- **Expediente N.º: PS/00134/2021**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: En fecha 15 de agosto de 2020, ***A.A.A.*** (en adelante, el reclamante) interpuso reclamación ante la Agencia Española de Protección de Datos, contra la AGENCIA ESTATAL CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS con NIF Q2818002D (en adelante, el reclamado).

La reclamante presentó una solicitud de información pública dirigida al reclamado, por medio del Portal de la Transparencia del Gobierno. En fecha 13 de junio de 2019, el reclamado dictó una resolución sobre su caso permitiendo el acceso parcial a la información solicitada, publicando de forma abierta la resolución, ya que, aunque se colocaba un rectángulo negro encima de su nombre y apellidos, este texto no era eliminado, y aparecía en el pdf, por lo que era posible acceder a él y localizarlo utilizando un buscador de Internet o un editor de pdf. La resolución figura en la URL: ***URL.1. Además, la resolución publicada incluye el código CSV, permitiendo visualizar el documento original en el que constan los datos personales de la reclamante.

Fecha en la que tuvieron lugar los hechos reclamados: 01 de febrero de 2021.

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 al reclamado, 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.

En fecha 17 de diciembre de 2020, se recibe respuesta del reclamado, indicando que:

"No obstante, atendiendo al tiempo transcurrido y la solicitud de la afectada se procede a considerar su solicitud y a atender a la misma adoptando las medidas necesarias".

TERCERO: En fecha 29 de enero de 2021, de conformidad con el artículo 65 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por la reclamante contra el reclamado.

CUARTO: A la vista de los hechos denunciados en la reclamación y de los documentos aportados por la reclamante, de los hechos y documentos de los que ha tenido conocimiento esta Agencia, 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 los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 del Reglamento (UE)

2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, 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),teniendo conocimiento de los siguientes extremos:

ENTIDAD INVESTIGADA

AGENCIA ESTATAL CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS, con NIF Q2818002D y con domicilio en c/ Serrano 117, 28006, Madrid (Madrid).

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

En fecha 01/02/2021 se realizan las siguientes comprobaciones:

- Se obtiene impresión de pantalla de la URL:

URL.1. Se verifica que se trata de un documento pdf en el cual, realizando una búsqueda del texto "A.A.A.***", se encuentra una ocurrencia (una de una: 1/1), si bien dicho texto no se visualiza al estar, al parecer, oculto con un rectángulo negro. Se verifica que se puede extraer de este documento, copiando y pegando, el texto de debajo del rectángulo negro, resultando: "***Dª A.A.A.***".

- Se comprueba que el buscador Google encuentra el texto "***A.A.A.***" en el referido documento pdf.

En fecha 10/02/2021 se realizan las siguientes comprobaciones:

- Se intenta el acceso a la dirección URL:
***URL.1 Se verifica la página ya no se encuentra.

- Se verifica que utilizando el motor de búsqueda de Google el texto "***A.A.A.***" se sigue encontrando. Al acceder mediante el enlace mostrado por Google, no se encuentra la publicación de la página. Se verifica que la citada página se encuentra en la caché de Google.

Con fecha 10/02/2021 se ha requerido información y documentación al reclamado con los siguientes resultados:

Sobre los motivos por los cuales han estado publicados el nombre y los apellidos de la reclamante en la web www.csic.es y la fecha en la cual se ha eliminado la publicación, los representantes de la entidad realizan al respecto las siguientes manifestaciones:

> *"Los motivos ya fueron respondidos en escrito del delegado de Protección de Datos de 20-10-2020, que se adjunta y reproduce:*
>
> *Al amparo de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (LT) se suministra información a la sociedad en general resultando aplicables, eso sí, los principios de minimización de datos y los criterios de daño, ponderación, proporcionalidad.*

Criterios aplicables tanto a la publicidad activa –obligada, periódica y actualizada (art 5 LT)- como a la divulgada como consecuencia del ejercicio por el solicitante del derecho de acceso (Cap. III LT).

Doble vía que finalizará en una convergencia en la divulgación porque el derecho de acceso supone una vía adicional de hacer pública una información que no se incluye inicialmente en la publicidad activa, a la que se incorpora al tener que constar la información de relevancia jurídica prevista en el artículo 7 de la LT, entre la que se encontrarán las respuestas dadas a las solicitudes de acceso.

