Procedimiento Nº: A/00024/2015

RESOLUCIÓN: R/00910/2015

En el procedimiento A/00024/2015, instruido por la Agencia Española de Protección de Datos a la entidad BINTERNATIONAL SPAIN, S.R.L., vista la denuncia presentada por D. ***A.A.A.***, y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 3 de abril de 2014, tuvo entrada en esta Agencia un escrito de D. ***A.A.A.*** (en lo sucesivo el denunciante), en el que se reconoce usuario del portal de búsqueda de empleo www.binternational.es, al que ha subido su CV. Según expone, en el apartado "*ver mi curriculum*" de la "*zona de usuarios*" del sitio web, el botón que permite visualizar su CV dirige a la dirección web ***http://www.....***, en la que basta con modificar el último dígito para visualizar el CV de otro usuario, por lo que deduce que cualquier otra persona podría tener acceso a su perfil, sin ni siquiera estar inscrito.

Aporta copia de tres CV accedidos por el denunciante a través del sitio web citado, además del suyo.

SEGUNDO: A la vista de los hechos denunciados, en fase de actuaciones previas, por los Servicios de Inspección de esta Agencia se tuvo conocimiento de los siguientes extremos, que constan detallados en el Informe de Actuaciones Previas elaborado:

1. La compañía BINTERNATIONAL SPAIN, S.R.L. (en lo sucesivo BINTERNATIONAL SPAIN), propietaria del portal denunciado, es responsable del fichero denominado "*usuarios*", inscrito en el Registro General de Protección de Datos y cuya finalidad se describe así: "*gestión de datos para la preselección de candidatos para vacantes profesionales*".
2. En fecha 8 de abril por la Inspección de Datos se realizó una búsqueda en Google del nombre y apellidos del denunciante, restringida al sitio *binternational.es*, no obteniéndose resultados.
3. En fecha 15 de abril por la Inspección se constató que el CV del denunciante era directamente accesible en internet a través de la dirección web indicada en la denuncia. Se constató asimismo que al modificar los dígitos de la dirección web podía accederse a los CV de otras personas.
4. En respuesta al requerimiento de la Inspección, BINTERNATIONAL SPAIN ha declarado: "*Hasta la fecha de recepción de la solicitud de información por parte de AGPD, no teníamos constancia de la quiebra de seguridad manifestada en su escrito, por lo que pensábamos que al no haber recibido ninguna comunicación de nuestros candidatos, las medidas de seguridad implantadas inicialmente funcionaban sin fisuras. En el momento de la recepción de su escrito pudimos comprobar a través de la empresa de informática que contratamos para el mantenimiento de la misma, que efectivamente había una quiebra de seguridad, e inmediatamente procedimos a sellar dicha quiebra, y nos pusimos a investigar las causas.*"
5. En relación con el funcionamiento del sitio web, la compañía ha detallado el procedimiento por el que se dan de alta los usuarios en el sitio web www.binternational.es, así como las

medidas implantadas para almacenar los documentos CV que estos suben. Según se expone: "*Estos ficheros PDF asociados a los candidatos se guardan en la web en la carpeta* ***www.....****, pero esta información no es visible por el usuario, y solo puede hacerse visible si el administrador de la web así lo quiere. Si un candidato quiere modificar datos de las plantillas de su CV, se tiene que validar con usuario y contraseña, y si además quiere sustituir el CV en formato PDF, el nuevo archivo que suba a la web sustituirá al antiguo. Un candidato que se ha validado con su usuario y contraseña en la web, puede acceder a su CV en PDF, para verlo o descargárselo, y es en ese momento cuando en la barra de navegación aparece la ruta del CV. Ahora bien, si dicha ruta la copia e intenta utilizar un navegador de búsqueda, no podrá visualizar dicho currículo, si las condiciones de seguridad están bien implementadas. [...] Aun con el acceso abierto a la carpeta* ***www.....****, donde están almacenados los CV de los candidatos, para visualizar uno en concreto a través de un navegador como Google, tendríamos que acertar con el código de curriculumxxxxx.pdf. Y teniendo en cuenta que no todos los usuarios suben CV, es difícil acertar, al tener 99.999 posibilidades. […]* Del total de usuarios registrados con un número asociado a cada uno de ellos, solo un pequeño porcentaje tienen asociado un fichero de cv en la carpeta ***www.....***, por lo que acertar probando números es bastante complicado. *La quiebra de seguridad viene debido a que se supone que alguien poniendo en un buscador google o similar la dirección* ***www...../.....*** *siendo xxxxx un número cualquiera, y probando varios, ha podido ver el curriculumxxxxx.pdf de un candidato o de varios."*

