



Expediente N°: E/00614/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **ACCOR HOTELES ESPAÑA** y **MNEMON GROUP** en virtud de denuncia presentada por D^a. **A.A.A.** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 11 de octubre de 2013 tiene entrada en esta Agencia escrito de D^a. **A.A.A.** (en adelante la denunciante) comunicando posible infracción a la Ley Orgánica 15/1999 motivada por la existencia de cámaras de videovigilancia cuyo titular es la entidad **ACCOR HOTELES ESPAÑA** (en adelante el denunciado) instaladas en el establecimiento con denominación comercial "**HOTEL NOVOTEL GIRONA**" ubicado en (C/.....1) (**GIRONA**), enfocado hacia vía pública.

La denunciante manifiesta ser la coordinadora de una empresa externa que trabaja subcontratada con el **HOTEL NOVOTEL GIRONA**, y que el correo ordinario que le llega a su nombre de la empresa de limpieza con la que trabaja, se lo abre muchas veces la secretaria del hotel y el sr. director sin su consentimiento, en estos documentos salen reflejadas las nóminas suyas y de sus empleadas como también contratos en el que están sus datos personales y otros.

Se han quejado durante tiempo al director de este hotel y a su empresa **MNEMON GROUP SL** y no le hacen caso, dicen que no tiene importancia.

También informa del incumplimiento de videovigilancia en la entrada del hotel sin la información previa: están grabando datos de vehículos y personas de la vía pública.

Adjunta copia de DNI, reportaje fotográfico y sobre de la empresa **MNEMON GROUP SL** con dirección del hotel a la atención del Responsable del Dpto Limpieza.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

1. Con fecha 13 de febrero de 2014 se solicita información al responsable del establecimiento teniendo entrada en esta Agencia con fecha 7 y 17 de marzo escrito del denunciado en el que manifiesta:

El representante del denunciado aporta copia del poder notarial que le otorga la representación.

El responsable del local es la representada **ACCOR HOTELES ESPAÑA, S.A.**

La finalidad de la instalación de las cámaras en el **HOTEL NOVOTEL GIRONA**, perteneciente a la cadena hotelera **ACCOR** es la de vigilancia y protección de bienes y personas.

Las mencionadas cámaras fueron instaladas por la empresa especializada y

autorizada **COMSAT SEGURETAT, S.L.**, cuyo contrato de prestación de servicio se adjunta como Documento 1.

El bien vigilado y protegido no es otro que la propia finca, el hotel construido en su interior y las personas que acceden y se alojan en dichas instalaciones. Las cámaras, ubicadas en el jardín, enfocan hacia las dos direcciones que marcan el camino de entrada al Hotel. Cada cámara enfoca en una dirección para no dejar ángulos muertos. Una de ellas enfoca desde el portal de entrada en dirección a la rampa que lleva a la entrada del Hotel y la otra enfoca hacia el portal de entrada al recinto.

Adicionalmente, estas cámaras tienen sendas máscaras de privacidad implementadas por software que evitan la obtención y visualización en el monitor ubicado en el interior del Hotel de imágenes que excedan del perímetro de las instalaciones del mismo, entendiéndose aquí comprendido su jardín, siendo imposible la identificación a través de las cámaras de cualquier persona que se ubique fuera del recinto, según puede apreciarse en las fotografías adjuntas como Documento 2 (imágenes 2 y 3).

Se acompaña como Documento 3 el cartel utilizado para dar cumplimiento al principio de información y las fotografías de los mismos instalados en el Hotel. Estos carteles se encuentran ubicados de manera claramente visible en todos los puntos de acceso a la propiedad, incluyendo entradas de vehículos. El cartel hace referencia a **"ACCOR HOTELES ESPAÑA, S.A."** como responsable del tratamiento y a la dirección **"(C/.....1), Gerona"**, como dirección a la que pueden dirigirse las solicitudes de derechos de acceso, rectificación, cancelación y oposición (en adelante, "derechos ARCO").

Existen impresos informativos que están en todo momento a disposición de los ciudadanos en la recepción del Hotel. En dichos impresos constan los detalles completos del responsable del tratamiento a efectos del ejercicio de los derechos ARCO, al igual que en el cartel informativo referido anteriormente, junto con la restante información prevista legalmente. Se acompaña al presente escrito, como Documento 4 el modelo de formulario informativo en cuestión en relación con el tratamiento de los datos que, en su caso, pueda tener lugar con motivo de la instalación del sistema de videovigilancia.

En cuanto al procedimiento de distribución de formularios, los mismos se encuentran, preimpresos y preparados, a disposición de los interesados, en el mostrador de recepción del Hotel, conociendo el personal de ACCOR su obligación de entregarlos al solicitante.

