

Expediente N°: E/04446/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante D^a. **D.D.D.** en virtud de denuncia presentada por D. **C.C.C.** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha de 2 de abril de 2013 tiene entrada en esta Agencia escrito de D. **C.C.C.** (en adelante el/la denunciante) comunicando posible infracción a la Ley Orgánica 15/1999, de 13 de diciembre, motivada por cámaras de videovigilancia cuyo titular es Dña. **D.D.D.** (en adelante la denunciada) instaladas en la finca ubicada en **A.A.A. B.B.B.)**.

En su denuncia, el denunciante manifiesta que tiene constancia de que la denunciada tiene una cámara de grabación, que graba la vía pública, situada o escondida en un cajetín de luz perforado en la fachada de su vivienda.

Asimismo, indica que en el interior de la vivienda se encuentra el dispositivo de grabación multimedia a través del cual se recogen imágenes que “están siendo manipuladas y entregadas como pruebas en un pleito”, siendo difundidas dichas imágenes sin el consentimiento de los implicados.

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 23 de agosto de 2013 se solicita información a la denunciada, respecto a diversos aspectos del sistema de videovideovigilancia denunciado, teniendo entrada en esta Agencia con fecha 27 de septiembre de 2013, escrito de la denunciada en el que manifiesta que *“habiendo recibido escrito, por medio del presente pongo de manifiesto que en el Juzgado de Instrucción número 3 de los de La Laguna se siguen Diligencias Urgentes número **E.E.E.**”, y que “todo tiene que ver con actividades personales y domésticas”*.

2.Con fecha 7 de octubre de 2013, se reitera requerimiento de solicitud de información a la denunciada, en el que se reproduce el contenido del anterior, respondiendo dicha denunciada, con fecha de entrada en la Agencia de 31 de octubre de 2013, que *“se insiste en que todo tiene que ver con actividades personales o domésticas y que, en cualquier caso, se refiere a grabaciones en la vivienda de la que no es titular”*.

3.Con fecha 8 de noviembre de 2013, se solicita colaboración del Ayuntamiento de la Ciudad de TACORONTE (Jefatura de la Policía Local), sin que conste respuesta alguna a dicha solicitud de colaboración.

4.Con fecha 16 de enero de 2014, se solicita colaboración a la Guardia Civil de TACORONTE, recibéndose –con fecha 30 de enero de 2014- informe, del que da

traslado el Teniente Coronel Jefe de la Comandancia de Santa Cruz de Tenerife, confeccionado por la UNIDAD ORGÁNICA DE LA POLICÍA JUDICIAL, en el que se expone, en síntesis, lo siguiente:

- Según la denunciada, fue ella misma quien instaló la cámara, si bien no necesitó de una instalación propiamente dicha, ya que era la webcam del ordenador de su hija, que la sacaba al exterior en ciertas ocasiones.
- La instaló, según su manifestación, a raíz de diversos problemas con su ex pareja, interponiendo varias denuncias en sede judicial.
- Por todo ello, y para tener pruebas, comenzó a sacar a la ventana la webcam que estaba conectada al ordenador de su hija, poniéndola orientada hacia la puerta del garaje.
- Que la cámara no estaba siempre puesta, al contrario, solamente la ponía en la ventana eventualmente cuando se producía algún altercado. Que no estaba anclada a ningún sitio, ya que la webcam tenía un pequeño trípode con el que podía dejarla en el alféizar de la ventana.
- Que hace mucho tiempo que no ha vuelto a utilizar la webcam.
- No dispone de carteles ni de formularios informativos.
- En el momento de la confección de este informe, no existen cámaras instaladas en la fachada vivienda, ni elementos que hagan suponer que se hubieran instalado con anterioridad cámaras de videovigilancia ancladas en la fachada o instalación eléctrica.
- Al tratarse de una webcam, descargaba lo grabado directamente en el ordenador de su hija, por lo que no existen monitores de un sistema de videovigilancia como tal. No obstante, se significa que el ordenador de su hija se encuentra instalado en la misma habitación en la que está la ventana donde ponía la webcam.
- No hay un sistema de videovigilancia instalado como tal. No obstante al ordenador de su hija podrían acceder la denunciada, su hija y su madre, aunque según la manifestación de la denunciada las dos últimas ni siquiera sabían que existían esas grabaciones.
- El sistema de grabación era la grabación en el disco duro de un ordenador personal, únicamente de los momentos cuando se producía algún altercado. No existe una instalación fija de un sistema de videovigilancia.
- A las grabaciones accedía únicamente la propia denunciada.
- No existe un tiempo predeterminado de conservación de las imágenes. Una vez grabadas, conservaba únicamente las que eran de interés para los procedimientos judiciales que tenían en curso en ese momento. Actualmente la denunciada dice no tener imágenes grabadas.
- No existe código de inscripción en el Registro General de Protección de Datos, ni documento de seguridad.
- La webcam no estaba conectada a ninguna central de alarmas, ni fue instalada por ninguna empresa de seguridad.

