

Expediente Nº: E/06110/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **APPLE RETAIL SPAIN S.L** en virtud de denuncia presentada por la **POLICIA MUNICIPAL DE MADRID** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha de 12 de agosto de 2014 tiene entrada en esta Agencia escrito remitido por ÁREA DE GOBIERNO DE SEGURIDAD Y EMERGENCIAS, DIRECCIÓN GENERAL DE SEGURIDAD, en el que se remite informe del CUERPO DE POLICÍA MUNICIPAL, UID CENTRO SUR, comunicando posible infracción a la Ley Orgánica 15/1999 motivada por la existencia de cámaras de videovigilancia en el establecimiento con denominación comercial **APPLE STORE** sito en **(C/.....1), MADRID** y cuyo titular es la entidad **APPLE RETAIL SPAIN S.L** (en adelante el denunciado).

En el mencionado informe la Policía manifiesta que en visita de inspección girada al citado establecimiento observan: *"...un sistema de videovigilancia compuesto por 21 cámaras de grabación, una de las cuales se localiza en la zona de entrada a la tienda grabando el exterior de la vía pública. No existen carteles informativos de zona videovigilada que señalicen los dispositivos"*.

Adjunta a su informe, boletín de denuncia nº *****.

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 fechas 6 de octubre y 5 de noviembre de 2014 se solicita información al responsable del sistema de videovigilancia instalado, teniendo entrada en esta Agencia escritos de fechas 22 de octubre, 5 y 12 de noviembre de 2014, en los cuales manifiesta:

*La entidad **APPLE RETAIL SPAIN S.L** es responsable del establecimiento en el que se localiza el sistema de videovigilancia investigado.*

La empresa Orion Security Solutions Limited, realizó la instalación del sistema de cámaras.

Se adjunta copia del contrato de instalación número *****, suscrito entre las partes con fecha 14 julio de 2014 (documento **Anexo 1**).

Considerando que Apple Store suele sufrir intentos de robo y teniendo en cuenta que han sido objeto de acciones violentas y actos delictivos en el pasado, la entidad consideró necesaria la instalación

del sistema de vigilancia, con el fin de proteger a los empleados, clientes y el propio inmueble y evitando así la sustracción de productos en la tienda.

Existen carteles de zona videovigilada que informan sobre el tratamiento de datos personales mediante el sistema de cámaras, localizados en varios mostradores de la tienda.

Además existen formularios informativos a disposición de los interesados, según establece el art. 3.b de la Instrucción 1/2006.

En documento **Anexo 2** se acompaña reportaje fotográfico.

*El sistema de videovigilancia está compuesto por 48 cámaras fijas, sin capacidad de zoom, ubicadas según se indica en los planos de situación adjuntos (documento **Anexo 3**). Sólo una de ellas se encuentra localizada en el exterior, captando la entrada a la tienda (**pantalla 1, Anexo 4**).*

Se incorpora reportaje fotográfico de las capturas de pantalla del sistema de cámaras (documento **Anexo 4**), de cuyo análisis se desprende:

*La imagen captada por la **cámara 1 (fila 1)** presenta una máscara de privacidad, observándose una parte de vía pública mínima e inmediata al acceso a la tienda.*

*La imagen captada por la **cámara 2 (fila 1)** recoge desde el interior uno de los accesos a la tienda, pudiendo distinguirse parte de la vía pública a través de las cristaleras del establecimiento.*

El resto de imágenes corresponden a diversas áreas interiores del local.

No existen monitores de visualización ni transmisión en directo. Solo se accede a las grabaciones en caso de que produzcan incidentes específicos.

El acceso a las imágenes se realiza mediante contraseña desde un ordenador específico. Sólo determinado equipo de personas acceden al sistema, compuesto por: el Store Leader, los Senior Store Managers del Apple Store de la tienda así como los miembros correspondientes del equipo de Loss Prevention de Apple. No hay terceras personas con acceso al sistema de videovigilancia.

Las imágenes grabadas se conservan en un videograbador digital, ubicado en la tienda. Las imágenes se conservan hasta un máximo de 30 días.

Existe fichero inscrito en el Registro General de Protección de Datos, cuya finalidad es la "gestión de sistemas internos de CCTV para finalidades de seguridad" (documento **Anexo 5**).

No se aporta copia del Documento de Seguridad.

El sistema de videovigilancia no se encuentra conectado a sistema de alarma central.

