Procedimiento nº.: PS/00114/2015

ASUNTO: Recurso de Reposición Nº RR/00781/2015

Examinado el recurso de reposición interpuesto por la entidad **PERSAVI SPORT, S.L.** contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos en el procedimiento sancionador, PS/00114/2015, y en base a los siguientes,

HECHOS

PRIMERO: Con fecha 25 de agosto de 2015, se dictó resolución por la Directora de la Agencia Española de Protección de Datos en el procedimiento sancionador, PS/00114/2015 , en virtud de la cual se imponía a la entidad PERSAVI SPORT SL, una sanción de 2.500€, por la vulneración de lo dispuesto en el artículo 6.1 y una sanción de 1.000€ por la vulneración de lo dispuesto en el artículo 11.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), infracciones tipificadas como graves en el artículo 44.3.b) y 44.3.h), de conformidad con lo establecido en el artículo 45.2, 4 y 5 de la citada Ley Orgánica.

Dicha resolución, que fue notificada al recurrente en fecha 1 de septiembre de 2015, fue dictada previa la tramitación del correspondiente procedimiento sancionador, de conformidad con lo dispuesto en el artículo 127 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

SEGUNDO: Como hechos probados del citado procedimiento sancionador, PS/00114/2015, quedó constancia de los siguientes:

> *<<PRIMERO: Con fecha 8 de abril de 2014, de Don **A.A.A.**denunció ante la AEPD que en el gimnasio PERSAVI SPORT CLUB SANTA JUSTA, se han colocado unos monitores instalados donde aparecen las fotografías de los clientes que acceden al gimnasio. Según manifestó, las fotografías se encuentran en el hall de entrada a la vista cualquiera que acceda a las instalaciones y sin haber informado en ningún momento a los socios de la instalación de dichos monitores.*
>
> *Asimismo, manifiesta que el responsable del gimnasio facilitaba información de los socios a los monitores que prestan sus servicios en el mismo, y que trabajaban como entrenadores personales (folios 1-3).*
>
> *SEGUNDO: El titular del establecimiento denunciado es la entidad PERSAVI SPORT, S.L., con NIF B******* (folio 8, entre otros).*
>
> *TERCERO: Según consta en el Acta de Inspección E/3007/2014-I/01 realizada por la Inspección de Datos en fecha 9 de marzo de 2015, y respecto a la comunicación de datos, los representantes de la entidad reconocieron que durante algún tiempo se proporcionaba información de Nombre y número de teléfono de los socios a los entrenadores personales que trabajan para el gimnasio, y que pertenecen a la empresa externa ENSA SPORT, S.L., con la que manifiestan que mantienen suscrito un contrato de prestación de Servicios. No obstante alegan que esto dejó de hacerse hace en el mes de septiembre de 2014 (folios 10-11).*

CUARTO: Respecto al sistema de videovigilancia, consta en la citada Acta de Inspección lo siguiente:

"El citado gimnasio cuenta con seis plantas y tiene instalado, desde el año 2007, un sistema de videovigilancia, que cuenta con 16 cámaras ubicadas en diferentes recintos, con la finalidad de seguridad en general (personal, instalaciones, clientes). La distribución es la siguiente:

- *Cuatro en el sótano del edificio, donde también se encuentra la piscina, estando situadas dos de ellas dentro del recinto de la misma y las otras dos en la sala de squash y spa, y en el acceso al despacho donde se encuentra la sala de control.*
- *Tres en la planta baja, donde se encuentra la recepción y acceso de los socios, y la entrada a la cafetería.*
- *Una en la planta primera, en donde se encuentra la sala de cardio y recepción de centro médico.*
- *Una en la segunda, donde se encuentra la zona de pádel.*
- *Dos en la tercera planta, donde se encuentran salas de actividades múltiples.*
- *Dos en la planta cuarta, una en la sala de spinning y otra en la sala de actividades múltiples.*
- *Una en la planta quinta, donde se encuentra otra sala de actividades múltiples.*
- *Existen carteles informativos de la existencia de cámaras de videovigilancia ubicados junto a cada una de las cámaras, aunque el nombre de la entidad que figura en los mismos es el correspondiente a la antigua denominación de la entidad, el domicilio donde han de dirigirse para el ejercicio de los derechos ARCO es el mismo.*
- *Las imágenes son visualizadas en dos monitores, uno de ellos ubicado en la sala de control que se encuentra en el sótano del edificio y el otro en recepción, no obstante, a las imágenes guardadas solo se accede desde la sala de control, el otro solo se visualizan imágenes en tiempo real.*
- *Las imágenes se conservan durante un periodo de cuatro días.*
- *El sistema no está conectado a ninguna central receptora de alarmas.*
- *No existe ninguna cámara instalada en las salas utilizadas como vestuarios ni en el exterior del edificio.*
- *Con relación a los monitores existentes en recepción, donde se muestra la fotografía del socio que accede a las instalaciones, manifiesta que dicho sistema existe desde el principio, aunque se colocaron hace aproximadamente un año dos monitores situados enfrente de la recepción, para un mejor control de las personas que accedían, ya que en algunos momentos la entrada se masifica. Sólo se utilizan cuando se produce esta masificación. Generalmente solo se encuentra activo un monitor pequeño situado encima del mostrador de recepción, en el que se visualizan las fotografías de las ocho últimas personas que han*

accedido, las cuales se obtienen del fichero de socios, cuando éste pasa la ficha con el identificador, a través del lector situado en el torno de entrada.

La finalidad del sistema es evitar que acceda a las instalaciones personas que no son socios utilizando el carnet de un socio. No se visualiza el nombre del socio".

El Acta adjunta reportaje fotográfico en el que se observan las imágenes captadas por un total de dieciséis cámaras. De su análisis se desprende que se han instalado cámaras de videovigilancia en el Gimnasio, Piscina y Spa del Centro que captan imágenes de las personas que se introducen dentro de su campo de visión.

(folios 8-41)>>

TERCERO: La entidad **PERSAVI SPORT, S.L.** ha presentado en fecha 25 de septiembre de 2015, en esta Agencia Española de Protección de Datos, recurso de reposición fundamentándolo, básicamente, en lo alegado en el transcurso del procedimiento e insiste en los siguientes motivos:

1. Existencia del consentimiento tácito por parte de los socios y usuarios del centro deportivo, que prestaron sus datos en el momento de la contratación y al haber sido informados mediante carteles informativos colocados con anterioridad a la denuncia interpuesta, *"por lo que es específico, informado e inequívoco",* añadiendo que ninguno de ellos ha ejercitado sus derechos personales frente a tal tratamiento.

2. Respecto al incumplimiento del artículo 11.1, que los datos de los socios y usuarios del centro deportivo, únicamente fueron cedidos en aquellos supuestos en los que el socio autorizaba la cesión y que la AEPD no practicó las actuaciones necesarias como recibir declaración de la persona de la entidad que proporcionaba información a ENSA SPORT, en la que hubiera confirmado que sólo proporcionaba los nombres y números de teléfono de las socios que autorizaban esa cesión.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el presente recurso la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto 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 (en lo sucesivo LRJPAC).

II

En relación con las manifestaciones efectuadas por ***PERSAVI SPORT SL***, reiterándose básicamente, en las alegaciones ya presentadas a lo largo del procedimiento sancionador, debe señalarse que todas ellas ya fueron analizadas y desestimadas en los Fundamentos de Derecho del II al IX, ambos inclusive, de la Resolución recurrida, tal como se transcribe a continuación:

<< ***II***

Con carácter previo, debe señalarse que 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".

La LOPD, viene a regular el derecho fundamental a la protección de datos de las personas físicas, esto es, el derecho a disponer de sus propios datos sin que puedan ser utilizados, tratados o cedidos sin su consentimiento, con la salvedad de las excepciones legalmente previstas.

En cuanto al ámbito de aplicación de la citada norma, 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".

En lo que respecta al concepto de "fichero" el artículo 3.b) de la LOPD lo define como "todo conjunto organizado de datos de carácter personal", con independencia de la modalidad de acceso al mismo.

