

Expediente Nº: E/00494/2016

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante **BANCO POPULAR ESPAÑOL S.A, FONCASERVI, S.L., GEA 21 S.A, INVERSIONES INMOBILIARIAS CANVIVES S.A** en virtud de denuncia presentada por D. **A.A.A.** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fechas 28 de diciembre de 2015 tiene entrada en esta Agencia escrito remitido por D. **A.A.A.** (en adelante el denunciante) comunicando posible infracción a la Ley Orgánica 15/1999 motivada por la existencia de cámaras de videovigilancia en el **EDIFICIO XXXX 1** sito (C/...1), **SEVILLA**, cuyo titular es **INVERSIONES INMOBILIARIAS CANVIVES S.A** (en adelante el denunciado).

En escrito el denunciante manifiesta *“la instalación de un sistema de videovigilancia en el edificio “XXXX 1”, en el cual presta sus servicios. En principio el sistema de CCTV emitía imágenes en tiempo real y era controlado desde la entrada del inmueble y la sala de contadores. La empresa FONCASERVI S.L, no informó a los trabajadores de la finalidad de la instalación ni se recabó en ningún momento el consentimiento para la grabación de sus imágenes. A raíz de una inspección de la DGP en el año 2012 se desconectaron los monitores de visualización, aunque las cámaras presuntamente siguen funcionando. No existen carteles informativos de zona videovigilada ni se dispone de formularios informativos para el ejercicio de los derechos ARCO, desconociendo por tanto la entidad responsable del sistema de videovigilancia”*.

Adjunta a su denuncia reportaje fotográfico del sistema.

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:

- 1.1** Con fechas 2 y 16 de febrero y 18 de abril de 2016 se solicita información a la entidad **FONCASERVI S.L**, en relación con el sistema de videovigilancia instalado en el centro de trabajo sito en (C/...1), **EDIFICIO XXXX 1**, de **Sevilla**.

Con fechas 16 y 17 de marzo y 4 de mayo de 2016 tienen entrada en esta Agencia escritos, en los que manifiesta:

No ser propietaria del edificio en el que se localiza el sistema de videovigilancia investigado.

FONCASERVI S.L es una empresa de prestación de servicios de distinta índole, limitándose exclusivamente a desarrollar las funciones propias de recepción mediante el personal auxiliar de servicios.

Así ofrece sus servicios en el **Edificio XXXX 1**, mediante contrato suscrito con

fecha 1 de septiembre de 2014 con la empresa **INVERSIONES INMOBILIARIAS CANVIVES S.A.**

Se acompaña copia del citado contrato de prestación de servicios, entre cuyas estipulaciones queda reflejado las siguientes funciones a prestar: "... revisión de las instalaciones en general, con cierre y apertura de ventanas y puertas, control de entradas y salidas ordinarias de clientes, información de accesos, organización y control de la evacuación de clientes cuando se requiera por cualquier motivo y exigencia del cumplimiento de las normas propias del establecimiento" (**Doc.1**).

FONCASERVI no ha realizado la instalación del sistema de videovigilancia, ni lo utiliza para el desempeño de sus funciones. Por tanto no tiene acceso a las cámaras.

Afirma que desde que la compañía presta sus servicios en el **Edificio XXXX**, el sistema no ha estado operativo.

Desconoce el titular y responsable actual del sistema de videovigilancia instalado. Informa que el edificio fue adquirido por **BANCO POPULAR** hace años, mediante adjudicación por procedimiento concursal seguido contra el anterior titular **GEA 21 S.A.**

1.2 Con fecha 22 de marzo de 2016 se solicita información del sistema a la entidad **BANCO POPULAR ESPAÑOL S.A.**, teniendo entrada en esta Agencia escritos de fechas 5 y 12 de abril de 2016 en los que manifiesta: "no ser el propietario del edificio XXXX 1 de Sevilla, ni disponer de sucursal en la citada dirección".

1.3 Con fecha 18 de abril de 2016 se solicita información del sistema a la entidad **GEA 21 S.A.**, la cual comunica a esta Agencia con fecha 28 de abril de 2016 en los siguientes términos:

En el mes de Julio de 2009, resolvió el contrato de arrendamiento de las oficinas sitas en el **Edificio XXXX I de Sevilla** con la mercantil **INVERSIONES GEMOVE S.L.** No dispone por tanto de información alguna acerca del sistema de videovigilancia investigado.

1.4 Con fechas 4 de mayo y 1 de junio de 2016, se solicita información del sistema de videovigilancia a la mercantil **INVERSIONES INMOBILIARIAS CANVIVES S.A.**

Del análisis de las manifestaciones y documentación aportada a esta Agencia, se desprende:

La sociedad mercantil **INVERSIONES INMOBILIARIAS CANVIVES S.A** (en adelante **CANVIVES**), es propietaria desde el 13 de marzo de 2014 de los locales que integran el edificio XXXX 1 (en adelante el Edificio), adquirido tras el otorgamiento de escritura de ampliación de capital social para cuya suscripción de acciones por parte de Banco Popular Español S.A se aportó, entre otros, el referido Edificio que había obtenido por operación de dación en pago de deuda elevada a público mediante escritura otorgada por **INVERSIONES GEMOVE S.L.**, anterior

propietaria.

En documentos **Doc.'s 1-2 bis** se adjuntan copias de las escrituras suscritas de ampliación de capital social y de dación en pago de deuda otorgada.

Desde que CANVIVES es titular del Edificio, el sistema de videovigilancia ya se encontraba fuera de servicio y nunca ha estado en funcionamiento.

