

Expediente Nº: E/01719/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **GRUPO HOSTELERO PAREDES S.L** en virtud de denuncia presentada por la **DIRECCION GENERAL DE LA GUARDIA CIVIL** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha de 17 de enero de 2013 tiene entrada en esta Agencia escrito remitido por la DIRECCIÓN GENERAL DE LA GUARDIA CIVIL, en el que se remite informe de la COMANDANCIA DE MURCIA – COMPAÑÍA DE TORRE PACHECO-PAPIF DE CABO DE PALOS, comunicando posible infracción a la Ley Orgánica 15/1999 motivada por la existencia de cámaras de videovigilancia, en el establecimiento con denominación comercial **HOTEL MOU** sito en (C/.....1) (**MURCIA**) y cuyo titular es la sociedad **GRUPO HOSTELERO PAREDES S.L** (en adelante el denunciado).

En el mencionado informe, la Comandancia de la Guardia Civil manifiesta que durante inspección realizada en el establecimiento denunciado se observa un sistema de videovigilancia de CCTV con grabación de imágenes, compuesto por tres cámaras de las cuales dos enfocan a la vía pública. No existe cartel informativo en lugar visible que advierta sobre la existencia de cámaras de videovigilancia y no dispone de impresos informativos sobre el tratamiento de datos personales.

Adjunta a su denuncia reportaje fotográfico.

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 19 de abril de 2013 se solicita información al titular del sistema dirigida a la dirección del establecimiento denunciado, resultando la misma devuelta por el servicio de Correos con la indicación "AUSENTE REPARTO".
2. Con fecha 14 de mayo de 2013 se reitera la solicitud de información dirigida al domicilio del responsable y gerente del establecimiento según se indica en el acta de denuncia, resultando la misma recepcionada con fecha 20 de mayo de 2013.
3. Con fecha 24 de julio de 2013 se solicita información a la GERENCIA MUNICIPAL DE URBANISMO DEL AYUNTAMIENTO DE CARTAGENA en relación a la titularidad del establecimiento denunciado. Teniendo entrada en esta Agencia escrito de fecha 26 de agosto de 2013 en el que el Jefe del Departamento Administrativo de Licencias de Actividad comunica:

*El titular de la licencia para actividad de Café Bar Restaurante en XXXXXXXXXXXX, s/n (C/.....1), es **GRUPO HOSTELERO***

PAREDES S.L; con domicilio a efectos de notificaciones en (C/.....2)...

4. Con fecha 24 de julio de 2013 se solicita colaboración a la OFICINA DE SEGURIDAD CIS DE LA GUARDIA CIVIL, con objeto de realizar las actuaciones oportunas encaminadas a la investigación del sistema de videovigilancia denunciado. Teniendo entrada en esta Agencia escrito de fecha 26 de septiembre de 2013 en el que la **Patrulla Fiscal y de Fronteras, Base en Cabo de Palos**, informa:

*Personados agentes de la Guardia Civil en el establecimiento denominado HOTEL MOU, sito en (C/.....1) y entrevistados con el administrador de la empresa **GRUPO HOSTELERO PAREDES S.L**, en calidad de titular del citado local, éste manifiesta desconocer la persona o empresa que realizó la instalación del sistema de videovigilancia...no teniendo en su poder documento alguno que pueda constatar dicha instalación. Asimismo comunica que las cámaras no están en funcionamiento y que únicamente tienen una finalidad disuasoria.*

No existe cartel alguno que informe del sistema de cámaras de videovigilancia así como tampoco disponen de modelo de formulario informativo a disposición de los ciudadanos.

Se comprueba la existencia de seis videocámaras, ubicadas en los siguientes lugares:

- o Cámara 1: sistema fijo, instalada en la pared del patio trasero propio del local y enfocada hacia el patio.*
- o Cámara 2: sistema fijo, instalada en el comedor de trabajadores y enfocando las mesas del comedor.*
- o Cámara 3: sistema móvil, instalada en la recepción del local y enfocando el mostrador.*
- o Cámara 4 y Cámara 5: sistema fijo y móvil respectivamente, instaladas a ambos extremos de la barra del bar y enfocando hacia la misma.*
- o Cámara 6: sistema móvil, instalada en la puerta de acceso desde el parking al local y enfocando hacia la pista de baile.*

Los agentes en el momento de la inspección hacen constar que las cámaras no están conectadas.