Por su parte el artículo 3.d) de la LOPD define al responsable del fichero o tratamiento como la "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento."

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". 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.

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".

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.

Así, de conformidad con la normativa expuesta, el denunciado dispone de datos personales y los utiliza, lo que constituye un tratamiento de datos personales del que es responsable, toda vez que es quien decide sobre la finalidad, contenido y uso del citado tratamiento.

III

En primer lugar, se imputa a la entidad ***PERSAVI SPORT, S.L.*** *como titular del gimnasio PERSAVI SPORT CLUB SANTA JUSTA sito en c/ José Laguillo, s/n, 41003 de Sevilla, la comisión de una infracción del artículo 6.1 de la LOPD, que dispone lo siguiente:*

"1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado".

Respecto a la legitimación en el tratamiento de las imágenes, la respuesta se encuentra en el artículo 2 de la Instrucción 1/2006, que establece que: "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".

El tratamiento de datos sin consentimiento constituye un límite al derecho fundamental a la protección de datos. Este derecho, en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre, (F.J. 7 primer párrafo), "...consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un particular (...)".

Son pues elementos característicos del derecho fundamental a la protección de datos personales, los derechos del afectado a consentir sobre la recogida y tratamiento de sus datos personales y a saber de los mismos.

En el presente expediente, cabe apreciar que las cámaras instaladas captan imágenes de personas, de conformidad con lo anteriormente expuesto. Dichas imágenes, incorporan datos personales de las personas que se introducen dentro de su campo de visión y, por lo tanto, los datos personales captados están sometidos al consentimiento de sus titulares, de conformidad con lo que determina la LOPD.

Dicho tratamiento, por tanto, ha de contar con el consentimiento de los afectados, circunstancia que no se ha acreditado.

A la vista de lo expuesto, ***el tratamiento realizado de las imágenes procedentes de los monitores situados en la entrada del establecimiento que muestran las fotografías de los socios a los clientes que acceden al gimnasio y el sistema de videovigilancia situado en las zonas de Gimnasio, Piscina y Spa*** *del centro que captan imágenes de las personas que se introducen dentro de su campo* ***se considera excesivo, inadecuado y no pertinente*** *en relación con el ámbito y la finalidad de videovigilancia a la que responde la instalación de las cámaras, incumpliéndose con ello el principio de*

proporcionalidad que deben regir el tratamiento de datos personales.

Como se recoge en el Informe 100399/2014 del Gabinete Jurídico de esta AEPD, respecto a la colocación de cámaras de videovigilancia en centros de Spa y actividades deportivas, "… No resultaría proporcional la captación de imágenes en las áreas de piscinas, toboganes, Spa, taquillas o en las que se realizan prácticas deportivas, ni en el área de botiquín si en la misma se prestan servicios médicos o de primeros auxilios, ni en general en ninguna otra zona en la que la intimidad de las personas pueda verse comprometida…"

Por otra parte, la Audiencia Nacional en su sentencia ***de 20 de noviembre de 2013, relativa al recurso 377/12, promovido por un establecimiento deportivo que captaba imágenes de las piscinas y áreas de duchas considera que la captación de dichas imágenes suponen "una intromisión en la privacidad de los usuarios y de la protección de datos, pues aunque se trate de un establecimiento público se han estado captando datos de los clientes realizando unas actividades privadas … que no sólo eran visibles por el personal del establecimiento, sino que también eran grabadas en un fichero, que supone un tratamiento automatizado de datos de carácter personal particularmente intrusivo para la intimidad de las personas…" .***

En conclusión, la conducta analizada supone una vulneración por parte de la entidad denunciada de lo previsto en el aludido artículo 6.1 de la LOPD.

IV

Por otra parte, la Directiva 95/46/CE en su Considerando 14 afirma:

"(14)Considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos;".

