

Expediente Nº: E/05885/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **BANCO BILBAO VIZCAYA ARGENTARIA SA** y, **TRANSCOM WORLDWIDE SPAIN S.L.** en virtud de denuncia presentada por D. **A.A.A.** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 2 de septiembre de 2014 tiene entrada en esta Agencia escrito de D. **A.A.A.** en calidad de representante sindical de la Confederación General del Trabajo de la empresa **TRANSCOM WORLDWIDE SPAIN S.L.** (en adelante el denunciante) comunicando posible infracción a la Ley Orgánica 15/1999 motivada por cámaras de videovigilancia instaladas en el centro de trabajo perteneciente al cliente **BANCO BILBAO VIZCAYA ARGENTARIA SA** (en adelante el denunciado) para el que presta servicios **TRANSCOM WORLDWIDE SPAIN S.L.** ubicado en (C/.....1) - MADRID.

El denunciante manifiesta que en el centro de trabajo perteneciente al cliente BBVA para el que presta servicios Transcom Worldwide Spain, S.L., sito en la C/ Isla Sicilia, 3, 1 planta, 28034 — Madrid, se hallan instaladas unas cámaras de seguridad que complementan la labor de vigilancia del personal específicamente contratado para ello a través de una empresa de seguridad.

Asimismo manifiesta que, el funcionamiento de esas cámaras, algunas de las cuales incluso están orientadas a la vía pública, podría vulnerar el principio de adecuación y proporcionalidad exigido por el Art. 4 de la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, amén del derecho de información, rectificación y cancelación prescrito con carácter general en el Título III de la Ley Orgánica de Protección de Datos de Carácter Personal, siendo titulares de este derecho entre otros los trabajadores de Transcom Worldwide Spain, S.L. que allí desempeñan su labor.

Por último, aporta escrito dirigido a la empresa **TRANSCOM WORLDWIDE SPAIN S.L.**, para que se les facilite copia del contrato que rige el uso de las cámaras de seguridad en el edificio propiedad del BBVA, sin haber obtenido respuesta al respecto.

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. Con fecha 25 de septiembre de 2014 se solicita información a **TRANSCOM WORLDWIDE SPAIN S.L.** teniendo entrada en esta Agencia con fecha 8 de octubre de 2014 escrito del representante de la entidad en el que manifiesta que el sistema de video vigilancia al que se hace referencia pertenece a BBVA. Transcom en ningún momento ha

intervenido ni ha tenido ninguna relación con el mismo. Su instalación es obra de BBVA, que opera por su cuenta dicho sistema de videovigilancia. Así, Transcom no lleva a cabo ningún tratamiento de datos en relación las cámaras de videovigilancia, no tiene acceso a las imágenes captadas por las mismas bajo ninguna circunstancia, y tampoco colabora en ningún sentido con BBVA en su funcionamiento.

2. Con fecha 14 de enero de 2015 se solicita información a **BANCO BILBAO VIZCAYA ARGENTARIA SA**, en adelante BBVA, teniendo entrada en esta Agencia con fecha 29 de enero de 2015 escrito del representante de la entidad en el que manifiesta:

- BBVA no realizó la instalación de las citadas cámaras sino que las mismas estaban ya instaladas cuando se adquirió el edificio en el año 2004.
- La decisión de mantener las cámaras de videovigilancia en el edificio de la Calle de Isla Sicilia número 3, se ha producido dado que en dicho edificio se halla ubicado el servicio de atención telefónica a clientes del grupo BBVA, desde esta plataforma los clientes realizan todo tipo de operaciones bancarias y financieras, desde transferencias hasta la gestión de tarjetas de crédito o débito, gestión de números PIN, etc.

Por esta circunstancia, este centro tiene que estar dotado con un servicio de vigilancia 24h durante los 365 días del año con la finalidad de protección tanto a los operadores de este servicio como a los medios técnicos y de servicio que allí se ubican, evitando con ello la intrusión de personas que pudiesen, bajo coacción o por otros sistemas, realizar operaciones ilícitas contra la Entidad o sus clientes.

Por otra parte, BBVA como entidad financiera, se encuentra dentro de la red de infraestructuras críticas identificadas por el Ministerio del Interior, debiendo ser protegida contra los posibles actos terroristas, evitando daños personales y, en su caso, materiales que pudiesen provocar la paralización de la normal actividad de la Entidad.

- Aportan reportaje fotográfico de los carteles donde se informa de la existencia de cámaras de videovigilancia así como la identidad del responsable de las mismas ante quién pueden ejercitarse los derechos de protección de datos de carácter personal.