Existe un sistema de videovigilancia limitado a dos cámaras y un monitor de visualización.

El croquis que se aporta como Documento 5, muestra las dos cámaras que forman parte del sistema de videovigilancia. Las dos cámaras están instaladas sobre un poste de la entrada al recinto del Hotel para vigilar el acceso. La Cámara 1 enfoca hacia la rampa de acceso al edificio del Hotel y la Cámara 2 enfoca hacia el portal de entrada en la propiedad, cubriendo el ángulo muerto que deja la Cámara 1 para vigilar la entrada al recinto.

Ninguna de las dos cámaras dispone de zoom o de posibilidad de movimiento.

En el Documento 2 se puede ver el monitor de visualización de las imágenes

captadas por las cámaras instaladas.

Se acompaña como Documento 2 (Imagen 1), fotografía de las cámaras incluidas en el croquis, indicando el número de cámara, junto con las correspondientes imágenes que capta cada una de dichas cámaras. Como aclaración, las imágenes que constan en el Documento 2 (imágenes 2 y 3) son fotografías hechas al monitor que muestra, en tiempo real, las imágenes captadas por las cámaras.

Las personas que cuentan con acceso al sistema de videovigilancia son exclusivamente los empleados de ACCOR que trabajan en las instalaciones del Hotel y que precisan dicho acceso para el desempeño de sus funciones. En concreto, acceden al sistema de videovigilancia los empleados con los siguientes cargos: director, jefe de servicio y encargado de mantenimiento. Ningún tercero tiene acceso al sistema de videovigilancia.

El sistema de videovigilancia instalado no graba las imágenes que se obtienen. En su lugar, las mismas son proyectadas en tiempo real en el correspondiente monitor instalado en el "back-office" u oficina en la trastienda tal y como se puede apreciar en las fotografías adjuntas como Documento 2 (imágenes 6, 7 y 8). En concreto, se eligió esta ubicación del monitor de visualización de las imágenes captadas para garantizar que tan sólo las personas autorizadas puedan acceder a las mismas, restringiendo así su acceso por toda persona no autorizada.

El sistema de videovigilancia no está conectado a ninguna central de alarmas.

2. Con fecha 24 de febrero de 2014 se solicita información a **MNEMON GROUP** teniendo entrada en esta Agencia con fecha 7 de marzo escrito en el que quien se identifica como administrador único manifiesta:

Respecto de la Razón Social de la empresa y número de CIF: La empresa **MNEMON**, tiene su razón social (**C/.....2**) (**Madrid**)

Respecto de la especificación detallada del procedimiento de envío por correo ordinario a sus trabajadores de la información relativa a su relación con la empresa, ya sean nóminas; contratos de trabajo o cualquier otra y medidas adoptadas para asegurar la confidencialidad del envío:

- o Las nóminas de los trabajadores son entregadas en mano por las coordinadoras del proyecto a que se refiera, en reuniones mensuales, así como cualquier documentación que se refiera a la relación de la empresa con los trabajadores.
- o Elaboradas las nóminas por el personal de administración, autorizados para acceder al fichero de nóminas con su usuario y contraseña, son metidas en sobres y entregadas a las coordinadoras que hacen el reparto.
- o Las coordinadoras, además, tienen autorización para acceder al fichero de nóminas con su usuario y contraseña.
- o No se envía ningún tipo de documentación que se refiera a la relación de la empresa con sus trabajadores por correo electrónico u ordinario

- o Los ficheros de nóminas de la empresa **MNEMON GROUP** están declarados en la Agencia de Protección de Datos y que cumplen todos los requisitos de la LOPD.

FUNDAMENTOS DE DERECHO

I

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

II

En primer lugar procede situar el contexto normativo en materia de videovigilancia. Así el artículo 1 de la LOPD dispone: *“La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar”*

En cuanto al ámbito de aplicación de la LOPD, el artículo 2.1 de la misma señala: *“La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado”*, definiéndose el concepto de dato de carácter personal en el apartado a) del artículo 3 de la LOPD, como *“Cualquier información concerniente a personas físicas identificadas o identificables”*.

El artículo 3 de la LOPD define en su letra c) el tratamiento de datos como aquellas *“operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias”*.

El artículo 5.1. f) del 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.

La Exposición de Motivos de la Instrucción 1/2006, de 8 de noviembre, de esta Agencia Española de Protección de Datos, relativa al tratamiento de los datos con fines de videovigilancia señala que: *“La seguridad y la vigilancia, elementos presentes en la sociedad actual, no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos, para de esta manera mantener la confianza de la ciudadanía en el sistema democrático”*. Sigue señalando: *“Las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999...”*.