El Grupo de protección de las personas, en lo que respecta al tratamiento de datos personales, creado en virtud del artículo 29 de la citada Directiva 95/46/CE, en su Dictamen 4/2004, adoptado en fecha 11/02/2004, relativo al tratamiento de datos personales mediante vigilancia por videocámara, formula distintos criterios para evaluar la legalidad y conveniencia de instalar sistemas de captación de imágenes en zonas públicas.

Por otra parte, para determinar si el supuesto que se analiza implica el tratamiento de datos relacionados con personas identificables, el citado Grupo considera que los datos constituidos por imagen y sonido son personales aunque las imágenes se utilicen en el marco de un sistema de circuito cerrado y no estén asociados a los datos personales del interesado, incluso, si no se refieren a personas cuyos rostros hayan sido filmados, e independientemente del método utilizado para el tratamiento, la técnica, el tipo de equipo, las características de la

captación de imágenes y las herramientas de comunicación utilizadas. A efectos de la Directiva, se añade, el carácter identificable también puede resultar de la combinación de los datos con información procedente de terceras partes o, incluso, de la aplicación, en el caso individual, de técnicas o dispositivos específicos.

En cuanto a las obligaciones y precauciones que deberán respetarse por los responsables del tratamiento de los datos se mencionan, entre otras, la de evitar las referencias inadecuadas a la intimidad; especificar de forma clara e inequívoca los fines perseguidos con el tratamiento y otras características de la política de privacidad (momento en que se borran las imágenes, peticiones de acceso); obtención del consentimiento del interesado basado en una información clara; mantener la necesaria proporcionalidad entre los datos y el fin perseguido, obligándose al empleo de sistemas idóneos con respecto a dicho fin y a minimizar los datos por parte del responsable del tratamiento; datos que han de ser adecuados, pertinentes y no excesivos y deberán retenerse durante un plazo en consonancia con las características específicas de cada caso.

Por tanto, la captación de imágenes con fines de vigilancia y control, como es el caso que nos ocupa, se encuentra plenamente sometida a lo dispuesto en la LOPD, ya que constituye un tratamiento de datos de carácter personal.

De acuerdo con los preceptos transcritos, la videocámara 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 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.

La proporcionalidad es un elemento fundamental en todos los ámbitos en los que se instalen sistemas de videovigilancia, dado que son numerosos los supuestos en los que la vulneración del mencionado principio puede llegar a generar situaciones abusivas, máxime en el entorno de establecimientos en los que se realizan actividades que pudieren repercutir negativamente, y de modo muy especial, en el honor, en la libertad personal y en la propia imagen, con una incidencia especialmente grave en el espacio privado e íntimo de las personas.

Es decir, aunque pueda resultar justificable el uso de técnicas de videovigilancia por motivos de seguridad, en ningún caso resulta admisible la instalación de cámaras en espacios protegidos en los que se desarrollen actividades cuya práctica pueda afectar muy especialmente a la imagen, a la vida privada o a la intimidad de las personas, y ello en atención a la naturaleza de los derechos fundamentales que pueden verse afectados, entre los que se encuentra el de la protección de datos. Así, el responsable del tratamiento debe valorar esta circunstancia a fin de respetar tales derechos y adoptar otros medios de prevención y protección menos intrusivos y lesivos para los afectados y, en todo caso, especialmente respetuosos con su dignidad.

Por lo tanto, en este supuesto aunque la medida utilizada por la entidad titular del establecimiento en dicha dependencia fuera susceptible de cumplir el objetivo de seguridad de las instalaciones y personas, no es ponderada ni

equilibrada.

V

El artículo 44.3.b) de la LOPD considera infracción grave:

"Tratar los datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en esta Ley y sus disposiciones de desarrollo."

En función de lo expuesto cabe apreciar la existencia de la infracción denunciada por cuanto el motivo de la instalación de las videocámaras es la captación de imágenes de personas, que, tal y como anteriormente se ha referido, constituyen datos de carácter personal, no acreditándose que se cuente con el consentimiento de los afectados cuyos datos personales se tratan por las cámaras instaladas, tal y como establece el artículo 6.1 de la LOPD.

