



Expediente N°: E/01577/2017

### RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **KAIZOKU 2013, S.L.** en virtud de denuncia presentada por D. **A.A.A.** y teniendo como base los siguientes

#### HECHOS

**PRIMERO:** Fecha de entrada de la denuncia: 8 de febrero de 2017

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

Denuncia a: **KAIZOKU 2013, S.L.**

Por los siguientes hechos según manifestaciones del denunciante: La existencia de una zona videovigilada en el establecimiento, con posible captación de la vía pública, sin que existan carteles que la señalicen. Asimismo denuncia la exhibición, a terceras personas, de grabaciones en las que se ve al denunciante, tal y como él mismo pone de manifiesto, golpeando la puerta de entrada del establecimiento y a partir de las cuales, según afirma, es posible identificarle claramente.

Y, entre otra, anexa la siguiente documentación:

Cuatro declaraciones juradas de personas que manifiestan que la titular del establecimiento denunciado les ha mostrado imágenes del denunciante correspondientes a la madrugada del 10 de abril de 2016 sobre las 2:30 horas.

Reportaje fotográfico de fecha 25 de diciembre de 2016, que muestra las puertas de acceso al establecimiento.

En respuesta a la solicitud de información realizada por esta Agencia con fecha 7 de marzo de 2017, con objeto de analizar si la conducta denunciada constituye un incumplimiento legal en el ámbito sobre el que la Agencia Española de Protección de Datos tiene atribuidas competencias, con fecha 3 de abril de 2017 tiene entrada en el registro respuesta del denunciante en el que facilita el domicilio de instalación del sistema de videovigilancia así como la identidad de los presuntos responsables.

Y anexa la siguiente documentación:

Reportaje fotográfico de la cámara de videovigilancia así como la zona del exterior del local que según indica el denunciante en su escrito, presupone puede ser captada por la referida cámara.

**SEGUNDO:** Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

Con fecha 3 de mayo de 2017 se solicita información al titular del establecimiento, teniendo entrada en esta Agencia con fecha 24 de mayo de 2017 escrito del denunciado en el que manifiesta:

Respecto a la adecuación de la instalación del sistema de videovigilancia:

1. El Responsable del sistema de videovigilancia es la mercantil KAIZOKU2013, S.L.
2. La instalación de las cámaras del sistema de videovigilancia las realizó la empresa SECURITAS DIRECT, adjuntando como evidencia el contrato de instalación, el clausulado del mismo con las referencias a las obligaciones establecidas en la LOPD así como la certificación de las condiciones particulares del contrato de mantenimiento y la conexión a la Central Receptora de Alarmas.
3. Respecto de la finalidad por la cual se han instalado las cámaras, el denunciado manifiesta que el objetivo de la instalación del sistema de videovigilancia es salvaguardar la viabilidad del negocio porque, previo a la instalación de las cámaras, se produjeron varios robos que fueron denunciados ante la Comisaría de la Policía Autónoma Vasca en Hernani.
4. Respecto de la información facilitada sobre la existencia de cámaras, se aportan fotografías de varios carteles que señalizan la existencia de estas, situados tanto en las entradas del establecimiento como en el interior del mismo, y que responden al modelo de cartel de zona videovigilada. Facilita detalle del cartel donde puede identificarse la identidad del responsable del fichero ante el que ejercer los derechos ARCO. Aporta además copia del formulario informativo sobre el sistema de videovigilancia al que se refiere el artículo 3.b de la Instrucción 1/2006 y que el denunciado manifiesta tener a disposición de los clientes y describe el procedimiento para hacer entrega del mismo ante una solicitud de información o para el ejercicio de derechos ARCO. Además de los referidos carteles, el denunciado aporta fotografía de un cartel de la empresa SECURITAS DIRECT, situado en la fachada del local, donde se advierte de la existencia de alarma con grabación de imágenes.
5. En relación a los lugares en los que se encuentran ubicadas las cámaras de videovigilancia, aporta plano de situación en el que se marca el emplazamiento concreto de las cámaras así como fotografía de todas y cada una de ellas. El denunciado refiere tener instaladas cinco cámaras; tres de ellas situadas en la pared, detrás de la barra del establecimiento, enfocadas hacia el interior de la taberna, con capacidad de zoom, y otras dos, situadas sobre las puertas de entrada al establecimiento, que no graban y sólo realizan fotos. Sólo una de las cámaras situadas detrás de la barra e identificada como "cámara máquina Nº 3" y que está enfocada hacia la máquina de tabaco, por la ubicación de esta última, capta parcialmente una pequeña proporción de la calle aledaña a la puerta de entrada, tal y como puede apreciarse a partir de las imágenes facilitadas del sistema de monitorización.
6. Respecto a este último, el denunciado no acredita dónde está ubicado el monitor de control aunque sí manifiesta que las imágenes grabadas se almacenan en un dispositivo "nube" facilitado por el proveedor de servicios de seguridad SECURITAS DIRECT y que se conservan por un período de 48 horas transcurrido el cuál, son borradas. A dicho dispositivo sólo acceden mediante usuario y clave de acceso los dos administradores mancomunados de la mercantil a través de lo que, según se desprende de las imágenes facilitadas y de lo indicado en el clausulado del contrato de prestación de servicios de seguridad, parece ser una aplicación móvil.



Aporta código de inscripción del fichero en el Registro General de Protección de Datos con número \*\*\*CODIGO.1, comprobándose, tal y como figura en Diligencia incorporada a las actuaciones de inspección, que este se corresponde con el fichero identificado como "Videovigilancia".

8. El denunciado manifiesta que el sistema de videovigilancia está conectado a una Central Receptora de Alarmas gestionada por la empresa proveedora de servicios de alarmas conectadas para hogar y negocios, SECURITAS DIRECT.

Respecto a si las imágenes grabadas en la madrugada del 10 de abril de 2016 han sido exhibidas a terceros el investigado afirma que las declaraciones juradas aportadas han sido realizadas por amigos y familiares del denunciante y que son falsas, argumentándolo en las siguientes manifestaciones:

El día de los hechos, uno de los administradores de la mercantil fue avisado, sobre las 2:30 por la empresa de servicios de seguridad, en relación a un salto de alarma. Personado en el establecimiento pudo comprobar que la puerta estaba dañada y antes de interponer la correspondiente denuncia, al visualizar las grabaciones de las cámaras de seguridad, constató que la cámara identificada como "cámara máquina Nº 3" graba como una persona arremete contra la puerta de entrada, en varias ocasiones, causando daños materiales.

El investigado manifiesta en la respuesta al requerimiento realizado que en la grabación no se percibe ningún rasgo facial pero que intuyó, por desavenencias previas, que podía tratarse del denunciante, tal y como después confirmo la persona que le acompañaba en el momento de los hechos, según consta tanto en el escrito de respuesta al requerimiento como en el certificado de realización de denuncia aportado.

No obstante, y ante la afirmación de que el investigado identificó al denunciante al visionar los hechos grabados por las cámaras que figura en el acuerdo posterior firmado entre denunciante e investigado para evitar acciones judiciales y por el que el denunciante reconocía los hechos y abonaba una cantidad en concepto de indemnización por los daños cometidos como contrapartida a que el investigado renunciara a emprender acciones civiles y penales, esta Agencia, con objeto de aclarar las discrepancias advertidas, requirió nuevamente a la mercantil investigada, con fecha 29 de mayo de 2017 y número de registro de salida \*\*\*REGISTRO.1, solicitando copia de la denuncia y de las imágenes de los hechos denunciados.

Con fecha 19 de junio de 2017 y número de registro de entrada \*\*\*REGISTRO.2, se recibe respuesta al requerimiento de información practicado y en el que el investigado se afirma y ratifica en lo anteriormente manifestado en relación al hecho de que en las imágenes visionadas, a las personas grabadas, no se les percibe absolutamente ningún rasgo facial ni eran identificables, percibiéndose únicamente, la figura de las mismas pero no el rostro ni la vestimenta. Asimismo manifiesta que el hecho de que en el acuerdo se plasmase que se identificó al denunciante en las imágenes grabadas era tan solo una estrategia procesal para que reconociese los actos cometidos y que fue la confesión de la persona que acompañaba al denunciante en el momento de los hechos lo que le permitió ser conocedora de la identidad del mismo.

Visionadas las grabaciones aportadas y en las que pueden apreciarse los hechos que

constan en la denuncia realizada en la Comisaría de la Policía Autónoma Vasca en Hernani en la madrugada del 10 de abril de 2016, se incorpora como Diligencia a las actuaciones de inspección de referencia captura de una de las imágenes de las grabaciones efectuadas en la que, a través del cristal del establecimiento, puede apreciarse la silueta de una persona constatando que, tras realizar una ampliación del área que comprende el rostro del individuo, no se aprecian ni distinguen rasgos que permitan una identificación del mismo.

## **FUNDAMENTOS DE DERECHO**

### **I**

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

El artículo 126.1, apartado segundo, 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 establece:

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

### **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.** denuncia la existencia de cámaras de videovigilancia en el establecimiento, con denominación comercial **“KAIZOKU TABERNA”**, con posible captación de la vía pública, sin que existan carteles que la señalicen. Asimismo denuncia la exhibición, a terceras personas, de grabaciones en las que se ve al denunciante, tal y como él mismo pone de manifiesto, golpeando la puerta de entrada del establecimiento y a partir de las cuales, según afirma, es posible identificarle claramente.

Ante dicha denuncia, la Inspección de Datos de esta Agencia solicita diversa información al responsable del sistema, teniendo entrada contestación del mismo aportando diversa documentación en relación a la empresa de seguridad SECÚRITAS DIRECT ESPAÑA, encargada de los dispositivos denunciados, adjuntando contrato de instalación, el clausulado del mismo con las referencias a las obligaciones establecidas en la LOPD así como la certificación de las condiciones particulares del contrato de mantenimiento y la conexión a la Central Receptora de Alarmas.

Respecto de la finalidad por la cual se han instalado las cámaras, la denunciada manifiesta que el objetivo de la instalación del sistema de videovigilancia es salvaguardar la viabilidad del negocio porque, previo a la instalación de las cámaras, se produjeron varios robos que fueron denunciados ante la Comisaría de la Policía Autónoma Vasca en Hernani.

Procede en primer lugar, entrar a valorar el cumplimiento del deber de información por parte del establecimiento denunciado.

El tratamiento de las imágenes por parte del responsable, obliga a que se cumpla con el deber de informar a los afectados, en los términos establecidos en el artículo 5.1 de la LOPD el cual reza lo siguiente:

*“1. Los interesados a los que se soliciten datos personales deberán ser*

*previamente informados de modo expreso, preciso e inequívoco:*

*a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.*

*b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.*

*c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.*

*d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.*

*e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante”.*

En cuanto al modo en que hay de facilitarse la información recogida en el artículo 5 de la LOPD, debe tenerse en cuenta el artículo 3 de la Instrucción 1/2006, que establece lo siguiente:

*“Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán:*

*a) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y*

*b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999.*

*El contenido y el diseño del distintivo informativo se ajustará a lo previsto en el Anexo de esta Instrucción.”*

*“ANEXO-*

*1. El distintivo informativo a que se refiere el artículo 3.a) de la presente Instrucción deberá de incluir una referencia a la «LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS», incluirá una mención a la finalidad para la que se tratan los datos («ZONA VIDEOVIGILADA»), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.”*

En el caso que nos ocupa, consta aportado por la entidad denunciada fotografías de los carteles informativos de la existencia de las cámaras, situados tanto en las entradas del establecimiento como en el interior del mismo, y que responden al modelo de cartel de zona videovigilada. Dichos carteles son acordes al que se refiere el artículo



3 a) de la Instrucción, en relación al artículo 5 de la LOPD.

Aporta además copia del formulario informativo sobre el sistema de videovigilancia al que se refiere el artículo 3.b de la Instrucción 1/2006 y que el denunciado manifiesta tener a disposición de los clientes y describe el procedimiento para hacer entrega del mismo ante una solicitud de información o para el ejercicio de derechos ARCO.

Además de los referidos carteles, el denunciado aporta fotografía de un cartel de la empresa SECURITAS DIRECT, situado en la fachada del local, donde se advierte de la existencia de alarma con grabación de imágenes.

Por lo tanto la 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.



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 la entidad denunciada, del fichero denominado “VIDEOVIGILANCIA”, cuya finalidad es la videovigilancia de las instalaciones, en el Registro General de la Agencia Española de Protección de Datos.

#### IV

Una vez acreditado que el sistema de videovigilancia cumple el deber de información e inscripción de fichero, debemos entrar en la cuestión planteada por el denunciante relativa a la captación de su imagen en el exterior del establecimiento y parte de la vía pública.

Respecto a la captación de imágenes en la vía pública, a través de un sistema de videovigilancia, 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”.

En el caso que nos ocupa, del visionado del video (objeto de denuncia), requerido a la denunciada, se desprende que la cámara situada en el interior del establecimiento, capta zona del interior del mismo y parte de vía pública, a través del cristal del establecimiento, así como a tres personas, siendo bastante difícil el poder identificar a una persona situada al final del ángulo de captación de vía pública que realiza la cámara. A este respecto el denunciante manifiesta que a través de la cámara se le pudo identificar; sin embargo la denunciada manifiesta que en la grabación no se percibe ningún rasgo facial pero que intuyó, por desavenencias previas, que podía tratarse del denunciante, tal y como después confirmó la persona que le acompañaba en el momento de los hechos, según consta tanto en el escrito de respuesta al requerimiento como en el certificado de realización de denuncia aportado.

No obstante, y ante la afirmación de que el investigado identificó al denunciante al visionar los hechos grabados por las cámaras que figura en el acuerdo posterior firmado entre denunciante e investigado para evitar acciones judiciales y por el que el denunciante reconocía los hechos y abonaba una cantidad en concepto de indemnización por los daños cometidos como contrapartida a que el investigado renunciara a emprender acciones civiles y penales, esta Agencia, con objeto de aclarar las discrepancias advertidas, requirió nuevamente a la mercantil investigada, con fecha 29 de mayo de 2017, solicitando copia de la denuncia y de las imágenes de los hechos denunciados.



