Expediente Nº: E/03063/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

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

HECHOS

PRIMERO: En fechas 13 y 17 de mayo de 2013, respectivamente, tienen entrada en esta Agencia las denuncias de dos usuarias del sitio web www.letsbonus.com, que aportan copia del mensaje electrónico que les ha sido remitido desde ...@.....letsbonus..... informando de que se había detectado un acceso indebido a los sistemas informáticos del grupo.

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 el mensaje electrónico aportado por las denunciantes, fechado el 27 de abril de 2013, se expone: "*La única información que podría haberse visto afectada se limita a nombre, dirección de correo electrónico, fecha de nacimiento y contraseña. En todos los casos, las contraseñas están encriptadas, por lo tanto resulta muy poco probable que pudieran ser descifradas. Los datos de las tarjetas de crédito/débito no se han visto afectados en ningún momento. Para garantizar que tu cuenta está totalmente segura, hemos expirado tu actual contraseña y, por lo tanto, se te requerirá crear una nueva contraseña la próxima vez que intentes acceder a tu cuenta.* Para tu comodidad puedes cambiar ahora tu contraseña a través de este enlace: *[…] Te aconsejamos también que para la seguridad de tus datos personales, consideres cambiarla contraseña en otras webs donde uses la misma o parecida. La seguridad de tu información es nuestra prioridad. […] ya hemos tomado medidas adicionales para aumentar la seguridad de nuestros sistemas y evitar cualquier problema en el futuro. LetsBonus nunca te pedirá información personal o datos relativos a tu cuenta por correo electrónico. Siempre te dirigiremos a nuestra web -indicando que te registres- antes hacer cualquier cambio en tu cuenta. Por favor, haz caso omiso de los emails que pudieses recibir afirmando ser de LetsBonus y te solicitan dicha información o dirigirte una web diferente que pida estos datos. Si tienes alguna duda sobre este proceso, por favor visita nuestras preguntas frecuentes. […] Ahí encontraras las instrucciones de cómo crear una nueva contraseña y la respuesta a otras preguntas que puedan surgirte. así como un formulario para poder solicitar información adicional."*

2. En respuesta al requerimiento de la Inspección, LETS BONUS, S.L.U. ha manifestado que fue adquirida, en enero de 2012, por la multinacional estadounidense LivingSocial, Inc., con establecimiento principal en Washington, DC y adherida al acuerdo *Safe Harbor* (Puerto Seguro) suscrito entre la Unión Europea y el Departamento de Comercio de Estados Unidos.

3. Según declara la compañía, hasta el primer trimestre del año 2013 mantuvo su propia plataforma electrónica para los datos de sus usuarios y en esas fechas comenzó la transición de determinados servicios web y de alojamiento de datos a la matriz estadounidense, que actúa en calidad de encargado del tratamiento de los

datos personales de los que es responsable la compañía española. A este respecto, LETS BONUS, S.L.U. ha aportado a la Inspección copia del contrato de tratamiento de datos suscrito entre ambas compañías el 23 de febrero de 2013, donde se hace referencia a las previsiones del artículo 12 de la LOPD, en relación con los servicios de alojamiento (*hosting*) prestados por la compañía estadounidense. Se ha aportado asimismo el anexo de cinco páginas donde se detallan las medidas de seguridad que esta compañía se comprometió a adoptar, de acuerdo con las exigencias del Reglamento de desarrollo de la LOPD, aprobado mediante Real Decreto 1720/2007, de 21 de diciembre (RLOPD).

4. LETS BONUS, S.L.U. ha declarado que el 12 de abril de 2013 LivingSocial, Inc. detectó una actividad no autorizada en su red interna. Tan pronto como se detectó esta intrusión no autorizada, contrató consultores de seguridad externos para ayudar en el análisis forense y en las medidas tecnológicas de protección y la denunció a las autoridades competentes, concretamente, al FBI. En el momento de atender el requerimiento de la Inspección, ni la compañía estadounidense ni la española tenían conocimiento de que se hubiera producido algún fraude o algún perjuicio a los usuarios relacionados con la incidencia, ya que el alcance fue limitado y la información accesible era poco crítica, no existiendo evidencia de que los datos de tarjetas de crédito se hubieran visto afectados.

5. Según lo declarado por LETS BONUS, S.L.U., la compañía estadounidense LivingSocial, Inc. llegó a la conclusión de que el acceso se había realizado por un intruso externo, que adquirió y utilizó un limitado número de credenciales válidas propias de un empleado autorizado, para conseguir acceso a su red interna (VPN) y a su base de datos.

6. LETS BONUS, S.L.U. ha aportado copia de la anotación incorporada a su *Registro de Incidencias* y ha detallado a la Inspección las acciones reactivas realizadas, tanto por la propia compañía responsable como por la compañía estadounidense encargada del tratamiento. La compañía responsable entiende que no estaba legalmente obligada a realizar las notificaciones individuales, ya que los riesgos asociados eran muy bajos, aunque optaron por llevarlas a cabo con el fin de maximizar la transparencia y reducir al mínimo cualquier riesgo de daño residual. Según expone, notificó a un total de 4.834.086 usuarios españoles.

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, el acceso a los datos de los usuarios del sitio web denunciado fue 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 o encargados 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, tras detectarse el acceso, por parte del responsable del fichero y por el encargado del tratamiento, por lo que, de conformidad con la reseñada Sentencia, tampoco procede imputar vulneración alguna 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 LETS BONUS, S.L.U. y a cada una de las 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