La mercantil no dispone de documentación relativa a su instalación ni información sobre la causa y finalidad que la motivó.

En documento **Doc.18** se adjunta certificación, emitida con fecha 9 de junio de 2016 por la empresa de seguridad **IMACO SISTEMAS S.L**, acreditando *“que el sistema de grabación se encuentra deshabilitado y sin funcionamiento, no disponiendo de disco duro para el almacenamiento de imágenes ni conexión de cámaras”*.

Dado que el sistema no funciona, no se localizan carteles informativos de zona videovigilada en el edificio.

*El sistema, que cuenta con 20 años de antigüedad, está integrado por un total de 11 cámaras; de las cuales, 3 cámaras se ubican en la fachada exterior. Se distribuyen según se indica en los planos de situación adjuntos (**Doc.'s 3-6**).*

Se acompaña reportaje fotográfico del sistema de cámaras instalado (**Doc.'s 7-17**)

El monitor de visualización no se encuentra en funcionamiento.

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

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 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, 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 expediente se denuncia por D. **A.A.A.**, la instalación de un sistema de videovigilancia en el edificio “**XXXX 1**”, en el cual presta sus servicios sin que la empresa **FONCASERVI S.L.** haya informado a los trabajadores de la finalidad de la instalación ni se haya recabado en ningún momento el consentimiento para la grabación de sus imágenes.

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

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

Del concepto de consentimiento se desprende la necesaria concurrencia para que

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

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

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

c) Informado, es decir que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce. Precisamente por ello el artículo 5.1 de la LOPD impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen.

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

El apartado 2 del artículo 6 de la LOPD exige del necesario consentimiento cuando los datos se refieran *“a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento...”*

En el ámbito laboral, el Ordenamiento el Ordenamiento Jurídico Español, regula en el Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo de 24 de Octubre de 1995, los poderes de Dirección del empresario y es en éste articulado donde hallamos la oportuna legitimación.

El artículo 20.3 del texto refundido de la Ley del Estatuto de los Trabajadores (ET), aprobado, por Real Decreto Legislativo 2/2015, de 23 de octubre, dispone que : *“El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores con discapacidad”*.

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

Es necesario en este punto diferenciar si la instalación de la cámara en el centro

de trabajo es como medida de vigilancia y control del empresario, para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales o si es una medida de seguridad para proteger la instalación y sus empleados.

En el primer caso, es decir cuando el objetivo de la instalación de las cámaras va dirigido al cumplimiento por los trabajadores de sus deberes laborales, sería necesario por parte del empresario, garantizar el derecho de información en la recogida de las imágenes, mediante información a los trabajadores del alcance específico que se va a dar a las mismas para el control laboral, como establece la Sentencia del Tribunal Constitucional 29/2013, de 11 de febrero de 2013, debe ir precedido de *“una información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida. Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo”*.

En el segundo caso, es decir cuando la finalidad es de vigilancia y protección de las instalaciones y personal de la empresa, es necesario el cumplimiento de la LOPD, el Reglamento de Desarrollo de la LOPD y la Instrucción 1/2006. Por lo tanto, debería cumplirse, entre otros, el deber de información recogido en el artículo 5 de la LOPD, disponiendo de distintivos informativos de zona de videovigilancia acordes a la Instrucción 1/2006 e impresos informativos.

Una vez realizadas las aclaraciones precedentes, en el caso que nos ocupa, la entidad **FONCASERVI S.L.**, manifiesta, a la solicitud de información de esta Agencia, que no es propietaria del edificio en el que se localiza el sistema de videovigilancia investigado ni ha realizado la instalación del sistema de videovigilancia, ni lo utiliza para el desempeño de sus funciones. Por tanto no tiene acceso a las cámaras. Manifiesta que se trata de una empresa de prestación de servicios de distinta índole, limitándose exclusivamente a desarrollar las funciones propias de recepción mediante el personal auxiliar de servicios. Ofrece sus servicios en el **Edificio XXXX 1**, mediante contrato suscrito con fecha 1 de septiembre de 2014 con la empresa **INVERSIONES INMOBILIARIAS CANVIVES S.A.**, afirmando que desde que la compañía presta sus servicios en el **Edificio XXXX**, el sistema no ha estado operativo.

Solicitada información del sistema de videovigilancia a la mercantil **INVERSIONES INMOBILIARIAS CANVIVES S.A.**, manifiesta que es propietaria desde el 13 de marzo de 2014 de los locales que integran el edificio **XXXX 1** y desde que **CANVIVES** es titular del Edificio, el sistema de videovigilancia ya se encontraba fuera de servicio y nunca ha estado en funcionamiento.

Aporta en prueba de ello, certificación, emitida con fecha 9 de junio de 2016 por la empresa de seguridad **IMACO SISTEMAS S.L.**, acreditando *“que el sistema de grabación se encuentra deshabilitado y sin funcionamiento, no disponiendo de disco duro para el almacenamiento de imágenes ni conexión de cámaras”*.

Por tanto, a la vista de la documentación aportada se desprende que el citado sistema de videovigilancia se encuentra inoperativo y por lo tanto ni captan ni graban imágenes.

A este respecto, 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.”*

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.

A la vista de lo expuesto, al no haberse acreditado la captación o grabación de imágenes de datos personales por parte del denunciado al margen de la normativa de protección de datos, al encontrarse inoperativo el sistema de videovigilancia y

atendiendo al principio de presunción de inocencia, 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 **FONCASERVI, S.L., INVERSIONES INMOBILIARIAS CANVIVES S.A** y a D. **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 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 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 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.

Mar España Martí

Directora de la Agencia Española de Protección de Datos