Junto con su informe, la Guardia Civil actuante acompaña un reportaje fotográfico

para mejor comprensión de los hechos, compuesto de cinco fotografías. Según se indica, no se aprecia la instalación de cámara alguna en el inmueble.

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

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

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

El artículo 5.1. f) del 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.” (el subrayado es de la Agencia Española de Protección de Datos).

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. **C.C.C.**, denuncia la existencia de una cámara de grabación en la fachada de la vivienda en la que habita la denunciada, siendo las grabaciones obtenidas por la misma utilizadas para su aportación a procedimientos judiciales y difundidas en redes sociales.

Pues bien, solicitada con fecha 16 de enero de 2014 la inestimable colaboración a la Guardia Civil de TACORONTE, para que obtuviese diversa información relativa al sistema de videovigilancia denunciado, remiten con fecha 30 de enero de 2014 informe, confeccionado por la UNIDAD ORGÁNICA DE LA POLICÍA JUDICIAL, con motivo de la inspección realizada en fecha 28 de enero de 2014, en el domicilio denunciado, en el que se recoge que, fue la denunciada la que instaló la cámara, si bien no necesitó de una instalación propiamente dicha, ya que era la webcam del ordenador de su hija, que la sacaba al exterior en ciertas ocasiones. La instaló, según la denunciada, a raíz de diversos problemas con su ex pareja, interponiendo varias denuncias en sede judicial. Por todo ello, y para tener pruebas, comenzó a sacar a la ventana la webcam que estaba conectada al ordenador de su hija, poniéndola orientada hacia la puerta del garaje. Asimismo manifiesta que la cámara no estaba siempre puesta, al contrario, solamente la ponía en la ventana eventualmente cuando se producía algún altercado y que hace mucho tiempo que no ha vuelto a utilizar la webcam. Los agentes actuantes manifiestan que en el momento de la confección del informe, no existen cámaras instaladas en la fachada vivienda, ni elementos que hagan suponer que se hubieran instalado con anterioridad cámaras de videovigilancia ancladas en la fachada o instalación eléctrica.

Por lo tanto, a la fecha de la visita de inspección por el citado cuerpo no existía ninguna cámara de videovigilancia en el domicilio de la denunciada, manifestando ésta que nunca tuvo un sistema de videovigilancia propiamente dicho sino que puntualmente grababa con la webcam del ordenador de su hija cuando se producía algún incidente, con la finalidad de poder aportarlo como prueba en los procedimientos judiciales que tenía aperturados. Asimismo manifiesta la denunciada que hace mucho tiempo que no ha tenido que utilizar la webcam.

Una vez formulada dichas aclaraciones, en el presente supuesto, se plantearía la aportación de las grabaciones efectuadas por la denunciada, sin el consentimiento del denunciante, en el seno de un procedimiento judicial. En este punto hemos de estudiar

las implicaciones que lo denunciado presenta al respecto del derecho a la protección de datos en relación con el derecho a la tutela judicial efectiva de los protagonistas, por lo que partiremos de un análisis general relativo a la conexión de dichos derechos. Así, al respecto del derecho a la tutela judicial efectiva, nuestra norma suprema en el artículo 24 de la Constitución Española, en sus apartados 1 y 2, dispone lo siguiente:

“1. Todas las personas tienen derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que en ningún caso, pueda producirse indefensión.

2. Asimismo, todos tienen derecho a utilizar los medios de prueba pertinentes para su defensa.”

Así, constitucionalmente se consagra el derecho de los ciudadanos, ya sean personas físicas o jurídicas, a la tutela judicial efectiva y al derecho a utilizar los medios de prueba que consideren adecuados para el sostenimiento de su pretensión. Sin embargo, de dicha previsión, surge una colisión entre el derecho a la protección de datos de carácter personal y el derecho a la tutela judicial efectiva de los jueces y tribunales referida, contenido en el artículo 24 de la Constitución, anteriormente transcrito, dadas a los bienes jurídicos afectados en su aplicación.

Por ello, ante tales situaciones, el Legislador ha creado un sistema en que el derecho a la protección de datos de carácter personal cede en aquellos supuestos en que el propio Legislador (constitucional u ordinario) haya considerado la existencia de motivos razonados y fundados que justifiquen la necesidad del tratamiento de los datos, incorporando dichos supuestos a normas de, al menos, el mismo rango que la que regula la materia protegida.

En efecto, la exigibilidad del consentimiento del titular de los datos que pudieran ser objeto de un tratamiento en un procedimiento judicial, para dicho tratamiento de sus datos supondría dejar a disposición de aquél el almacenamiento de la información necesaria para que una persona pueda ejercer, en plenitud, su derecho a la tutela judicial efectiva. Así, la falta de estos datos o la dependencia en su aplicación a quien manejara la titularidad del dato, implicaría, lógicamente, una merma en la posibilidad de aportación por el interesado de *“los medios de prueba pertinentes para su defensa”*, vulnerándose otra de las garantías derivadas del citado derecho a la tutela efectiva y coartándose la posibilidad de obtener el pleno desenvolvimiento de este derecho.

Tal y como sostiene reiterada jurisprudencia del Tribunal Constitucional (por todas, STC 186/2000, de 10 de julio, con cita de otras muchas) *“el derecho a la intimidad no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho”*.

Por otro lado, junto a lo dispuesto en el artículo 6.2 de la LOPD, el artículo 11 de la LOPD, recoge otras excepciones, a la exigencia del consentimiento:

“1.- Los datos de carácter personal objeto de tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2.-El consentimiento exigido en el apartado anterior no será preciso:

a.-Cuando la cesión esté autorizada en una ley.(...)

d.-Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas.(...)” (el subrayado es de la Agencia Española de Protección de Datos).

En este sentido, entraría en liza lo dispuesto en el artículo 299 de la Ley 1/2000, de 7 de enero de Enjuiciamiento Civil, que admite la aportación como medio de prueba, de medios de reproducción de imágenes que sean relevantes para el proceso. Así establece, el precitado artículo:

“1. Los medios de prueba de que se podrá hacer uso en juicio son:

- 1. Interrogatorio de las partes.*
- 2. Documentos públicos.*
- 3. Documentos privados.*
- 4. Dictamen de peritos.*
- 5. Reconocimiento judicial.*
- 6. Interrogatorio de testigos.*

2. También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso..

3. Cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias”.

Por lo tanto, en cuanto a lo aportado en el juicio, dicho cuerpo legal admite la aportación como medio de prueba de los medios de reproducción de la palabra, el sonido y la imagen, lo cual implica la posibilidad de tratamiento de datos dentro de

dichas propuestas de prueba, debiendo ser el correspondiente órgano jurisdiccional quien se manifieste sobre la legitimidad de lo presentado, por lo que, en el caso de que esta Agencia impusiera una eventual sanción, dicha circunstancia colisionaría con el ejercicio del derecho constitucional a una tutela judicial efectiva.

Además, hemos de tener en cuenta que, la Audiencia Nacional en sentencia de 22 de octubre de 2010 (rec. 409/2009) nos dice, en cuanto a la obtención de medios probatorios y su validez en el procedimiento, pese a no ser solicitadas ni obtenidas por vía judicial, lo siguiente:

“De un lado ha de tenerse en cuenta que una de las causas que excluye la necesidad de consentimiento para la cesión de datos personales es que la comunicación que deba efectuarse tenga por destinatarios a los Jueces o Tribunales (Art. 11.2.d) LOPD).

Excepción en la que no es descabellado incluir aquellos supuestos en que se trata de pruebas que, si bien inicialmente no han sido solicitadas por el Juez o Tribunal, sino aportadas por las partes, con posterioridad no consta que las mismas hayan sido rechazadas, sino incorporada por el Juez a las actuaciones, tal y como, parecer ser, y así se desprende del acta de juicio, ocurrió en el presente supuesto.