Los carteles se ubican de tal forma que cualquier persona que acceda al inmueble, necesariamente ha de pasar por delante de dichos carteles informativos y quedar informada de lo que en los mismos se declara.

- Asimismo se aporta modelo de solicitud para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de datos personales.

- El edificio cuenta con cámaras analógicas de circuito cerrado de Televisión, siendo recogidas las señales de video de estas cámaras por dos videograbadores digitales de 16 entradas de video cada uno. Aportan planos de situación de las mismas con la numeración de cada una de ellas.

- Las cámaras solo captan grabaciones en zonas de paso, vías de evacuación, cuartos técnicos y perímetro, nunca captan imágenes de puestos de trabajo. En ningún caso las cámaras se han instalado como medida de vigilancia, control o ubicación de los trabajadores sino para la seguridad y vigilancia del centro de trabajo.

- Aportan reportaje fotográfico de las cámaras y de las imágenes que captan cada una de ellas, de lo que se desprende que todas recogen imágenes interiores excepto las cámaras exteriores dotadas de máscara de privacidad para evitar la

captación de viviendas y vías públicas.

- Las imágenes captadas por las cámaras se visualizan desde el puesto permanente de seguridad, atendido las 24 horas de cada día y los 365 días del año por personal de Seguridad Privada habilitado, según Ley 5/2014 de Seguridad Privada, pertenecientes a la empresa SEGURISA (Servicios Integrales de Seguridad S.A). Aportan copia del contrato vigente.

-

- Los monitores de visualización quedan ocultos al público, impidiendo la visualización salvo al personal de seguridad autorizado al efecto y para el cumplimiento de sus finalidades. Aportan fotografía de los monitores.

- Las personas que pueden tener acceso al sistema de videovigilancia instalado son aquellas personas que disponen de usuario autorizado y contraseña personalizada, dichas claves son otorgadas por el responsable de BBVA al personal de vigilancia. El desarrollo de sus funciones se realiza mediante un compromiso de confidencialidad nominativo entre los usuarios de los mismos y el responsable de las grabaciones (BBVA).

- El tiempo de conservación de las grabaciones de imágenes es de 20 días. En ningún caso el sistema admite grabaciones superiores a los 30 días.

- Aportan copia del justificante de inscripción del fichero de videovigilancia en el Registro General de Protección de Datos con el Código de inscripción número ***CÓD.1.

- Aportan copia del Documento de Seguridad.

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 expediente D. **A.A.A.** en calidad de representante sindical de la Confederación General del Trabajo de la empresa **TRANSCOM WORLDWIDE SPAIN S.L.** denuncia la posible infracción a la Ley Orgánica 15/1999 motivada por cámaras de videovigilancia instaladas en el centro de trabajo perteneciente al cliente **BANCO BILBAO VIZCAYA ARGENTARIA SA** (en adelante el denunciado) para el que presta servicios **TRANSCOM WORLDWIDE SPAIN S.L.** ubicado en **(C/.....1) - MADRID.**

En primer lugar, cabe decir que ante dicha denuncia los Servicios de Inspección de esta Agencia solicitan, con fecha 25 de septiembre de 2014, información a **TRANSCOM WORLDWIDE SPAIN S.L.** teniendo entrada en esta Agencia con fecha 8 de octubre de 2014 escrito del representante de la entidad en el que manifiesta que el sistema de video vigilancia al que se hace referencia pertenece a BBVA. Transcom en ningún momento ha intervenido ni ha tenido ninguna relación con el mismo. Su instalación es obra de BBVA, que opera por su cuenta dicho sistema de videovigilancia. Así, Transcom no lleva a cabo ningún tratamiento de datos en relación las cámaras de

videovigilancia, no tiene acceso a las imágenes captadas por las mismas bajo ninguna circunstancia, y tampoco colabora en ningún sentido con BBVA en su funcionamiento.

Con fecha 14 de enero de 2015 se solicita información a BBVA, teniendo entrada en esta Agencia con fecha 29 de enero de 2015 escrito del representante de la entidad en el que manifiesta que BBVA no realizó la instalación de las citadas cámaras sino que las mismas estaban ya instaladas cuando se adquirió el edificio en el año 2004 si bien se tomó la decisión de mantener las cámaras de videovigilancia en el edificio de la Calle de Isla Sicilia número 3, dado que en dicho edificio se halla ubicado el servicio de atención telefónica a clientes del grupo BBVA, desde esta plataforma los clientes realizan todo tipo de operaciones bancarias y financieras, desde transferencias hasta la gestión de tarjetas de crédito o débito, gestión de números PIN, etc.