La garantía del derecho a la protección de datos, conferida por la normativa de referencia, requiere que exista una actuación que constituya un tratamiento de datos personales en el sentido expresado. En otro caso las mencionadas disposiciones no serán de aplicación.

Por su parte, la citada Instrucción 1/2006, dispone en su artículo 1.1 lo siguiente:

“1. La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras.

El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas.

Se considerará identificable una persona cuando su identidad pueda determinarse mediante los tratamientos a los que se refiere la presente instrucción, sin que ello requiera plazos o actividades desproporcionados.

Las referencias contenidas en esta Instrucción a videocámaras y cámaras se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita los tratamientos previstos en la misma.”

La Instrucción 1/2006 en su artículo 2 establece lo siguiente:

“1. Sólo será posible el tratamiento de los datos objeto de la presente instrucción, cuando se encuentre amparado por lo dispuesto en el artículo 6.1 y 2 y el artículo 11.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Sin perjuicio de lo establecido en el apartado anterior la instalación de cámaras y videocámaras deberá respetar en todo caso los requisitos exigidos por la legislación vigente en la materia.”

De lo anteriormente expuesto se desprende que el concepto de dato personal, según la definición de la LOPD, requiere la concurrencia de un doble elemento: por una parte, la existencia de una información o dato y, por otra, que dicho dato pueda vincularse a una persona física identificada o identificable, por lo que la imagen de una persona física identificada o identificable constituye un dato de carácter personal.

De acuerdo con los preceptos transcritos, la cámara reproduce la imagen de los afectados por este tipo de tratamientos y, a efectos de la LOPD, la imagen de una persona constituye un dato de carácter personal, toda vez que la información que capta concierne a personas que las hacen identificadas o identificables y suministra información sobre la imagen personal de éstas, el lugar de su captación y la actividad desarrollada por el individuo al que la imagen se refiere.

III

En el presente D^a. **A.A.A.** denuncia la instalación por un lado, de un sistema de videovigilancia ubicado en el HOTEL NOVOTEL GIRONA que pudiera vulnerar la normativa e protección de datos, y por otra parte , que el correo ordinario que le llega a su nombre a la denunciante, de la empresa de limpieza para la que trabaja, se lo abren sin su consentimiento la secretaria y el Director del hotel.

En primer lugar, respecto a la denuncia efectuada por la denunciante de apertura del correo ordinario que llega a su nombre, sin su consentimiento, por parte del Hotel Novotel Girona cabe decir que solicitada información, por parte de la Inspección de Datos de esta Agencia, a la empresa **MNEMON GROPUR S.L.** (empresa subcontratada por el Hotel, para la que la denunciante presta sus servicios) ésta manifiesta que, respecto de la especificación detallada del procedimiento de envío por correo ordinario a sus trabajadores de la información relativa a su relación con la empresa, ya sean nóminas; contratos de trabajo o cualquier otra y medidas adoptadas para asegurar la confidencialidad del envío, el procedimiento es el siguiente:

- o Las nóminas de los trabajadores son entregadas en mano por las coordinadoras del proyecto a que se refiera, en reuniones mensuales, así como cualquier documentación que se refiera a la relación de la empresa con los trabajadores.
- o Elaboradas las nóminas por el personal de administración, autorizados para acceder al fichero de nóminas con su usuario y contraseña, son metidas en sobres y entregadas a las coordinadoras que hacen el reparto.
- o Las coordinadoras, además, tienen autorización para acceder al fichero de nóminas con su usuario y contraseña.
- o No se envía ningún tipo de documentación que se refiera a la relación de la empresa con sus trabajadores por correo electrónico u ordinario.

A este respecto, la denunciante no aporta más elemento que pueda corroborar sus afirmaciones, que sus propias manifestaciones, lo cual se articula como insuficiente para iniciar procedimiento administrativo sancionador alguno, en materia de protección de datos de carácter personal, dado que para ello es necesario que exista una mínima

aportación probatoria que permita identificar la existencia de indicios de infracción de la normativa en materia de protección de datos de carácter personal y que permita desvirtuar el principio a la presunción de inocencia que es aplicable a todo administrado.

Así las cosas, hemos de tener en cuenta que, en base a sus especiales consecuencias, el derecho administrativo sancionador es especialmente garantista con los administrados, por lo que le son de aplicación, sin excepciones, pero con matices, los principios del procedimiento penal, destacando entre ellos el principio de presunción de inocencia, el cual ha de ser respetado en la imposición de cualesquiera sanciones, pues el ejercicio del *ius puniendi* en sus diversas manifestaciones está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones.