Por otra parte, y si bien es cierto que los procedimientos judiciales tampoco son ajenos a la normativa de protección de datos, tal y como indicamos en la SAN 9-10-2009 (Rec. 37/2009) dado que el derecho de protección de datos, en cuanto derecho fundamental y autónomo previsto en el artículo 18.4 CE , vincula a todos los poderes públicos (Art. 53 CE) y entre ellos al Poder Judicial, tal y como igualmente indica la STS 18-9-2006 Rec. 274/2002 . Sin embargo dicha LOPD debe ser aplicada con gran cautela, y en la medida en que resulte compatible con las funciones propias (jurisdiccionales y no jurisdiccionales) de los referidos órganos judiciales, pues la singularidad de la actividad jurisdiccional y los intereses que en ella subyacen, exigen en ocasiones una limitación o modulación de los derechos y garantías de los ciudadanos.

Además de que el sometimiento de los ficheros judiciales a la LOPD ha de entenderse (según la misma SAN 9-10-2009 Rec. 37/2009) sin menoscabo de la función jurisdiccional y, por tanto, atinente a lo que debe considerarse como "aspecto accesorio" o administrativo de la función jurisdiccional, centrándonos concretamente en el procedimiento judicial, existen también en él una serie de intereses y garantías que ostentan un trascendente valor en dicho proceso, tales como el del verdadero esclarecimiento de los hechos o el legítimo ejercicio del derecho de defensa de las partes, que han de ser ponderados en aquellos casos en que dichos intereses y garantías confluyen con el derecho contemplado en el artículo 18.4 CE , hasta el punto de que pueden llegar a implicar una importante limitación de tal derecho de protección de datos personales." (el subrayado es de la Agencia Española de Protección de Datos).

Pero es que a mayor abundamiento, la propia Sentencia nº **F.F.F.** dictada por la

Audiencia Provincial de Madrid ante el recurso de apelación interpuesto por el denunciante ante esta Agencia, contra la Sentencia dictada por el Juzgado de 1ª Instancia e Instrucción de Navalcarnero, recoge sentencias del Tribunal Supremo y Constitucional clarificadoras del caso que se plantea. Así *“La Sentencia de 6 de abril de 1994 corrobora la legitimidad de la prueba consistente en una filmación videográfica si la misma no ha vulnerado algún derecho, es decir, si con ello no se ha violado la intimidad o la dignidad de la persona afectada por la filmación. Es el propio Tribunal Constitucional el que estima admisible la captación de la imagen del sujeto cuando la misma conducta de aquel o las circunstancias en que se encuentre inmerso justifiquen el descenso de las barreras de reserva para que prevalezca el interés ajeno o el público que pudieran colisionar con aquél. (STC 99/1994)...”*.

Por otro lado, de conformidad con la doctrina del Tribunal Constitucional, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan, basta recordar que (como sintetizan las SSTC 66/1995, de 8 de mayo [RTC 1995\66], F.5; 55/1996, de 28 de marzo [RTC 1996\55], FF. 6, 7, 8 y 9; 207/1996, de 16 de diciembre [RTC1996\207], F.4.e) y 37/1998, de 17 de febrero [RTC 1998\37], F.8) para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

La medida adoptada por la denunciado resulta idónea y necesaria ya que se trataba de recabar pruebas de los incidentes que se producían para su aportación a un procedimiento judicial; y es equilibrada pues la grabación se limita a una determinada zona, y a un intervalo reducido de tiempo en los momentos en los que se produce los mismos.

Por lo tanto en el supuesto que nos ocupa, la captación de las imágenes objeto de denuncia fueron utilizadas como medio de prueba en un procedimiento judicial cumpliendo los requisitos de finalidad y proporcionalidad exigidos por la actual normativa en materia de protección de datos.

IV

Por otro lado, respecto a las manifestaciones del denunciante de que la denunciada ha difundido las imágenes captadas en redes sociales, hay que tener en cuenta que el Tribunal Constitucional viene manteniendo que los principios y garantías del procedimiento judicial penal son, en principio y con las oportunas modulaciones,

aplicables al procedimiento administrativo sancionador, dado que también este es manifestación del ordenamiento punitivo del Estado, resultando clara la plena virtualidad del principio de presunción de inocencia. En tal sentido, el Tribunal Constitucional, en Sentencia 76/1990 considera que el derecho a la presunción de inocencia comporta *“que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio”*.

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

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

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

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

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

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, haya vulnerado la normativa de protección de datos.

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

misimos, a no confesarse culpables y a la presunción de inocencia”.

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 las manifestaciones del denunciante y por lo tanto la vulneración denunciada por lo que 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:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a D^a. **D.D.D.** y a D. **C.C.C..**

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