VI

En segundo lugar, se imputa a PERSAVI SPORT, S.L. la infracción del artículo 11 de la LOPD que establece lo siguiente:

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

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

a)Cuando la cesión está autorizada en una Ley.

b)Cuando se trate de datos recogidos de fuentes accesibles al público.

c)Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

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. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e)Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f)Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3.Será nulo el consentimiento para la comunicación de los datos de carácter

personal a un tercero cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar.

4.El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

5.Aquél a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

6.Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores."

Así, el artículo 11.1 de la LOPD exige el consentimiento del afectado, o bien, habilitación legal (artículo 11.2.a) de la LOPD) para la cesión de datos de carácter personal.

En el presente caso, consta acreditado en el Acta de Inspección de fecha 9 de marzo de 2015, y respecto a la comunicación de datos, que los representantes de la entidad reconocieron que durante algún tiempo se proporcionaba información de Nombre y número de teléfono de los socios a los entrenadores personales que trabajan para el gimnasio, y que pertenecen a la empresa externa ENSA SPORT, S.L., con la que manifiestan que mantienen suscrito un contrato de prestación de Servicios. No obstante esto dejó de hacerse hace en el mes de septiembre de 2014 (folios 10-11).

VII

Procede contestar a las alegaciones de la entidad denunciada a la propuesta de resolución respecto a la cesión de datos a un tercero. Persavi manifiesta la indefensión de esa entidad sobre la base de unos hechos que no resultan probados y que exclusivamente han sido manifestados por un usuario que ha decidido darse de baja en las instalaciones, e insiste en que si bien no existe vínculo contractual con la tercera empresa, ENSA SPORT, toda vez que existía un acuerdo verbal, que tiene validez jurídica como cualquier contrato escrito.

En este sentido hay que recordar que es la propia entidad la que ha reconocido los hechos, según se ha manifestado más arriba (Hecho Probado Tercero), pero incluso también lo reconoce en sus alegaciones a la propuesta en la que manifiesta que "Si bien antaño se procedía a ceder datos de forma directa a la entidad ENSA SPORT, esa práctica cedió después de la visita de los inspectores de la Agencia…".

En cuanto a la validez del acuerdo verbal, dicho contrato no resultaría correcto en materia de protección de datos si no contempla las consideraciones del artículo 11 de la LOPD, como se ha expuesto en el Fundamento de Derecho anterior. Pero, a mayor abundamiento, procede señalar que la entidad

denunciada no cumple tampoco lo estipulado en el artículo 12 de la citada norma, que regula el acceso a los datos por cuenta de terceros:

> *"1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.*
>
> *2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.*
>
> *En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.*
>
> *3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.*
>
> *4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente".*

Por lo tanto, dichas alegaciones deben ser desestimadas.

VIII

La infracción de lo dispuesto en el artículo 11 de la LOPD se encuentra tipificada como grave en el artículo 44.3.k) de la misma norma, que considera como tal "La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello en los términos previstos en esta Ley y sus disposiciones reglamentarias de desarrollo, salvo que la misma sea constitutiva de infracción muy grave".

En el presente caso consta acreditada la comisión imputada toda vez que la entidad denunciada cedió los datos personales relativos a nombre, apellidos y teléfono de los socios de su entidad a la empresa externa ENSA SPORT, S.L. a fin de que los entrenadores de la entidad les pudieran ofrecer promociones sobre sus servicios.

IX

El artículo 45 de la LOPD, apartados 1 a 5, según redacción introducida por la Ley 2/2011, de 4 de marzo, de Economía Sostenible, establece:

"1. Las infracciones leves serán sancionadas con multa de 900 a 40.000 euros.

2. Las infracciones graves serán sancionadas con multa de 40.001 a 300.000 euros.

3. Las infracciones muy graves serán sancionadas con multa de 300.001 a 600.000 euros.

1. La cuantía de las sanciones se graduará atendiendo a los siguientes criterios:

a) El carácter continuado de la infracción.
b) El volumen de los tratamientos efectuados.
c) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.
d) El volumen de negocio o actividad del infractor.
e) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
f) El grado de intencionalidad.
g) La reincidencia por comisión de infracciones de la misma naturaleza.
h) La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.
i) La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.
j) Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:

a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado 4 de este artículo.
b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.
c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.
d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.
e) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente.»