6. El administrador de BINTERNATIONAL SPAIN ha declarado que ha solicitado al proveedor de servicios de alojamiento de la web información de actividad de la página, para comprobar quién y en qué fechas ha tenido acceso a la misma, detectando que desde una dirección IP ajena a la compañía, entre el 17/02/2014 y el 25/02/2014 se habían realizado 445 accesos con un ordenador Macintosh. Según se expone, la compañía tiene sospechas de que los accesos habían sido efectuados por un exsocio, "*que habría manipulado el sistema de la página (tanto directamente como a través de un tercero) para inhabilitar la protección de los currículos y, acto seguido, denunciar los hechos ante la AEPD",* habiéndose puesto los hechos en conocimiento del Grupo Especial de Delitos Telemáticos, para la averiguación de lo sucedido.
7. La compañía ha detallado a la Agencia las medidas tomadas tras recibir el requerimiento de la Inspección, que incluyen:
   - Contactar con la empresa de informática contratada para el mantenimiento de la web, y cambiar el usuario y contraseñas del administrador.
   - Cerrar el acceso no autorizado detectado y dejar dicho acceso solo al administrador de la web a las carpetas donde estaban alojados los CV.
   - Impedir temporalmente el acceso al CV de los candidatos.
   - Solicitar a Google la eliminación de las direcciones ***www...../*** de la cache de los motores de búsqueda.
   - Negación de la indexación de la web para todos los motores de búsqueda, con objeto de impedir en lo sucesivo el acceso a cualquier dato privado alojado en la web.

   Revisar los procedimientos de cambio de contraseñas y control de accesos en el documento de seguridad.
8. La compañía asegura haber cambiado de empresa de mantenimiento de la web y haber contratado el desarrollo de una nueva web con medidas de seguridad más amplias, no admitiendo la subida de información asociada a la de los formularios que tienen que rellenar los candidatos para estar registrados, por lo que no podrán exponer sus CV públicamente al no existir los mismos en nuestro alojamiento.
9. BINTERNATIONAL SPAIN ha manifestado: "*A pesar de no tener ninguna reclamación por parte de los candidatos, enviamos e-mail informando de la quiebra de seguridad, pidiendo disculpas y recordando el apartado 2 recogido en las Condiciones Generales de Registro de*

candidatos, por si consideran oportuno ejercer el derecho de Cancelación de datos."

10. BINTERNATIONAL SPAIN considera que la actividad desarrollada "*es una página Web sin ánimo de lucro que no percibe cantidad alguna de los demandantes de empleo, que introducen de sus datos, a los efectos de optar a un proceso de selección de las empresas solicitantes, por lo que dichos candidatos asumen las Condiciones de Registro, y la exposición de sus datos curriculares a los distintos empleadores a efectos de optar a un puesto de trabajo*."
11. Con fecha 12/12/2014, por los Servicios de Inspección de la AEPD se intentó acceder a la dirección web ***http://www.....***, obteniéndose un mensaje de error.

TERCERO: Con fecha 27/01/2015, el Director de la Agencia Española de Protección de Datos, por virtud de lo dispuesto en el artículo 45.6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), acordó someter a la entidad BINTERNATIONAL SPAIN a trámite de audiencia previa al apercibimiento, en relación con la denuncia por infracción del artículo 9 de la LOPD, en relación con los artículos 91 y 93 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, tipificada como grave en el artículo 44.3.h) de la citada Ley Orgánica.

