Procedimiento nº.: E/03868/2013

ASUNTO: Recurso de Reposición Nº RR/00193/2014

Examinado el recurso de reposición interpuesto por D. ***A.A.A.*** contra la resolución dictada por el Director de la Agencia Española de Protección de Datos en el expediente de actuaciones previas de inspección E/03868/2013, y en base a los siguientes

HECHOS

PRIMERO: Con fecha 29 de enero de 2014, se dictó resolución por el Director de la Agencia en el expediente de actuaciones previas de inspección E/03868/2013, procediéndose al archivo al no apreciarse vulneración a la normativa de protección de datos.

Dicha resolución fue notificada al recurrente en fecha 4 de febrero de 2014, según acuse de recibo del servicio de Correos que figura en el expediente.

SEGUNDO: D. ***A.A.A.*** (en lo sucesivo el recurrente) ha presentado a través de su representante legal, en fecha 25 de febrero de 2014 en el Registro de la Delegación del Gobierno en Murcia y fecha de entrada en esta Agencia el 4 de marzo de 2014, recurso de reposición, fundamentándolo básicamente en:

- Que la denunciada aporta reportaje fotográfico del cartel informativo existente sin que conste la fecha de su colocación ni se haya acreditado tal extremo.

- Que la propia denunciada declara la colocación de dos cámaras de videovigilancia, si bien según el reportaje fotográfico aportado consta la colocación de un solo cartel informativo, fuera de la zona videovigilada, incumpliendo el deber de información del artículo 3 de la Instrucción 1/2006.

- Que la denunciada alega contar con los correspondientes formularios informativos que pone a disposición de la AEPD, si bien que cuente con los referidos formularios no acredita que estos estén a disposición de los trabajadores y clientes ni que estos hayan sido informados de su existencia. Asimismo, a este respecto, la AEPD no ha desplegado actividad alguna al objeto de verificar que los trabajadores y público de la mercantil conocen la existencia de las cámaras.

- Que se omite el dato relativo a la fecha de creación del fichero de videovigilancia en el Registro General de Protección de datos.
- Que por parte de la AEPD no se ha constatado actividad investigadora alguna a fin de constatar la finalidad recogida en el fichero registrado, ni se ha realizado examen de las imágenes obtenidas ni actividad investigadora tendente a comprobar los requisitos técnicos exigidos en orden a la captación y destrucción de los datos tratados.
- Que se vulnera los derechos fundamentales a la intimidad personal del artículo 18.1 CE y de la protección de datos de carácter personal del artículo 18.4 de la CE.
- Que en cuanto al derecho a la intimidad no se cumple el juicio de idoneidad, necesidad

ni proporcionalidad.

- Que en relación a la protección de datos y la tutela judicial efectiva no se puede confundir la libertad de elección en los medios de prueba que nuestro derecho autoriza con la legitimidad de los mismos, cuestión esta última que no competente dictaminar a esta Agencia, siendo el denunciante el que queda en una situación de indefensión, sin que se pueda aseverar por la AEPD la legitimidad del interés alegado por la entidad denunciada, el cumplimiento de los requisitos exigidos por la LOPD, ni que dicho interés debe prevalecer sobre los derechos del denunciante.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el presente recurso el Director de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto 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 (en lo sucesivo LRJPAC).

II

El recurrente muestra su disconformidad con la resolución ahora recurrida en varias cuestiones que serán seguidamente analizadas.

Así en primer lugar, respecto a que por parte de la AEPD no se ha realizado actividad investigadora alguna a fin de constatar diversos aspectos del sistema de videovigilancia denunciado cabe decir que, tanto el artículo 12 del RD 1398/1993 como el artículo 122 del RD 1720/2007, de 21 de Diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, establecen que "*se podrán realizar actuaciones previas con objeto de determinar si concurren circunstancias que justifiquen tal iniciación*"(art. 122 RD 1720/2007), o lo que es lo mismo, no existe una obligatoriedad en la realización de dichas actuaciones, sino que deberán llevarse a cabo cuando existan elementos con la suficiente fuerza, que permita entender que, en efecto, se ha producido la infracción alegada, circunstancia que no concurre en el presente caso.

