



Expediente N°: E/05778/2016

### RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante **UNIVERSIDAD INTERNACIONAL DE LA RIOJA** en virtud de denuncia presentada por D. **C.C.C.** y teniendo como base los siguientes

#### HECHOS

**PRIMERO:** Con fecha 11 de octubre de 2016 tiene entrada en esta Agencia escrito de D. **C.C.C.** (en adelante el denunciante) comunicando posible infracción a la Ley Orgánica 15/1999 motivada por cámaras de videovigilancia cuyo titular es la entidad **UNIVERSIDAD INTERNACIONAL DE LA RIOJA** (en adelante el denunciado) instaladas en el recinto de la "**UNIVERSIDAD INTERNACIONAL DE LA RIOJA**" ubicado en **A.A.A.**.

El denunciante manifiesta que en el recinto de la universidad hay instaladas cámaras de videovigilancia a una altura superior a la valla perimetral que pudieran estar captando imágenes de la viviendas colindantes, incluida la suya. Adjunta 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:

Con fecha 1 de febrero de 2017 se solicita información al denunciado, teniendo entrada en esta Agencia con fecha 21 de febrero de 2017 escrito del mismo en el que manifiesta:

- El responsable del fichero del sistema de videovigilancia es la UNIVERSIDAD INTERNACIONAL DE LA RIOJA, S.A. con C.I.F. \*\*\*CIF.1.
- La mercantil que realizó la instalación de las citadas cámaras fue INGELEC RIOJA, S.L., empresa subcontratada por CONSTRUCCIONES AMENABAR S.A., a quién la mercantil ÍNSULA RIOJANA, S.L. propietaria del edificio, le encomendó la reforma integral del mismo y que actualmente están alquiladas por la UNIR.
- Las finalidades con las que se están tratando las imágenes son las de garantizar la seguridad de los bienes y de las personas que se encuentran dentro las instalaciones o que transitan las mismas.
- Respecto a los carteles donde se informa de la existencia de cámaras de videovigilancia y en los que se informa de los extremos que exige el artículo 5 de LOPD, esto es, de la identidad del responsable ante quien se pueden ejercitar los derechos de acceso, rectificación, cancelación y oposición, están ubicados en:
  - > El interior del edificio, en el mostrador de la recepción.
  - > El exterior del edificio en las puertas de acceso peatonales.
- El sistema dispone de 27 cámaras sin posibilidad de movimiento automatizado y que no disponen de zoom.

Aportan planos de situación donde se señala la ubicación de cada una de las cámaras numeradas, así como de los carteles de videovigilancia.

Aportan reportaje fotográfico de las cámaras y de las imágenes que captan cada una de las cámaras.

De la número uno a la cuatro, son video porteros, cuya cámara solo se activa en el momento de la llamada y no se ve reflejada o almacenada en el sistema de videovigilancia.

Todas las cámaras de exteriores están ubicadas en la fachada del edificio o en los postes situados dentro del recinto, enfocando el interior. Las imágenes mínimas que se captan del exterior del recinto se encuentran pixeladas. El modelo de cámara "Mobotix DualDome D15" incorpora 2 objetivos que están orientados en 2 direcciones distintas, por eso se obtienen dos imágenes distintas.

Todas las cámaras del interior son el mismo modelo, tienen visión de 360º y están ancladas al techo y están ubicadas en pasillos, ascensores, escaleras y zonas de paso.

No existen cámaras instaladas en el exterior del recinto, y las imágenes que toman de la vía pública están pixeladas. Las cámaras están expresamente configuradas para evitar la captación de imágenes fuera del recinto. Las cámaras en las cuales pudiera quedar expuesta alguna zona de la vía pública tienen configurada, a través del propio panel de la cámara, una "zona oscura" en la cual queda su contenido pixelado. Se puede apreciar el estado del pixelado en el detalle de las cámaras 5 (entrada principal), 6 (escalera rampa exterior) y 7 (pasillo lateral exterior) Cualquier imagen almacenada aparece con las zonas que pudiesen llegar a captar de la vía pública pixeladas e irreconocibles.

- No hay ningún ordenador con acceso a la red de video vigilancia, ni pantallas de monitorización. La instalación de cámaras y unidad de almacenamiento de imágenes está realizada en una red de datos aislada de la red corporativa, por lo tanto, no es viable el acceso al panel de video vigilancia.
- Las personas que puede acceder al sistema de videovigilancia son: el Jefe de Área Departamento Facility Services, Informática, Telecomunicaciones y Servicios de UNIR y el Director del Departamento Facility Services, Informática, Telecomunicaciones y Servicios de UNIR. No interviene ningún tercero.
- El sistema de grabación de las cámaras de la número 5 a la 27, está basado en eventos por detección de movimiento, esto consiste en que la cámara solo se activa y graba imágenes cuando detecta movimiento. Las imágenes son almacenadas en un videograbador sito en el edificio de UNIR y en la misma red de datos de videovigilancia, pudiendo acceder en exclusiva el Jefe de Área y el Director del Departamento Facility Services, Informática, Telecomunicaciones y Servicios de UNIR

Las imágenes se conservan por un plazo de 15 días.

