Expediente Nº: E/03773/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos en virtud de cinco denuncias presentadas y teniendo como base los siguientes

HECHOS

PRIMERO: Entre el 22 de junio y el 10 de julio de 2013 tuvieron entrada en la Agencia las denuncias de cinco personas, en calidad de representantes de distintos órganos del Ayuntamiento de Alicante: la Policía Local, la Sección Sindical de UGT, el Sindicato Profesional de Policía Local y Bomberos (SPPLB-CV), la Secretaría Autonómica del SEP-CV y CSI-F Unión Provincial de Alicante, respectivamente. Estos escritos refieren la publicación, en la dirección web http://....., de datos personales de 750 policías municipales, los días 22, 23 y 24 de junio. El representante de la Policía Local manifiesta que se ha solicitado, al proveedor de servicios que aloja el sitio web, con sede en Estados Unidos, la retirada inmediata de los datos, a través del buzón ....@.....

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:

1. En fecha 25 de junio de 2013, por la Inspección de Datos se verificó que, aunque el fichero ya no era accesible a través de la dirección web indicada, aún podía accederse al mismo a través de la memoria caché del buscador *Google*.
2. En el informe de actuaciones de Inspección se hace referencia a la documentación remitida a la Agencia por el Ayuntamiento de Alicante, con fecha de registro de entrada de 26 de agosto de 2013:

   <<El Ayuntamiento de Alicante ha aportado copia del Informe emitido por la Unidad Informática de la Policía Local en relación con la incidencia de seguridad que ha permitido que un fichero con datos personales de los policías locales del Ayuntamiento haya sido publicado en el portal pastebin.com e indexados por los buscadores (Google). En dicho informe figura:

   > *El viernes 21 de junio sobre las 19:45h, se recibió una llamada telefónica indicando que varios Agentes de la Policía Local habían localizado sus datos personales, publicados en la web pastebin.com.*
   >
   > *Inmediatamente se comprobó la existencia del listado completo de 752 funcionarios pertenecientes al Cuerpo de la Policía Local, incluyendo a jubilados, así como aquellos que fallecieron estando en activo.*

   La información contenía los siguientes datos: Nombre, 1° Apellido, 2° Apellido, Fecha de Ingreso, Fecha de Nacimiento, Sistema de Trabajo, Teléfono particular, Teléfono corporativo, Observaciones, Estudios y Domicilio particular.

   Esta información se presenta en formato texto, separado por comas "," (fichero csv), y conteniendo la palabra reservada "NULL", cuando el campo no contenía información.

Estos datos y su presentación coinciden con la aplicación de "Seguridad, Fichas de personal".

Se verifica que la página que aloja los datos se encuentra ubicada en Los Ángeles, (Estados Unidos) y el servidor se encuentra ubicado en Illinois (Estados Unidos).

Procedieron a realizar búsqueda con el primer registro que figuraba en el listado a través de Google (argumento de búsqueda número de D.N.I. y dos apellidos), comprobando que se accedía a todo el fichero.

Comprueban que el proveedor de servicios de la página (ISP) es "GigeNET" y localizan la dirección de correo ....@..... donde se reporta el abuso del uso de los servicios y proceden a enviar un correo informando de la publicación de datos personales para su inmediata eliminación. Este correo fue contestado inmediatamente por GigeNet.

Se procede a poner en conocimiento de la Agenda Española de Protección de Datos estos hechos y se presenta denuncia ante el Cuerpo Nacional de Policía y ante la Brigada Provincial de Policía Judicial de la U.D.E.F. —Grupo de delincuencia económica y Delitos Tecnológicos-.

Se continuó con la investigación, obteniendo las siguientes conclusiones:

- *La web pastebin.com es el instrumento de difusión del grupo ciberhackitivista Anonymous.*
- *En el final del listado figura el grupo hacker "Anonymous" como se aprecia en la siguiente captura: Indicando "Somos Anonymous. Somos legión. No perdonamos. No olvidamos. Es lo que esperan de nosotros." A este respecto, tanto en el listado aportado por uno de los denunciantes como el obtenido por la Inspección de Datos ubicado en la memoria caché de Google consta la siguiente frase: "We are Anonymus. We are legion. We do not forgive. We do not forget. Expect us".*

[…]

El Ayuntamiento de Alicante ha aportado impresión de pantalla del Registro de Incidencias e Informe de la incidencia informática donde consta:

Una vez solicitado por la Unidad Informática de la Policía Local la eliminación del listado de la web de pastebin.com se ha comprobado que fue efectiva el 25 de junio de 2013.

Se han revisado los archivos de seguimiento del servidor web del Ayuntamiento (log) detectándose actividades anómalas en los sistemas de información municipal en los periodos de:

14/04/2013 desde las 21:51:27 h. hasta las 21:53:58 h.

01/05/2013 desde las 9:13:01 h. hasta las 21:17:16 h.

07/05/2013 desde las 20:14:41 h. hasta las 20:19:23 h.

10/05/2013 desde las 22:20:35 h. hasta las 22:36:57 h.

Dicha actividad corresponde a intentos de ataque basados en técnicas avanzadas de hacking, por lo cual se estima que en algún momento se habría podido acceder a datos de los servidores municipales.

Las medidas de seguridad habituales en las instalaciones informáticas y sus conexiones a Internet consisten principalmente en un cortafuegos (firewall) que restringe el acceso a los diferentes servicios usando los puertos TCP/UDP y direcciones IP y adicionalmente de sistemas antivirus, antispam, filtrado de contenidos y aplicaciones.