En primer lugar, debe entrarse a valorar el cumplimiento del deber de información por parte de la entidad responsable del sistema de videovigilancia BBVA.

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, constan aportadas por la entidad BBVA fotografías de la existencia de cartel informativo de la existencia de las cámaras, ubicados en las fachadas de acceso y en el vestíbulo principal, acordes al que hace referencia el citado artículo 3.a) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD. Asimismo se aporta modelo de solicitud para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de datos personales.

Respecto al formulario informativo a disposición de los interesados, si bien en este caso, el establecimiento denunciado tienen instalados los carteles informativos de conformidad con el artículo 5.1 de la LOPD y conforme a lo estipulado en el Anexo de la Instrucción 1/2006, también deberá disponer de los citados impresos, exigidos por el artículo 3. b) de la citada Instrucción, a disposición de los interesados. Estos formularios puedan estar preimpresos y preparados por el responsable del tratamiento, o tener la posibilidad de imprimirlos en el momento de su demanda, bien por tener preparado un documento Word o por tener conexión a Internet que permita acceder a la página web de la Agencia Española de Protección de Datos y poder descargarse el modelo de formulario referido.

Por 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.

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, consta la inscripción por parte del BBVA, del fichero denominado “Videovigilancia”, en el Registro General de la Agencia Española de Protección de Datos en fecha 28/09/2007

Asimismo las imágenes se conservan por un periodo de 20 días de conformidad con el artículo 6 de la citada Instrucción, que recoge: *“Los datos serán cancelados en el plazo máximo de un mes desde su captación”.*

IV

Por otro lado, respecto a la posible captación de imágenes de la vía pública, a través del sistema de videovigilancia instalado, cabe decir que 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”.

Para que la excepción recogida en el artículo 4.3 de la Instrucción 1/2006 resulte aplicable no deberá existir una posibilidad de instalación alternativa, sin poder interpretarse que dicho precepto constituye una habilitación para captar imágenes en espacios públicos, puesto que en ningún caso puede admitirse el uso de prácticas de vigilancia más allá del entorno objeto de la instalación y en particular en lo que se refiere a los espacios públicos circundantes, edificios contiguos y vehículos distintos de los que accedan al espacio vigilado.

En el caso que nos ocupa, del reportaje fotográfico de las cámaras y de las imágenes que captan cada una de ellas, se desprende que todas las cámaras interiores recogen imágenes de zonas de paso, vías de evacuación, cuartos técnicos, no captan imágenes de puestos de trabajo. Las cámaras exteriores están dotadas de una máscara de privacidad para evitar la captación de espacios públicos más allá de lo que resulta proporcional. El espacio público captado con las citadas máscaras con las máscaras de privacidad no infringen 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

No obstante, se le recomienda la sustitución de las cámaras que tienen máscaras de privacidad (informáticas-electrónicas) por otros tipos de cámara o dispositivos que no generen expectativas de captación de la vía pública o bien una reorientación de dichas

cámaras para evitar la generación de dicha expectativa.

V

Por último señalar que BBVA tiene suscrito contrato de prestación de servicio de seguridad con la entidad **SEGURISA, SERVICIOS INTEGRALES DE SEGURIDAD, S.A.** en fecha 1 de abril de 2011. En dicho contrato se desarrolla las cláusulas relativas a confidencialidad (cláusula sexta) y acceso a datos personales (cláusula séptima), de conformidad con lo previsto en el artículo 12 de la LOPD.

Las imágenes captadas por las cámaras se visualizan desde el puesto permanente de seguridad, atendido las 24 horas de cada día y los 365 días del año por personal de Seguridad Privada habilitado, según Ley 5/2014 de Seguridad Privada, pertenecientes a la empresa SEGURISA.

Las personas que pueden tener acceso al sistema de videovigilancia instalado son aquellas personas que disponen de usuario autorizado y contraseña personalizada, dichas claves son otorgadas por el responsable de BBVA al personal de vigilancia. El desarrollo de sus funciones se realiza mediante un compromiso de confidencialidad nominativo entre los usuarios de los mismos y el responsable de las grabaciones (BBVA), determinado en el contrato suscrito entre las partes.

A la vista de lo expuesto se procede al archivo del presente expediente de actuaciones previas.

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 **BANCO BILBAO VIZCAYA ARGENTARIA SA, TRANSCOM WORLDWIDE SPAIN S.L.** 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