Es más, las SSAN de 8 de abril y 22 de julio de 2010, ponen de relieve que aunque los artículos 122 y siguientes del RLOPD se desprende la posibilidad de llevar a cabo las denominadas actuaciones previas con anterioridad a la iniciación del procedimiento sancionador con el objeto de determinar si concurren circunstancias que justifiquen tal iniciación, puede haber sin embargo supuestos en los que, a tenor de las circunstancias concurrentes, y desprendiéndose del somero análisis del relato de hechos de la denuncia que los mismos en ningún caso son susceptibles de vulnerar la LOPD, que ni siquiera sea necesario, ni haya justificación ninguna para iniciar dichas actuaciones de inspección.

Asimismo al hilo de todo lo anterior, ha de recordarse al recurrente, los principios aplicables al procedimiento sancionador y su iniciación. Los expedientes sancionadores de la Agencia Española de Protección de Datos son expedientes siempre iniciados de

oficio por el Director de la Agencia Española de Protección de Datos, de conformidad a lo previsto en el artículo 122.2 del RGLOPD, como así ha mantenido la Audiencia Nacional en sentencias como, entre otras, la dictada en marzo de 2006(REC 319/2004). Por tanto es competencia exclusiva de la Agencia Española de Protección de Datos valorar si existen responsabilidades administrativas que han de ser depuradas en un procedimiento sancionador y, en consecuencia, la decisión sobre su apertura, no existiendo obligación de iniciar procedimiento ante cualquier petición realizada por tercero, sino que la misma ha de basarse en la existencia de elementos que justifiquen dicho inicio de actividad sancionadora. Así lo establece el artículo 11.2 del Real Decreto 1398/1993, de 4 de Agosto, por el que se aprueba el Reglamento de Procedimiento para el Ejercicio de la Potestad Sancionadora, que es del tenor siguiente:

"*La formulación de una petición no vincula al órgano competente para iniciar procedimiento sancionador, si bien deberá comunicar al órgano que la hubiera formulado los motivos por los que, en su caso, no procede la iniciación del procedimiento.*

Cuando se haya presentado una denuncia, se deberá comunicar al denunciante la iniciación o no del procedimiento cuando la denuncia vaya acompañada de una solicitud de iniciación"

Junto a ello debe tenerse en cuenta el criterio restrictivo mantenido por la Audiencia Nacional en Sentencia de 1 de abril de 2011 acerca de la puesta de la protección de datos al servicio de otros intereses por legítimos que sean: *"La seriedad que conlleva el ejercicio de la potestad sancionadora aconseja que se pongan en marcha los mecanismos administrativos y jurisdiccionales correspondientes solo cuando se suponga que se ha producido una verdadera violación del derecho fundamental a la protección de datos".*

Así las cosas, en la resolución recurrida, como así establece como necesario el artículo 11.2 del RD 1398/1993 antes referenciado, se ponía de manifiesto la aportación de elementos objetivos de carácter probatorio por parte de la entidad denunciada que impedían la iniciación siquiera de actuaciones inspectores.

- Por otro lado, respecto a las manifestaciones del recurrente relativas a la protección de datos y la tutela judicial efectiva siendo el denunciante el que queda en una situación de indefensión, cabe decir que, en nuestro derecho, el principio de la carga de la prueba de los hechos denunciados le corresponde al denunciante, al que le corresponde probar los hechos en que sustenta sus peticiones, para así permitir iniciar actuaciones que pudieran concretarse en un procedimiento sancionador. El propio Tribunal Constitucional, en su sentencia 76/1990, considera que para quebrar el derecho a la presunción de inocencia aplicable a todo sujeto de derecho, es necesario *" 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".(el subrayado es de la Agencia Española de Protección de Datos).

Asimismo, la valoración de la prueba debe someterse a los criterios generales de valoración admitidos en Derecho, siendo totalmente aplicables los principios de la libre valoración probatoria e incluso el de la valoración conjunta de la practicada; si bien la valoración y eficacia de dicha prueba en esa vía, no vincula a la Jurisdicción Contenciosa-Administrativa, la cual puede separarse de la valoración efectuada en sede administrativa, y ello, con el material probatorio que considere pertinente, tanto el actuado administrativamente por el interesado, cuanto por la prueba procesal misma en su sede jurisdiccional, en la que debemos considerar comprendido en cuanto a su valoración, las actuaciones de la Administración ante la que ahora se recurre, formalizadas en su correspondiente expediente.