Así, la activación de un procedimiento ha de fundamentarse en una mínima aportación de elementos que puedan justificar el inicio de actuaciones, no pudiendo fundamentarse en afirmaciones no debidamente acreditadas, más aún cuando al respecto puede entrar en liza un juego de contradicción entre lo afirmado por cada una de las partes, sin un sustento probatorio que refuerce las argumentaciones de cada uno y que permita sostener un procedimiento sancionador.

El Tribunal Constitucional, en Sentencia 76/1990 considera que el derecho a la presunción de inocencia comporta :

“que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio”.

De acuerdo con este planteamiento, el artículo 130.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en lo sucesivo LRJPAC), establece que:

“Sólo podrán ser sancionados por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aun a título de simple inobservancia.”

La Sentencia del Tribunal Constitucional de 20/02/1989 indica que:

“Nuestra doctrina y jurisprudencia penal han venido sosteniendo que, aunque ambos puedan considerarse como manifestaciones de un genérico favor rei, existe una diferencia sustancial entre el derecho a la presunción de inocencia, que desenvuelve su eficacia cuando existe una falta absoluta de pruebas o cuando las practicadas no reúnen las garantías procesales y el principio jurisprudencial in dubio pro reo que pertenece al momento de la valoración o apreciación probatoria, y que ha de juzgar

cuando, concurre aquella actividad probatoria indispensable, exista una duda racional sobre la real concurrencia de los elementos objetivos y subjetivos que integran el tipo penal de que se trate.”

Asimismo, se debe tener en cuenta, en relación con el principio de presunción de inocencia lo que establece el art. 137 de LRJPAC:

“1. Los procedimientos sancionadores respetarán la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario.”

En definitiva, de acuerdo a todo lo anterior, la aplicación del principio de presunción de inocencia impide imputar una infracción administrativa cuando no se haya obtenido y comprobado la existencia de una prueba de cargo acreditativa de los hechos que motivan esta imputación, por lo que para este caso, no existen evidencias materiales de infracción por parte del denunciado, más que las propias afirmaciones de la denunciante, por lo que en cuanto a esta cuestión procede el archivo del presente expediente de actuaciones previas.

IV

En segundo lugar, manifiesta la denunciante la existencia de un sistema de videovigilancia en la entrada al Hotel incumpliendo el deber de información y captando imágenes de la vía pública.

Así, debe entrarse a valorar en primer lugar el cumplimiento del deber de información por parte del establecimiento denunciado.

En primer lugar, hay que señalar que las cámaras de videovigilancia aunque no graben, recogen 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”*.

Así el criterio establecido respecto a esta materia en la LOPD, se complementa con lo dispuesto en el artículo 1 de la Instrucción 1/2006 donde se delimita el ámbito subjetivo de ésta señalando que:

“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”.

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”.

En cuanto al modo en que haya de facilitarse dicha información, debe tenerse en cuenta el artículo 3 de la Instrucción 1/2006 que establece que *“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 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 pueden 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.”

Por tanto la reproducción de imágenes a tiempo real, como es el caso que nos

ocupa, suponen un tratamiento de datos personales al amparo no sólo desde el ámbito de aplicación de la Instrucción 1/2006, sino de la Ley Orgánica 15/1999. Ahora bien, sobre la cuestión sobre si este tipo de tratamiento, genera o no fichero, es preciso indicar que el artículo 7.2 de la Instrucción 1/2006, establece: *“A estos efectos, no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real”*.

En consecuencia, al amparo de lo dispuesto en los artículos 3 y 7.2 de la Instrucción 1/2006, la utilización de sistemas de videocámaras con fines de seguridad, que no graban imágenes, constituyen un tratamiento de datos que obliga a informar del mismo, pero no genera ningún fichero, si bien esto no exime del cumplimiento del resto de deberes establecidos por la LOPD y la Instrucción 1/2006. No obstante, en el caso de que el establecimiento denunciado decidiera proceder a su grabación deberá previamente proceder a la inscripción de dicho fichero, en el Registro General de Protección de Datos de esta Agencia

En el presente caso se aportan por el Hotel fotografías de la existencia de carteles informativos de la existencia de las cámaras ubicados en todos los puntos de acceso al Hotel, incluyendo entradas de vehículos. Dichos carteles son acordes al previsto en el artículo 3 a) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD. Asimismo, se aportan formulario informativo a disposición de los interesados en la recepción del Hotel, de conformidad con el artículo 3. b) de la citada Instrucción.

