



Expediente N°: E/07306/2012

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la **CENTRALES NUCLEARES ALMARAZ TRILLO A.I.E.**, en virtud de denuncia presentada por la **DIRECCIÓN GENERAL DE LA GUARDIA CIVIL** y por D^a. **A.A.A.** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha de 1 de octubre de 2012 tiene entrada en esta Agencia un escrito remitido desde la Comandancia de la Guardia Civil en Cáceres (Compañía Navalmoral de la Mata) en el que se adjunta denuncia de Dña. **A.A.A.** en calidad de *****CARGO.1** de Almaraz (en adelante la denunciante), en la que declara que fecha 17 de septiembre de 2012 la responsable de la empresa de seguridad **EULEN** de la **CENTRAL NUCLEAR DE ALMARAZ** (en adelante la **CNA**), le ha comunicado en la puerta de acceso a la **CNA** que la conversación telefónica mantenida entre ambas al número de teléfono de la Alcaldía del Ayuntamiento de Almaraz el día 14 de septiembre de 2012 entre las 13:00 y las 14:00 horas "la tiene grabada". Igualmente la denunciante manifiesta a la Guardia Civil que los jóvenes que con ella se encontraban reivindicando agrupados en la puerta de la **CNA** son grabados "sin informar de ello" dado que han podido observar que el movimiento de las cámaras de vigilancia hacia donde se encontraba el grupo. La denunciante manifiesta que el tema de la conversación telefónica ha sido las reivindicaciones que diariamente se llevaban a cabo en las inmediaciones de la CNA.

La Guardia Civil adjunta Diligencia de exposición con número de expediente ********* en la que informan acerca de las actuaciones llevadas a cabo el 17 de septiembre de 2012 poniendo de manifiesto:

- Tras entrevistarse con D. **B.B.B.** como Responsable de Seguridad Física de la CNA y Dña. **C.C.C.** como Responsable delegada en Extremadura de la entidad **EULEN** han confirmado que se realizó la conversación telefónica con la *****CARGO.1 DE ALMARAZ** para hablar sobre las reivindicaciones que se venían sucediendo en los días laborables a la hora de entrada y salida de la jornada laboral de la **CNA** y que dicha llamada se realizó desde un teléfono de la **CNA** desde la que aleatoriamente se hacen grabaciones de las llamadas salientes.
- Con relación a las grabaciones que se han realizado al grupo de personas que se agrupan por la mañana y tarde en las inmediaciones de la puerta de la **CNA** el Responsable de Seguridad Física manifiesta que dicha instalación dispone de sistema de videovigilancia autorizado que continuamente se encuentra grabando y que las mismas tienen una duración en el sistema de tres días, y manifiesta que las grabaciones de las cámaras se limitan a los espacios privados propiedad de la **CNAT (Almaraz-Trillo)** salvo la puerta de acceso a la **CNA** que graba los espacios públicos por resultar imprescindible para la finalidad de

videovigilancia que se pretende y que resulta imposible evitarlo por razón de la ubicación de aquéllas, declarando que dichos datos se evita cualquier tratamiento innecesario para la finalidad perseguida.

- La **CNA** es una infraestructura que se encuentra sometida a medidas de seguridad específicas frente a actos de sabotaje e intrusiones.
- Aportan reportaje fotográfico en el que se muestran carteles de zona videovigilada instalados en la CNA y en el que se hace constar que los afectados pueden ejercitar sus derechos en **(C/.....1) (MADRID)**, “PROTECCIÓN DE DATOS DE LAS CENTRALES NUCLEARES ALMARAZ-TRILLO AIE.”

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 27 de mayo de 2013 se solicita información a la entidad **CENTRALES NUCLEARES ALMARAZ TRILLO A.I.E.** (en adelante el denunciado) teniendo entrada en esta Agencia escrito de respuesta en fecha 13 de junio de 2013 en el que se pone de manifiesto:

- Las causas que han motivado la instalación de las cámaras son el cumplimiento de la normativa vigente en materia nuclear y en la importancia que tiene la protección física de la instalación para la salvaguardia de la población y del medio ambiente así como la seguridad nacional e internacional.