No obstante, ese trasvase de información entre la suministrada en respuesta a un acceso solicitado y publicidad activa requiere previa disociación salvo que concurran circunstancias relevantes (art 14. 3 LT).

En tal sentido deben tenerse en cuenta dos circunstancias:

1) Por una parte la relevancia política de la solicitante que puede justificar y en todo caso debe tenerse en cuenta respecto a la divulgación de su identidad lo que deriva en que, en todo caso, su eventual divulgación no resulta desproporcionada.

(…)

Y en tal sentido siguen estando accesibles libremente al público en la actualidad informaciones al respecto por voluntad de la propia afectada, resultando aplicable lo previsto en el artículo de la 15 LT: «1. Si la información solicitada contuviera datos personales que revelen la ideología, afiliación sindical, religión o creencias, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso

(…)

Lo que se desarrolla a continuación.

1) Las personas públicas tienen más limitada su esfera de privacidad
político son objeto de una mayor exposición de sus datos ante la opinión pública, diluyendo voluntariamente la privacidad de sus datos y sus actuaciones.

Circunstancia que ha sido ratificada por varias fuentes:

-El Grupo de Trabajo del artículo 29

Ha emitido una guía interpretativa sobre los conceptos desarrollados por el TJUE en relación con el derecho al olvido, que resultan trascendentes para el presente supuesto. En la misma entiende que este derecho se limita en las personas con relevancia pública y que son "figuras públicas" quienes están

destinados a desarrollar un papel en la vida pública y/o utilicen recursos públicos para el desarrollo de la actividad.

El Tribunal Supremo

Que expone en (por todas) la Sentencia 1175/2020 de 17 Sep. 2020, los factores para ponderar relevancia pública y protección de datos.

Precisar el contenido de los factores de ponderación relativos a la relevancia pública de la información, desde su perspectiva objetiva (actividad) y subjetiva (carácter público o privado de la persona afectada); así como la incidencia del factor tiempo en la calidad de los datos del interesado difundidos y en el ejercicio del derecho al olvido.

El Tribunal Constitucional

Así, la Sentencia 107/1998 del Tribunal Constitucional concreta que:

"el valor preponderante de las libertades públicas del art. 20 de la Constitución, en cuanto se asienta en la función que éstas tienen de garantía de una opinión pública libre indispensable para la efectiva realización del pluralismo político, solamente puede ser protegido cuando las libertades se ejerciten en conexión con asuntos que son de interés general por las materias a que se refieren y por las personas que en ellos intervienen y contribuyan, en consecuencia, a la formación de la opinión pública, alcanzando entonces su máximo nivel de eficacia justificadora frente al derecho al honor, el cual se debilita, proporcionalmente, como límite externo de las libertades de expresión e información, en cuanto sus titulares son personas públicas, ejercen funciones públicas o resultan implicadas en asuntos de relevancia pública, obligadas por ello a soportar un cierto riesgo de que sus derechos subjetivos de la personalidad resulten afectados por opiniones o informaciones de interés general, pues así lo requieren el pluralismo político, la tolerancia y el espíritu de apertura, sin los cuales no existe sociedad democrática.

*2) La actividad política de la **A.A.A.** no es obsoleta*

(…)

Por lo que la divulgación también era adecuada -según los criterios establecidos en la citada STS 1175/2020- teniendo en cuenta la incidencia del factor tiempo en la calidad de los datos del interesado difundidos y en el ejercicio del derecho al olvido.

3)La pregunta de transparencia estaba relacionada con su actividad política.

(…)

Lo que abunda en la justificación del conocimiento de que la pregunta tenía su origen en el contexto y entorno del partido referido, al formularla una persona vinculada al mismo.

Por lo que la publicación de sus datos personales resultaba justificada desde la perspectiva también objetiva (además de subjetiva) según la citada STS 1175/2020.

4) Incluso si se considerara obsoleta debiera haberse dirigido al buscador

*Es más, incluso si se considerara que **A.A.A.** es una ex política -lo que se contradice no solo con el tenor de la pregunta presentada a través del portal de transparencia, sino con su permanencia en la red con tal condición- debiera haberse dirigido, ejerciendo el derecho, al buscador, no al CSIC como editor.*

En tal sentido se manifiesta la Sentencia de la Sección Primera de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de fecha 5 de febrero de 2015, en la que se señaló lo siguiente, de conformidad con la Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 (Sentencia "Costeja" sobre derecho al olvido), respecto a una persona que había abandonado la política hacía diez años (tiempo transcurrido sustancialmente mayor al que podría considerarse):

"La consecuencia lógica es que quien ejercita el derecho de oposición ha de indicar ante el responsable del tratamiento, o ante la Agencia Española de Protección de Datos, que la búsqueda se ha realizado a partir de su nombre como persona física, indicar los resultados o enlaces obtenido a través del buscador así como el contenido de la información que le afecta y que constituye un tratamiento de sus datos personales a la que se accede a través de dichos enlaces, para que de ese modo tanto el responsable del tratamiento como la propia Agencia cuente con los elementos necesarios para llevar a cabo el juicio de ponderación a que se refiere la Sentencia dl Tribunal de Luxemburgo; así se deduce también del artículo 35 del Reglamento de Protección de Datos.

*Así las cosas, pasamos a aplicar lo expuesto anteriormente al supuesto que nos ocupa. **B.B.B.**, ejercitó en abril de 2009 el derecho de oposición al tratamiento de sus datos personales debido a que al introducir su nombre en el buscador de Google aparecía la referencia a una página web del Boletín de la Comunidad de Madrid nº XXX, de ***FECHA.1, en el que se publicaban las candidaturas de las elecciones municipales de ***FECHA.2 de San Sebastián de los Reyes (Madrid). Pues bien, dicha información carece de relevancia que justificara que prevaleciera el interés del público general de dichos datos personales sobre los derechos reconocidos en los artículos 7 y 8 de la Carta Europea de Derechos Fundamentales. Estamos ante un tratamiento de datos inicialmente lícito por parte del buscador Google que dado el contenido de la información y el tiempo transcurrido no son necesarios en relación con los fines para los que se recogieron o trataron.*

Por otro lado, la libertad de información se encuentra satisfecha por la subsistencia en la fuente, es decir, en el sitio web donde se publica la información, sin que el hecho de eliminar de la lista de resultados los vínculos a la página web objeto de reclamación por la afectada, impida que utilizando otros datos se llegue a la citada página web, pero no a partir de su nombre."

5) Se ha procedido a la supresión de la identidad

*No obstante, lo cual, como se expuso en el escrito de 20-10-2020, se ha procedido, atendiendo a la solicitud trasladada, a suprimir la referencia a la identidad de **A.A.A.** como solicitante de información al amparo de la Ley de Transparencia. Lo que se desarrolla en el siguiente apartado.*

*En consecuencia, la inserción de la identidad en el contexto expresado resultaba correcta al revestir innegable relevancia la identidad y filiación de la reclamante con un partido, ***PARTIDO.1, involucrado en la cuestión sobre la que se formulaba la pregunta. **A.A.A.**, aun hoy en día, mantiene inserciones vinculadas a su actividad política por lo que no resultaba obsoleta.*

Todo ello sin perjuicio de que se procediera y decidiera su supresión con carácter precautorio y en respuesta a la solicitud. "

Sobre la Fecha en la cual se ha eliminado, los representantes del reclamado han manifestado:

"No obstante lo cual se procedía, como se expuso, a considerar la solicitud y a adoptar las medidas oportunas como precaución.

Se adjuntan documentos con los logs del sistema filtrado para ese archivo. Se puede acreditar que a partir de las 13:59:36 del 1 de febrero al acceder a la página web se obtenía un error 404, es decir el archivo había sido correctamente eliminado de la Web del CSIC.

Se entiende, por otra parte, que cuando se producen accesos consecutivos con error los algoritmos que utilizan los buscadores, por ejemplo, Google, terminan suprimiendo la referencia al considerarlos obsoletos.

No obstante, lo anterior, se solicitó a Google que retirase la URL de la caché. Se adjunta un documento en el que se comprueba que, al menos con fecha de 11 de febrero a las 19:00, se había cursado más de una petición de anulación de la URL de la caché, apareciendo la solicitud como duplicada.

Lo que no puede el editor es retirar la referencia y la caché de los servidores de la citada compañía que siguen la programación propia de la multinacional que, según el requerimiento trasladado, permanecía el 10-2-2021."

Aportan copia de lo que parecen líneas de registro de ficheros de *log* de los servidores HTTP del reclamado, en los que a partir de las 13:49:52 del 1 de febrero de 2021 aparece el código de error 404 al acceder al fichero pdf citado. (A las 13:49:51 horas figura aun el código 200 de no error u OK).

Aportan copia de impresiones de pantalla de Google Search Console donde se solicita a Google la retirada de la URL donde se encuentra en pdf. En la impresión de pantalla se indica que se bloquean las URL de los resultados de la búsqueda y se borra su fragmento y la versión almacenada en caché.

Se ha comprobado que a fecha de la realización del presente informe no aparece el citado documento pdf en la caché de Google.

Se ha requerido información sobre la existencia en su organización de un procedimiento escrito para la anonimización de los datos personales de resoluciones y otros documentos que sean publicados en la web. Información sobre si los procedimientos incluyen las actuaciones a seguir en caso de errores. Información sobre si se considera la posible indexación por buscadores de los datos personales publicados por error, así como la eliminación de estos índices tanto del buscador como de su posible memoria caché. Copia de estos procedimientos en caso afirmativo.

Los representantes del reclamado han manifestado:

"Al respecto deben significarse varias circunstancias

a) criterios de anonimización en el CSIC

La inserción de datos personales en la web del CSIC vinculados a proyectos no es habitual. Gran parte de los proyectos se refieren a investigaciones en vida no humana y materia, con presencia únicamente de los datos de los investigadores implicados.

Los tratamientos más profusos en tratamiento de datos personales en el CSIC son los vinculados a Bolsa de trabajo y convocatorias. Al respecto, desde hace años se procede del siguiente modo, en aplicación de los criterios de la Disposición adicional séptima de la ley 3/2018 de Protección de Datos Personales y garantía de los derechos digitales:

Bolsa de Trabajo

El CSIC gestiona, a través de su Sede Electrónica, múltiples convocatorias de empleo y formación, así como una bolsa de trabajo con miles de solicitantes y que da lugar a miles de contratos cada año, aproximadamente 3.000 personas.

La información de la Bolsa que muestra datos personales es la que figura en los listados de méritos, tanto provisionales como definitivos.

Como criterio de anonimización en todos los listados de méritos provisionales y definitivos, así como en las resoluciones, figura:

- NIF anonimizado: solo permite ver cuatro caracteres, el resto va con asteriscos.
- El nombre y los apellidos van en claro.

Se adjunta un ejemplo de un listado de méritos provisionales (fichero: LP_GP12_10022021.pdf) y otro de méritos definitivos (ejemplo: LD_SOLAUT_36201.pdf).

Convocatorias

El CSIC gestiona distintas convocatorias internas de distintas modalidades, JAES, Garantía Juvenil y otro tipo de puestos.

En todos los documentos (listados de admitidos, excluidos, fases superadas, resoluciones, etc.) aparece el nombre y apellidos de los participantes en la convocatoria. Nunca aparece el NIF, que es sustituido por la referencia de su solicitud o contrato al que se presentan, según la modalidad de la convocatoria.

La sede muestra muy distintos tipos de listado, según las diferentes fases del procedimiento, pero en todos ellos se sigue el mismo criterio: No figura el NIF sino la Referencia de la Solicitud y sí se muestran el nombre y apellido.

Se adjunta como ejemplo una resolución.

b) instrucciones y medidas organizativas, de coordinación, información y apoyo a trabajadores y unidades para la anonimización.

El CSIC se compone de 120 institutos y centros. Muchos de los cuales disponen de páginas web. El punto de coordinación en los mismos son las gerencias.

Para la articulación de las políticas de protección de datos, en concreto en lo que refiere a publicación en las páginas web, el delegado de Protección de datos dispone de una habilitación para enviar correos a todos los gerentes de los ICUs del CSIC:

autorizadosldtger@listas.csic.es

Adicionalmente, a los criterios trasladados para cada supuesto concreto a las unidades competentes en el sentido expuesto, se dispone de un apartado "protección de datos" en la intranet del CSIC donde figura información accesible a los más de 11.000 trabajadores del centro.

En la misma se encuentra insertada la siguiente instrucción que hace referencia a la guía de la AEPD de anonimización, así como la propia Guía.

La información de carácter personal en la Web debe evitarse si no está justificado. Se entiende como información de carácter personal los Nombres y Apellidos, DNI o Equivalente, Direcciones Postales y Electrónicas, Teléfonos, Facturas, etc. de las personas físicas.
Tal circunstancia alcanza a la posible identificación indebida de profesionales representantes Los datos de terceros profesionalmente implicados, el gerente de una empresa, el abogado que representa etc. será asimismo anonimizados cuando no esté justificada su inserción. Así como de referencias numéricas, códigos de distinto tipo, que podrían permitir la identificación indebida de una persona física.
Ello obliga a considerar el conjunto de criterios a aplicar en el desarrollo de las tareas de anonimización de carácter semiautomatizado.

En las resoluciones que se hagan públicas en las que se dé la circunstancia de la existencia de un único afectado se debe optar por la norma de estilo consistente en citar una única vez su identidad anonimizada:
"D. Juan Español Español, xxx en adelante "el afectado/interesado/denunciante""
Y evitar reproducir el nombre más adelante. A veces se introduce esa regla de estilo, pero, a pesar de todo, se corre el riesgo de anonimización en la primera cita reproduciendo el nombre posteriormente.
Deben tenerse en cuenta las orientaciones de anonimización emitidas por la Agencia Española de Protección de Datos:
https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-procedimientos-anonimizacion.pdf

Debe tenerse de manera especial en cuenta lo recogido en la Disposición adicional séptima de la ley 3/2018 de Protección de Datos Personales y garantía de los derechos digitales.

Disposición adicional séptima.
Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.

Cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.
Cuando se trate de la notificación por medio de anuncios, particularmente en los supuestos a los que se refiere el artículo 44 de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.
Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos.
En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.
A fin de prevenir riesgos para víctimas de violencia de género, el Gobierno impulsará la elaboración de un protocolo de colaboración que defina procedimientos seguros de publicación y notificación de actos administrativos, con la participación de los órganos con competencia en la materia

Para más información o aclaraciones contactar con delegadoprotecciondatos@csic.es

Debe significarse adicionalmente que tanto en las reuniones periódicas con los gerentes, así como con los restantes trabajadores, en especial de nuevo

ingreso, se realiza un recordatorio al respecto de la obligación de anonimizar datos cuando corresponda.

Adicionalmente el correo de delegadoprotecciondatos@csic.es se encuentra a disposición del personal, también a efectos de inserción de datos en la web.

El DPD como es preceptivo está involucrado y es consultado cuando hay alguna cuestión sobre la que pueden concurrir dudas o problemas como el suscitado, habiendo respondido en 2020 a 75 dudas o consultas, todo ello sin perjuicio de actividades acometidas por propia iniciativa y en otros entornos.

Tal involucración es mayor en procedimientos en los que en principio se van a tratar datos, como convocatorias y otras resoluciones de personal o ayudas en el sentido expuesto.

c) Procedimientos para detectar errores

Para la eventual detección de errores se realiza un análisis de los archivos indexados en buscadores usando un software específico que se utiliza principalmente para encontrar metadatos e información oculta en los documentos que examina y que se publican en la página web.

Los documentos que se analizan son generalmente los archivos de Microsoft Office, Open Office, o ficheros PDF, y estos documentos se buscan utilizando tres posibles buscadores que son Google, Bing y DuckDuckGo.

Hay que aclarar que no se analiza el contenido de los documentos, sino los metadatos asociados, como por ejemplo un correo personal, un nombre etc. Se adjunta el informe generado en el que no se detectan metadatos sensibles en la web institucional.

Por otra parte, para octubre de 2021 está previsto hacer la auditoría bianual por AENOR incluyendo web y sede. Se adjunta el documento vigente con la certificación de AENOR de cumplimiento del Esquema Nacional de Seguridad. "

QUINTO: En fecha 1 de septiembre de 2021, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por la presunta infracción del artículo 5.1.f) del RGPD y artículo 32 del RGPD, tipificada en el artículo 83.5 del RGPD. Notificado el acuerdo de inicio, el reclamado presentó escrito de alegaciones en el que, en síntesis, manifestaba que la relevancia política de la solicitante debía tenerse en cuenta respecto a la divulgación de su identidad lo que derivaba en que, en todo caso, su eventual divulgación no resultaba desproporcionada, que la actividad política de la reclamante no era obsoleta, que la pregunta de transparencia estaba relacionada con su actividad política, que se había procedido a la supresión de la identidad, que no se concretaban las medidas de seguridad técnicas y organizativas necesarias que habían resultado vulneradas, que en el presente caso concurría la figura de concurso medial ya que "una infracción es un medio necesario para la comisión de otra" y solicitaba que se tuvieran en cuenta los argumentos expuestos y se procediera a archivar el expediente

SEXTO: En fecha 16 de noviembre de 2021 se formuló propuesta de resolución, proponiendo:

<< Que por la Directora de la Agencia Española de Protección de Datos se dirija un apercibimiento a la AGENCIA ESTATAL CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS, con NIF Q2818002D, por una infracción del artículo 5.1. f) del RGPD, conforme a lo dispuesto en el artículo 83.5 del RGPD, calificada como muy grave a efectos de prescripción en el artículo 72.1 i) de la LOPDGDD y por infracción del artículo 32 del RGPD, conforme a lo dispuesto en el artículo 83.4 del citado RGPD, calificada como grave a efectos de prescripción den el artículo 73 apartado f) de la LOPDGDD. >>

SÉPTIMO: En fecha 23 de noviembre de 2021, la parte reclamada presentó escrito de alegaciones a la Propuesta de Resolución, en el que, en síntesis, manifiesta que las alegaciones han sido analizadas de manera parcial y se reiteran los argumentos ya expuestos en alegaciones anteriores.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS

PRIMERO: En fecha 15 de agosto de 2020, la reclamante interpuso reclamación ante la Agencia Española de Protección de Datos, contra la AGENCIA ESTATAL CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS, toda vez que el reclamado dictó una resolución sobre su caso permitiendo el acceso parcial a la información solicitada, publicando de forma abierta la resolución, ya que, aunque se colocaba un rectángulo negro encima de su nombre y apellidos, este texto no era eliminado, y aparecía en el pdf, por lo que era posible acceder a él y localizarlo utilizando un buscador de Internet o un editor de pdf.

SEGUNDO: Se verifica que se trata de un documento pdf en el cual, realizando una búsqueda del texto se encuentra una ocurrencia (una de una: 1/1), si bien dicho texto no se visualiza al estar, al parecer, oculto con un rectángulo negro. Se comprueba que se puede extraer de este documento, copiando y pegando, el texto de debajo del rectángulo negro.

TERCERO: En fecha 10/02/2021, se intenta el acceso a la dirección URL y se verifica que la página ya no se encuentra. Se comprueba que utilizando el motor de búsqueda de Google el texto "***A.A.A.***" se sigue encontrando. Al acceder mediante el enlace mostrado por Google, no se encuentra la publicación de la página. Se verifica que la citada página se encuentra en la caché de Google.

FUNDAMENTOS DE DERECHO

PRIMERO: En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en los arts. 47 y 48.1 de la LOPDGDD, la

Directora de la Agencia Española de Protección de Datos es competente para resolver este procedimiento.

SEGUNDO: En relación con las manifestaciones efectuadas por la parte reclamada, reiterándose básicamente en las alegaciones ya presentadas a lo largo del procedimiento sancionador, debe señalarse que todas ellas no sólo fueron analizadas y desestimadas, sino que se tuvieron en cuenta para formular la Propuesta de resolución, cuyos Fundamentos de Derecho continúan plenamente vigentes, y que se resumen en lo siguiente:

En primer lugar, el derecho fundamental de la reclamante, a que sus datos no sean utilizados de forma sorpresiva, asociados al desarrollo de su tarea, suponen un uso no legítimo de dichos datos, no adecuado, necesario, ni justificado. Debe tenerse en cuenta que la normativa de protección de datos no efectúa una distinción entre datos públicos y privados, permitiendo sin más, el uso de datos que la afectada haya hecho públicos, sino que otorga con carácter general una protección a los datos personales determinando aquéllos supuestos en que dicho tratamiento resulta conforme a la misma.

El Tribunal Constitucional, viene a establecer el derecho a la protección de datos como derecho fundamental autónomo. En virtud de este derecho fundamental, el ciudadano, con carácter general, puede decidir sobre sus propios datos.

En este sentido debe tomarse en consideración, la doctrina jurisprudencial del Tribunal Constitucional en esta materia, que configura el derecho a la protección de datos como un derecho fundamental autónomo, diferenciado del derecho fundamental a la intimidad. Señala así en su Sentencia 292/2000, lo siguiente:

"*De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que, por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo*."

La aludida Sentencia 292/2000 determina, asimismo, el contenido del derecho a la protección de datos personales señalando en su fundamento jurídico 7:

"*De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos 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. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele."

El objeto de protección del derecho fundamental a la protección de datos, no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que ya estaría protegido por el artículo 18.1 de la Constitución, sino los datos de carácter personal. Es decir, el TC viene a extender este derecho fundamental a los datos personales públicos, que por el hecho de ser públicos no pueden escapar al poder de disposición del propio interesado o afectado, no constriñéndose a los relativos a la vida privada o íntima de la persona, sino que los datos amparados y protegidos son todos aquellos que identifiquen o permitan la identificación de la persona, que puedan configurar su perfil ideológico, racial, sexual, económico, etc.

El derecho fundamental a la protección de datos se concreta en un poder de disposición y de control sobre los datos personales. De esta manera, la persona debe quedar facultada para decidir cuáles de sus datos proporcionar a un tercero, sea la Administración o un particular, decidir cuáles puede este tercero recabar, saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

Este derecho, así configurado, requiere como complementos indispensables, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, así como poder oponerse a esa posesión y usos.

Por tanto, cualquier actuación que suponga privar a la persona de aquellas facultades de disposición y control sobre sus datos personales, constituirá un ataque y una vulneración de su derecho fundamental a la protección de datos. En este sentido se pronunció el TC, en Sentencia 11/1981, de 8 de abril, *"se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección"*.

En segundo lugar, de los hechos probados en este procedimiento, se desprende que la entidad reclamada en su calidad de organismo público responsable del tratamiento de datos de carácter personal debió adoptar las medidas necesarias para impedir cualquier acceso a la información de carácter personal que contenía dicha documentación. Tales medidas no fueron adoptadas totalmente en el presente caso, como lo acredita el hecho de que en su página web figuraban los datos identificativos de la reclamante de este procedimiento.

La anonimización de datos debe considerarse como una forma de eliminar las posibilidades de identificación de las personas. El avance de la tecnología y la información disponible hacen difícil garantizar el anoniA.A.A. absoluto, especialmente a lo largo del tiempo, pero, en cualquier caso, la anonimización va a ofrecer mayores garantías de privacidad a las personas.

En este sentido, la utilización de medidas como, por ejemplo, los mecanismos y protocolos de anonimización que conlleven la definición del equipo de trabajo, la formación del personal, las medidas de confidencialidad, el uso de posibles estándares, la utilización de códigos de buenas prácticas, etc., definen de forma explícita la intención y diligencia del responsable del tratamiento en los procesos de anonimización de datos personales.

No obstante, se comprueba que se ha retirado el documento objeto de conflicto del presente procedimiento, lo que evidencia que se dieron todos los pasos necesarios para la pronta resolución del problema.

La Audiencia Nacional, en varias sentencias, entre otras las de fechas 14 de febrero y 20 de septiembre de 2002 y 13 de abril de 2005, exige a las entidades que operan en el mercado de datos, una especial diligencia a la hora de llevar a cabo el uso o tratamiento de tales datos o su cesión a terceros, visto que se trata de la protección de un derecho fundamental de las personas a las que se refieren los datos, por lo que los depositarios de éstos deben ser especialmente diligentes y cuidadosos a la hora de realizar operaciones con los mismos y deben optar siempre por la interpretación más favorable a la protección de los bienes jurídicos protegidos por la norma.

Por último, el artículo 29.5 de la Ley 40/2015 se refiere a lo que se conoce como “concurso medial de infracciones administrativas”, que resulta de aplicación cuando una infracción más leve sirve como medio para cometer otra más grave. Para que resulte de aplicación, es necesario que se verifique la concurrencia de una pluralidad de acciones, que, a su vez, den lugar a una pluralidad de infracciones (por ejemplo, dos hechos y dos infracciones); con la particularidad de que una de ellas sea instrumento o medio necesario para la perpetración de la otra.

De acuerdo con los fundamentos anteriores, consta que se ha producido una acción, la vulneración de la seguridad del tratamiento de los datos al no anonimizarlos adecuadamente, lo que ha tenido como consecuencia una infracción de resultado por la pérdida de confidencialidad de estos. Al no concurrir varias acciones, no se está ante un “concurso medial”, ni cabe aplicar al caso el citado artículo 29.5.

En consecuencia, las alegaciones deben ser desestimadas, significándose que las

argumentaciones presentadas no desvirtúan el contenido esencial de la infracción que se declara cometida ni suponen causa de justificación o exculpación suficiente.

Se imputa a la parte reclamada la comisión de una infracción por vulneración del artículo 5.1.f) del RGPD, que rige el principio de confidencialidad e integridad de los datos personales, así como la responsabilidad proactiva del responsable del tratamiento de demostrar su cumplimiento y artículo 32 del RGPD.

TERCERO: El artículo 5.1. f) del RGPD que establece:

"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»)".

De esta manera, la exposición en la web del reclamado da lugar a la ruptura del vínculo de confidencialidad del responsable de los datos.

El artículo 5 de la LOPDGDD, Deber de confidencialidad, señala lo siguiente:

"1. Los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3.Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento".

CUARTO: En cuanto a la seguridad de los datos personales, el artículo 32 del RGPD *"Seguridad del tratamiento",* establece que:

"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".

Hay que señalar que el RGPD en el citado precepto no establece un listado de las medidas de seguridad que sean de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, señalando que la determinación de las medidas técnicas y organizativas deberá realizarse teniendo en cuenta: la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En todo caso, al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, 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 y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

En este mismo sentido el considerando 83 del RGPD señala que:

"(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar

los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como 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, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".

La responsabilidad del reclamado viene determinada por la quiebra de seguridad puesta de manifiesto por el reclamante, ya que es responsable de tomar decisiones destinadas a implementar de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para asegurar la confidencialidad de los datos, restaurando su disponibilidad e impedir el acceso a los mismos en caso de incidente físico o técnico.

QUINTO: El artículo 83.5 del RGPD dispone lo siguiente:

"5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;"

Por su parte, el artículo 71 de la LOPDGDD, bajo la rúbrica "*Infracciones*" determina lo siguiente: *Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica.*

A efectos del plazo de prescripción de las infracciones, el artículo 72 de la LOPDGDD, bajo la rúbrica de infracciones consideradas muy graves, establece lo siguiente:

"1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

(…)

i) La vulneración del deber de confidencialidad establecido en el artículo 5 de esta ley orgánica."

La vulneración del artículo 32 RGPD se encuentra tipificada en el artículo 83.4.a) del citado RGPD en los siguientes términos:

"4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43."

(…)

A efectos del plazo de prescripción de las infracciones, el artículo 73 de la LOPDGDD, bajo la rúbrica *"Infracciones consideradas graves",* establece lo siguiente:

"*En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*

(…)

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.

En el presente caso, concurren las circunstancias infractoras previstas en el artículo 83.5 y 83.4 del RGPD, arriba transcritos.

SEXTO: Establece la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en el Capítulo III relativo a los "*Principios de la sancionadora*", en el artículo 28 la bajo la rúbrica "*Responsabilidad*", lo siguiente:

"1. 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."

La falta de diligencia a la hora de implementar las medidas apropiadas de seguridad con la consecuencia del quebranto del principio de confidencialidad constituye el elemento de la culpabilidad.

SÉPTIMO: El artículo 58.2 del RGPD, señala lo siguiente*:*

2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

(…)

"b) dirigir a todo responsable o encargado del tratamiento un apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento."

Por su parte, el ordenamiento jurídico español ha optado por no sancionar con la imposición de multa administrativa a las entidades públicas sino con apercibimiento, tal como se indica en el artículo 77.1. c) y 2. 4. 5. y 6 de la LOPDGDD:

1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción."

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: SANCIONAR CON APERCIBIMIENTO a la AGENCIA ESTATAL CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS, con NIF Q2818002D, por una infracción del artículo 5.1.f) del RGPD y del artículo 32 del RGPD, tipificadas en los artículos 83.5 del RGPD y 83.4 del RGPD, respectivamente.

SEGUNDO: NOTIFICAR la presente resolución a AGENCIA ESTATAL CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS.

TERCERO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

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 conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, 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.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-231221

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