Con tal motivo, se concedió a BINTERNATIONAL SPAIN plazo para formular alegaciones que transcurre sin que en esta Agencia se haya recibido escrito alguno.

HECHOS PROBADOS

1. La entidad BINTERNATIONAL SPAIN es titular del sitio web www.binternational.es.

2. El sitio web www.binternational.es está diseñada para que los usuarios puedan registrase como tales e incorporar a la misma su CV, que se almacena en la *carpeta* ***www.....***. El usuario puede acceder posteriormente a su CV para sustituirlo o modificarlo previa autenticación con nombre de usuario y contraseña. El acceso al CV por parte de un usuario genera una URL con la siguiente configuración ***www...../.....*** *siendo xxxxx el número asignado al documento del usuario de que se trate*. Dicha URL se visualiza en la pantalla.

3. El denunciante se registró como usuario dela web www.binternational.es e incorporó su CV a la misma.

4. Con fecha 03/04/2014, se recibe en la AEPD un escrito del denunciante en el que informa que, a través de la web www.binternational.es, en el apartado "*ver mi curriculum*" de la "*zona de usuarios*", el botón que permite visualizar su CV dirige a la dirección web ***http://www.....***, en la que basta con modificar el último dígito para visualizar el CV de otro usuario. Con su denuncia aportó copia de tres CV accedidos por el denunciante a través del citado sitio web.

5. Con fecha 08/04/2014, los Servicios de Inspección de la AEPD realizaron una búsqueda en Google, con el nombre y apellidos del denunciante como criterio, restringida al sitio *binternational.es*, no obteniéndose resultados.

6. Con fecha 15/04/2014, los Servicios de Inspección de la AEPD comprobaron que el CV del denunciante era directamente accesible en internet a través de la dirección web www.binternational.es. Se constató asimismo que al modificar los dígitos de la dirección web podía accederse a los CV de otros usuarios de dicha web.

7. En su respuesta al requerimiento de la Inspección de Datos, BINTERNATIONAL SPAIN admitió la existencia de la quiebra de seguridad denunciada.

8. Con fecha 12/12/2014, los Servicios de Inspección de la AEPD intentaron acceder a la dirección web ***http://www.....***, obteniéndose un mensaje de error.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento el Director de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 37.g) en relación con el artículo 36 de la LOPD.

II

El artículo 18.4 de la Constitución Española establece en que: *"la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*", consagrándose así el derecho a la protección de datos como un derecho autónomo, incluso del propio derecho a la intimidad, tal y como ha indicado la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre.

El artículo 1 de la LOPD dispone: *"La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".*

En cuanto al ámbito de aplicación de la citada norma, el artículo 2.1 de la misma señala que *"La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado"*; definiéndose el concepto de dato de carácter personal en el artículo 3.a) de la citada LOPD como *"Cualquier información concerniente a personas físicas identificadas o identificables"*.

En este mismo sentido se pronuncia el artículo 2.a) de la Directiva 95/46/CE, del Parlamento y del Consejo, de 24/10/1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en lo sucesivo la Directiva), según el cual se entiende por dato personal *"toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social"*.

En el presente caso, ha quedado acreditado que el fichero accedido, atendiendo a su contenido (datos personales identificativos de los afectados y datos curriculares, con detalle de su formación y experiencia profesional), se encuentra incluido dentro del ámbito de aplicación establecido en la LOPD y sus normas de desarrollo.

III

El Titulo VII sobre *Infracciones y sanciones*, en el artículo 43, de la LOPD establece:

"1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley."

El artículo. 3 de la LOPD establece las definiciones de responsable de fichero o tratamiento y de encargado de tratamiento:

"d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".
"g) Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".

IV

Se imputa a la entidad BINTERNATIONAL SPAIN el incumplimiento del principio de seguridad de los datos personales que constan en sus ficheros.

El Art. 7 del Convenio Nº 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, establece:

"Seguridad de los datos:
Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados".

