y demás de general aplicación,

El Director de la Agencia Española de Protección de Datos **RESUELVE:**

**PRIMERO: IMPONER** a la entidad **CAFÉ IRUÑA S.A.**, por una infracción del artículo 5 de la LOPD, tipificada como leve en el artículo 44.2.d) de dicha norma, una multa de 601,01 € (seiscientos un euro con un céntimo de euro) de conformidad con lo establecido en el artículo 45.1,4 de la citada Ley Orgánica.

**SEGUNDO: IMPONER** a la entidad **CAFÉ IRUÑA S.A.**, por una infracción del artículo 26 de la LOPD, tipificada como leve en el artículo 44.2.c) de dicha norma, una multa de 601,01 € (seiscientos un euro con un céntimo de euro), de conformidad con lo establecido en el artículo 45.1, 4 de la citada Ley Orgánica.



**TERCERO: NOTIFICAR** la presente resolución a **CAFÉ IRUÑA S.A.** con domicilio en (C/.....) y a **D. O.O.O. Y D. Z.Z.Z.** con domicilio en (C/.....)

**CUARTO:** Advertir al sancionado que la sanción impuesta deberá hacerla efectiva en el plazo de pago voluntario que señala el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso en la cuenta restringida nº 0000 0000 00 0000000000 abierta a nombre de la Agencia Española de Protección de Datos en el Banco Bilbao Vizcaya Argentaria, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo. Si recibe la notificación entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si recibe la notificación entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

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.

Madrid, 30 de septiembre de 2008

EL DIRECTOR DE LA AGENCIA ESPAÑOLA  
DE PROTECCIÓN DE DATOS



Fdo.: Artemi Rallo Lombarte