- **Expediente N.º: EXP202408951**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y en base a los siguientes

HECHOS

PRIMERO: Con fecha 5 de junio de 2024 se interpuso reclamación ante la Agencia Española de Protección de Datos por una posible infracción imputable a **COMUNIDAD DE PROPIETARIOS A.A.A.** con NIF ***NIF.1** (en adelante, C.P.).

Los hechos que se pone en conocimiento de esta autoridad son:

La parte reclamante expone que la comunidad de propietarios reclamada decidió en junta general ordinaria celebrada el 3 de junio de 2020 instalar un sistema de acceso biométrico mediante detector de huellas para acceder a la piscina, una zona común de la comunidad, lo que entiende como un tratamiento de datos no proporcional existiendo otros métodos menos intrusivos.

Junto al escrito, se aporta:

- Fotografías de la puerta de acceso a una piscina donde se visualiza un sistema de apertura de dicha puerta mediante huella dactilar.

- Copia de comunicado informativo titulado "*Comunicado - Instalación Detector Huellas Piscina*", de fecha 23 de mayo de 2024, con el siguiente contenido:

> *"Sevilla, 23 de MAYO de 2024*
>
> *Estimado Propietario/a,*
>
> *Nos ponemos en contacto con usted por orden del Sr. Presidente, en calidad de Secretarias-Administradores de la* ***Comunidad de Propietarios A.A.A.*** *para informarle del siguiente asunto de su interés.*
>
> *Les informamos que tal y como se aprobó en la Junta Ordinaria de fecha 03-06-2020, en los próximos días, se va a proceder a instalar un lector de huellas para el acceso a la piscina.*
>
> *La recogida de huellas se realizará los siguientes días:*
>
> *- LUNES 27/05/24 de 12.00 horas a 13:00 horas por la empresa* ******EMPRESA.1****.*
> *- MIERCOLES 29/05/24 de 8:00 horas a 14:00 horas por el mantenedor.*

- MIERCOLES 05/06/24 de 8:00 horas a 14:00 horas por el mantenedor.

La empresa instaladora del servicio y el equipo de lector de huellas están homologados y cumple con la normativa de la U.E. Los propietarios dan su consentimiento para que la huella sea única y exclusivamente utilizada para este fin.

Es importante que todos los propietarios/inquilinos se preocupen de dejar su huella registrada los días indicados para poder acceder al recinto de la piscina, ya que, agotado el plazo de registro, sólo se podrá acceder mediante este sistema y cualquier persona que no siga este procedimiento, estará incumpliendo lo acordado en la Junta de Propietarios.

Teniendo en cuenta la oleada de robos y actos vandálicos que ha sufrido esta Comunidad en los últimos meses. rogamos a los vecinos qua extremen las precauciones y se cumplan todos los acuerdos adoptados.

Sin otro particular y en espera que nuestra colaboración les sea de ayuda les saluda

*Atentamente **B.B.B.**- Secretaria – Administradora."*

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a C.P., para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

La notificación del traslado de la reclamación, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue realizada en fecha 20 de junio de 2024 como consta en el acuse de recibo que obra en el expediente.

Con fecha 18 de julio de 2024 se recibe en esta Agencia escrito de respuesta de solicitud de información,

"Preliminar. – Antecedentes.
Resulta conveniente realizar una sucinta redacción de los hechos que han provocado la interposición de la reclamación efectuada ante la AEPD por parte de uno de los usuarios de la piscina.
*En relación con la realidad física de la comunidad de propietarios de *****DIRECCIÓN.1 y ***DIRECCIÓN.2**, estas constituyen una única unidad constructiva, aunque a efectos formales se divide en dos comunidades distintas. Por una parte, el edificio perteneciente a la comunidad de propietarios de *****DIRECCIÓN.1** está formado por 20 viviendas, 32 plazas de garaje*

aparcamiento y 12 trasteros, asimismo, la piscina y el patio de vecinos son zonas comunes de esta comunidad de vecinos. Por su parte, el edificio de la comunidad de propietarios de ******DIRECCIÓN.2*** *está compuesta únicamente por 3 viviendas, pero los vecinos de esta comunidad pueden acceder a las plazas de garaje de las cuales son propietarios y a la piscina, en virtud de la servidumbre de paso constituida a su favor por la promotora de las viviendas, pues la misma promotora llevó a cabo la rehabilitación de* ******DIRECCIÓN.2*** *y la construcción de* ******DIRECCIÓN.1****.*