2. Con fecha 19 de noviembre de 2014 se solicita al responsable del sistema información complementaria.

Teniendo entrada en esta Agencia con fecha 9 de diciembre de 2014, escrito al que adjuntan:

*Planos de situación con la identificación de cada una de las cámaras que integran el sistema (**Anexo 3**).*

*Copia CD del Protocolo y Documento de Seguridad de Videovigilancia – Apple Retail Spain S.L 2014 (**Anexo 6**).*

3. Mediante diligencia de inspección, con fecha 12 de noviembre de 2014 se constata la existencia del fichero denominado **CCTV** inscrito con el código *****CÓD.1** cuyo responsable figura **APPLE RETAIL SPAIN S.L.**
4. Con fecha 8 de julio de 2015 inspectores de esta Agencia giran visita de inspección al establecimiento **APPLE STORE** sito en (**C/.....1**), de **MADRID**, constatando los siguientes hechos:

Existen carteles informativos de zona videovigilada en todas las puertas de acceso al establecimiento.

*Se acompaña documento gráfico (**Doc.1**)*

*En documento **Doc. 2** se incorporan los planos de situación del total de cámaras que integran el sistema de videovigilancia, distribuidas en tres plantas (sótano, baja y primera).*

*En la planta baja del establecimiento se localizan un total de 22 cámaras interiores, de las cuales se adjunta reportaje fotográfico con las imágenes captadas por nueve de las cámaras, señaladas al efecto como CAM1- CAM9 (documento **Doc.3**).*

*En la fachada anexa a la (**C/.....2**) se localiza una cámara exterior ubicada en la puerta de entrada de mercancías al local.*

*Se adjunta reportaje fotográfico de la cámara y de la imagen captada y visualizada en el monitor del sistema (**Doc.4**).*

El monitor de visualización del sistema se ubica en la sala del manager. Su acceso mediante clave y contraseña está limitado al Director de la tienda y el Responsable de Seguridad.

Se comprueba que las imágenes más antiguas conservadas en el sistema datan del 16 de junio de 2015.

*Se acompaña impresiones de pantalla del sistema (documento **Doc.5**).*

A las cuestiones planteadas por los inspectores actuantes durante la visita de inspección, el representante de la compañía inspeccionada manifiesta:

Los datos de contacto del representante legal, que figuran en el expediente, han cambiado; por lo que solicita que el domicilio a efectos de notificaciones sea el domicilio social de la empresa.

El sistema de cámaras no dispone de movilidad ni capacidad de zoom.

El sistema de alarma es independiente del sistema de

videovigilancia instalado.

Respecto a los documentos gráficos adjuntos al Acta de Inspección y una vez analizados los mismos, se constata:

- o En relación a las cámaras ubicadas en la planta baja del establecimiento, los dispositivos indicados como CAM1 a CAM9 recogen imágenes del interior del local desde distintos ángulos, distinguiéndose zonas del perímetro interior acristalado de la tienda a través del cual se visualiza una parte del ancho de acera pública que circunda el establecimiento.
- o La CAM2 interior se orienta hacia los accesos a la tienda desde la Plaza de la Puerta del Sol. Capta la imagen de las tres puertas acristaladas de acceso y del espacio de acera pública inmediato a las mismas.
- o La cámara exterior, indicada como CAM10, presenta máscara de privacidad y se encuentra orientada hacia uno de los accesos a la tienda, concretamente a la entrada de mercancías. Recoge un ángulo de la fachada y del espacio mínimo de acera inmediato a la misma.

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 la **POLICÍA MUNICIPAL, UID CENTRO SUR**, denuncia la posible infracción a la Ley Orgánica 15/1999 motivada por la existencia de cámaras de videovigilancia en el establecimiento con denominación comercial **APPLE STORE** sito en **(C/.....1), MADRID** y cuyo titular es la entidad **APPLE RETAIL SPAIN S.L**, sin carteles informativos de zona videovigilada y estando una cámara en la zona de entrada a la tienda grabando el exterior de la vía pública

En primer lugar, debe entrarse a valorar el cumplimiento del deber de información por parte de la entidad denunciada.

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, en inspección realizada en fecha 8 de julio de 2015, por inspectores de esta Agencia al establecimiento denunciado constatan la existencia de carteles informativos de zona videovigilada en todas las puertas de acceso al establecimiento. Asimismo, en documentación aportada por la denunciada se constata la existencia de carteles de zona videovigilada en los mostradores del interior de la tienda. Dichos carteles son acordes al que hace referencia el citado artículo 3.a) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD. Además existen formularios informativos a disposición de los interesados, de conformidad con el artículo 3.b. de la citada Instrucción.

Por lo tanto la entidad denunciada, cumple el deber de información, en cuanto al sistema de videovigilancia, recogido en el artículo 5 de la LOPD, anteriormente transcrito.

Por otro lado, respecto al cumplimiento de la inscripción de ficheros, el artículo 26.1 de la LOPD, recoge lo siguiente:

“1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos”

El responsable del fichero es el titular del fichero que contiene datos de carácter personal. Sobre él van a recaer las obligaciones que establece la LOPD. . El responsable del fichero, antes de disponerse a someter datos personales a tratamiento, deberá cumplir con los requisitos de la normativa de protección de datos, teniendo en cuenta su naturaleza y la naturaleza de los datos que va a someter a tratamiento.

El apartado d) del artículo 3 de la LOPD define al responsable del fichero o tratamiento como aquella persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento. El artículo 43 de la LOPD sujeta a su régimen sancionador precisamente al responsable del fichero o tratamiento.

El reglamento de desarrollo de la LOPD, aprobado por RD 1720/2007, de 21 de diciembre, complementa esta definición en el apartado q) del artículo 5, en el que señala lo siguiente:

“q) Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados”.

El responsable del fichero es, en suma, quien debe garantizar el derecho fundamental de protección de datos personales de todas las personas cuyos datos almacena. Por ello, va a estar obligado a llevar a cabo una serie de actuaciones dirigidas a la protección de los datos, a su integridad y a su seguridad.

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

El responsable debe notificar su fichero a la Agencia Española de Protección de Datos, que dispondrá inscribirlo en el Registro General de Protección de Datos. La notificación de inscripción del fichero facilitará que terceros puedan conocer que se está produciendo un tratamiento con una finalidad determinada y los afectados tendrán la oportunidad de ejercitar sus derechos ante el responsable.

Además este es el criterio que se hace constar en la Instrucción 1/2006 , al señalar en su artículo 7 que *“1-La persona o entidad que prevea la creación de ficheros de videovigilancia deberá notificarlo previamente a la Agencia Española de Protección de Datos, para su inscripción en el Registro General de la misma.*

Tratándose de ficheros de titularidad pública deberá estarse a lo establecido en el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal.

2.-A estos efectos, no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real.”

En el caso que nos ocupa, consta la inscripción por parte de **APPLE RETAIL**

SPAIN, S.L., del fichero denominado “CCTV”, en el Registro General de la Agencia Española de Protección de Datos, en fecha 16/11/2010 y entre sus finalidades está la videovigilancia, seguridad y el control de accesos a edificios.

Asimismo las imágenes se conservan por un tiempo máximo de 30 días, de conformidad con el artículo 6 de la Instrucción 1/2006, que recoge: *“Los datos serán cancelados en el plazo máximo de un mes desde su captación”*.

IV

Por último, 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”.

Precisamente la redacción del artículo 4 de la Instrucción 1/2006, no viene sino a recoger el principio de proporcionalidad del artículo 4 de la LOPD. Quiere ello decir que la grabación de imágenes en un lugar público, no está permitida en ningún supuesto. Ahora bien, si las cámaras están instaladas en la entrada de un edificio, por el campo de visión de ésta podría captar un porcentaje reducido de la vía pública, no siendo necesario en éste caso obtener el consentimiento de los transeúntes.

En este sentido, la posibilidad de captar un pequeño ángulo de la vía pública a través de una cámara de vigilancia, ésta deberá de cumplir el principio de proporcionalidad, sin que sea posible extender la grabación de imágenes a un alcance mayor al que resulte necesario para garantizar la seguridad de las instalaciones. Por ello, la referencia a los alrededores de las instalaciones, únicamente resultaría ajustada a la normativa de protección de datos en caso de que la misma se refiera exclusivamente a aquellos espacios públicos sin cuya grabación resultaría en todo punto imposible el control de la seguridad en el acceso a las instalaciones, sin que en modo alguno esta referencia pueda entenderse efectuada, con carácter general a la vía pública.

En el caso que nos ocupa, y centrándonos en las cámaras que realizan captaciones de vía pública, se constata por los inspectores actuantes de esta Agencia que en relación a las cámaras ubicadas en la planta baja del establecimiento, los dispositivos indicados como CAM1 a CAM9 recogen imágenes del interior del local desde distintos ángulos, distinguiéndose zonas del perímetro interior acristalado de la tienda a través del cual se visualiza una parte del ancho de acera pública que circunda el establecimiento; la CAM2 interior se orienta hacia los accesos a la tienda desde la Plaza de la Puerta del Sol y capta la imagen de las tres puertas acristaladas de acceso y del espacio de acera pública inmediato a las mismas; y la cámara exterior, indicada como CAM10, presenta máscara de privacidad y se encuentra orientada hacia uno de los accesos a la tienda, concretamente a la entrada de mercancías y recoge un ángulo de la fachada y del espacio mínimo de acera inmediato a la misma. Por lo tanto, las imágenes captadas 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. Así, el sistema de videovigilancia instalado, realiza un tratamiento proporcional de las imágenes, en relación con el ámbito y las finalidades que podrían justificaban su recogida.

Por lo tanto, a la vista de todo lo expuesto, en el presente caso no se aprecia vulneración de la normativa aplicable a la protección de datos, por lo que procede el 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:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a **APPLE RETAIL SPAIN S.L** y a **POLICIA MUNICIPAL DE MADRID**.

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