

Expediente Nº: E/02895/2017

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **ABANCA CORPORACION BANCARIA** en virtud de denuncia presentada por D. **A.A.A.** y teniendo como base los siguientes

HECHOS

PRIMERO: Fecha de entrada de la denuncia: 3 de abril de 2017

Denunciante: D. **A.A.A.**

Denuncia a: **ABANCA**

Por los siguientes hechos según manifestaciones del denunciante: disponer de cámaras de videovigilancia instaladas de forma que pueden captar imágenes de personas circulando por la vía pública y por no disponer de avisos de zona videovigilada.

Fotografías de la cámara denunciada.

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. Existe una única cámara exterior en la oficina de **ABANCA CORPORACION BANCARIA** (en adelante **ABANCA**) situada en la (C/...1), tiene una finalidad disuasoria dentro del plan de seguridad de la entidad para evitar robos y atracos, **encontrándose fuera de servicio**. Aportan fotografía de la cámara, coincidente con las que aparece en las fotos aportadas junto a la denuncia.

Aportan como documentación acreditativa de dicho extremo un certificado expedido por **SECURITAS SEGURIDAD ESPAÑA, S.A.**, entidad que en la actualidad realiza las labores de mantenimiento del sistema de videovigilancia, en el que consta que la citada oficina de **ABANCA** cuenta con una cámara exterior que no se encuentra conectada al equipo de grabación existente.

2. El sistema de seguridad fue instalado en su día por **BOSCH SEGURIDAD Y CONTROL, SL** con el que suscribieron un contrato al efecto que fue comunicado al Ministerio del Interior, cuya copia aportan.
3. La finalidad de la instalación es la seguridad, habida cuenta de la actividad del local protegido así como el haber sido objeto de actos delictivos (tales como robos u otro tipo de atentados contra las instalaciones) y el riesgo para clientes, empleados y el resto de ciudadanos.

Aportan al respecto recortes de prensa que recogen diversos atentados cometidos contra oficinas de la entidad. Señalan a mayor abundamiento la detonación de bombas en cajeros automáticos de **ABANCA** en fechas 10 de marzo, 13 de agosto de 2013 y 25 de febrero de 2015.

4. Respecto de la **información facilitada a terceros** sobre la existencia de un sistema de videovigilancia, aportan dos fotografías del cartel donde se informa

de la zona videovigilada, así como de la entidad responsable (ABANCA) ante la que ejercer los derechos. Se aprecia que se encuentran situados en la puerta de acceso a la oficina

Aportan copia del formulario informativo que debe estar a disposición de los ciudadanos.

FUNDAMENTOS DE DERECHO

I

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

II

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

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

III

Con carácter previo, procede situar la materia de videovigilancia en su contexto normativo.

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

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

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

El artículo 5.1. f) del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal aprobada 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.

IV

En el presente caso, se denuncia la posible vulneración de la normativa de protección de datos por la existencia de cámaras de videovigilancia instaladas en la oficina de **ABANCA CORPORACION BANCARIA**, sita en de (C/...1), orientadas a la vía pública y sin avisos de zona videovigilada.

En primer lugar, debe tenerse en cuenta, en el presente supuesto, que estamos ante un establecimiento de crédito, sujeto a normativa específica.

La instalación de un sistema de seguridad en la Oficina bancaria que incluye videovigilancia, es consecuencia de la aplicación de la Ley 5/2014 de 4 de abril, de Seguridad Privada y del Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada y que continua vigente en lo que no se oponga a la citada Ley.

En concreto de lo establecido en el artículo 42 de la Ley de Seguridad Privada y en los artículos 119 y siguientes del Real Decreto 2364/1994, Sección 1ª Bancos, cajas y demás entidades de crédito, que expresamente establece, en su artículo 120.1 la necesaria instalación de equipos o sistema de captación y registro con capacidad para obtener imágenes.

A este respecto, la Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana regula la acción preventiva y vigilancia que debe llevarse a cabo y señala, respecto de las Medidas de seguridad en establecimientos e instalaciones, lo siguiente en su artículo 26: *“Establecimientos e instalaciones obligados a adoptar medidas de seguridad. Reglamentariamente, en desarrollo de lo dispuesto en esta Ley, en la legislación de seguridad privada, en la de infraestructuras críticas o en otra normativa sectorial, podrá establecerse la necesidad de adoptar medidas de seguridad en establecimientos e instalaciones industriales, comerciales y de servicios, así como en*

las infraestructuras críticas, con la finalidad de prevenir la comisión de actos delictivos o infracciones administrativas, o cuando generen riesgos directos para terceros o sean especialmente vulnerables”.

Por su parte, el Real Decreto 2364/1994, en cuanto a medidas de seguridad en general, establece en sus artículos 111.1, y 112.1.c) lo siguiente:

“111.1. De acuerdo con lo dispuesto en el artículo 13 y en la disposición adicional de la Ley Orgánica 1/1992, sobre protección de la seguridad ciudadana, y con la finalidad de prevenir la comisión de actos delictivos, la Secretaría de Estado de Interior, para supuestos supraprovinciales, o los Gobernadores Civiles podrán ordenar que las empresas industriales, comerciales o de servicios adopten las medidas de seguridad que, con carácter general o para supuestos específicos, se establecen en el presente Reglamento”.