La pretensión de la parte reclamante de la inutilización del sistema de acceso a la piscina mediante lector de huellas ya fue suscitada ante el Juzgado de Primera Instancia n.º X de Sevilla. En dicho procedimiento la parte reclamante, al igual que en su actual reclamación ante la AEPD, solicitó la declaración de nulidad del acuerdo adoptado en Junta de Propietarios el día 3 de junio de 2020.

La sentencia ***XXX/YYYY*** *del Juzgado de Primera Instancia Número X de Sevilla de 12 de noviembre de 2021 desestimó la demanda interpuesta por la reclamante declarando "no haber lugar a la impugnación del acuerdo adoptado por la misma, en el punto 2º del orden del día de la Junta Extraordinaria de Propietarios de fecha 3 de junio de 2020".*

En lo que respecta a la vulneración de la normativa de protección de datos, el Juzgado, en su fundamento de derecho noveno de la referida sentencia, consideró que:

> *"el acuerdo impugnado no resulta contrario a la ley o a los estatutos, no limita en modo alguno el derecho real de servidumbre de paso establecido en favor de los demandantes, ni cuenta con entidad suficiente para considerar infringida la normativa sobre control de datos personales, como asimismo se argumenta en el escrito de demanda, tratándose por otra parte de un sistema muy común y extendido en la actualidad para el acceso a diversos recintos públicos que precisan de control de identidad o aforo, como piscinas o zonas deportivas en general".*

El interés que trasciende a ambas reclamaciones es el particular del referido denunciante. La pretensión es hacer un uso ilimitado de la piscina comunitaria, dotando a su propiedad -destinada a arrendamiento turístico- de unas instalaciones de las que puedan disfrutar sus inquilinos. Por lo tanto, el denunciante no vela por la protección de los datos de carácter personal, sino que trata boicotear cualquier medida que suponga la limitación del uso de las instalaciones comunes. Ello supone, a nuestro entender, un uso espurio de la normativa reguladora de la protección de datos de carácter personales.

- *SEGUNDA. – Información relativa al caso.*

  1.- <u>Base jurídica del tratamiento, y en su caso, circunstancia que levanta la prohibición para tratar categorías especiales de datos, según el artículo 9 del RGPD</u>.

  […]

  El acuerdo de implantación del sistema de huellas para controlar el acceso a la piscina se acordó por mayoría mediante votación en Junta General Extraordinaria, el 3 de junio de 2020 y, a día de hoy, es un acuerdo legalmente válido que cuenta con el consentimiento de los propietarios.

Para la adopción del acuerdo se valoraron otros medios de control del acceso a la piscina, pero la mayoría de los propietarios, entre los que se encuentra el denunciante, rehusaron optar por otras alternativas (tales como la contratación de una persona que llevara a cabo funciones de vigilancia u otro tipo de sistemas de acceso más rudimentarios), debido a que conllevaban un gasto mucho más elevado que la instalación del sistema lector de huellas o porque no aseguraban el control de acceso a la piscina.
Adicionalmente, este acuerdo se ha visto reforzado con el consentimiento expreso otorgado por cada uno de los propietarios que han registrado sus huellas para acceder a la piscina comunitaria. Acto consciente y expreso por parte de cada uno de ellos.

