



Expediente Nº: E/02703/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

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

HECHOS

PRIMERO: Con fecha 21 de febrero de 2014 tiene entrada en esta Agencia escrito de D. **A.A.A.** (en adelante el denunciante) comunicando posible infracción a la Ley Orgánica 15/1999 motivada por cámara de videovigilancia cuyo titular es la entidad **ABANCA Corporación Bancaria S.A.** (antigua **NOVAGALICIA BANCO S.A.**) (en adelante el denunciado) instalada en **SUCURSAL DE (C/.....1) - SANTIAGO DE COMPOSTELA (A CORUÑA)**, sin cartel de zona videovigilada, enfocada hacia vía pública.

El denunciado declara que la mencionada entidad dispone de cámara enfocando a la vía pública. Las grabaciones están en posesión de la Guardia Civil y de los juzgados. Manifiesta que no consta distintivo de zona videovigilada en su exterior. Adjunta dos fotografías supuestamente captadas por las cámaras denunciadas y publicadas en un programa de una cadena de televisión.

Con fecha 28 de abril de 2014 tiene entrada en esta Agencia escrito de la Unidad Central de Seguridad Privada de la Dirección General de la Policía remitiendo documentación presentada por el denunciante en relación a los mismos hechos denunciados.

Con fecha 12 de octubre de 2014 tiene entrada en esta Agencia escrito del denunciante remitiendo informe R.11.Q/1776/13 del Defensor del Pueblo gallego de 16/09/2014.

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:

Desde el pasado día 27 de junio de 2014, NCG BANCO, S.A. opera en el Mercado bajo la marca comercial ABANCA.

Con fecha 13 de mayo de 2014 se solicita información a la entidad denunciada teniendo entrada en esta Agencia con fecha 13 de junio y 24 de noviembre de 2014 escritos en los que manifiesta:

1. La entidad responsable es NCG BANCO, S.A. (NOVAGALICIA BANCO).
2. La empresa de seguridad que realizó la instalación del sistema de videovigilancia en

la oficina denunciada fue BOSCH Seguridad y Control, S.L.

NOVAGALICIA BANCO y BOSCH Seguridad y Control, S.L. han venido suscribiendo, cada año, dos contratos, de duración anual, de prestación de servicios de seguridad para la red de oficinas de aquél, a saber, el contrato de mantenimiento de los sistemas de seguridad y el contrato de conexión a central receptora de alarmas. Aporta copia de los contratos para el año 2014, como Anexos I y II, respectivamente, consignados por escrito, con arreglo a modelo oficial, y comunicados al Ministerio del Interior.

3. La instalación de las videocámaras de seguridad en la oficina referida responde, conforme a la finalidad prevista en el artículo 1 de la Ley 23/1992, de 30 de julio, de Seguridad Privada (LSP), a la necesidad de garantizar adecuadamente la protección de la seguridad de las personas y de los bienes, habida cuenta de la naturaleza de dicha oficina y de la actividad que en la misma se desarrolla.

Se aportan como Anexo III, recortes de prensa que hacen referencia a diversos atentados cometidos contra distintas oficinas de NOVAGALICIA BANCO (anteriormente, CAIXA GALICIA), como el cometido el 23/07/2005 contra la Oficina Central de CAIXA GALICIA en Santiago de Compostela.

4. Por lo que se refiere al cartel donde se informa de la existencia de videocámaras de seguridad, se acompaña, como Anexo IV, la fotocopia en tamaño reducido del adhesivo antivandálico correspondiente a dicho cartel, significando que éste se encuentra ubicado en la puerta exterior de la sucursal referida.
5. Respecto del modelo del formulario informativo que ha de estar a disposición de los ciudadanos según se recoge en el artículo 3.b de la Instrucción 1/2006, se adjunta como Anexo V la fotocopia de dicho modelo. Acerca del procedimiento establecido para distribuir los citados formularios ante una petición de los mismos, dicho procedimiento se basa en la exposición de los formularios en los tableros de anuncios ubicados en lugares destacados de las oficinas, en la forma indicada en el apartado 3 de la Norma Tercera de la Circular 5/2012, de 27 de junio, del Banco de España, a entidades de crédito y proveedores de servicios de pago, sobre transparencia de los servicios bancarios y responsabilidad en la concesión de préstamos. Copia del formulario informativo al que se refiere el artículo 3.b de la Instrucción 1/2006 se entregará por la oficina a toda persona que lo desee, a su simple solicitud.
6. La oficina de referencia dispone de quince videocámaras de seguridad, esto es:
 - a. Una videocámara de seguridad exterior, ubicada en la fachada de la propia oficina.
 - b. Catorce videocámaras de seguridad interiores: diez ubicadas en los puestos de trabajo, una en la entrada de la sucursal, una que enfoca el cajero automático y dos en la planta -1.