Visionadas las grabaciones aportadas pueden apreciarse tres personas que, tras realizar una ampliación del área que comprende el rostro del individuo, no se distinguen claramente los rasgos que permitieran una identificación del mismo, únicamente con dichas imágenes. No obstante, aun cuando así fuera, la captación de los mismos se realizó en el espacio inmediatamente anexo a la cristalera de la tienda, siendo proporcional la captación de dicho espacio, a la finalidad de seguridad pretendida

Por lo tanto, a la vista de lo expuesto, las imágenes captadas por las cámaras que componen el sistema, no se entienden que infrinjan 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.

## V

Por último, respecto a las manifestaciones del denunciante de que la denunciada ha mostrado las imágenes captadas por las cámaras a varias personas (de las que presenta declaración), preguntada al respecto a la denunciada, ésta niega los hechos.

El artículo 10 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), establece que *“El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero, o en su caso, con el responsable del mismo”*.

El deber de secreto que incumbe a los responsables de los ficheros y a quienes intervienen en cualquier fase del tratamiento, recogido en el artículo 10 de la LOPD, comporta que el responsable de los datos almacenados o tratados no pueda revelar ni dar a conocer su contenido teniendo el *“deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo”*. Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la protección de datos a que se refiere la Sentencia del Tribunal Constitucional 292/2000 y, por lo que ahora interesa, comporta que los datos personales no pueden ser conocidos por ninguna persona o entidad ajena fuera de los casos autorizados por la Ley.

Este deber de guardar secreto, que incumbe a los responsables de ficheros y a quienes intervengan en cualquier fase del tratamiento, incluye el deber de guardarlos, y lo contempla como obligación que subsistirá aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Ahora bien, en el supuesto denunciado 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”*.

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

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”*.

De acuerdo con la citada doctrina jurisprudencial cabe concluir que, en el presente caso, no se han aportado evidencias firmes de los que pueda deducirse que la denunciada, hayan vulnerado el deber de secreto.

La Constitución Española, considera, en su artículo 24.2, el derecho a la presunción de inocencia como un derecho fundamental:

*“2. Asimismo, todos tienen derecho al Juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia”* (el subrayado es de la Agencia Española de Protección de Datos).

Conforme a lo anterior, el Tribunal Supremo señala, en su Sentencia de fecha 26/10/98, el derecho a la presunción de inocencia *“no se opone a que la convicción judicial en un proceso pueda formarse sobre la base de una prueba indiciaria, pero para*



*que esta prueba pueda desvirtuar dicha presunción debe satisfacer las siguientes exigencias constitucionales: los indicios han de estar plenamente probados – no puede tratarse de meras sospechas – y tiene que explicitar el razonamiento en virtud del cual, partiendo de los indicios probados, ha llegado a la conclusión de que el imputado realizó la conducta infractora, pues, de otro modo, ni la subsunción estaría fundada en Derecho ni habría manera de determinar si el proceso deductivo es arbitrario, irracional o absurdo, es decir, si se ha vulnerado el derecho a la presunción de inocencia al estimar que la actividad probatoria pueda entenderse de cargo.”*

En tal sentido, el Tribunal Constitucional, en su Sentencia 24/1997, establece que “los criterios para distinguir entre pruebas indiciarias capaces de desvirtuar la presunción de inocencia y las simples sospechas se apoyan en que:

*a) La prueba indiciaria ha de partir de hechos plenamente probados.*

*b) Los hechos constitutivos de delito deben deducirse de esos indicios (hechos completamente probados) a través de un proceso mental razonado y acorde con las reglas del criterio humano, explicitado en la sentencia condenatoria (SSTC 174/1985, 175/1985, 229/1988, 107/1989, 384/1993 y 206/1994, entre otras)” (el subrayado es de la Agencia Española de Protección de Datos).*

En el presente caso, en las actuaciones previas de investigación realizadas por los Servicios de Inspección de esta Agencia, no se ha podido obtener pruebas que corroboren y acrediten que la denunciada vulnerara el deber de secreto al que se refiere el artículo 10 de la LOPD.

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

Por lo tanto, de acuerdo con lo señalado,

**Por la Directora de la Agencia Española de Protección de Datos,**

**SE ACUERDA:**

**PROCEDER AL ARCHIVO** de las presentes actuaciones.

**NOTIFICAR** la presente Resolución a **KAIZOKU 2013, S.L.** y **D. A.A.A. .**

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

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley



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

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