- Aportan copia de la resolución de inscripción del fichero de videovigilancia en el Registro General de Protección de Datos con el código **D.D.D.** y la cláusula de información.
- Aportan copia del documento de seguridad.
- El sistema de videovigilancia no está conectado a una central de alarmas, si



no que existe un servicio de conexión a la central receptora de alarmas contratado a VIDEOSEGUR, S.L. (SEGURIDAD 2000) totalmente independiente. Aportan copia del contrato y copia de la habilitación como empresa de seguridad.

## **FUNDAMENTOS DE DERECHO**

### **I**

Es competente para resolver la Directora 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**

El artículo 126.1, apartado segundo, del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD) establece:

*“Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.”*

### **III**

En primer lugar, procede situar en el contexto normativo la 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.

#### IV

En el presente expediente se denuncia por parte de D. **C.C.C.** la existencia de un sistema de videovigilancia en la **UNIVERSIDAD INTERNACIONAL DE LA RIOJA** que pudieran estar captando imágenes de la viviendas colindantes, incluida la suya.

En primer lugar, debe entrarse a valorar el cumplimiento del deber de información e inscripción de ficheros, por parte de la entidad denunciada.

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 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.”*

En el caso que nos ocupa, se ha aportado por parte de la entidad denunciada, fotografías de la existencia de cartel informativo de la existencia de las cámaras, ubicados en el interior del edificio (en el mostrador de recepción y en el exterior del edificio en las puertas de acceso peatonal. Dichos carteles son acordes al que hace referencia el citado artículo 3.a) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD. Asimismo, consta aportado modelo de cláusula informativa a disposición de los clientes, de conformidad con el artículo 3.b) de la citada Instrucción.

Por lo tanto la citada entidad, cumple el deber de información, en cuanto al sistema de videovigilancia, recogido en el artículo 5 de la LOPD, anteriormente transcrito.

Por otro lado, respecto al cumplimiento de la inscripción de ficheros, el artículo 26.1 de la LOPD, 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”*

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.

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.

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.”*

En el caso que nos ocupa, consta la inscripción por parte de la UNIVERSIDAD INTERNACIONAL DE LA RIOJA, del fichero denominado “VIDEOVIGILANCIA”, en el Registro General de la Agencia Española de Protección de Datos, cuya finalidad es la videovigilancia.

Asimismo, las imágenes se conservan por un periodo de 15 días, de conformidad con el artículo 6 de la citada Instrucción 1/2006 que recoge: *“Los datos serán cancelados en el plazo máximo de un mes desde su captación”.*

## V

Por último, respecto a la posible captación a través de las cámaras denunciadas de espacios ajenos, hay que señalar que 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”.

Precisamente la redacción del artículo 4 de la Instrucción 1/2006, no viene sino a recoger el principio de proporcionalidad del artículo 4 de la LOPD.

En este sentido, la posibilidad de captar un pequeño ángulo de la vía pública a través de una cámara de vigilancia, ésta deberá de cumplir el principio de proporcionalidad, sin que sea posible extender la grabación de imágenes a un alcance mayor al que resulte necesario para garantizar la seguridad de las instalaciones. Por ello, la referencia a los alrededores de las instalaciones, únicamente resultaría ajustada a la normativa de protección de datos en caso de que la misma se refiera exclusivamente a aquellos espacios públicos sin cuya grabación resultaría en todo punto imposible el control de la seguridad en el acceso a las instalaciones, sin que en modo alguno esta referencia pueda entenderse efectuada, con carácter general a la vía pública.

En el caso que nos ocupa, la denunciada aporta reportaje fotográfico de las cámaras y de las imágenes que captan cada una de las mismas. De la número uno a la cuatro, son videoporteros, cuya cámara solo se activa en el momento de la llamada y no se ve reflejada o almacenada en el sistema de videovigilancia. Todas las cámaras de exteriores están ubicadas en la fachada del edificio o en los postes situados dentro del recinto, enfocando el interior. Las imágenes mínimas que se captan del exterior del recinto (vía pública) se encuentran pixeladas. Es decir, las cámaras en las cuales pudiera quedar expuesta alguna zona de la vía pública tienen configurada, a través del propio panel de la cámara, una "zona oscura" en la cual queda su contenido pixelado. Se puede apreciar el estado del pixelado en el detalle de las cámaras 5 (entrada principal), 6 (escalera rampa exterior) y 7 (pasillo lateral exterior) Cualquier imagen almacenada aparece con las zonas que pudiesen llegar a captar de la vía pública pixeladas e irreconocibles, por lo que 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. Por lo tanto, el sistema de videovigilancia, realiza un tratamiento proporcional de las imágenes, en

relación con el ámbito y las finalidades que podrían justificar su recogida.

A la vista de todo lo expuesto, en el presente caso no se aprecia vulneración de la normativa aplicable a la protección de datos, por lo que procede el archivo del presente expediente de actuaciones previas.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

**SE ACUERDA:**

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a **UNIVERSIDAD INTERNACIONAL DE LA RIOJA** y D. **C.C.C.**.

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

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.

Mar España Martí  
Directora de la Agencia Española de Protección de Datos