- **Expediente N.º: EXP202410836**

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: Con fecha 12 de julio de 2024, se presentó reclamación con número de registro de entrada REGAGE24e00052655466 ante la Agencia Española de Protección de Datos contra ***SERVICIO GALLEGO DE SALUD (SERGAS)*** con NIF ***Q6550006H*** (en adelante, la parte reclamada).

Los motivos en que basa la reclamación son los siguientes:

La parte reclamante expone que una trabajadora (celadora) del hospital reclamado ha facilitado sus datos personales a un tercero (vigilante de seguridad), para que interpusiera una denuncia contra su pareja en el Juzgado ******JUZGADO.1,*** siendo esta desestimada.

Aporta copia del Atestado ***(...)*** de la Guardia Civil del Puesto de ******LOCALIDAD.1*** y copia de las Diligencias Previas ******PROCEDIMIENTO.1***, del Juzgado ******JUZGADO.1***, donde el tercero declara cómo y a través de quién había obtenido los datos de la reclamante, para poder denunciar a su pareja ya que desconocía su filiación.

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 la parte reclamada, 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.

El traslado, 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) mediante notificación electrónica, no fue recogido por el responsable, dentro del plazo de puesta a disposición, entendiéndose rechazada conforme a lo previsto en el art. 43.2 de la LPACAP en fecha 19/08/2024, como consta en el certificado que obra en el expediente.

Aunque la notificación se practicó válidamente por medios electrónicos, dándose por efectuado el trámite conforme a lo dispuesto en el artículo 41.5 de la LPACAP, a título informativo se envió una copia por correo postal que fue notificada fehacientemente en fecha 23/08/2024. En dicha notificación, se le recordaba su obligación de relacionarse electrónicamente con la Administración, y se le informaban de los medios de acceso a dichas notificaciones, reiterando que, en lo sucesivo, se le notificaría exclusivamente por medios electrónicos.

Con fecha 24/09/2024 se recibe en esta Agencia escrito de respuesta indicando lo siguiente:

*"Con fecha de 16 de septiembre de 2024 se recibe una "Solicitud de documentación adicional" de la Agencia Española de Protección de Datos (AEPD) donde se indica: "Con motivo de un incidente de su pareja con un vigilante de seguridad del* ******HOSPITAL.1****de su pareja con un vigilante de seguridad del* ******HOSPITAL.1,*** *personal del centro sanitario facilitó al citado vigilante su nombre, apellidos y DNI, información que únicamente disponía en tanto que la parte reclamante era paciente del Hospital"*

*Debemos indicar que una vez consultado con el área sanitaria de* ***(…)*** *que es donde la reclamante indica que ha producido supuestamente el incidente, no queda acreditado que el origen de los datos se haya producido dentro de los tratamientos de la Conselleria/sergas que es lo que la reclamante indica y no aporta ninguna prueba que corrobore su afirmación.*

*Para ello debemos indicar que:*

*• La vigilancia del hospital se realiza a través de un contrato público* ***(…)*** *adjudicado a la empresa Servicios SPR, que entre las funciones asignadas tienen el control en cuanto a seguridad y vigilancia.*

*• El vigilante de seguridad que es la persona que presenta la denuncia ante la Guardia Civil, no es un empleado del Servicio Público de Salud.*

*• En el atestado policial aparecen más datos que los de la reclamante. No se puede concluir que la aparición de esos datos haya tenido un origen en el Sergas, dado que existen otras fuentes de información de los que se podrían obtener. En el Sistema Público de Salud de Galicia desconocen el origen de esa información.*

*• En este sentido, no se acredita quién es la celadora* ***A.A.A.****, no se acredita que los datos los haya obtenido la celadora en el ejercicio de sus funciones ni cuando los ha aportado, incluso si los ha aportado.*

*En el supuesto caso de que se los aportase* ***"A.A.A."*** *tampoco sabemos si los tenía por otro cualquier tipo circunstancia.*

*En conclusión, no se aporta ninguna evidencia que los datos se obtuviesen de los sistemas de información/tratamientos de información de la Conselleria de Sanidad/Servizo Galego de Saúde (Sergas). Dado que la única información que tenemos es la información declarada por el vigilante de seguridad* ***B.B.B.."***

TERCERO: Con fecha 12 de octubre de 2024, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada.

## FUNDAMENTOS DE DERECHO

### I
### Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 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 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
### Seguridad del tratamiento

El artículo 32 del RGPD estipula lo siguiente:

*"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:*

*a) la seudonimización y el cifrado de datos personales;*

*b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*

*c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*

*d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*

*2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.*

*3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.*

*4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros."*

III
Integridad y confidencialidad

La letra f) del artículo 5.1 del RGPD propugna:

*"1. Los datos personales serán:*

*(…)*

*f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)."*

IV
Conclusión

La parte reclamante expone que una trabajadora (celadora) del hospital reclamado ha facilitado sus datos personales a un tercero (vigilante de seguridad), para que interpusiera una denuncia contra su pareja en el Juzgado ******JUZGADO.1,*** siendo esta desestimada.

La Conselleria de Sanidad/Servizo Galego de Saúde (Sergas) afirma que no está acreditado que la identificación fuera obtenida por el guardia de seguridad a través de los datos del hospital, pudiendo haber sido facilitados por otra persona.

El principio de presunción de inocencia impide imputar una infracción administrativa cuando no se haya obtenido y constatado una prueba de cargo que acredite los hechos que motivan la imputación o la intervención en los mismos del presunto infractor.

El Tribunal Constitucional (SSTC 131/2003 y 242/2005, por todas) se ha pronunciado en ese sentido al indicar que una de las exigencias inherentes al derecho a la presunción de inocencia es que la sanción esté fundada en actos o medios probatorios de cargo o incriminadores de la conducta imputada y que recae sobre la Administración pública actuante la carga probatoria de la comisión del ilícito administrativo y de la participación en él del denunciado. Por su parte, el artículo 28.1

de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público establece como uno de los principios de la potestad sancionadora el de la “Responsabilidad”, determinando al respecto 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”.*

Igualmente, se debe tener en cuenta lo que establece el artículo 53.2 la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, establece que: *“Además de los derechos previstos en el apartado anterior, en el caso de procedimientos administrativos de naturaleza sancionadora, los presuntos responsables, tendrán los siguientes derechos:*

(…)

*b) A la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario”*

La Conselleria de Sanidad/Servizo Galego de Saúde (Sergas) afirma que no puede acreditarse quién es la celadora ***A.A.A.,*** ni que los datos personales de la parte reclamante los haya obtenido la celadora en el ejercicio de sus funciones ni cuando los ha aportado, incluso si los ha aportado.

Por lo demás, respecto a los presuntos hechos únicamente disponemos de un atestado, consistente básicamente en la declaración del guardia de seguridad, lo cual no resulta suficiente para imputar una infracción a la parte reclamada.

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de 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 la responsabilidad por el tratamiento de acuerdo con lo señalado, 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 ***SERVICIO GALLEGO DE SALUD (SERGAS)*** y a la parte reclamante.

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 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 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