Expediente Nº: E/02318/2018

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **LINKEDIN SPAIN, S.L.,** teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha de 24/04/2018 la Directora de la Agencia Española de Protección de Datos acuerda iniciar las presentes actuaciones de investigación en relación a un fallo de seguridad en la red social LINKEDIN ocurrido con fecha 22/04/2018 que habría permitido que los atacantes accedieran a datos privados de miles de usuarios de la red y a la información pública de los perfiles. Dicho acceso se produciría a través del botón *"Autocompletar"* de LINKEDIN, mediante un botón *"invisible"* que una vez pulsado permitiría el acceso a los referidos datos.

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:

Se ha realizado un requerimiento de información a LINKEDIN SPAIN SL que, según se puede leer en su contestación, ha tenido la cortesía de trasladar la petición a LINKEDIN IRELAND UNLIMITED COMPANY. Esta entidad sería la que controla los datos personales de los usuarios que residen en la Unión Europea, Espacio Económico Europeo y Suiza, y tiene su establecimiento principal en Irlanda, donde reside su administración central.

En relación al caso que se está investigando, LINKEDIN SPAIN SL aporta la siguiente información:

> La función *"Autofill"* (Autocompletar) permite a aquellos que visitan un sitio web rellenar previamente un formulario en tal web con información de su perfil en LINKEDIN. Tal funcionalidad solo está disponible en sitios web pre-aprobados por LINKEDIN.
>
> El fallo de seguridad fue causado por un error en el software de LINKEDIN, que facilitó la posibilidad de que terceros de mala fe insertaran el código de "autofill" en sus sitios web, no pre-aprobados por LINKEDIN, y de esta forma recolectaran datos sobre aquellos usuarios conectados a LINKEDIN que visitaban tales sitios web.
>
> Tan pronto como tuvieron conocimiento del problema, realizaron las siguientes medidas:
>
> - Implementar un parche para restringir la función *"Autofill"* a sitios pre-aprobados por LINKEDIN
> - Implementar un parche para requerir confirmación por parte de usuarios de LINKEDIN antes de que sus datos se autocompleten.

Indican que tras la investigación de su equipo de seguridad pueden confirmar que no hay indicios de que los datos personales de los miembros de LINKEDIN se hubieran visto comprometidos como resultado de este problema.

De Internet se puede extraer la siguiente información adicional:

La vulnerabilidad fue descubierta por A.A.A., trabajador de la empresa Lightning Security, el 09/04/2018. A.A.A. notificó la vulnerabilidad a la empresa, y ésta respondió de forma rápida, teniendo preparada al día siguiente (10/04/2018) una medida de seguridad temporal en forma de "parche". Sin embargo, no fue hasta varios días después (19/04/2018) cuando perfeccionó el "parche", para evitar que dicha funcionalidad fuera vulnerable en caso de que la página pre-aprobada por LINKEDIN también fuera comprometida. En la URL *https://lightningsecurity.io/blog/linkedin/* se encuentra explicada y documentada la vulnerabilidad por parte de la persona que lo descubrió.

Según se explica en dicha web y en otras donde se reporta la noticia, la pieza del código de *"Autocompletar"* está asociada al presionado de un botón. El atacante necesita que la víctima pulse dicho botón, y para conseguirlo de forma inadvertida, tiene la opción de colocar un botón invisible que ocupa toda la pantalla de su sitio web, de manera que con que el visitante acceda a la página y haga click con el ratón sobre dicha página sería suficiente para activar el código de "Autocompletar" y acceder a los datos personales del perfil público del usuario.

Condición necesaria previa para la recolección efectiva de datos personales es que el usuario que pulsa el botón invisible disponga de una cuenta en la red social LINKEDIN, y que además tenga iniciada sesión en el navegador. Esto último se puede comprobar en una página web de LINKEDIN dotada de un botón con la característica de *"Autocompletar"* (*https://business.linkedin.com/marketing-solutions/cx/17/02/the-sophisticated-marketers-guide-to-linkedin*)

Además, como se menciona en su página web, A.A.A. descubrió también que los datos personales del perfil son accedidos por el componente de *"Autocompletar"* sin importar la configuración de privacidad que tenga establecida su usuario para cada uno de ellos. Es decir, aunque un determinado dato personal existiese en el perfil pero no hubiese sido configurado por su titular para ser mostrado públicamente para su visualización por usuarios de LINKEDIN (o para cualquier visitante de la red social, sea usuario de LINKEDIN o no), este dato personal sería recolectado igualmente por el componente de "Autocompletar". Este funcionamiento es contrario a las especificaciones que ofrece LINKEDIN en la información del componente (*https://www.linkedin.com/help/lms/answer/85810/your-profile-information-on-linkedin-autofill?lang=en*)

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

El artículo 126.1, apartado segundo, del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD) establece:

"Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso."

III

El artículo 9 de la LOPD establece en relación con la seguridad de los datos que:

"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".

Por otra parte, el artículo 93 del RLOPD establece que:

"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".

IV

En el presente caso, las actuaciones de investigación tienen lugar como consecuencia de una fallo o quiebra se seguridad en la red social LINKEDIN posibilitando el acceso a datos privados de miles de usuarios de la citada red.

La red social LINKEDIN, que tiene una finalidad de tipo profesional, orientada a la empresa, negocio y empleo, que partiendo del perfil de cada usuario, que libremente revela su experiencia laboral y sus destrezas, pone en contacto a millones de empresas y empleadores.

Hay que señalar que teniendo en cuenta el fallo de seguridad detectado yb una vez analizado el mismo hubiera sido imposible acceder a un gran volumen datos de una sola vez. Por otra parte, no se tiene constancia de que existan usuarios afectados, ni denuncias registradas en la AEPD, ni revelación de datos personales, ni de atancante/s que hubieran obtenido partido o beneficio de la posible quiebra o vulnerabilidad en la seguridad de la red social.

Además, notificada sobre la posible quiebra la empresa respondió de manera inmediata teniendo preparada mecanismo de seguridad temporal y completándola en los días sucesivos.

A este respecto, la Sentencia de la Audiencia Nacional de 25/06/2015 ha señalado lo siguiente: *"En interpretación del citado artículo 9, esta Sala ha señalado en múltiples sentencias, (SSAN, Sec. 1ª, de 13 de junio de 2002, Rec. 1517/2001; 7 de febrero de 2003 Rec. 1182/2001; 25-1-2006 Rec. 227/2004; 28 de junio de 2006 Rec. 290/2004 etc), que la obligación que dimana del mismo no se cumple con la adopción de cualquier medida, pues deben ser las necesarias para garantizar aquellos objetivos que marca el precepto, y por supuesto, no basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva. Hemos considerado, en consecuencia, que se impone una obligación de resultado, consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros. En definitiva, toda responsable de un fichero (o encargada de tratamiento) es, por disposición legal, una deudora de seguridad en materia de datos debiendo asegurarse de que dichas medidas o mecanismos se implementen de manera efectiva en la práctica".*

En el caso examinado, resulta destacable la diligencia observada por parte de la empresa titular tras detectarse que la posible quiebra de seguridad podría afectar a los datos de los usuarios, sin que se tenga constancia como se ha expuesto con anterioridad que hasta la fecha se haya detectado acceso a datos, ni incidencia sobre dicho asunto, ni evidencias de vulnerabilidad efectiva en los datos de carácter personal de usuario alguno.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a **LINKEDIN SPAIN, S.L.**

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 Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, 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.

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