Se constata que no existen monitores donde se visualicen las imágenes así como tampoco dispositivo de grabación.

El administrador de la empresa denunciada muestra a los agentes el lugar en el que dice que estaba instalado el antiguo sistema de visualización y grabación de imágenes. En el momento de la inspección únicamente se encuentra un monitor desenchufado de la toma de alimentación y datos no existiendo dispositivo de grabación alguno.

Se adjunta reportaje fotográfico de la ubicación de las cámaras y las zonas susceptibles de grabación.

El sistema de videovigilancia no se encuentra conectado a ninguna

central de alarma.

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 la materia de videovigilancia en su contexto normativo. 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.” (el subrayado es de la Agencia Española de Protección de Datos).

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 caso que nos ocupa, se denuncia la existencia de un sistema de videovigilancia instalado en el establecimiento con denominación comercial **HOTEL MOU**, contraviniendo la normativa de protección de datos.

Con fecha 24 de julio de 2013 se solicita, por los Servicios de Inspección de estas Agencia, colaboración a la OFICINA DE SEGURIDAD CIS DE LA GUARDIA CIVIL, con objeto de realizar las actuaciones oportunas encaminadas a la investigación del sistema de videovigilancia denunciado, teniendo entrada en esta Agencia escrito de fecha 26 de septiembre de 2013 en el que la **Patrulla Fiscal y de Fronteras, Base en Cabo de Palos**, informa:

*Personados agentes de la Guardia Civil en el establecimiento denominado HOTEL MOU, sito en (C/.....1) y entrevistados con el administrador de la empresa **GRUPO HOSTELERO PAREDES S.L.**, en calidad de titular del citado local, éste manifiesta desconocer la persona o empresa que realizó la instalación del sistema de videovigilancia...no teniendo en su poder documento alguno que pueda constatar dicha instalación. Asimismo comunica que las cámaras no están en funcionamiento y que únicamente tienen una finalidad disuasoria.*

No existe cartel alguno que informe del sistema de cámaras de videovigilancia así como tampoco disponen de modelo de formulario informativo a disposición de los ciudadanos.

Se comprueba la existencia de seis videocámaras, ubicadas en los siguientes lugares:

- o *Cámara 1: sistema fijo, instalada en la pared del patio trasero propio del local y enfocada hacia el patio.*
- o *Cámara 2: sistema fijo, instalada en el comedor de trabajadores y enfocando las mesas del comedor.*
- o *Cámara 3: sistema móvil, instalada en la recepción del local y*

enfocando el mostrador.

- o *Cámara 4 y Cámara 5: sistema fijo y móvil respectivamente, instaladas a ambos extremos de la barra del bar y enfocando hacia la misma.*
- o *Cámara 6: sistema móvil, instalada en la puerta de acceso desde el parking al local y enfocando hacia la pista de baile.*

Los agentes en el momento de la inspección hacen constar que las cámaras no están conectadas.

Se constata que no existen monitores donde se visualicen las imágenes así como tampoco dispositivo de grabación.

El administrador de la empresa denunciada muestra a los agentes el lugar en el que dice que estaba instalado el antiguo sistema de visualización y grabación de imágenes. En el momento de la inspección únicamente se encuentra un monitor desenchufado de la toma de alimentación y datos no existiendo dispositivo de grabación alguno.

Por lo tanto a la fecha de inspección por parte del citado cuerpo el sistema de videovigilancia no se encuentra operativo ni existe dispositivo de grabación alguno

Así, no puede obviarse que al Derecho Administrativo Sancionador le son de aplicación, con alguna matización pero sin excepciones, los principios inspiradores del orden penal, resultando clara la plena virtualidad de los principios de presunción de inocencia. La presunción de inocencia debe regir sin excepciones en el ordenamiento sancionador y ha de ser respetada 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. En tal sentido, 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 aún a título de simple inobservancia.*”

Conforme señala el Tribunal Supremo (STS 26/10/98) el derecho a la presunción de inocencia “*no se opone a que la convicción judicial en un proceso pueda formarse sobre la base de una prueba indiciaria, pero para que esta prueba pueda desvirtuar dicha presunción debe satisfacer las siguientes exigencias constitucionales: los indicios han de estar plenamente probados – no puede tratarse de meras sospechas – y tiene que explicitar el razonamiento en virtud del cual, partiendo de los indicios probados, ha llegado a la conclusión de que el imputado realizó la conducta infractora, pues, de otro*

modo, ni la subsunción estaría fundada en Derecho ni habría manera de determinar si el proceso deductivo es arbitrario, irracional o absurdo, es decir, si se ha vulnerado el derecho a la presunción de inocencia al estimar que la actividad probatoria pueda entenderse de cargo.”

El Tribunal Constitucional, en su Sentencia 24/1997, tiene establecido que “los criterios para distinguir entre pruebas indiciarias capaces de desvirtuar la presunción de inocencia y las simples sospechas se apoyan en que:

a) La prueba indiciaria ha de partir de hechos plenamente probados.

b) Los hechos constitutivos de delito deben deducirse de esos indicios (hechos completamente probados) a través de un proceso mental razonado y acorde con las reglas del criterio humano, explicitado en la sentencia condenatoria (SSTC 174/1985, 175/1985, 229/1988, 107/1989, 384/1993 y 206/1994, entre otras).”

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.”

En definitiva, aquellos principios impiden imputar una infracción administrativa cuando no se haya obtenido y acreditado una prueba de cargo acreditativa de los hechos que motivan esta imputación o de la intervención en los mismos del presunto infractor, aplicando el principio “*in dubio pro reo*” en caso de duda respecto de un hecho concreto y determinante, que obliga en todo caso a resolver dicha duda del modo más favorable al interesado.

En el presente caso, al no haberse acreditado el funcionamiento del sistema de videovigilancia denunciado, no se ha podido constatar la captación o grabación de imágenes de datos personales por parte del denunciado, contraviniendo la normativa de protección de datos, ni siquiera consta, según manifiesta el informe elaborado por la Guardia Civil con fecha de entrada en esta Agencia el 26 de septiembre de 2013, que se enfoque espacio público generando una indebida expectativa de captación de imágenes, por lo que se procede al archivo del presente expediente de actuaciones previas.

No obstante, a pesar de que se proceda al archivo del presente expediente por los motivos expuestos, la mercantil titular del establecimiento denunciado debe tener en

cuenta los requisitos que se desarrollan seguidamente, en materia de videovigilancia, por si decidiera en un futuro proceder a poner en funcionamiento el citado sistema.

Así, en primer lugar debe indicarse que no es necesario ninguna autorización para la instalación de un sistema de videovigilancia, si bien, el tratamiento de las imágenes deberá cumplir los requisitos exigibles en materia de protección de datos de Carácter Personal, recogidos en la Ley Orgánica y, en particular, en la Instrucción 1/2006 de la Agencia Española de Protección de Datos, como son, entre otros, los relativos a que las imágenes que se capten sean las necesarias y no excesivas para la finalidad perseguida; el deber de informar a los interesados, tanto a través de la colocación de carteles informativos como mediante la puesta a disposición de aquéllos de impresos en que se detalle la información; la notificación de la existencia de los ficheros a la Agencia Española de Protección de Datos; o la implantación de medidas de seguridad.

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”.

Tal y como marca la Instrucción, las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999 y el artículo 5 del Real Decreto 1720/2007, de 21 de diciembre, que considera como dato de carácter personal la información gráfica o fotográfica. Se excluyen el tratamiento de imágenes en el ámbito personal y doméstico, entendiéndose por tal el realizado por una persona física en el marco de una actividad exclusivamente privada o familiar.

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, 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”*.

No obstante, en el caso de que el responsable del sistema de videovigilancia decidiera proceder a la grabación de las imágenes obtenidas por el mismo, deberá previamente proceder, a la inscripción de dicho fichero, en el Registro General de Protección de Datos de esta Agencia, según recoge el artículo 7 de la Instrucción 1/2006 y 26.1 de la LOPD.

Asimismo, 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.

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.

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.

Los datos serán cancelados (mediante bloqueo) en el plazo máximo de un mes desde su captación.

El responsable deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado. Asimismo cualquier persona que por razón del ejercicio de sus funciones tenga acceso a los datos deberá de observar la debida reserva, confidencialidad y sigilo en relación con las mismas. El responsable deberá informar del deber de secreto a las personas con acceso a los 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 **GRUPO HOSTELERO PAREDES S.L** y a la **DIRECCION GENERAL DE LA GUARDIA CIVIL**.

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.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la citada LJCA, sólo podrá interponer 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 LJCA, 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