La instalación de las cámaras viene avalada por el carácter de la infraestructura que se pretende proteger, hecho que se justifica con:

- o Ley 25/1964 de 29 de abril sobre energía nuclear y normas de desarrollo de la misma.
- o Ley 15/1980 de 22 de abril de creación del Consejo de Seguridad Nuclear reformada por Ley 33/2007 de 7 de noviembre.
- o Ley 1308/2011 de 26 de septiembre sobre protección física de las instalaciones y los materiales nucleares y de las fuentes radioactivas.
- o Ley 8/2011 de 28 de abril por la que se establecen medidas para la protección de las infraestructuras críticas.
- o Real Decreto 704/2011 de 20 de mayo por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
- o Primer Plan de Protección de las Infraestructuras Críticas de 7 de mayo de 2007 así como la elaboración de un primer Catálogo Nacional de Infraestructuras Estratégicas.
- o Estrategia global sobre protección de infraestructuras críticas del Consejo Europeo de 20 de octubre de 2004.



- o Directiva 2008/114 sobre identificación y designación de Infraestructuras Críticas Europeas.
 - o Directrices establecidas por el Consejo de Seguridad Nuclear para la protección de las instalaciones nucleares concretamente la Instrucción **IS-09** que establece los “criterios aplicables al diseño, implantación, operación y mantenimiento de los procedimientos y servicios de protección física de las instalaciones y los materiales nucleares” en la cual existe una parte accesible al público y otra con carácter confidencial en base a garantizar la efectividad de las medidas de protección física interior de las instalaciones, actividades y materiales, la parte confidencial de la Instrucción IS-09 puede ser únicamente consultada por personas autorizadas por razón de su función.
 - o Instrucción de Seguridad IS-09 sobre criterios aplicables al diseño, implantación operación y mantenimiento de los sistemas, procedimientos y servicios de protección física de las instalaciones y los materiales nucleares.
- Aporta modelo de formulario informativo a disposición de los ciudadanos según recoge el artículo 3.b de la Instrucción 1/2006 y fotografía del cartel de zona videovigilada que se encuentra en el acceso a las CNA y adjunta formulario informativo relativo al cumplimiento de la normativa específica del Consejo de Seguridad Nuclear que se entrega a la firma a las personas que acceden al recinto de la CNA.
 - Con relación a la ubicación de las cámaras y las imágenes captadas por las mismas y a la ubicación de los monitores sobre los que se visualizan las imágenes; según lo “preceptuado en el artículo 4º de la Instrucción de Seguridad IS-09 del Consejo de Seguridad Nuclear no es posible aportar dicha información por formar parte del Plan de Seguridad definidor de la política general para garantizar la seguridad del conjunto de sus instalaciones clasificado “conforme a lo que establece la legislación vigente en materia de secretos oficiales, debiendo constar expresamente en el instrumento de su aprobación” y el Centro Nacional de Protección de Infraestructuras Críticas es el responsable de garantizar a los agentes del Sistema autorizados el acceso a toda o parte de la información contenida en dichos planes velando por la confidencialidad y la seguridad de la misma (Art. 23.4 del RD/2011 de 20 de mayo). En dicho sentido las cámaras y sistemas de video-vigilancia de la CNA se encuentran sometidas a inspecciones periódicas del Consejo de Seguridad Nuclear, Guardia Civil y Policía Nacional.
 - Las cámaras no graban sonido, las imágenes se graban y el código de inscripción de fichero con finalidad de videovigilancia es *****COD.1** en el Registro General de la Agencia Española de Protección de Datos y la denominación del fichero es “FICHERO DE SEGURIDAD”, aporta copia de documento de inscripción de fichero.
 - Con relación a los hechos que ocurrieron en septiembre de 2012, **CNAT** no tiene constancia documental alguna de los hechos acontecidos el día 17 de septiembre de 2012. Sin embargo, se ha podido verificar que Dña. **C.C.C.** Directora de Seguridad de **EULEN SEGURIDAD SA** para

Extremadura no presta servicios en la **CNA**, y manifiesta que mantuvo una conversación con la *****CARGO.1 DE ALMARAZ** en relación con la contratación como vigilantes para la **CNA** de varios convecinos de la localidad.

Asimismo en fecha 17 de septiembre de 2012 tuvo lugar a las puertas de las instalaciones de la **CNA** una concentración de protesta que no contaba con autorización y conocimiento de la autoridad competente, acudiendo a este acto de protesta la propia *****CARGO.1 DE ALMARAZ**. Con relación a la grabación de voz no es posible realizar dichas grabaciones ni con el sistema de videovigilancia ni con la propia centralita de la **CNA** ya que carece de recursos técnicos necesarios que permitan la grabación de conversaciones telefónicas.

- Aportan la siguiente información:
 - o Anexo 1: Protocolo para el ejercicio de los derechos de ARCO.
 - o Anexo 2: Contrato de arrendamiento de servicio de seguridad con la entidad EULEN.
 - o Anexo 3: Documento de confidencialidad para el personal que presta servicio en la CNA.
 - o Anexo 4: Inscripción de fichero denominado “SEGURIDAD” en el Registro General de la Agencia Española de Protección de Datos.
 - o Anexo 5: Documento de Seguridad de Ficheros con Datos de Carácter Personal.
 - o Recorte de prensa del diario “EL PERIÓDICO” de fecha 14 de septiembre de 2009 en el que se informa sobre la protesta de vecinos de Almaraz relativa a las contrataciones de la entidad **EULEN** realizada frente a la puerta principal de la **CNA**.

FUNDAMENTOS DE DERECHO

I

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

II

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

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

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

El artículo 5.1. f) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, define datos de carácter personal como: *“Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables”*.

En este mismo sentido se pronuncia el artículo 2.a) de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, según el cual, a efectos de dicha Directiva, se entiende por dato personal *“toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social”*. Asimismo, el Considerando 26 de esta Directiva se refiere a esta cuestión señalando que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a aquélla.

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

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

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

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

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

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

Las referencias contenidas en esta Instrucción a videocámaras y cámaras se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita los tratamientos previstos en la misma.” (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 presente D^a. **A.A.A.** en calidad de ***CARGO.1 de Almaraz declara que en fecha 17 de septiembre de 2012 la responsable de la empresa de seguridad **EULEN** de

la **CENTRAL NUCLEAR DE ALMARAZ** (en adelante la **CNA**) le ha comunicado en la puerta de acceso a la **CNA** que la conversación telefónica mantenida entre ambas al número de teléfono de la Alcaldía del Ayuntamiento de Almaraz el día 14 de septiembre de 2012 entre las 13:00 y las 14:00 horas "la tiene grabada". Igualmente la denunciante manifiesta a la Guardia Civil, que los jóvenes que con ella se encontraban reivindicando agrupados en la puerta de la **CNA** son grabados "sin informar de ello", dado que han podido observar que el movimiento de las cámaras de vigilancia hacia donde se encontraba el grupo.

Pues bien, en primer lugar respecto a la supuesta grabación de la conversación telefónica denunciada cabe decir que, no existen pruebas al respecto que acrediten dicha afirmación. Así las cosas, hemos de tener en cuenta que, en base a sus especiales consecuencias, el derecho administrativo sancionador es especialmente garantista con los administrados, por lo que le son de aplicación, sin excepciones, pero con matices, los principios del procedimiento penal, destacando entre ellos el principio de presunción de inocencia, el cual ha de ser respetado en la imposición de cualesquiera sanciones, pues el ejercicio del *ius puniendi* en sus diversas manifestaciones está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones.

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

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

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

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

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

"Nuestra doctrina y jurisprudencia penal han venido sosteniendo que, aunque ambos puedan considerarse como manifestaciones de un genérico favor rei, existe una diferencia sustancial entre el derecho a la presunción de inocencia, que desenvuelve su eficacia cuando existe una falta absoluta de pruebas o cuando las practicadas no reúnen las garantías procesales y el principio jurisprudencial in dubio pro reo que pertenece al momento de la valoración o apreciación probatoria, y que ha de juzgar cuando, concurre aquella actividad probatoria indispensable, exista una duda racional sobre la real concurrencia de los elementos objetivos y subjetivos que integran el tipo

penal de que se trate.”

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

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

En definitiva, 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 segundo lugar, respecto a la grabación de la imagen de la denunciante junto a otras personas que se encontraban a las puertas de entrada a la **CNA**, sin haber sido informados al respecto, debe entrarse a valorar el cumplimiento de los requisitos exigidos en videovigilancia, por parte de la **CNA**.

Así, respecto al cumplimiento del deber de información, 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, consta aportado por la **CNA** fotografías del cartel informativo de la existencia de las cámaras, ubicado en las puertas de acceso a las CNA. 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 aporta copia de la cláusula informativa a disposición de los afectados, de conformidad con el artículo 3.b) de la citada Instrucción. Por otro lado, adjunta formulario informativo relativo al cumplimiento de la normativa específica del Consejo Seguridad Nuclear que se entrega a la firma, a las personas que acceden al recinto de la **CNA**.

Por lo tanto la **CNA**, 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.

En el caso que nos ocupa, el denunciado, es responsable del fichero dado que decide sobre la finalidad, contenido y uso del tratamiento derivado de las imágenes, requisitos necesarios para considerarse responsable del fichero, al amparo del artículo 3 d) de la LOPD.

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, las cámaras no graban sonidos y consta la inscripción por parte de **CENTRALES NUCLEARES ALMARAZ TRILLO A.I.E.**, del fichero denominado “SEGURIDAD”, en el Registro General de la Agencia Española de Protección de Datos, cuya finalidad es la seguridad y control de acceso a las instalaciones y videovigilancia.

IV

Una vez analizado el deber de información e inscripción de ficheros, procede analizar el apartado 1 y 2 del artículo 6 de la LOPD, que disponen:

“1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando 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; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

Respecto a la legitimación en el tratamiento de las imágenes, la respuesta se encuentra en el artículo 2 de la Instrucción 1/2006, que establece que: “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”.

Así, hasta la entrada en vigor, el pasado 27 de diciembre de 2009, de la Ley 25/2009, de modificación de diversas leyes para su adaptación a la Ley sobre el libre acceso a las actividades de servicios y sus ejercicio (conocida como “Ley Ómnibus”), la legitimación del tratamiento de los datos de carácter personal en materia de videovigilancia, a excepción de los casos, prácticamente imposibles dada su dificultad práctica, en los que se hubiera obtenido el consentimiento inequívoco de cada una de las personas que resulten captadas o grabadas como consecuencia del uso de las cámaras, puede proceder, en función del ámbito de aplicación, bien de la Ley 23/1992, de 30 de julio, de Seguridad Privada (en adelante LSP), o bien de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

Así hasta la entrada en vigor de la citada Ley 25/2009, la legitimación para el tratamiento la legitimación para el tratamiento por particulares y empresas de imágenes captadas a través de dispositivos de videovigilancia sólo era posible en caso de que

dichos sistemas hubieran sido contratados con empresas de seguridad privada, debidamente acreditadas ante el Ministerio del Interior, al que además debía notificarse el contrato que se hubiese celebrado, conforme a lo exigido por la Ley 23/1992, de 30 de julio de Seguridad Privada.

La Ley 25/2009 ha suprimido para la mayor parte de los casos estas exigencias, al liberalizar la comercialización, entrega, instalación y mantenimiento de estos dispositivos, de forma que ya no será necesario acudir para su puesta en funcionamiento a una empresa de seguridad privada ni cumplir las obligaciones de notificación del contrato al Ministerio del Interior..

En concreto el artículo 14 de la nueva Ley modifica el artículo 5.1 e) de la Ley 23/1992, de 30 de julio de Seguridad Privada, añadiendo una Disposición Adicional Sexta a la Ley de Seguridad Privada con la siguiente redacción:

“Disposición Adicional Sexta. Exclusión de las empresas relacionadas con equipos técnicos de seguridad:

Los prestadores de servicios y las filiales de empresas de seguridad que vendan, entreguen, instalen o mantengan equipos técnicos de seguridad, siempre que no incluyan la prestación de servicios de conexión con centrales de alarma, quedan excluidas de la legislación de seguridad privada, siempre y cuando no se dediquen a ninguno de los otros fines definidos en el artículo 5, sin perjuicio de otras legislaciones específicas que pudieran resultarles de aplicación.”

La interpretación de la mencionada disposición determina que cualquier particular o empresa cuya actividad no sea la propia de una empresa de seguridad privada podrá; “vender, entregar, instalar y mantener equipos técnicos de seguridad” sin necesidad de cumplir las exigencias previstas en la Ley de Seguridad Privada para tales empresas. De este modo, dado que la Ley permite la instalación y mantenimiento de dichos equipos por empresas distintas a las de seguridad privada, legitima a quienes adquieran de estos dispositivos para tratar los datos personales derivado de la captación de las imágenes sin necesidad de acudir a empresas de seguridad privada, siendo dicho tratamiento conforme a lo previsto en la Ley Orgánica de Protección de Datos de Carácter Personal.

No obstante, la instalación de un sistema de videovigilancia conectado a una central de alarma, sí seguirá requiriendo la concurrencia de los requisitos exigidos hasta ahora; esto es, que el dispositivo sea contratado, instalado y mantenido por una empresa de seguridad privada autorizada por el Ministerio del Interior y que el contrato sea notificado a dicho Departamento.

En todo caso, el tratamiento de las imágenes deberá cumplir los restantes 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.

En el caso que nos ocupa, consta aportado contrato de arrendamiento de servicios de seguridad (vigilancia y protección) con la empresa de seguridad autorizada **EULEN SEGURIDAD, S.A.**, así como documento de confidencialidad al respecto. Por lo tanto, el sistema de videovigilancia es mantenido por una empresa de seguridad, debidamente autorizada, por lo que el tratamiento de los datos de las personas que acceden a la misma se encuentra habilitado por la LSP.

V

Por último, respecto a las manifestaciones de la denunciante relativas a que ha sido grabada junto con otras personas en la puerta de la **CNA** “sin informar de ello”, cabe decir, que como ya ha sido desarrollado “ut supra”, la **CNA** cumple el deber de información respecto al sistema de videovigilancia instalado, según información facilitada al respecto y en segundo lugar, hay que tener en cuenta el tipo de instalación en el que se encuentra el sistema de videovigilancia. Así el motivo de la instalación de las cámaras se debe al cumplimiento de la normativa vigente en materia nuclear y en la importancia que tiene la protección física de la instalación para la salvaguardia de la población y del medio ambiente, así como para la seguridad nacional e internacional.

Dadas las características de la instalación, está sometida a diversas normativas al respecto entre la que se encuentra las Directrices establecidas por el Consejo de Seguridad Nuclear para la protección de las instalaciones nucleares concretamente la Instrucción **IS-09**, que establece los “*criterios aplicables al diseño, implantación, operación y mantenimiento de los procedimientos y servicios de protección física de las instalaciones y los materiales nucleares*” en la cual existe una parte accesible al público y otra con carácter confidencial en base a garantizar la efectividad de las medidas de protección física interior de las instalaciones, actividades y materiales, la parte confidencial de la Instrucción IS-09 puede ser únicamente consultada por personas autorizadas por razón de su función.

Así respecto a la captación de imágenes en las puertas de acceso a la **CNA**, hay que señalar que para entender las especialidades derivadas del tratamiento de las imágenes en vía pública, es preciso conocer la regulación que sobre esta materia se contempla en el artículo 1 de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos que establece: “*La presente Ley regula la utilización por las Fuerzas y Cuerpos de Seguridad de videocámaras para grabar imágenes y sonidos en lugares públicos abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías*

y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública”.

Por lo tanto, 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. Quiere ello decir que,

si las cámaras están instaladas en la entrada de un edificio, por el campo de visión de ésta podría captar un porcentaje reducido de la vía pública.

En el caso que nos ocupa, la **CNAT** manifiesta que atiende al principio de proporcionalidad exigido por la normativa de protección de datos de carácter personal ya que la captación de imágenes se circunscribe al espacio de vía pública imprescindible como es el caso de la zona de acceso a la entidad. En este caso, según toda la normativa que les es de aplicación (IS-09), es necesario captar los accesos, puertas o entradas, por lo que en dichos términos las imágenes captadas no infringirían 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.

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

Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a **CENTRALES NUCLEARES ALMARAZ TRILLO A.I.E.**, a la **DIRECCIÓN GENERAL DE LA POLICIA Y GUARDIA CIVIL** y a D^a. **A.A.A.**

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

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



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