De conformidad con el análisis realizado se ha incurrido en las infracciones descritas. Así, ha quedado acreditado que la entidad PERSAVI SPORT, S.L. como titular del establecimiento con denominación comercial PERSAVI SPORT CLUB SANTA JUSTA utiliza sus cámaras de videovigilancia que captan imágenes de las zonas de gimnasio, spa y piscina y que muestra las imágenes de los socios que acceden al establecimiento mediante unos monitores ubicados a la entrada del mismo de forma inadecuada y excesiva, sin contar con el consentimiento de los afectados para el tratamiento de sus datos personales.

Por otra parte, consta acreditado que la entidad denunciada cedió los datos personales relativos a nombre, apellidos y teléfono de los socios de su entidad a la empresa externa ENSA SPORT, S.L. a fin de que los entrenadores de la entidad les pudieran ofrecer promociones sobre sus servicios.

Sin embargo, ha de tenerse en cuenta que la complejidad de las normas que regulan el tratamiento de datos personales a través de sistemas de videovigilancia requieren una especial cualificación técnica, lo que lleva a apreciar la existencia de una cualificada disminución de la culpabilidad, al no poder obviarse que la conducta infractora se realizó por una entidad no habituada al tratamiento de datos personales.

En este caso, una vez analizadas las circunstancias concurrentes, se considera procedente la aplicación de lo establecido en el artículo 45.5 de la LOPD, no apreciándose obstáculo alguno ni indefensión o perjuicio para ninguna de las partes por dicha aplicación.

Por otro lado respecto de los criterios que recoge el art. 45.4 relativos a la aplicación del principio de proporcionalidad en la graduación del importe de la sanción, y según las indicaciones del art. 131.3 de la LRJPAC (Ley 30/92 de 26 de noviembre), que establece: "en la determinación normativa del régimen sancionador, así como en la imposición de sanciones por las Administraciones Públicas se deberá guardar la debida adecuación entre la gravedad del hecho constitutivo de la infracción y la sanción aplicada, considerándose especialmente los siguientes criterios para la graduación de la sanción a aplicar: a) la existencia de intencionalidad o reiteración, b) la naturaleza de los perjuicios causados, c) la reincidencia", se concluye que de la secuencia de hechos expuesta en esta resolución, valorada en aplicación de dichos criterios, toda vez que se ha constatado que el denunciado continúa captando imágenes con las cámaras de videovigilancia que superan su propiedad sin que se haya corregido esta situación, permiten que en este caso se considere procedente la imposición de una sanción en la cuantía de 2.500 euros por la infracción del artículo 6.1 y de 1.000 euros por la infracción del artículo 11.1 de la LOPD.>>

X

PERSAVI SPORT, S.L. solicita que se considere que el establecimiento cuenta con el consentimiento tácito por parte de los socios y usuarios del centro deportivo, que

prestaron sus datos en el momento de la contratación y al haber sido informados mediante carteles informativos colocados con anterioridad a la denuncia interpuesta, *"por lo que es específico, informado e inequívoco",* añadiendo que ninguno de ellos ha ejercitado sus derechos personales frente a tal tratamiento.

En relación con esta alegación hay que señalar que para que exista consentimiento, elemento base en el tratamiento de los datos, deben concurrir los requisitos legalmente previstos para considerar que se ha obtenido libremente el consentimiento. El artículo 3 h) de la LOPD lo define como *"Toda manifestación de voluntad libre, inequívoca, específica e informada mediante la que el interesado consienta el tratamiento de datos personales que le conciernen."*

Del concepto de consentimiento se desprende la necesaria concurrencia para que el mismo pueda ser considerado conforme a derecho de los cuatro requisitos enumerados en dicho precepto. Un adecuado análisis del concepto exigirá poner de manifiesto cuál es la interpretación que ha de darse a estas cuatro notas características del consentimiento, tal y como la misma ha indicado en numerosas Resoluciones de la AEPD, siguiendo a tal efecto los criterios sentados en las diversas recomendaciones emitidas por el Comité de Ministros del Consejo de Europa en relación con la materia que nos ocupa. A la luz de dichas recomendaciones, el consentimiento habrá de ser:

a)Libre, lo que supone que el mismo deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil.