Cierto es que esta Agencia en cuanto a la prueba, en el Fundamento de Derecho VI de la resolución ahora recurrida recoge textualmente: *"Por lo tanto, en cuanto a lo aportado en el juicio, dicho cuerpo legal admite la aportación como medio de prueba de los medios de reproducción de la palabra, el sonido y la imagen, lo cual implica la posibilidad de tratamiento de datos dentro de dichas propuestas de prueba, debiendo ser el correspondiente órgano jurisdiccional quien se manifieste sobre la legitimidad de lo presentado, por lo que, en el caso de que esta Agencia impusiera una eventual sanción, dicha circunstancia colisionaría con el ejercicio del derecho constitucional a una tutela judicial efectiva".*

Como recoge el citado texto de la resolución, esta Agencia no le compete determinar la legitimidad de las pruebas aportadas al juicio siendo el órgano jurisdiccional competente quien se manifieste al respecto. Esta Agencia solo entró a valorar la procedencia del sistema de videovigilancia instalado con una finalidad de seguridad, verificando si cumplía con los requisitos establecidos en materia de protección de datos.

Al hilo de estas cuestiones, respecto a las manifestaciones del recurrente de que ha sido él, el que se ha quedado en una situación de indefensión cabe decir que, a la entidad denunciada una vez presentada denuncia por el ahora recurrente, se le pidió en fase de actuaciones previas todo tipo de información y aportación de pruebas del sistema de videovigilancia denunciado. Igualmente el denunciante aportó todos los documentos y pruebas que estimó conveniente. Por lo tanto, en forma alguna se puede compartir la indefensión esgrimida por el recurrente porque no se ha producido una situación de indefensión real o material, pues como tiene señalado el Tribunal Constitucional la indefensión relevante es una indefensión no meramente formal sino material, es decir que haya originado al recurrente un menoscabo real de su derecho de defensa causándole un perjuicio real y efectivo (SSTC 155/1988, de 22 de julio; 212/1994, de 13 de julio; 137/1996, de 16 de septiembre; 89/1997, de 5 de mayo;78/1999, de 26 de abril, entre otras), situación que no se ha producido en el

presente caso.

-Respecto a las manifestaciones del recurrente respecto a la ausencia de información del sistema de videovigilancia tanto a los trabajadores de ***PRAXAIR ESPAÑA, S.L.,*** como de aquellos que prestan sus servicios en otras empresas subcontratadas, 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 concurran los requisitos legalmente previstos para considerar que se ha obtenido libremente el consentimiento.

El artículo 3 h) de la LOPD lo define como "*Toda manifestación de voluntad libre, inequívoca, específica e informada mediante la que el interesado consienta el tratamiento de datos personales que el conciernen".*

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

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

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

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

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

La concurrencia de estos requisitos resulta de difícil cumplimiento en el ámbito laboral. En consecuencia, vista la dificultad que entraña obtener el consentimiento, la Agencia Española de Protección de Datos, ha entendido que lo procedente es acudir a las normas que legitimen el tratamiento de los datos. Por tanto, en el ámbito laboral, el

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

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

De todo ello se desprende que el empresario, en este caso la entidad denunciada, se haya 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.).*

En el caso que nos ocupa, según se señala por la entidad denunciada: *"Las cámaras se han instalado únicamente por razones de seguridad, habida cuenta que en la Planta donde se hallan ubicadas venían produciéndose robos de material (en concreto botellas) del que* ***PRAXAIR ESPAÑA, S.L.U.*** *era depositario. En este sentido, es importante resaltar que la instalación de dichas cámaras no constituye una media de control de la actividad laboral de los empleados de* ***PRAXAIR ESPAÑA, S.L.U****. amparada en el artículo 20.3 del Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores, pues se ignoraba en el momento de su instalación la naturaleza de las personas que efectuaban dichos robos".*

De la documentación obrante en el expediente, se extrae que, en el presente supuesto, el tratamiento de datos por medio de cámaras y/o videocámaras con fines de seguridad queda incardinado en la esfera del interés legítimo de la entidad denunciada, por cuanto la misma tiene un evidente interés en la instalación de cámaras de seguridad; y la finalidad de seguridad es también legítima, sin que se oponga a norma u obligación de ningún tipo.

Por lo tanto el sistema de videovigilancia cumple una función de seguridad, sin que conste ni se hayan aportado pruebas al respecto por parte del denunciante, que acrediten que el sistema de videovigilancia es utilizado para fines distintos que no sean los de seguridad de las instalaciones y del personal que trabaja o transita por las mismas.

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 (como es el caso que nos ocupa).

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, se aplicaría toda

la normativa y jurisprudencia recogida “ut supra”, es decir 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.