2 y 3. – Finalidad del tratamiento y garantía de los datos. Información a los usuarios.
En cuanto al tratamiento de los datos que realiza el sistema del lector de huellas ha de afirmarse que, tal y como refleja la comunicación realizada por la comunidad de propietarios a los usuarios de la piscina el 23 de mayo de 2024 que forma parte del Anexo I del expediente N.º: ***(…)****, se informó a los vecinos de que la empresa instaladora y el lector de huellas están homologados y cumplen la normativa de protección de datos, además, en la misma se recalca que los propietarios han dado el consentimiento para el uso de su huella a fin de acceder a la piscina.*
Se adjunta el Documento 2 donde la empresa desarrolladora del sistema del lector de huellas declara cumplir con los requisitos y estándares del RPGD. Los datos biométricos no son usados ni almacenados en línea. El sistema tan solo reconoce una determinada huella para conceder o denegar el acceso, pero no se puede identificar a la persona que ha registrado su huella.
Tampoco se puede reconstruir la huella a partir de los datos almacenados en el sistema porque solo se extraen determinadas características o rasgos de la huella, en la declaración del funcionamiento que realiza la empresa fabricante asegura que los datos almacenados están encriptados mediante un cifrado doble. Del mismo modo, tanto la empresa fabricante como la empresa instaladora aseguran que los datos almacenados no serán utilizados para otro fin distinto al del reconocimiento de la huella por parte del sistema para que este conceda el acceso.

2) La C.P. aportó como Documento 2 una *"Declaración sobre los productos* ***(…)*** *que cumplen con los estándares GDPR de UE"* donde se recoge:

> *"La información, ya sean imágenes de huellas dactilares o imágenes de rostros, está codificada y cifrado por el algoritmo* ***(…)*** *y almacenado, y no puede usarse ni * restaurado por cualquier individuo u organización. […]*
> *La información biométrica de todos los usuarios se almacenará únicamente en la ubicación del usuario, no será almacenada en nube pública, ningún tercero organizaciones partidarias. […]*
> *A través del* ***o*** *Protocolo de control y el protocolo de cifrado universal HTTPS para transmisión, cualquier organización de terceros e individuo no puede descifrar y restaurar la transmisión de datos. […]*

> *Cualquier individuo u organización que utilice los sistemas de **(...)** y el equipo requiere autenticación y una estricta gestión de derechos operativos, y el sistema y el equipo serán bloqueados contra el uso no autorizado por parte de cualquier personal u organización o autorizada. […]*
> *El usuario puede elegir transferir la información biométrica del dispositivo al propio del cliente Tarjeta RFID sin afectar al uso normal del cliente. Cuando el sistema y el dispositivo son amenazados indebidamente por cualquier tercero, el usuario puede elegir para permitir que el dispositivo elimine automáticamente todos los datos e inicialice el dispositivo.*

3) La empresa que instaló el sistema lector de huellas emitió una nota informativa a la vista de la comunicación de la AEPD, la cual se aportó como Documento 3. En ella, la empresa declara que el día 27 de mayo de 2024 se instaló el sistema de acceso y que, tras su colocación, se grabaron las huellas de los propietarios que acudieron. Igualmente, la empresa recuerda que no se recogió ningún dato más allá de la huella y tampoco cuentan con un sistema de datos en el que se asocie la huella a otro tipo de datos como nombres, DNI, etc.

Asimismo, responde lo siguiente:

> *"4. – Categoría de los interesados.*
> *Los interesados son los propietarios usuarios de la piscina.*
> *A los interesados se le ha facilitado toda la información relativa al tratamiento de los datos recogidos para el acceso.*
> *5.- Evaluación de Impacto realizado o motivos por el que no se ha realizado.*
> *Como ya se ha dicho, los usuarios de la piscina fueron informados del funcionamiento del sistema, tanto en Junta de Propietarios como por escrito, y estos aceptaron la finalidad y funcionamiento del tratamiento de sus datos.*
> *No se ha realizado la Evaluación de Impacto relativa a la protección de datos a la que se refiere el art. 35 del RGPD, ya que según la lista orientativa de tipos de tratamientos que no requieren una Evaluación de Impacto relativa a la protección de datos elaborada por la AEPD, no se considera necesaria en el supuesto de:*
>
> > *6. Tratamientos realizados por comunidades y subcomunidades de propietarios tal como se definen en el artículo 2 (a, b y d) de la Ley 49/1960 de Propiedad Horizontal.*
>
> (…)"

TERCERO: Con fecha 21 de agosto de 2024, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VIII, de la LOPDGDD.

Como consecuencia de las actuaciones realizadas, se ha tenido conocimiento de los siguientes extremos:

En fecha 24 de octubre de 2024 se realizó una solicitud de información a la C.P. En fecha 18 de noviembre de 2024 tuvo entrada la respuesta, que incluye los siguientes documentos 1 y 2 y describe el sistema de lectura dactilar:

- Como documento 1 se aportó el acta de la Junta General Extraordinaria de la Comunidad de Propietarios celebrada en fecha 3 de junio de 2020:

  "En el punto n.º 2 del orden del día se deliberó acerca de si los propietarios estaban de acuerdo con instalar un acceso a la piscina a través de un sistema identificativo de huella dactilar para controlar el aforo de la piscina.
  (…)
  Dos vecinos manifiestan su negativa al sistema de huella ya que entienden que con ese sistema no se podría realizar un control efectivo, ni del aforo máximo, no en la entrada y salida de los usuarios de la piscina.

  Proponen que la medida efectiva para el control de acceso y uso de la piscina sería la contratación de un socorrista o controlador (persona física), la cual, sí podría evitar, por ejemplo, la entrada de varias personas a la vez con la huella de un solo vecino podría controlar el horario de turnos que se establezca para el baño, así como el número máximo de personas dentro de la lámina de agua. Asimismo, exponen sus dudas sobre cómo se efectuará el registro de las huellas dactilares y, para el caso de no tener una persona física controlando, la opción del sistema de huella se podría sustituir por la emisión de unas llaves de acceso o tarjetas.

  (…) varios vecinos exponen que la contratación de un controlador físico supondría un coste inasumible para la Comunidad y manifiestan que el sistema de huella dactilar es suficientemente efectivo para el control de acceso al recinto de la piscina. (…) la intención no es prohibir ni limitar el acceso a ningún propietario ni inquilino del inmueble, simplemente se quiere regular y controlar la entrada al recinto de la piscina.

  La instalación del sistema de lector de huellas dactilares se aprobó con 19 votos favorables, 3 votos en contra (los tres procedentes de propietarios únicamente de garajes) y 1 abstención."

- Como documento 2 se aportó la Sentencia ***XXX/YYYY*** del Juzgado de Primera Instancia Número X de Sevilla, de 11 de noviembre de 2021:

  "FUNDAMENTOS DE DERECHO
  PRIMERO. – Consiste la pretensión de la parte actora en la solicitud de que por este Juzgado se declare nulo y sin efecto el acuerdo adoptado con el número 2º del orden del día, de la Junta General Extraordinaria celebrada por la comunidad demandada el día 3 de Junio de 2020, por infracción de lo dispuesto en el artículo 18.1.a) de la LPH, y resultar contrario a la ley y a los estatutos de la comunidad, y en su defecto, por resultar contrario al apartado c) del mencionado artículo 18 LHP, al suponer un grave perjuicio para los actores

que no tienen obligación jurídica de soportarlo, habiéndose incurrido en su adopción en abuso de derecho, (…).
NOVENO. En suma, el acuerdo impugnado no resulta contrario a la ley o a los estatutos, no limita en modo alguno el derecho real de servidumbre de paso establecido en favor de los demandantes, ni cuenta con entidad suficiente para considerar infringida la normativa sobre control de datos personales, como asimismo se argumenta en el escrito de demanda ,tratándose por otra parte de un sistema muy común y extendido en la actualidad para el acceso a diversos recintos públicos que precisan de control de identidad o aforo, como piscinas o zonas deportivas en general. (…)
FALLO
Que desestimo la demanda interpuesta por (…) VS la COMUNIDAD*, y declaro no haber lugar a la impugnación del acuerdo adoptado por la misma, en el punto 2º del orden del día de la Junta Extraordinaria de Propietarios de fecha 3 de Junio de 2020, y todo ello con expresa condena en costas procesales a la parte actora."*

