- Procedimiento Nº: E/07044/2019

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: La reclamación interpuesta por D. ***A.A.A.*** (en adelante, el reclamante) tiene entrada con fecha 04/06/2018 en la Agencia Española de Protección de Datos. La reclamación se dirige contra COMUNIDAD DE PROPIETARIOS R.R.R., con NIF ******NIF.1*** (en adelante, el reclamado). Los motivos en que basa la reclamación son: la instalación de un control de acceso al club social anejo a la vivienda basado en la huella dactilar sin que se ofrezca otra alternativa; han obtenido la huella de su hijo sin consentimiento previo.

Y, entre otra, anexa la siguiente documentación:

 Acta de la junta general extraordinaria de la COMUNIDAD DE PROPIETARIOS R.R.R. de 26/09/2017 donde se aprueba la instalación de tornos con reconocimiento de huella para el acceso a las instalaciones.

El 30/08/2018, se recibe nuevo escrito del reclamante indicando además que no ha podido ejercitar su derecho de acceso ante la reclamada. Manifiesta también, que recibe correos masivos de las actas de las reuniones donde figuran sus datos personales, e incluso, una oferta comercial de una compañía de telefonía.

Trasladada la reclamación a la reclamada, el 24/10/2018 se recibe respuesta manifestando que:

 El 26/09/2017 acuerdo en junta de propietarios de la instalación de torno con apertura mediante huella digital.
 El 02/06/2018 apertura de las instalaciones.
 El 03/06/2018 se producen los hechos denunciados

Que el día en que se producen los hechos, el hijo del reclamante accede a las instalaciones acompañado de un adulto que no era su padre. El presidente de la comunidad de propietarios que se encontraba en las instalaciones y advirtiendo el hecho, preguntó al controlador cómo había accedido el menor a la piscina. Conocedor de que el padre no había otorgado consentimiento para el escaneo de la huella del menor, solicitó al controlador que eliminara de inmediato este dato y facilitó al menor un formulario para la recogida de consentimiento por parte de su padre. Reiteró al controlador las instrucciones a seguir para evitar que volviera a suceder una situación similar.

Se adjunta acta de 08/05/2018 en el que consta que se mantiene como forma alternativa de acceso, la presentación del carné con fotografía, para lo que resulta necesario que los propietarios aporten las fotografías correspondientes.

Se adjuntan varias comunicaciones por correo electrónico entre la administración de la reclamada y el reclamante. Entre ellos, la parte administradora pone de manifiesto:

 La existencia de acceso alternativo a las instalaciones como se venía haciendo con anterioridad, pero que por error, no se informó correctamente al controlador. Cuestión que fue subsanada el segundo día de apertura de las instalaciones.

 Informa también al reclamante de que los datos de la huella del menor fueron eliminados en cuanto se detectó que la autorización no había sido firmada y se informó al menor del hecho.

 Que informó al reclamante de que para ejercer sus derechos de acceso y supresión, debía dirigirse a la administración de la comunidad que es la responsable del tratamiento.

Hay que señalar que todas las actuaciones mencionadas dieron lugar al expediente E/09127/2018

El 20/11/2018 se inician actuaciones previas de investigación en el seno del citado expediente, extendiéndose un tiempo superior a 12 meses por lo que el 06/06/2019, se acordó proceder al archivo de las mismas y abrir nuevas actuaciones de investigación.

Como consecuencia de ello con fecha de 24/06/2019 se recibe recurso de reposición contra el archivo de las actuaciones manifestando el reclamante que la pretensión que motivó la reclamación no había sido debidamente subsanada.

El 16/10/2019, teniendo en cuenta que el archivo recurrido solo declaraba la caducidad de las actuaciones previas por el transcurso de doce meses, resolviendo iniciar nuevas actuaciones previas para aclarar los hechos denunciados y sancionar si la actuación de la entidad denunciada no es conforme al RGPD, se resuelve desestimar el recurso interpuesto contra la resolución de 06/06/2019.

SEGUNDO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la reclamación, teniendo conocimiento de los siguientes extremos:

Habiéndose iniciado nuevas actuaciones de investigación, se obtienen las siguientes conclusiones:

 Requerido a la reclamada información facilitada a los encargados de tomar las huellas, comunicación enviada al reclamante comunicándole los datos que consten a la administradora de la comunidad de su hijo, el tratamiento de las huellas

recabadas, y el estado actual del acceso a la piscina, con fecha de 28/08/2019 se recibe en esta Agencia contestación al requerimiento remitido por la administración de la reclamada manifestando que se ha hecho llegar a todos los comuneros el documento “Clausula - Deber de información” donde se indica la finalidad de los tratamientos de acceso a la piscina y se recaba el consentimiento del tratamiento de forma independiente para la finalidad administrativa, para el acceso mediante carné y para el acceso mediante huella dactilar.

Añaden que la persona contratada para el control de acceso a la piscina recibe, entre la documentación que debe firmar en el contrato, una hoja informativa sobre el tratamiento de toma de huella para acceso a la piscina, en la que se recogen las siguientes obligaciones:

o Confidencialidad de los datos incluso después de haber finalizado la relación con el titular y en caso de cambiar el control de acceso mediante huella, la eliminación de todos los datos recabados relativos a las huellas.
o El deber de informar a los comuneros de que existe un método alternativo para el acceso a la piscina
o La necesidad de que el comunero haya dado el consentimiento para el tratamiento mediante el documento *“Clausula - Deber de información”* y la inmediata eliminación de sus datos cuando el consentimiento sea revocado.
o El deber de informar a todo comunero que lo solicite del procedimiento para ejercer sus derechos y ante quien.

Respecto a la comunicación al reclamante, recuerdan que no tienen constancia de que el reclamante haya ejercido formalmente el derecho de acceso a sus datos ni al del menor en ningún momento, pese a que se le informó que debía hacerlo por escrito y dirigirlo a la presidencia de la comunidad según correo electrónico de fecha 30/08/2018 que se adjunta. Añaden, que este procedimiento también está indicado en el documento *“Clausula - Deber de información”* donde se recogió el consentimiento del reclamante para algunos de tratamientos de datos y en el tablón de anuncios de la comunidad.

Con respecto al tratamiento indican el funcionamiento técnico del sistema que crea un patrón en función de la huella y que solo se tratan los datos de huella de los comuneros que han dado su consentimiento expreso mediante la cumplimentación del documento *“Clausula - Deber de información”.*

Respecto a la situación actual de acceso a la piscina, informan que están activos los dos sistemas de control, por huella dactilar y por carné con fotografía que el controlador compara con la fotografía almacenada en la base de datos.

Y adjuntan, entre otros, los siguientes documentos:

- Documento “Clausula - Deber de información”
- Contratos con terceros actualizados. Documentación entregada y firmada por el encargado del acceso a la piscina.
- Registro de actividades de tratamiento actualizado (Nivel especialmente protegido)

- Análisis de riesgos de los tratamientos de datos personales actualizado (Nivel especialmente protegido)
- Correo electrónico dirigido al reclamante indicando el procedimiento a seguir para el ejercicio del derecho de acceso, rectificación y cancelación.
- “Clausula - Deber de información” con los consentimientos concedidos por el reclamante

 Se observa por tanto, que en esta segunda temporada de piscina, se han recabado los consentimientos de forma más precisa y se ha informado en todo momento y por varias vías, del procedimiento a seguir para el ejercicio de derechos del interesado.

Se han actualizado los contratos con terceros con acceso a datos y especialmente el contrato con el controlador de acceso recogiendo claramente todas sus obligaciones, confidencialidad y secreto del tratamiento de datos, y se adjuntado una adenda específica para el tratamiento de datos de huella dactilar.

Igualmente se ha actualizado el registro de actividades de tratamiento y el análisis de riesgos incluyendo las características del tratamiento de datos biométricos para el acceso a la piscina.

## FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

El reclamante ha manifestado a que se tomó la huella de su hijo sin su consentimiento, no habiéndosele facilitado el acceso a los datos que le fueron recabados y que el procedimiento de acceso a las instalaciones es totalmente desproporcionado al no existir otro método alternativo para acceder a las mismas.

En primer lugar, hay que señalar que de la documentación aportada y de las actuaciones realizadas por los servicios de inspección de este centro directivo se constata que la toma de la huella del menor fue producto de un error y que detectado el mismo fue subsanado de manera inmediata eliminando los datos de carácter personal, sin que se hubiera procedido a tratamiento posterior alguno de los mismos por parte de la Comunidad.

Además, se informó al reclamante de la incidencia producida así como del procedimiento para el ejercicio de sus derechos sin que exista constancia de que el afectado hubiera ejercitado el derecho de acceso.