Todas las videocámaras de seguridad son fijas y no disponen de zoom.

7. Se adjunta como Anexo VI las fotografías de las quince videocámaras de seguridad de las que dispone la sucursal; y
8. Se adjunta como Anexo VII las fotografías de las imágenes que captan las citadas videocámaras.
 - a. la videocámara exterior se encuentra enfocada única y exclusivamente hacia la fachada de la oficina y sus accesos, en escrito de fecha

24/11/2014.

- b. la videocámara exterior está orientada de modo que la parte de vía pública que recoge se limita exclusivamente al acceso vigilado, sin recoger más imagen de la vía pública que la de la limitada porción de la misma que resulta imposible evitar por razón de la propia ubicación de la videocámara.
9. La empresa de seguridad BOSCH Seguridad y Control, S.L. dispone de monitores que permiten visualizar las imágenes captadas por las videocámaras como respuesta a la transmisión de una alarma de seguridad. Dichos monitores se hallan ubicados en las instalaciones que dicha empresa de seguridad ocupa en su dirección de A Coruña.
10. Los circuitos cerrados de televisión (CCTV) de las instalaciones de videovigilancia disponen, de manera individual y por centro, de un grabador digital.
11. El acceso a este grabador digital ---cuyo contenido es estrictamente reservado y confidencial y, por tanto, a las imágenes captadas, sólo se puede realizar desde la Central Receptora de Alarmas, siendo los operadores de la empresa de seguridad BOSCH Seguridad y Control, S.L., a la se ha encomendado la explotación de central de alarmas, los que pueden acceder a las mismas como respuesta a la gestión de una alarma o atendiendo a la solicitud de requerimiento emitido por Fuerzas y Cuerpos de Seguridad del Estado o Autoridad Judicial.

Puede tener acceso a las imágenes el Director de Seguridad de NOVAGALICIA BANCO (personal propio de la entidad de crédito) conforme a lo establecido en la LSP y en el Reglamento de Seguridad Privada, que la desarrolla, a los exclusivos fines previstos en el artículo 1 de la propia LSP, a saber, garantizar adecuadamente la protección de la seguridad de las personas y de los bienes.

12. Las imágenes grabadas, tal y como establece el vigente Reglamento de Seguridad Privada en su artículo 120, son conservadas durante quince días desde la fecha de la grabación. Las imágenes grabadas únicamente son, en su caso, utilizadas como medio de identificación de los autores de delitos contra las personas y contra la propiedad, siendo inutilizados tanto el contenido de los soportes como las imágenes una vez transcurrido el referido plazo de quince días desde la grabación, salvo que dispongan lo contrario las autoridades judiciales o las Fuerzas y Cuerpos de Seguridad competentes.
13. NOVAGALICIA BANCO notificó un fichero a la Agencia Española de Protección de Datos de Carácter Personal, habiendo sido inscrito el mismo en el Registro General de Protección de Datos bajo la denominación "SEGURIDAD FÍSICA", con la siguiente descripción de la finalidad: "GESTION Y CONTROL DE ACCESO FISICO A EDIFICIOS Y CAMARAS DE VIDEOVIGILANCIA". El código de inscripción del fichero es el nº *****CÓD.1.**

Mediante una diligencia se ha comprobado la inscripción del fichero en el RGPD de esta Agencia.

14. El sistema de videovigilancia está conectado a una central de alarmas.
 - a. Tal y como se ha manifestado en el punto 2º, la empresa de seguridad que realizó la instalación de las videocámaras fue BOSCH Seguridad y Control, S.L. Las fotocopias de los contratos de prestación de servicios de seguridad suscritos con BOSCH Seguridad y Control, S.L. se

adjuntan como Anexos I y II.

- b. La documentación acreditativa tanto de que BOSCH Seguridad y Control, S.L. está autorizada como empresa de seguridad privada por el órgano administrativo competente del Ministerio del Interior, con número de acreditación 2.665, la constituyen los siguientes escritos:

-La fotocopia de la Resolución del Director General de la Policía, de fecha 2/4/1998, de habilitación e inscripción en el correspondiente Registro del Ministerio del Interior de la empresa de seguridad BOSCH Seguridad y Control, S.L. Anexo VIII.

-La fotocopia de la Resolución del Director General de la Policía, de fecha 23/11/2010, por la que acuerda acceder a la petición formulada por BOSCH Seguridad y Control, S.L. de modificación del domicilio de la Central de Alarmas. Anexo IX.

- c. En cuanto a la notificación a la autoridad competente en materia de seguridad privada acerca de las características de la instalación de las videocámaras interiores y exteriores a que este escrito se refiere:

-Conforme a lo dispuesto en el párrafo segundo del punto 1 del artículo 136 del RSP, "Cuando se trate de la reforma de un establecimiento u oficina, anteriormente autorizados, que implique la adopción o modificación de medidas de seguridad (ya sean éstas medidas obligatorias o no, ya que la norma no distingue), bastará la comunicación a las dependencias policiales competentes, para su comprobación".

En el caso de la sucursal que ahora nos ocupa, la misma, como se explicita en los puntos siguientes, fue objeto de una reforma que implicó la actualización y ampliación del sistema de videovigilancia.

Dadas las características excepcionales del proceso de fusiones de entidades financieras que se ha venido desarrollando en España, la Dirección General de la Policía y de la Guardia Civil ha establecido un Protocolo de Comunicaciones a fin de coordinar las actuaciones policiales y las del sector financiero. Se adjunta la fotocopia de dicho Protocolo como Anexo X.

En virtud de lo dispuesto en el citado Protocolo de Comunicaciones, comunicación relativa a las oficinas afectadas por el correspondiente proceso de reestructuración, podrá realizarse a la finalización del citado proceso de reestructuración.

NOVAGALICIA BANCO estuvo inmerso en un proceso de reestructuración que se inició a comienzos del año 2011.

NOVAGALICIA BANCO es la entidad resultante de la escisión por segregación de los activos, pasivos y relaciones jurídicas que integraban el patrimonio afecto a la actividad financiera de Novacaixagalicia, entidad resultante, a su vez, de la fusión de Caixa Galicia y Caixanova.

El proceso de reordenación de la red de sucursales, dio comienzo a inicios del ejercicio 2011 y siguió desenvolviéndose a lo largo del ejercicio 2012, hasta su completa finalización.

A este respecto, se aportan al presente escrito:

como Anexo XI, la fotocopia del escrito presentado en la Subdelegación del Gobierno en A Coruña por NOVAGALICIA BANCO en fecha 21/11/2011, en el que se comunica a dicha Subdelegación el cierre de la Oficina sita en la calle

(C/.....2) (Santiago de Compostela) y el mantenimiento, como oficina receptora del negocio de aquélla, de la Sucursal denunciada, sita en la (C/.....3) (Santiago de Compostela); y

como Anexo XII un Oficio emitido en fecha 23/11/2011 por la Unidad Central de Seguridad Privada, dejando constancia de que NOVAGALICIA BANCO estaba dando cumplimiento a lo dispuesto en el Protocolo de Comunicaciones

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.”

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 caso, se denuncia la posible vulneración de la normativa de protección de datos por la existencia de cámaras de videovigilancia instaladas en la oficina del **ABANCA CORPORACIÓN BANCARIA S.A.** (antigua **NOVAGALACIA BANCO S.A.**) instaladas en **SUCURSAL DE (C/.....1)-SANTIAGO DE COMPOSTELA (A CORUÑA).**

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

El requisito del consentimiento del titular de los datos para el tratamiento, hay que ponerlo en relación, por un lado, con la información a la que hace referencia tanto el artículo 5 de la LOPD, como el artículo 3 de la Instrucción 12/2006, y por otro lado, con la dispensa de dicho consentimiento cuando ésta esté amparada en una ley, como es el caso de la normativa específica de seguridad.

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 1/1992, de 21 de febrero, sobre Protección de La Seguridad Ciudadana, en su artículo 13, en su Disposición Adicional Única y en su Disposición Final Cuarta, 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:

1. *“El Ministerio del Interior podrá ordenar, conforme a lo que disponga reglamentariamente, la adopción de las medidas de seguridad necesarias en establecimientos e instalaciones industriales, comerciales y de servicios, para prevenir la comisión de los actos delictivos que se puedan cometer contra ellos, cuando generen riesgos directos para terceros o sean especialmente vulnerables.*
2. *No obstante, las autoridades competentes podrán eximir de la implantación o el mantenimiento de medidas de seguridad obligatorias a los establecimientos, cuando las circunstancias que concurran en el caso concreto las hicieren innecesarias o improcedentes.*
3. *La apertura de los establecimientos que estén obligados a la adopción de medidas de seguridad estará condicionada a la comprobación, por las autoridades competentes, de la idoneidad y suficiencia de las mismas.*
4. *Los titulares de los establecimientos e instalaciones serán responsables de la adopción o instalación de las medidas de seguridad obligatorias, de acuerdo con las normas que respectivamente regulen, así como su efectivo funcionamiento y de la consecución de la finalidad protectora y preventiva propia de cada medida, sin perjuicio de la responsabilidad en que al respecto pueden incurrir sus empleados.”*

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 denuncia 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.

Por otro lado, el sistema se compone de quince cámaras, todas interiores menos una ubicada en la fachada de la oficina. De las fotografías aportadas de las imágenes captadas de la cámara exterior, se desprende que ésta está orientada y captando imágenes de la fachada de la oficina y acceso y un mínimo espacio anexo a la misma. Por lo tanto, la citada cámara cumpliría, 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”.

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.

A este respecto el denunciante aporta dos fotografías supuestamente captadas por las cámaras denunciadas y publicadas en un programa de una cadena de televisión. Respecto a esta cuestión cabe decir que, no existen pruebas aportadas que corroboren con la certeza necesaria que dichas imágenes proceden de las cámaras denunciadas. Ha de tenerse en cuenta que el Tribunal Constitucional viene manteniendo que los principios y garantías del procedimiento judicial penal son, en principio y con las oportunas modulaciones, aplicables al procedimiento administrativo sancionador, dado que también este es manifestación del ordenamiento punitivo del Estado, resultando clara la plena virtualidad del principio de presunción de inocencia. En tal sentido, el Tribunal Constitucional, en Sentencia 76/1990 considera que el derecho a la presunción de inocencia comporta *“que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio”*.

De acuerdo con este planteamiento, el artículo 130.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en lo sucesivo LRJPAC), establece que *“Sólo podrán ser sancionados por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aun a título de simple inobservancia.”*

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

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

En definitiva, la aplicación del principio de presunción de inocencia impide imputar una infracción administrativa cuando no se haya obtenido y comprobado la existencia de una prueba de cargo acreditativa de los hechos que motivan esta imputación.

En este punto procede traer a colación la Sentencia de la Audiencia Nacional de fecha 25/05/2001 que señala que *“de la valoración de la prueba obrante en el expediente administrativo se llega a la conclusión que no ha quedado debidamente acreditado este hecho integrador del tipo, es decir no se prueba que el Banco entregara al Sr... el respectivo extracto, suscitándole este hecho concreto serias dudas, frente a la exigible certidumbre”*. Y concluye afirmando que *sin negar que pudieron producirse los hechos como indica la denunciante, tampoco puede rechazarse la posibilidad que el extracto no le fuera entregado al marido por el Banco, sino que aquel lo obtuviera aprovechando alguna visita al domicilio o mediante la actuación de algún familiar, dicho ello en términos de pura hipótesis”*.

No obstante, como ya se ha desarrollado anteriormente, se ha acreditado en fase de actuaciones previas que, en la actualidad las cámaras de dicha entidad cumplen el principio de proporcionalidad, captando imágenes del interior de la oficina y la exterior, un espacio proporcional de vía pública. Por lo tanto el sistema de videovigilancia, realiza un tratamiento proporcional de las imágenes, en relación con el ámbito y las finalidades

que podrían justificar su recogida.

A la vista de lo expuesto, la entidad bancaria cumple respecto al sistema de videovigilancia instalado, la normativa relativa a la seguridad privada y es proporcional para la finalidad perseguida.

IV

Una vez desarrollado el cumplimiento por parte de la entidad bancaria de la normativa en materia de seguridad privada, procede analizar el cumplimiento del deber de información e inscripción de ficheros, exigido por la normativa de protección de datos.

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.”

La existencia de esta información en la recogida de datos que reconoce el artículo 5 de la LOPD, constituye un derecho del afectado que es objeto de protección por sí mismo, aunque también es, lógicamente, un complemento previo de la prestación del consentimiento.

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 donde 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 ubicados en la puerta exterior 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.

Por su parte, la Instrucción 1/2006, en su artículo 7 establece:

“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...”

En el caso que nos ocupa, se comprueba por la Subdirección General de Inspección de Datos la existencia de un fichero inscrito en el Registro General de Protección de Datos, con nombre SEGURIDAD FÍSICA, entre cuyas finalidades está la videovigilancia, en fecha 5 de enero de 2012.

V

En consecuencia, vistos los preceptos legales de aplicación y los hechos que

constan en las actuaciones previas de investigación, ha quedado acreditado que la sucursal denunciada, en la actualidad, informa de la existencia de cámaras de videovigilancia, tiene fichero inscrito, cumple la normativa de seguridad privada y son proporcionales a la finalidad perseguida, por lo tanto que se procede el archivo del presente expediente.

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 **ABANCA CORPORACIÓN BANCARIA S.A. (antiguo NOVAGALICIA BANCO S.A.)** y a D. **A.A.A.**.

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