En el segundo caso, es decir cuando la finalidad es de vigilancia y protección de las instalaciones y personal de la empresa, (como es el caso que nos ocupa), 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.

Pues bien, en el caso que nos ocupa, y contestado a las alegaciones realizadas por el recurrente relativas al cartel informativo de zona videovigilada, se aportó por la denunciada fotografías que constatan la existencia en el único acceso existente a las zonas videovigiladas, en un pilar del mismo, del cartel acorde al que hace referencia el citado artículo 3.a) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD.

Debe informarse al recurrente, dado que manifiesta precisamente que el cartel quedaría en los accesos a la zona videovigilada, que respecto a la ubicación del cartel no es necesario que se coloque debajo de cada cámara, siendo suficiente conforme a lo dispuesto en el artículo 3 a) de la Instrucción 1/2006, colocar el distintivo informativo en lugar suficientemente visible, tanto en espacios abiertos como cerrados. Por tanto, resultaría aconsejable que tratándose de un edificio sometido a videovigilancia que en la entrada del mismo se ubicará el cartel informativo, como así se ha realizado por la entidad denunciada, al instalar un cartel de zona videovigilada, cumpliendo todos los requisitos legalmente establecidos, visible para todas las personas que acceden a la planta, y estando precisamente ubicado en el único acceso a las zonas vigiladas.

En cuanto a la posibilidad de refundir en un solo cartel las exigencias de la normativa de seguridad privada y las de la Instrucción 1/2006, como sucede en el caso que nos ocupa, esta Agencia ha manifestado que *“La posibilidad de refundir en un cartel ambas exigencias, resultaría admisible, pero siempre, desde la perspectiva de la Agencia Española de Protección de Datos, que la información relativa al responsable del fichero, lugar donde pueden ejercitar sus derechos de acceso, rectificación, cancelación y oposición, sea clara y comprensible para los afectados”.*

-Asimismo, respecto a las manifestaciones del recurrente al formulario informativo, la entidad aporta copia de dicho formulario que se encuentra almacenados en la garita de control de acceso a planta estando a disposición de quien lo solicite. Así, esta Agencia ha venido manteniendo al respecto de los formularios informativos, que estos puedan estar preimpresos y preparados por el responsable del tratamiento, o tener la posibilidad de imprimirlos en el momento de su demanda, bien por tener preparado un documento Word o por tener conexión a Internet que permita acceder a la página web de la Agencia Española de Protección de Datos y poder descargarse el modelo de formulario referido.

Por lo tanto la entidad denunciada cumple el deber de información recogido en el artículo 5 de la LOPD, teniendo en cuenta que la finalidad del sistema de videoigilancia es la seguridad y no el control laboral de sus empleados.

- Respecto a las manifestaciones relativas al fichero de videovigilancia recalcando que se omite todo dato relativo a la fecha de su creación, se le informa y así consta en la diligencia levantada por el inspector actuante en fase de actuaciones previas, que existe inscrito el fichero denominado "CONTROL DE ACCESO, VISITAS Y VIDEOVIIGLANCIA", en fecha 6 de octubre de 2009 en el Registro General de Protección de datos de esta Agencia, figurando como responsable PRAXAIR ESPAÑA, S.L. y teniendo como finalidad la seguridad y control de acceso a edificios y videovigilancia.

- Por último respecto a las manifestaciones del recurrente que se vulnera los derechos fundamentales a la intimidad personal del artículo 18.1 CE y de la protección de datos de carácter personal del artículo 18.4 de la CE y que en cuanto al derecho a la intimidad no se cumple el juicio de idoneidad, necesidad ni proporcionalidad cabe sino reiterar la sentencia de 22 de octubre de 2010 (rec. 409/2009) de la Audiencia Nacional, recogida en el Fundamento de Derecho VI de la resolución recurrida que nos dice, en cuanto a la obtención de medios probatorios y su validez en el procedimiento, pese a no ser solicitadas ni obtenidas por vía judicial, lo siguiente:

"De un lado ha de tenerse en cuenta que una de las causas que excluye la necesidad de consentimiento para la cesión de datos personales es que la comunicación que deba efectuarse tenga por destinatarios a los Jueces o Tribunales (Art. 11.2.d) LOPD).

Excepción en la que no es descabellado incluir aquellos supuestos en que se trata de pruebas que, si bien inicialmente no han sido solicitadas por el Juez o Tribunal, sino aportadas por las partes, con posterioridad no consta que las mismas hayan sido rechazadas, sino incorporada por el Juez a las actuaciones, tal y como, parecer ser, y así se desprende del acta de juicio, ocurrió en el presente supuesto.

Por otra parte, y si bien es cierto que los procedimientos judiciales tampoco son ajenos a la normativa de protección de datos, tal y como indicamos en la SAN 9-10-2009 (Rec. 37/2009) dado que el derecho de protección de datos, en cuanto derecho fundamental y autónomo previsto en el artículo 18.4 CE , vincula a todos los poderes públicos (Art. 53 CE) y entre ellos al Poder Judicial, tal y como igualmente indica la STS 18-9-2006 Rec. 274/2002. Sin embargo dicha LOPD debe ser aplicada con gran cautela, y en la medida en que resulte compatible con las funciones propias (jurisdiccionales y no jurisdiccionales) de los referidos órganos judiciales, pues la singularidad de la actividad jurisdiccional y los intereses que en ella subyacen, exigen en ocasiones una limitación o modulación de los derechos y garantías de los ciudadanos.

Además de que el sometimiento de los ficheros judiciales a la LOPD ha de entenderse (según la misma SAN 9-10-2009 Rec. 37/2009) sin menoscabo de la función jurisdiccional y, por tanto, atinente a lo que debe considerarse como "aspecto accesorio" o administrativo de la función jurisdiccional, centrándonos concretamente en el procedimiento judicial, existen también en él una serie de intereses y garantías que ostentan un trascendente valor en dicho proceso, tales como el del verdadero esclarecimiento de los hechos o el legítimo ejercicio del derecho de defensa de las partes, que han de ser ponderados en aquellos casos en que dichos intereses y garantías confluyen con el derecho contemplado en el artículo 18.4 CE , hasta el punto de que pueden llegar a implicar una importante limitación de tal derecho de protección de datos personales." (el subrayado es de la Agencia Española de Protección de Datos)".

Pero es que a mayor abundamiento, la propia Sentencia nº *******/2012*** dictada por la Audiencia Provincial de Madrid ante el recurso de apelación interpuesto por el denunciante ante esta Agencia, contra la Sentencia dictada por el Juzgado de 1ª Instancia e Instrucción de Navalcarnero, recoge sentencias del Tribunal Supremo y Constitucional clarificadoras del caso que se plantea. Así *"La Sentencia de 6 de abril de 1994 corrobora la legitimidad de la prueba consistente en una filmación videográfica si la misma no ha vulnerado algún derecho, es decir, si con ello no se ha violado la intimidad o la dignidad de la persona afectada por la filmación. Es el propio Tribunal Constitucional el que estima admisible la captación de la imagen del sujeto cuando la misma conducta de aquel o las circunstancias en que se encuentre inmerso justifiquen el descenso de las barreras de reserva para que prevalezca el interés ajeno o el público que pudieran colisionar con aquél. (STC 99/1994)…".*

Por otro lado, de conformidad con la doctrina del Tribunal Constitucional, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan, basta recordar que (como sintetizan las SSTC 66/1995, de 8 de mayo [RTC 1995\66], F.5; 55/1996, de 28 de marzo [RTC 1996\55], FF. 6, 7, 8 y 9; 207/1996, de 16 de diciembre [RTC1996\207], F.4.e) y 37/1998, de 17 de febrero [RTC 1998\37], F.8) para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

La medida adoptada por la entidad denunciada de instalación de un sistema de videovigilancia resulta idónea, necesaria y equilibrada dado que ya que se trata de la instalación de un sistema de videoviglancia en el interior de las instalaciones de la entidad denunciada con una finalidad de seguridad, habida cuenta de varios robos de

material que se habían producido en la planta, cumpliendo como se ha acreditado todos las obligaciones que impone la normativa de protección de datos entre los que se encuentran el deber de información e inscripción de fichero.

En consecuencia, en el presente recurso de reposición, el recurrente no ha aportado nuevos hechos o argumentos jurídicos que permitan reconsiderar la validez de la Resolución impugnada.

Vistos los preceptos citados y demás de general aplicación,

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

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por D.***A.A.A.*** contra la resolución de esta Agencia dictada con fecha 29 de enero de 2014, en el expediente de actuaciones previas de inspección E/03868/2013.

SEGUNDO: NOTIFICAR la presente resolución 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 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, se podrá interponer 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 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, 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 del referido texto legal.

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