b)Específico, es decir referido a un determinado tratamiento o serie de tratamientos concretos y en el ámbito de las finalidades determinadas, explícitas y legítimas del responsable del tratamiento, tal y como impone el artículo 4.2 de la LOPD.

c) Informado, es decir que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce. Precisamente por ello el artículo 5.1 de la LOPD impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen.

d) Inequívoco, lo que implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado.

La Jurisprudencia de la Audiencia Nacional ha entendido que los requisitos del consentimiento, se agotan en la necesidad de que este sea "inequívoco", es decir, que no exista duda alguna sobre la prestación de dicho consentimiento, de manera que en esta materia el legislador, mediante el artículo 6.1 de la LO de tanta cita, acude a un criterio sustantivo, esto es, nos indica que cualquiera que sea la forma que revista el consentimiento, éste ha de aparecer como evidente, inequívoco - que no admite duda o equivocación- , pues éste y no otro es el significado del adjetivo utilizado para calificar al consentimiento.

Por tanto, de la presunción de un consentimiento tácito no puede ser estimado en el presente supuesto, pues dar carta de naturaleza a este tipo de interpretación pulverizaría la exigencia esencial del consentimiento, porque dejaría de ser inequívoco para ser "equívoco", es decir, su interpretación admitiría varios sentidos, es decir, su

interpretación admitiría varios sentidos y, por esta vía, se desvirtuaría la naturaleza y significado que desempeña como garantía en la protección de los datos, e incumpliría la finalidad que está llamado a verificar, esto es, que el poder de disposición de los datos corresponde únicamente a su titular. Es este el sentido recogido en la Sentencia de la Audiencia Nacional de 21 de noviembre de 2007 (Rec 356/2006) en su Fundamento de Derecho Quinto, Sentencias de 20 de julio de 2006 RJ 2006. 47381 y 10 de junio de 2005 RJ 2005. 43641 entre muchas otras, la reiterada jurisprudencia pone de manifiesto que «los hechos determinantes de la apreciación del consentimiento han de ser inequívocos -"falta concludentia"-, es decir, que con toda evidencia los signifiquen -S. 7 junio 1986 RJ 1986. 3296K sin posibilidad de dudosas interpretaciones -SS. 5 julio 1960, 14 junio 1963, 13 febrero 1978-», lo cual implica a su vez, que también sea un criterio consolidado en la doctrina a la hora de valorar el silencio como consentimiento tácito que «generalmente el mero conocimiento no implica conformidad, ni basta el mero silencio para entender que se produjo la aquiescencia.

A la vista de lo expuesto, del hecho de que los afectados por el tratamiento de las imágenes no se hayan opuesto de forma expresa al mismo no se puede inferir un consentimiento tácito como alega la entidad denunciada, procediendo desestimar la alegaciones efectuadas a este respecto.

En este sentido, se ha pronunciado esta Agencia Española de Protección de Datos, en su informe n° 0041/2008 al recoger: *" La consulta plantea cómo habrá de obtenerse el consentimiento respecto de las grabaciones obtenidas a través de cámaras de videovigilancia de conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal y la Instrucción 1/2006 de 8 de noviembre de 2006, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.*

1. En primer lugar, se plantea la posibilidad de obtener el consentimiento tácito, en esta materia, lo que exige tener en cuenta lo dispuesto en el artículo 6.1 de la Ley Orgánica 15/1999 que señala lo siguiente "El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa".

Por otro lado, respecto a la forma de obtener el consentimiento, es necesario acudir a lo dispuesto en del Real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la Ley Orgánica 15/1999, donde en el artículo 14, se regulan las formas de obtener el consentimiento señalando que "1. El responsable del tratamiento podrá solicitar el consentimiento del interesado a través del procedimiento establecido en este artículo, salvo cuando la Ley exija al mismo la obtención del consentimiento expreso para el tratamiento de los datos.