- El sistema de lectura de huella dactilar se describe como sigue:

  "El sistema de acceso utiliza el método de identificación biométrica (1: N), el cual venía instalado de fábrica.
  El sistema únicamente almacena los datos de las huellas que han sido registradas.
  El sistema almacena los datos desde que el usuario, por voluntad propia, decide registrar la huella. Hasta el momento, no han existido solicitudes de baja y, por lo tanto, no se han eliminado los datos existentes. En el momento en que el usuario solicite la baja del sistema los datos serán eliminados del mismo. Al no ser almacenados en ningún otro método de almacenamiento no podrán ser recuperados una vez que sean eliminados.
  El sistema de lectura de huella no utiliza información biométrica sin procesar. La información biométrica de todos los usuarios está codificada y cifrada por el algoritmo ***(…)****, lo cual impide que la información pueda usarse o ser restaurada por los miembros de la organización y mucho menos por individuos ajenos a ella.*
  Los datos biométricos de los usuarios se encuentran almacenados en el dispositivo lector de huellas. Los datos de las huellas se almacenan físicamente, no existe ningún almacenamiento online.
  Ninguna persona tiene acceso a los datos almacenados en el sistema."

- En relación con el número de usuarios afectados por el sistema de lectura de huella dactilar y la información que se les ha facilitado al respecto, la COMUNIDAD señala:

  "El sistema afecta a los propietarios de la Comunidad de Propietarios ***A.A.A.****; propietarios de la piscina, y a los propietarios de la Comunidad de Propietarios* ***C.C.C.****, a quienes se les permite el uso de la piscina, en virtud de la Escritura de Constitución de Servidumbres otorgada ante el Notario de Sevilla (…)*

  Actualmente existen (47) huellas registradas en el sistema."

- Como documento 3 se aportó el comunicado enviado a los propietarios en fecha 3 de mayo de 2024, comunicado que aportó también la parte reclamante junto con la reclamación.

- En relación con el análisis de riesgos para los derechos y libertades de las personas afectadas por los tratamientos de datos personales que se llevan a cabo a través del sistema de lectura de huella dactilar instalado la C.P. traslada:

> *"A causa de que el sistema de lector de huellas no permite el tratamiento de los datos y de que los datos no son almacenados en una ubicación distinta a la del sistema, no se ha realizado el análisis de riesgos para los derechos y libertades de las personas afectadas por los tratamientos de datos personales previsto en el art. 32 RGPD. La COMUNIDAD se cercioró de que la empresa y el sistema lector de huellas cumplían con los requisitos y las garantías adecuadas para el uso al que iba a ser destinado, por ello, ante la ausencia de riesgos posibles de procedió a su instalación con el consentimiento y aprobación de los propietarios-usuarios."*

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del RGPD confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 de la LOPDGDD, es competente para resolver estas actuaciones de investigación la Presidencia de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."*

II
Datos biométricos

Según el artículo 4.14 del RGPD, se consideran «datos biométricos» *los 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*;

Al respecto de dichos datos biométricos, el artículo 9.1 RGPD establece una prohibición general de tratamiento salvo que concurra alguna de las casusas de levantamiento de dicha prohibición previstas en el apartado 2 del mismo precepto.

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;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los

Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

III
Presunción de inocencia

El artículo 28.1 de la Ley 40/2015, de Régimen Jurídico del Sector Público señala que *"sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa".*

En relación con lo anterior, conviene señalar que, al Derecho Administrativo Sancionador, por su especialidad, le son de aplicación, con alguna matización, pero sin excepciones, los principios inspiradores del orden penal, resultando clara la plena virtualidad del principio de presunción de inocencia.

El Tribunal Constitucional en su Sentencia 76/1990, de 26 de abril, en relación con el derecho a la presunción de inocencia y del principio de culpabilidad establece: *No puede suscitar ninguna duda que la presunción de inocencia rige sin excepciones en el ordenamiento sancionador y ha de ser respetada en la imposición de cualesquiera sanciones, sean penales, sean administrativas en general o tributarias en particular,*

pues el ejercicio del ius puniendi en sus diversas manifestaciones está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones. En tal sentido, 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 inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio."

La Sentencia del Tribunal Constitucional de 20/02/1989 indica que *"nuestra doctrina y jurisprudencia penal han venido sosteniendo que, aunque ambos puedan considerarse como manifestaciones de un genérico favor rei, existe una diferencia sustancial entre el derecho a la presunción de inocencia, que desenvuelve su eficacia cuando existe una falta absoluta de pruebas o cuando las practicadas no reúnen las garantías procesales y el principio jurisprudencial in dubio pro reo que pertenece al momento de la valoración o apreciación probatoria, y que ha de juzgar cuando, concurre aquella actividad probatoria indispensable, exista una duda racional sobre la real concurrencia de los elementos objetivos y subjetivos que integran el tipo penal de que se trate."*

En conclusión, estos principios impiden imputar una infracción administrativa cuando no se haya obtenido y acreditado una prueba de cargo acreditativa de los hechos que motivan esta imputación o se conozca con certeza la identidad del presunto infractor, aplicando el principio *"in dubio pro reo"* en caso de duda.

En el presente caso, la reclamación plantea que la C.P. está realizando un tratamiento de datos biométricos consistente en la recogida de las huellas de los vecinos del inmueble al objeto de controlar el acceso a la zona comunitaria de piscina.

En respuesta a las actuaciones practicadas, la C.P. ha aportado la descripción del sistema de lectura de huella dactilar, en la que indica que no se ha recogido ningún dato más allá de la huella y que no cuentan con un sistema de datos en el que se asocie la huella a otro tipo de datos como nombres, DNI, etc. Los datos biométricos no son usados ni almacenados en línea y el sistema tan solo reconoce una determinada huella para conceder o denegar el acceso, pero no se puede identificar a la persona que ha registrado su huella.

Asimismo, informan de que: *"la información biométrica de todos los usuarios está codificada y cifrada por el algoritmo **(…)**, lo cual impide que la información pueda usarse o ser restaurada por los miembros de la organización y mucho menos por individuos ajenos a ella. Los datos biométricos de los usuarios se encuentran almacenados en el dispositivo lector de huellas. Los datos de las huellas se almacenan físicamente, no existe ningún almacenamiento online. Ninguna persona tiene acceso a los datos almacenados en el sistema."*

En el presente caso, durante las actuaciones previas de investigación realizadas y con la información que obra en el expediente, no ha quedado acreditado que las huellas dactilares registradas por la C.P. puedan ser atribuidas, a una persona física identificada o identificable.

Y ello por cuanto el Tribunal de Justicia de la Unión Europea- por todas, en la STJUE dictada el 4 de septiembre de 2025 en el asunto C-414/23P- señala: "que *un medio no puede ser utilizado razonablemente para identificar al interesado cuando el riesgo de identificación resulte, en realidad, insignificante porque la identificación de esa persona esté prohibida por la ley o sea prácticamente irrealizable, por ejemplo porque implique un esfuerzo desmesurado en cuanto a tiempo, costes y recursos humanos* (apartado 82)."

En consecuencia, procede aplicar el principio de presunción de inocencia.

A la vista de lo anterior, en el presente caso no se han hallado elementos probatorios suficientes que permitan acreditar e imputar la existencia de una infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

Todo ello sin perjuicio de las posibles actuaciones posteriores que esta Agencia pudiera llevar a cabo, aplicando los poderes de investigación y correctivos que ostenta.

Así pues, al no haber sido posible atribuir una infracción en el ámbito competencial de la protección de datos, por la Presidencia de la Agencia Española de Protección de Datos, SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

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

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente resolución se hará pública. La publicación se realizará una vez la resolución sea firme en vía administrativa.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la LPACAP, 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 Presidencia 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.

940-120525

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos