Expediente Nº: E/03031/2015

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante el EXCMO. AYTO. DE TORREVIEJA (ALICANTE), en virtud de denuncia presentada por Don ***A.A.A.,*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 23 de abril de 2015, tuvo entrada en esta Agencia un escrito remitido por Don ***A.A.A.,*** en el que declara que en la policía municipal del Ayuntamiento de Torrevieja, durante los últimos tres años, Agentes interinos, cuya función es regular el tráfico, tienen acceso ilimitado al Sistema Integrado de Gestión Operativa (SIGO) utilizando para ello claves de usuario de otros agentes que son funcionarios de carrera.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

Según manifiestan los representantes de la Policía Local de Torrevieja, no disponen de acceso a SIGO desde el año 2013. Por consiguiente, ningún funcionario de esta plantilla policial accede, en la actualidad, al referido sistema.

Desde la instauración del acceso al sistema SIGO en la Policía Local (año 2000) existieron tres accesos, que cesaron en su actividad en el 2013.

En la Comunidad Valenciana, no se restringen las funciones a realizar por los Policía Locales en interinidad, aunque sí se regula una matización en la Disposición Adicional, octava de la Ley 6/1999, de 19 de abril, de la Generalitat Valenciana, de Policías Locales y de Coordinación de las Policías Locales de la Comunidad Valenciana, que contempla: *"Hasta tanto no se desarrolle el procedimiento de selección para el nombramiento de funcionarios interinos previsto en esta Ley este personal no podrá portar armas de fuego, destinándose en consecuencia a servicios y funciones prioritariamente de policía Administrativa, Medio Ambiente y Tráfico y Seguridad Vial. ".* Esta Jefatura interpreta que la matización reseñada trae causa de que el funcionario policial interino no porta armas de fuego para su autodefensa. Igualmente se entiende que si cabe la realización de funciones complementarias al servicio, muchas de ellas relacionadas con el tráfico y seguridad vial, además de otras como atender llamadas telefónicas, trasmitir información e incidencias, incluso la consulta de datos, todo desde el interior de un inmueble dotado de medidas de seguridad de accesos.

Según indican representantes de la Jefatura de la Policía Local de Torrevieja, no se tiene conocimiento de que un funcionario de Policía Local en situación de interinidad y en materia de funciones le sean exigidos requisitos diferentes para acceder al sistema

SIGO u otra base de datos, respecto de los que ocupen plaza/puesto en propiedad. En materia del deber de confidencialidad el régimen legal aplicable a un funcionario, sea interino o no, es el mismo.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

En cuanto al régimen de ficheros de las Fuerzas y Cuerpos de Seguridad, el artículo 22 de la LOPD 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 realiza 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.

Por lo tanto, de acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.

2. **NOTIFICAR** la presente Resolución al EXCMO. AYTO. DE TORREVIEJA (ALICANTE) y 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 (artículo 48.2 de la LOPD), y de conformidad con lo establecido 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, 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 del referido texto legal.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la citada LJCA, sólo podrá interponer 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 LJCA, 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 del referido texto legal.

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