Por tanto, los hechos acaecidos implicarían un resultado no perseguido y por tanto, la comisión de un error. Hemos de tener en cuenta que, como pone de manifiesto la Audiencia Nacional, y en la medida en que no concurre voluntariedad en el acto, que no se ha producido un resultado especialmente lesivo, y que no consta la falta de cuidado en la actuación generalizada de la comunidad reclamada en sus funciones, sería contrario a la naturaleza del ámbito sancionador administrativo, sujeto a los principios de intervención mínima y proporcionalidad, imponer una sanción al respecto del acto producido, que puede resumirse en un mero error no merecedor de actuación sancionadora.

En este mismo sentido, la Sentencia de la Audiencia Nacional de 14 de diciembre de 2006, recurso nº 1363/2005, señala en sus Fundamentos Jurídicos lo siguiente: *"La resolución del presente recurso pasa por recordar, en primer lugar, que la culpabilidad es un elemento indispensable para la sanción que se le ha impuesto a la actora, tal como lo prescribe el artículo 1301.1 de la Ley 30/1.992 de 26 de noviembre, que establece que sólo pueden ser sancionados por hechos constitutivos de infracción administrativa los responsables de los mismos, aún a título de simple inobservancia.*

*Se ha de hacer hincapié en que esa simple inobservancia no puede ser entendida que en el derecho administrativo sancionador rija la responsabilidad objetiva.*

*Efectivamente, en materia sancionadora rige el principio de culpabilidad (SsTC 15/1999, de 4 de julio; 76/1990, de 26 de abril; y 246/1991, de 19 de diciembre), lo que significa que ha de concurrir alguna clase de dolo o culpa. Como dice la sentencia del Tribunal Supremo de 23 de enero de 1998 , "...puede hablarse de una decidida línea jurisprudencial que rechaza en el ámbito sancionador de la Administración la responsabilidad objetiva, exigiéndose la concurrencia de dolo o culpa, en línea con la interpretación de la STC 76/1990, de 26 de abril , al señalar que el principio de culpabilidad puede inferirse de los principios de legalidad y prohibición de exceso (artículo 25 de la Constitución) o de las exigencias inherentes al Estado de Derecho".*

III

En segundo lugar, el reclamante hace referencia a la instalación de un control de acceso al club social basado en la huella dactilar sin que se ofrezca otra alternativa al citado sistema de acceso.

Sin embargo, el reclamado ha indicado que en la situación actual para el acceso a las instalaciones entre las que se encuentra el servicio de piscina, se encuentran activados dos sistemas de control: por huella dactilar y por carné con fotografía que el controlador empleado compara con la fotografía almacenada en la base de datos.

En cuanto al establecimiento de un sistema de control basado en la huella dactilar, los datos biométricos están estrechamente vinculados a una persona dado que pueden utilizar una determinada propiedad única de un individuo para su identificación o autenticación.

Según el Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, *"Los datos biométricos cambian irrevocablemente la relación entre el cuerpo y la*

*identidad, ya que hacen que las características del cuerpo humano sean legibles mediante máquinas y estén sujetas a un uso posterior."*

En relación con ellos, el Dictamen precisa que cabe distinguir diversos tipos de tratamientos al señalar que *"Los datos biométricos pueden tratarse y almacenarse de diferentes formas. A veces, la información biométrica capturada de una persona se almacena y se trata en bruto, lo que permite reconocer la fuente de la que procede sin conocimientos especiales; por ejemplo, la fotografía de una cara, la fotografía de una huella dactilar o una grabación de voz. Otras veces, la información biométrica bruta capturada es tratada de manera que solo se extraen ciertas características o rasgos y se salvan como una plantilla biométrica."*

Los datos biométricos los define el artículo 4.14 del RGPD: «*datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;*

El tratamiento de estos datos está expresamente permitido por el RGPD cuando el empresario cuenta con una base jurídica, que de ordinario es el propio contrato de trabajo. A este respecto, la STS de 2 de julio de 2007 (Rec. 5017/2003), que ha entendido legitimo el tratamiento de los datos biométricos que realiza la Administración para el control horario de sus empleados públicos, sin que sea preciso el consentimiento previo de los trabajadores.

Sin embargo, debe tenerse en cuenta lo siguiente:

 El afectado al que se recogen las huellas para acceder a la piscina debe ser informado sobre estos tratamientos.
 Deben respetarse los principios de limitación de la finalidad, necesidad, proporcionalidad y minimización de datos.