El equipamiento afectado en este determinado caso es el firewall corporativo y el servidor Web del Ayuntamiento. En relación al firewall, fue instalado en el año 2008 manteniéndose constantemente actualizado. En cuanto al servidor Web, fue instalado en 2006. Desde la puesta en marcha de estos equipos, no se han tenido evidencias de fallos de seguridad en ninguno de ellos, por lo que se sospecha que ha sido un ataque que ha explotado alguna vulnerabilidad para la que no estaban preparados.>>

3. En el Informe de incidencia informática, dirigido por el Jefe del Departamento Técnico de Desarrollo Web y el Jefe del Departamento Técnico de Sistemas al Jefe del Servicio de Modernización de Estructuras Municipales, fechado el 1 de julio de 2013, se concluye: "*Por la forma y complejidad con que se han producido dichos ataques, se deduce que han sido llevados a cabo por personas con importantes conocimientos técnicos sobre la materia y que posiblemente se dediquen de forma habitual a realizar acciones de este tipo, lo cual ratifica la sospecha de que se trata de un grupo organizado y experimentado como Anonymous, tal y como se reivindicaba en los datos publicados".*

4. En el Informe de acciones correctoras, del Jefe del Departamento Técnico de Sistemas, fechado el 20 de agosto de 2013, se detallan las acciones correctoras realizadas tras identificarse la quiebra de seguridad explotada por la incidencia de seguridad del mes de junio. En este documento se expone: "*Tras el estudio de los ficheros de traza de actividad del servidor web del Ayuntamiento se localizó tráfico anómalo en distintos períodos de tiempo. Puestos en contacto con la empresa que montó los sistemas de seguridad del Ayuntamiento recomendaron la instalación de un sistema de prevención de intrusiones. Estos sistemas evitan la posibilidad de que muchos ataques que explotan fallos de seguridad de los sistemas expuestos a internet sean viables."* Se indica asimismo: *"Tras evaluarse las alternativas a tomar se procede a la instalación temporal de un sistema de prevención de intrusiones (IPS) en el acceso a internet. Adicionalmente se confirman los planes previos de renovación de todo el equipamiento de seguridad para el ejercicio 2014".*

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director 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

El artículo 9 de la LOPD establece:

"1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten 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 o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley."

En el Título VIII del Reglamento de desarrollo de la LOPD, aprobado mediante Real Decreto 1720/2007, de 21 de diciembre, se detallan los requisitos de seguridad que han de reunir los ficheros y tratamientos de datos de carácter personal, en función de la tipología de los datos involucrados.

En el presente caso, de acuerdo con la documentación que obra en el expediente, la filtración en internet de los datos de los policías municipales de Alicante, que figuraban en los ficheros del Ayuntamiento, tuvo lugar como consecuencia de un ataque al sitio web municipal, perpetrado por personas con importantes conocimientos técnicos.

A este respecto, procede tener en consideración la Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de fecha 25 de febrero de 2010 que, en relación con un caso similar al presente, señala lo siguiente:

> *"En el caso de autos, el resultado es consecuencia de una actividad de intrusión, no amparada por el ordenamiento jurídico y en tal sentido ilegal, de un tercero con altos conocimientos técnicos informáticos que rompiendo los sistemas de seguridad establecidos accede a la base de datos de usuarios registrados en www.portalatino.com, descargándose una copia de la misma. Y tales hechos, no pueden imputarse a la entidad recurrente pues, de otra forma, se vulneraría el principio de culpabilidad.*
>
> *El principio de culpabilidad, previsto en el artículo 130.1 de la Ley 30/1992, dispone que solo pueden ser sancionadas por hechos constitutivos de infracción administrativa los responsables de los mismos, aún a título de simple inobservancia. Esta simple inobservancia no puede ser entendida como la admisión en el derecho administrativo sancionador de la responsabilidad objetiva, que está proscrita después de la STC 76/1999, que señaló que los principios del ámbito del derecho penal son aplicables, con ciertos matices, en el ámbito del derecho administrativo sancionador, requiriéndose la existencia de dolo o culpa. En esta línea la STC 246/1999, de 19 de diciembre (RTC 1991/246), señaló que la culpabilidad constituye un principio básico del Derecho administrativo sancionador. Culpabilidad, que no concurre en la conducta analizada de Portal Latino".*

No obstante, aunque en la Sentencia no se considera probada una vulneración

del artículo 9 de la LOPD, sí se aprecia una conducta infractora por parte del responsable del fichero, en concreto la vulneración del deber de guardar secreto, al apreciar su tardanza en adoptar un comportamiento activo para impedir que se hicieran públicos en internet los datos personales comprometidos.

En el marco de las actuaciones de inspección realizadas por esta Agencia al respecto de otros casos de intrusión en sitios web (particularmente, en los procedimientos A/00368/2011, PS/00422/2012, A/00031/2013), se puso de manifiesto que los accesos indebidos a datos personales se habían visto favorecidos por la existencia de determinadas vulnerabilidades, ocasionadas por notables deficiencias en la implantación de las preceptivas medidas de seguridad por parte de los responsables del tratamiento.

En el presente caso, sin embargo, por la Inspección de Datos no ha logrado acreditarse el incumplimiento de ninguna de las obligaciones previstas en el citado Reglamento. Por otra parte, resulta destacable la diligencia observada por parte del Ayuntamiento de Alicante, tras detectarse la publicación de los datos de los policías municipales, para lograr su inmediata desaparición del sitio web donde se habían publicado, por lo que, de conformidad con la reseñada Sentencia, tampoco procede imputar al Ayuntamiento una vulneración del artículo 10 de la LOPD.

Por lo tanto, de acuerdo con lo señalado,

Por el Director de la Agencia Española de Protección de Datos,

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a cada uno de los denunciantes.

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 el Director 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.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos