Procedimiento nº.: E/03031/2015

ASUNTO: Recurso de Reposición Nº RR/00756/2015

Examinado el recurso de reposición interpuesto por Don ***A.A.A.,*** contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos en el expediente de actuaciones previas de inspección E/03031/2015, y en base a los siguientes

HECHOS

PRIMERO: Con fecha 31 de agosto de 2015, se dictó resolución por la Directora de la Agencia Española de Protección de Datos en el expediente de actuaciones previas de inspección E/03031/2015, procediéndose al archivo de actuaciones al no apreciar vulneración de lo dispuesto en la normativa de protección de datos.

Dicha resolución, que fue notificada al recurrente en fecha 9 de septiembre de 2015, según aviso de recibo que figura en el expediente.

SEGUNDO: Don ***A.A.A.*** ha presentado en esta Agencia, en fecha 25 de septiembre de 2015, recurso de reposición, exponiendo lo siguiente:

"Habiendo recibido la Resolución de Archivo de actuaciones Expediente E/03031/2015, en base a unos fundamentos de derecho que en absoluto vienen a ajustarse a lo denunciado por el suscribiente, pues aquí lo que se denuncia es la consulta de datos policiales que se ha venido realizando por un personal interino sin estar autorizado por la Dirección General de la Guardia Civil, haciendo uso de unas claves que pertenecían a funcionarios de carrera, suplantando la identidad de éstos. Es lamentable el poder comprobar la falta de rigor por parte de la Directora que ha procedido a la Resolución del Archivo, en base a unos fundamentos elucubrados sin entrar a valorar la gravedad de lo denunciado, siendo lo peor del caso que el Denunciante ha podido tener conocimiento de que estos hechos ya han sido realmente estudiados y condenados por la comisión de una FALTA GRAVE por el Director de la Agencia Española de Datos, en resolución R/02151/2014 de fecha 02/10/14, procedimiento AP/00024/2014, y usted parece omitir en todo momento centrándose en "las funciones del personal interino" en lugar de un posible delito de usurpación de identidad. Que este suscribiente, le ruega se lea la Resolución citada por su propio organismo, y antes de proceder al archivo de una denuncia con argumentos tan efímeros, le ruego lea con detenimiento la denuncia del Agente de Policía, así como la Resolución R/02151/2014 de fecha 02/10/14, y proceda a comprobar si ha quedado acreditado si se han llevado a cabo las medidas específicas que Ustedes mismos exigieron por estos hechos a la Policía Local de Torrevieja, resultando ser: Que acredite las medidas adoptada para garantizar el cumplimiento de los artículos 93 y 98 del Reglamento de Desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21/12 (en adelante RLOPD) en relación al Sistema SIGO.

-Que se remita la información que se ha incluido en el Documento de Seguridad en relación a las medidas establecidas para la gestión del acceso al Sistema SIGO.

-Que se realice la auditoría de seguridad en relación a los accesos al sistema SIGO remitiendo sus resultados a la AEPD.

Así como en el caso que lo estimaran oportuno, dieran el correspondiente traslado a Fiscalía por si pudiera observar en la forma que estuvieron accediendo a los datos estos agentes interinos, hubieran podido incurrir en algún tipo de infracción penal establecida en nuestro ordenamiento jurídico."

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el presente recurso la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en lo sucesivo LRJPAC).

II

Los ficheros de las Fuerzas y Cuerpos de Seguridad, regulados en el artículo 22 de la LOPD que indica:

"1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.

2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad."

La consulta a los ficheros accesibles a través de la aplicación SIGO supone acceder a ficheros de carácter policial y por tanto han de guardar las medidas de seguridad de este tipo de ficheros, de NIVEL ALTO (artículo 81.3.b del Reglamento de Desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21/12 (en adelante RLOPD), lo que conlleva que cumplan las medidas de los estadios anteriores, tanto a nivel BÁSICO como de nivel MEDIO, y además las más exigentes del nivel ALTO.

El artículo 9.1 de la LOPD precisa*: "El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garantice la seguridad de los datos de carácter personal y evite su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana del medio físico o natural".*

Por otro lado, el Reglamento de Desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre, establece, lo siguiente en dos artículo que desarrollan las medidas de seguridad:

Artículo 91:

"1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados."

Además de la infracción general de las medidas de seguridad puestas de manifiesto con la denuncia del denunciante, se observa en su caso que la consulta llevada a cabo aparece sin justificarse"

Artículo 93:

"1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible."

Artículo 96:

"1. A partir del nivel medio, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título."

De nivel alto que ha de cumplir, artículo 103:

"1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados."

Como consecuencia de una denuncia anterior, se tuvo conocimiento de lo siguiente: *"En el procedimiento ya se significó y se reitera, que continua implantada la tarjeta magnética individualizada de control de acceso para el personal autorizado, dispositivo de videovigilancia en la sala de Comunicaciones y Circular informativa sobre protección de Datos en la puerta de acceso a la dependencia", y añade que "en la actualidad, la Policía Local de Torrevieja carece de cualquier tipo de claves de acceso al terminal SIGO".*

Los accesos al terminal SIGO se realizaron, por parte de la Policía Local de Torrevieja, hasta el año 2013. El hecho de que lo hayan realizado funcionarios interinos no supone ninguna infracción a la normativa de protección de datos, ya que realizan las mismas funciones que un funcionario de carrera (al que sustituye) y tiene la misma obligación de guardar secreto que tiene el funcionario de carrera.

III

Don ***A.A.A.*** no ha aportado nuevos hechos o argumentos jurídicos que permitan reconsiderar la validez de la resolución impugnada. Las correcciones que se han realizado en la Policía Local de Torrevieja han sido consecuencia del procedimiento de infracción de Administraciones Públicas al que se refiere el recurrente.

Vistos los preceptos citados y demás de general aplicación,

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

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por Don ***A.A.A.*** contra la

resolución de esta Agencia dictada con fecha 31 de agosto de 2015, en el expediente de actuaciones previas de inspección E/03031/2015.

SEGUNDO: NOTIFICAR la presente resolución a Don ***A.A.A.***.

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa, se podrá interponer en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto según lo previsto en el artículo 46.1 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta del referido texto legal.

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