“112.1. Cuando la naturaleza o importancia de la actividad económica que desarrollan las empresas y entidades privadas, la localización de sus instalaciones, la concentración de sus clientes, el volumen de los fondos o valores que manejen, el valor de los bienes muebles u objetos valiosos que posean, o cualquier otra causa lo hicieran necesario, el Secretario de Estado de Interior para supuestos supraprovinciales, o los Gobernadores Civiles, podrán exigir a la empresa o entidad que adopte, conjunta o separadamente, los servicios o sistemas de seguridad siguientes:

“c) Instalación de dispositivos y sistemas de seguridad y protección.”

Asimismo, el citado Reglamento, en cuanto a medidas de seguridad específicas, dispone, en sus artículos 120.1.a) y f), lo siguiente:

“120.

1. En los establecimientos u oficinas de las entidades de crédito donde se custodien fondos o valores, deberán ser instalados, en la medida que resulte necesaria en cada caso teniendo en cuenta las circunstancias enumeradas en el artículo 112 de este Reglamento y los criterios que se fijen por el Ministerio de Justicia e Interior, oyendo a la Comisión Mixta Central de Seguridad Privada:

“a) Equipos o sistemas de captación y registro, con capacidad para obtener las imágenes de los autores de delitos contra las personas y contra la propiedad, cometidos en los establecimientos y oficinas, que permitan la posterior identificación de aquéllos, y que habrán de funcionar durante el horario de atención al público, sin que requieran la intervención inmediata de los empleados de la entidad.

Los soportes destinados a la grabación de imágenes han de estar protegidos contra robo, y la entidad de ahorro o de crédito deberá conservar los soportes con las imágenes grabadas durante quince días al menos desde la fecha de la grabación, en que estarán exclusivamente a disposición de las autoridades judiciales y de las dependencias de las Fuerzas y Cuerpos de Seguridad, a las que facilitarán inmediatamente aquellas que se refieran a la comisión de hechos delictivos.

El contenido de los soportes será estrictamente reservado, y las imágenes grabadas únicamente podrán ser utilizadas como medio de identificación de los autores de delitos contra las personas y contra la propiedad, debiendo ser inutilizados el

contenido de los soportes y las imágenes una vez transcurridos quince días desde la grabación, salvo que hubiesen dispuesto lo contrario las autoridades judiciales o las Fuerzas y Cuerpos de Seguridad competentes.”

“f) Carteles del tamaño que se determine por el Ministerio de Justicia e Interior u otros sistemas de información de análoga eficacia, anunciadores de la existencia de medidas de seguridad, con referencia expresa al sistema de apertura automática retardada y, en su caso, al sistema permanente de captación de imágenes .”

En el presente caso, esas imágenes se recogen precisamente, tal como establece la Ley de Protección de Seguridad Ciudadana ya citada “... para prevenir la comisión de los actos delictivos que se puedan cometer contra ellos, cuando generen riesgos directos para terceros o sean especialmente vulnerables...”.

Asimismo, el mencionado Reglamento de Seguridad Privada, en el ya citado artículo 120.a) establece la obligatoriedad de la instalación de equipos de captación de imágenes en las entidades de crédito, exclusivamente, para la identificación de autores de delitos contra las personas o la propiedad, así como el deber de custodiar dichas imágenes y de inutilizarlas “... las imágenes grabadas únicamente podrán ser utilizadas como medio de identificación de los autores de delitos contra las personas y contra la propiedad, debiendo ser inutilizados el contenido de los soportes y las imágenes una vez transcurridos quince días desde la grabación, salvo que hubiesen dispuesto lo contrario las autoridades judiciales o las Fuerzas y Cuerpos de Seguridad competentes.”

Por otra parte, la LOPD en su artículo 11 exige el consentimiento del interesado para la comunicación de sus datos a terceros, sin embargo también señala que no será preciso dicho consentimiento cuando la comunicación “...está autorizada en una Ley, o cuando tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas.”

Así, el Reglamento de Seguridad Privada en el citado artículo 120 a) establece, respecto de las posibles comunicaciones de las imágenes, que “...estarán exclusivamente a disposición de las autoridades judiciales y de las dependencias de las Fuerzas y Cuerpos de Seguridad, a las que facilitarán inmediatamente aquellas que se refieran a la comisión de hechos delictivos...”

En consecuencia, en el presente caso, la instalación por parte de la entidad denunciada, de cámaras de videovigilancia en sus oficinas, está habilitada por una Ley y su Reglamento y, además, constituye una medida de seguridad de obligado cumplimiento.

V

Por otro lado, procede analizar el cumplimiento del deber de información denunciado.

Así, en cuanto al deber de información, el artículo 5 de la LOPD establece:

“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.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de tránsito, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.”

“2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior”.

Asimismo, la Instrucción 1/2006, en su artículo 3 dispone lo siguiente:

“3. 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.”

El derecho a la información constituye el pilar necesario para el ejercicio de otros derechos que la ley reconoce, como son los derechos de acceso, rectificación, cancelación y oposición.

Ahora bien, el citado artículo 120. 1 .f) del Reglamento de Seguridad Privada,

establece que las entidades de crédito dónde existan medidas de seguridad consistentes en un sistema permanente de captación de imágenes deberán colocar "... *Carteles del tamaño que se determine por el Ministerio de Justicia e Interior u otros sistemas de información de análoga eficacia, anunciadores de la existencia de medidas de seguridad, con referencia expresa ..., en su caso, al sistema permanente de captación de imágenes.*"

En el caso que nos ocupa, en cuanto a la información proporcionada sobre cámaras de videovigilancia en la oficina bancaria, consta mediante su aportación a las actuaciones previas de Inspección, la existencia de cartel informativo ubicado en la puerta de acceso a la oficina en el que se informa de la existencia de las cámaras con indicación del responsable de las mismas. Asimismo, se aporta formulario informativo a disposición de los interesados, de conformidad con el artículo 3b) de la Instrucción 1/2006.

Por lo tanto la citada sucursal cumple el deber de información respecto al sistema de videovigilancia instalado.

Por último respecto a la captación de imágenes de la vía pública, el artículo 4.1 y 2 de la LOPD, que 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".

Así, 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.

En el caso que nos ocupa existe una única cámara exterior en la oficina de ABANCA, situada en la (C/...1), que tiene una finalidad disuasoria dentro del plan de seguridad de la entidad para evitar robos y atracos, encontrándose fuera de servicio. Aportan como documentación acreditativa de dicho extremo un certificado expedido por SECURITAS SEGURIDAD ESPAÑA, S.A., entidad que en la actualidad realiza las labores de mantenimiento del sistema de videovigilancia, en el que consta que la citada oficina de ABANCA cuenta con una cámara exterior que no se encuentra conectada al equipo de grabación existente.

Sobre esta cuestión debe señalarse que el Tribunal Constitucional ha declarado de forma reiterada 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 inculpativos 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, la Ley 40/2015, de 1 de octubre de Régimen Jurídico del Sector Público recoge en su artículo 28.1: *“Sólo podrán ser sancionados por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa”*

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 la imputación o de la intervención en los mismos del presunto infractor.

En el presente caso, al tratarse de una cámara fuera de servicio, no captaría imágenes de personas físicas identificadas o identificables, por lo que, al no quedar acreditada la existencia de un tratamiento de datos personales, la cuestión se encuentra al margen de la normativa de protección de datos. Por consiguiente es de aplicación el principio de presunción de inocencia, pues de la mera existencia de una cámara de videovigilancia no se desprende automáticamente que la misma funcione y que por tanto capte imágenes de personas y, en consecuencia, que exista un tratamiento de datos personales, no constando en el expediente indicio alguno de que dicho tratamiento se esté llevando a cabo.

Alcanzada la conclusión anterior, es conocido que en otros supuestos similares esta Agencia ha venido considerado que la instalación de dispositivos que generaban la apariencia de que habían sido instaladas cámaras de videovigilancia que, en su caso, podrían ser susceptibles de ser puestas en funcionamiento, con el consiguiente tratamiento de datos personales, podía generar una situación de alarma entre las personas, que entendían que eran vigiladas a través de dichos dispositivos, al producirse una apariencia de tratamiento. Teniendo esto en cuenta, y aun cuando por esta Agencia se acordaba el archivo del expediente en cuestión, se requería igualmente la retirada del dispositivo.

Sin embargo, esta Agencia consideró necesario revisar el mencionado criterio, en los términos que se plasman, entre otras, en la resolución del PS/00542/2015 de fecha 11 de noviembre de 2015. De este modo, la inexistencia de prueba alguna acerca de un posible de datos de carácter personal implica que la presente resolución de archivo no incorpore ningún tipo de requerimiento en el sentido que se ha mencionado, al prevalecer el principio de presunción de inocencia.

En todo caso, lo antedicho no impide que si constase acreditado en el futuro el tratamiento de los datos a través de la grabación de las imágenes o su visualización en tiempo real, vulnerando la normativa de protección de datos, esta Agencia pueda adoptar las medidas y llevar a cabo las actuaciones que procedan en virtud de las competencias que a la misma otorga la LOPD, a fin de garantizar el derecho fundamental a la protección de datos de carácter personal.

Asimismo se informa que el artículo 35 de la Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal, recoge: “La Agencia de

Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones". Por su parte, el artículo 37 de la LOPD delimita dichas funciones, destacando la primera de ellas que es "Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación...". Y es que según el artículo 1 de la LOPD, dicha norma 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". Por tanto, el ámbito propio de actuación de esta Agencia se refiere, con carácter general, a los datos de carácter personal definidos en el artículo 3. a) LOPD.

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

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

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

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