En todo caso, el tratamiento también deberá ser adecuado, pertinente y no excesivo en relación con dicha finalidad. Por tanto, los datos biométricos que no sean necesarios para esa finalidad deben suprimirse y no siempre se justificará la creación de una base de datos biométricos (Dictamen 3/2012 del Grupo de Trabajo del art. 29).

En relación con estos principios, la Sentencia de la Audiencia Nacional, de 19 de diciembre de 2019, señala lo siguiente: *"Respecto a si la medida se considera necesaria para satisfacer dicha necesidad, o si es esencial para responder a dicha necesidad y no sólo la más adecuada o rentable, hay que señalar que la implantación del sistema, como reiteradamente ha sostenido la parte a lo largo del procedimiento, no obedece a razones de comodidad, sino a evitar que pretendan acceder al gimnasio personas ajenas al mismo, ya que se evita llevar tarjetas, pulseras o dispositivos que pueden ser intercambiados con otros usuarios dando lugar a intrusismo y fraude, redundando su uso en un aumento de la calidad del servicio y seguridad de los clientes y de la propia empresa (…)."*

Y añade *"Enlazamos así con el principio de proporcionalidad estrictu sensu, pues las garantías adoptadas en el sistema de tratamiento de la huella por parte de la*

*entidad recurrente son relevantes a la hora de valorar la injerencia en el derecho fundamental de protección de datos y en la proporcionalidad de la medida. A tal fin debe tomarse en consideración que la entidad recurrente se ha preocupado por la confidencialidad con la conversión de la huella a su algoritmo y no ha conservado en el sistema la huella o puntos de la misma, sino el algoritmo, tratando de minimizar así la injerencia en el derecho fundamental.*

*A lo anterior hay que añadir que los datos son recogidos para el acceso y uso del gimnasio y los socios no pueden ser identificados para otros fines distintos a dicho acceso (…).”*

- Uso de plantillas biométricas: Los datos biométricos deberán almacenarse como plantillas biométricas siempre que sea posible. La plantilla deberá extraerse de una manera que sea específica para el sistema biométrico en cuestión y no utilizada por otros responsables del tratamiento de sistemas similares a fin de garantizar que una persona solo pueda ser identificada en los sistemas biométricos que cuenten con una base jurídica para esta operación.
- El sistema biométrico utilizado y las medidas de seguridad elegidas deberán asegurarse de que no es posible la reutilización de los datos biométricos en cuestión para otra finalidad.
- Deberán utilizarse mecanismos basados en tecnologías de cifrado, a fin de evitar la lectura, copia, modificación o supresión no autorizadas de datos biométricos.
- Los sistemas biométricos deberán diseñarse de modo que se pueda revocar el vínculo de identidad.
- Deberá optarse por utilizar formatos de datos o tecnologías específicas que imposibiliten la interconexión de bases de datos biométricos y la divulgación de datos no comprobada.
- Los datos biométricos deben ser suprimidos cuando no se vinculen a la finalidad que motivó su tratamiento y, si fuera posible, deben implementarse mecanismos automatizados de supresión de datos.

Por otra parte, la legitimación para el tratamiento de la huella dactilar para el acceso a las instalaciones por parte del reclamado debemos buscarlo en el artículo 9 y 6 del RGPD.

El artículo 9 del RGPD establece en sus apartados 1 y 2.a) lo siguiente:

*“1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.*

*2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:*

*a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;*

*(…)”*

El artículo 6.1.a) del RGPD indica:

*“1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:*

*a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;*
*(…)”*

El reclamado tiene legitimación, fundamentada en la normativa señalada, para efectuar el control de acceso siempre que cumpla los requisitos indicados.

No obstante, hay que indicar que con carácter previo a la decisión sobre la puesta en marcha de un sistema de control de este tipo y teniendo en cuenta sus implicaciones, el tratamiento de datos de una categoría especial (biométricos), etc., es preceptivo establecer un Registro de Actividades de Tratamiento de conformidad con el artículo 30 del RGPD y llevar a cabo una Evaluación de Impacto relativa a la protección de datos de carácter personal para evaluar la legitimidad del tratamiento, su proporcionalidad, la determinación de los riesgos existentes y medidas para mitigarlos de conformidad con lo establecido en el artículo 35 del RGPD.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a D. ***A.A.A.*** y a la COMUNIDAD DE PROPIETARIOS R.R.R., con NIF ******NIF.1.***

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, 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 de la referida Ley.

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