Por lo tanto el Hotel Novotel Girona cumple el deber de información respecto al sistema de videovigilancia.

Por último, respecto a la captación de imágenes de la vía pública, hay que señalar que para entender las especialidades derivadas del tratamiento de las imágenes en vía pública, es preciso conocer la regulación que sobre esta materia se contempla en el artículo 1 de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos que establece: *“La presente Ley regula la utilización por las Fuerzas y Cuerpos de Seguridad de videocámaras para grabar imágenes y sonidos en lugares públicos abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública”*.

Este precepto es preciso ponerlo en relación con lo dispuesto en el artículo 3 e) de la Ley Orgánica 15/1999, donde se prevé que: *“Se registrarán por sus disposiciones específicas y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:*

e) Los procedentes de las imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia”.

En virtud de todo lo expuesto, podemos destacar que la instalación de videocámaras en lugares públicos es competencia exclusiva de las Fuerzas y Cuerpos de Seguridad, de ahí que la legitimación para el tratamiento de dichas imágenes se complete en la Ley Orgánica 4/1997, señalándose en su artículo 2.2, en lo que hace mención a su ámbito de aplicación que *“2.2. Sin perjuicio de las disposiciones específicas contenidas en la presente Ley, el tratamiento automatizado de las imágenes y sonidos se regirá por lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizados de los Datos de Carácter Personal.”*

Así, la legitimación para el uso de instalaciones de videovigilancia se ciñe a la protección de entornos privados. La prevención del delito y la garantía de la seguridad en las vías públicas corresponden en exclusiva a las Fuerzas y Cuerpos de Seguridad del Estado.

No obstante, en algunas ocasiones la protección de los espacios privados sólo es posible si las cámaras se ubican en espacios como las fachadas. A veces, también resulta necesario captar los accesos, puertas o entradas, de modo que aunque la cámara se encuentre en el interior del edificio, resulta imposible no registrar parte de lo que sucede en la porción de vía pública que inevitablemente se capta. Por otra parte, las videocámaras deberán orientarse de modo tal que su objeto de vigilancia principal sea el entorno privado y la captación de imágenes de la vía pública sea la mínima imprescindible. Así, el artículo 4.1 y 2 de la LOPD, garantiza el cumplimiento del principio de proporcionalidad en todo tratamiento de datos personales, cuando señala 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”.

En este sentido, se pronuncia la Instrucción 1/2006, cuando señala en el artículo 4, lo siguiente:

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”.

Para que la excepción recogida en el artículo 4.3 de la Instrucción 1/2006 resulte aplicable no deberá existir una posibilidad de instalación alternativa, sin poder interpretarse que dicho precepto constituye una habilitación para captar imágenes en espacios públicos, puesto que en ningún caso puede admitirse el uso de prácticas de vigilancia más allá del entorno objeto de la instalación y en particular en lo que se refiere a los espacios públicos circundantes, edificios contiguos y vehículos distintos de los que accedan al espacio vigilado.

Pues bien, una vez explicada esta cuestión, cabe decir que las dos cámaras objeto de denuncia están instaladas en un poste de la entrada al recinto del Hotel para vigilar el acceso. Una de las cámaras enfoca la rampa de acceso al Hotel para vigilar el acceso y la otra cámara enfoca hacia el portal de entrada en la propiedad, cubriendo el ángulo muerto que deja la cámara primera para vigilar la entrada al recinto. Ninguna de las dos cámaras dispone de zoom ni posibilidad de movimiento. Aportan las imágenes que captan ambas cámaras de las que se desprende, que las mismas capturan zonas de la entrada del interior del recinto del Hotel encontrándose el resto de la imagen en ambas cámaras velado con una máscara de privacidad que impide captar zonas del exterior del recinto. Por lo tanto, las imágenes captadas no infringen el principio de proporcionalidad de los datos previsto en el artículo 4.1 de la Ley Orgánica de Protección de Datos, cuando se habla de que 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. Así la citada cámara, realizaría un tratamiento proporcional de las imágenes, en relación con el ámbito y las finalidades que podrían justificar su recogida, sin captar imágenes de la vía pública.

Por tanto, siguiendo el criterio de la citada Instrucción 1/2006, no puede considerarse, en el presente caso, que la instalación de las videocámaras en los términos expuestos vulnere los principios de calidad, proporcionalidad y finalidad del tratamiento.

A la vista de todo lo expuesto, se procede al archivo del presente expediente de actuaciones previas al no apreciarse vulneración a la actual normativa en materia de protección de datos.

Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:



1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a **ACCOR HOTELES ESPAÑA, MNEMON GROUP** y 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 Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

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