2. El responsable podrá dirigirse al afectado, informándole en los términos previstos en los artículos 5 de la Ley Orgánica 15/1999, de 13 de diciembre y 12.2 de este reglamento y deberá concederle un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto

se entenderá que consiente el tratamiento de sus datos de carácter personal.

En particular, cuando se trate de responsables que presten al afectado un servicio que genere información periódica o reiterada, o facturación periódica, la comunicación podrá llevarse a cabo de forma conjunta a esta información o a la facturación del servicio prestado, siempre que se realice de forma claramente visible.

3.En todo caso, será necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

4.Deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular, se considerará ajustado al presente reglamento los procedimientos en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento, la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

5. Cuando se solicite el consentimiento del interesado a través del procedimiento establecido en este artículo, no será posible solicitarlo nuevamente respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud."

El procedimiento descrito en el artículo 14 del Real Decreto 1720/2007, es el único que puede entenderse válido a la hora de obtener el consentimiento tácito y resulta de aplicación imposible cuando se trata de grabaciones o reproducciones en tiempo real de imágenes. En consecuencia, podemos concluir que en materia de videovigilancia resulta prácticamente imposible obtener el consentimiento, de las personas cuyas imágenes capten las cámaras por lo que es preciso acudir a una ley que habilite el tratamiento."

Por lo tanto, el tratamiento de datos sin consentimiento constituye un límite al derecho fundamental a la protección de datos. Este derecho, en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre, (F.J. 7 primer párrafo), "...consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un particular (...)".

En el caso analizado, de lo expuesto resulta que la instalación de las cámaras en el interior del establecimiento, si bien se encuentra justificada, en principio, por motivos de seguridad; el tratamiento realizado de las imágenes procedentes de los monitores situados en la entrada del establecimiento que muestran las fotografías de los socios a los clientes que acceden al gimnasio y el sistema de videovigilancia situado en las zonas de Gimnasio, Piscina y Spa del centro que captan imágenes de las personas que se introducen dentro de su campo se considera, como ya se indicó en la Resolución recurrida, excesivo, inadecuado y no pertinente en relación con el ámbito y la finalidad

de videovigilancia a la que responde la instalación de las cámaras, incumpliéndose con ello el principio de proporcionalidad que deben regir el tratamiento de datos personales.

XI

En cuanto a las manifestaciones de la entidad relativas a que los datos de los socios y usuarios del centro deportivo, únicamente fueron cedidos en aquellos supuestos en los que el socio autorizaba la cesión y que la AEPD no practicó las actuaciones necesarias como recibir declaración de la persona de la entidad que proporcionaba información a ENSA SPORT, en la que hubiera confirmado que sólo proporcionaba los nombres y números de teléfono de las socios que autorizaban esa cesión.

A este respecto procede señalar que, la entidad imputada no ha aportado en ningún momento, ni tan siquiera con motivo del presente recurso de reposición, contrato ni elemento alguno que autorizase la cesión que la propia entidad ha reconocido que estuvo realizando hasta el mes de septiembre de 2014, ni acreditación documenta de ninguno de los socios para que sus datos fueran cedidos a dicha entidad.

Por lo tanto, dichas alegaciones deben ser desestimadas.

XII

Por lo tanto, en el presente recurso de reposición, **PERSAVI SPORT, S.L.** no ha aportado nuevos hechos o argumentos jurídicos que permitan reconsiderar la validez de la resolución impugnada.

Vistos los preceptos citados y demás de general aplicación,

La Directora de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por **PERSAVI SPORT, S.L.** contra la Resolución de esta Agencia Española de Protección de Datos dictada con fecha 25 de agosto de 2015, en el procedimiento sancionador PS/00114/2015.

SEGUNDO: NOTIFICAR la presente resolución a la entidad **PERSAVI SPORT, S.L.**

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, se podrá interponer 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 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, 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 del referido texto legal.

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