El Art 17.1 de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, establece:

"Seguridad del tratamiento:
1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse"

La LOPD, traspuso al ordenamiento interno el contenido de la Directiva 95/46. En el artículo 9 de la citada LOPD se dispone lo siguiente:

"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 la 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".

El trascrito artículo 9 de la LOPD establece el *"principio de seguridad de los datos"* imponiendo la obligación de adoptar las medidas de índole técnica y organizativa que garanticen dicha seguridad, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el *"acceso no autorizado"* por parte de terceros.

Para poder delimitar cuáles sean los accesos que la Ley pretende evitar exigiendo las pertinentes medidas de seguridad es preciso acudir a las definiciones de *"fichero"* y *"tratamiento"* contenidas en la LOPD.

En lo que respecta al concepto de "*fichero*" el artículo 3.b) de la LOPD lo define como *"todo conjunto organizado de datos de carácter personal",* con independencia de la modalidad de acceso al mismo.

Por su parte el artículo 3.c) de la citada Ley Orgánica considera tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente procedimiento, la *"comunicación"* o *"consulta"* de los datos personales tanto si las operaciones o procedimientos de acceso a los datos son automatizados o no.

Sintetizando las previsiones legales puede afirmarse que:

a) Las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso, –la comunicación o consulta- de datos personales, es un tratamiento sometido a las exigencias de la LOPD.

b) Los ficheros que contengan un conjunto organizado de datos de carácter personal así como el acceso a los mismos, cualquiera que sea la forma o modalidad en que se produzca están, también, sujetos a la LOPD.

c) La LOPD impone al responsable del fichero la adopción de medidas de seguridad, cuyo detalle se remite a normas reglamentarias, que eviten accesos no autorizados.

d) El mantenimiento de ficheros carentes de medidas de seguridad que permitan accesos o tratamientos no autorizados, cualquiera que sea la forma o modalidad de éstos, constituye una infracción tipificada como grave.

Las medidas de seguridad se clasifican en atención a la naturaleza de la información tratada, esto es, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la misma. Dichas medidas, en el caso que nos ocupa, deben salvaguardar la confidencialidad y seguridad de los datos de carácter personal contenidos en los ficheros de la entidad BINTERNATIONAL SPAIN, relativos a los usuarios de su web www.binternational.es, correspondiendo adoptar las de nivel medio en atención al tipo de información que contiene, tal como se especifica en los artículos 80 y siguientes del RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Las medidas de seguridad de nivel básico están reguladas en los artículos 89 a 94, las de

nivel medio se regulan en los artículos 95 a 100 y las medidas de seguridad de nivel alto se regulan en los artículos 101 a 104, del Reglamento de desarrollo de la LOPD.

Los artículos 91 y 93 del citado Reglamento, aplicable a todos los ficheros y tratamientos automatizados, establecen:

"Artículo 91. Control de acceso.

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.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.
5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio".

Este artículo desarrolla las previsiones que deberá establecer el responsable del fichero para garantizar que los usuarios con accesos a datos personales o recursos, por haber sido previamente autorizados, sólo puedan acceder a tales datos y recursos. Para ello es necesario que se implanten mecanismos de control para evitar que un usuario pueda acceder a datos o funcionalidades que no se correspondan con el tipo de acceso autorizado para el mismo, en función del perfil de usuario asignado.

"Artículo 93. Identificación y autenticación.

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".

El artículo 5.2.b) del citado Reglamento define la "autenticación" como el procedimiento de comprobación de la identidad de un usuario; y el mismo artículo, letra h), se refiere a la "identificación" como el procedimiento de reconocimiento de la identidad de un usuario. Corresponde al responsable del fichero o tratamiento comprobar la existencia de la autorización exigida en el citado artículo 91, con un proceso de verificación de la identidad de la persona (autenticación) implantando un mecanismo que permita acceder a datos o recursos en función de la identificación ya autenticada. Cada identidad personal deberá estar asociada con un perfil de seguridad, roles y permisos concedidos por el responsable del fichero o tratamiento.

La vulneración de los preceptos citados aparece tipificada como infracción grave en el artículo 44.3.h) de la LOPD, que considera como tal, *"Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".*

En definitiva, la entidad BINTERNATIONAL SPAIN está obligada a adoptar, de manera efectiva, las medidas técnicas y organizativas previstas para sus ficheros, y, entre ellas, las dirigidas a impedir el acceso no autorizado por parte de terceros a los datos personales que constan en los mismos. En este caso, sin embargo, la citada entidad incumplió esta obligación, al haber quedado acreditada la posibilidad de acceder, sin restricción alguna, a los datos personales relativos a los usuarios de su web a través de la "Zona de usuarios" habilitada en la misma, en concreto a los datos curriculares con detalle de los datos personales identificativos, formación académica y experiencia profesional.

En concreto, consta en los Hechos Probados que el mencionado sitio web tiene habilitada una zona de usuarios que permite a los mismos, una vez identificados y autenticados a través de un código de usuario y una contraseña, acceder a sus CV, generándose una URL visible en pantalla con la siguiente configuración ***www...../.....*** siendo xxxxx el número asignado al documento del usuario de que se trate; y que, modificando el dato de "id" de la URL que se genera en el acceso, se podía visualizar y obtener copia de los CV de otros usuarios de la entidad, en formato pdf.

Se trata de deficiencias apreciadas en el sistema de información diseñado por la propia entidad BINTERNATIONAL SPAIN que quedaron acreditadas por la documentación aportada por el denunciante y por las comprobaciones realizadas por los Servicios de Inspección, habiendo sido reconocidos por la propia entidad imputada.

Así, los datos personales de los usuarios de la web www.binternational.es, resultaron accesibles por parte de otros usuarios terceros, siendo ello consecuencia de una insuficiente o ineficaz implementación de las medidas de seguridad. Dado que ha existido vulneración del *"principio de seguridad de los datos"*, se considera que BINTERNATIONAL SPAIN ha incurrido en la infracción grave descrita. BINTERNATIONAL SPAIN es responsable de la infracción señalada, habiendo quedado justificada, al menos, una falta de la diligencia debida en los hechos constatados plenamente imputable a dicha entidad.

Así lo ha declarado la Audiencia Nacional en un supuesto similar, examinado en la Sentencia de fecha 24/09/2010, en cuyo Fundamento de Derecho Séptimo se indica lo siguiente:

"A pesar de dichas alegaciones de la demanda y de conformidad con la normativa y la doctrina de esta Sala que se han expuesto en el fundamento jurídico anterior, consideramos que la infracción del deber de seguridad impuesta a XXX a tenor del artículo 9 de la LOPD, ha de ser confirmada por la misma.
Y ello dado que dicha entidad actora, como encargada del tratamiento de los datos personales de la compañía de seguros, estaba obligada a adoptar, de manera efectiva, las medidas técnicas y organizativas necesarias previstas en la normativa de aplicación, respecto de los ficheros informáticos de aquella y, entre ellas, las dirigidas a impedir el acceso no autorizado de terceros a los datos de los solicitantes de seguros "on line", que eran los que se contenían en el fichero "clientes" de tal compañía de seguros, que, como se ha indicado, requerían medidas de seguridad de nivel alto.
Ha quedado acreditado, por el contrario, que XXX incumplió esta obligación, al posibilitar el acceso a datos de personas físicas sin que existiera un procedimiento de cifrado o cualquier otro

que garantizara que la información obtenida en dichos accesos no podía ser identificada o manipulada por terceros, como pudo comprobar la Inspección de Datos, a través de la Web…
Ha de tomarse en consideración que, contrariamente a lo invocado en la demanda, no solo podían acceder al referido fichero de datos aquellos a quienes cualquier solicitante de un seguro on line les hubiera dado la secuencia de caracteres de la URL generada por cada solicitud, sino que también, con gran facilidad, cualquier suscriptor de un seguro on line podía acceder a los datos personales de todos los demás suscriptores de seguros on line en dicha entidad… y ello con una simple operación consistente en intercambiar cualquiera de las de las equis o números finales de cada una de las URL generadas, por otro u otros números…
Consideramos, por todo ello, que XXX infringió lo dispuesto en el artículo 9 de la LOPD…".

Este acceso por terceros a los datos personales reseñados supone la comisión, por parte de BINTERNATIONAL SPAIN, de una infracción del artículo 9.1 de la LOPD, al haberse constatado que tales hechos se producen por una deficiente implementación de las medidas de seguridad obligatorias según la naturaleza y el nivel de seguridad asignado al fichero en cuestión.

Asimismo, las deficiencias de seguridad en los sistemas de información de quedan igualmente probadas considerando las medidas implementadas como consecuencia del incidente de seguridad reseñado. BINTERNATIONAL SPAIN, una vez tuvo conocimiento de la quiebre de seguridad denunciada, cerró el acceso no autorizado detectado, dejando al administrador de la web el acceso a las carpetas donde estaban alojados los CV, solicitó a Google la eliminación de las direcciones ***www...../*** de la cache de los motores de búsqueda y adoptó las medidas pertinentes para impedir la indexación de la web por motores de búsqueda, además de revisar los procedimientos de cambio de contraseñas y control de accesos en el documento de seguridad.

Posteriormente, los Servicios de Inspección comprobaron que al intentar acceder a la dirección web ***http://www.....***, se obtenía un mensaje de error.

V

En este caso, se concluye que BINTERNATIONAL SPAIN no había adoptado las medidas técnicas y organizativas apropiadas, habiéndose acreditado la existencia de una relación entre el acceso y la inexistencia o ineficacia de las medidas.

En todo caso, en esta materia se impone una obligación de resultado, que conlleva la exigencia de que las medidas implantadas deben impedir, de forma efectiva, el acceso a la información por parte de terceros. Esta necesidad de especial diligencia en la custodia de la información por el responsable ha sido puesta de relieve por la Audiencia Nacional en la misma Sentencia citada en el Fundamento de Derecho anterior, así como en su Sentencia de 11/12/2008 (recurso 36/08), en la que indica lo siguiente: *"Como ha dicho esta Sala en múltiples sentencias…se impone, en consecuencia, una obligación de resultado, consistente en que se adoptan las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros…la recurrente es, por disposición legal una deudora de seguridad en materia de datos, y por tanto debe dar una explicación adecuada y razonable de cómo los datos han ido a parar a un lugar en el que son susceptibles de recuperación por parte de terceros, siendo insuficiente con acreditar que adopta una serie de medidas, pues es también responsable de que las mismas se cumplan y se ejecuten con rigor".*

El principio de culpabilidad es exigido en el procedimiento sancionador y así la STC 246/1991 considera inadmisible en el ámbito del Derecho administrativo sancionador una

responsabilidad sin culpa. Pero el principio de culpa no implica que sólo pueda sancionarse una actuación intencionada y a este respecto el artículo 130.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, dispone *"sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aun a título de simple inobservancia."*

El Tribunal Supremo (STS 16 de abril de 1991 y STS 22 de abril de 1991) considera que del elemento culpabilista se desprende *"que la acción u omisión, calificada de infracción sancionable administrativamente, ha de ser, en todo caso, imputable a su autor, por dolo o imprudencia, negligencia o ignorancia inexcusable."* El mismo Tribunal razona que *"no basta...para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa" sino que es preciso "que se ha empleado la diligencia que era exigible por quien aduce su inexistencia."* (STS 23 de enero de 1998).

A mayor abundamiento, la Audiencia Nacional en materia de protección de datos de carácter personal, ha declarado que *"basta la simple negligencia o incumplimiento de los deberes que la Ley impone a las personas responsables de ficheros o del tratamiento de datos de extremar la diligencia..."* (SAN 29de junio de 2001).

Por otra parte, ha de señalarse que es la entidad BINTERNATIONAL SPAIN la responsable del fichero y, por tanto, la obligada última a garantizar la seguridad de los datos, asegurando la efectividad de las medidas adoptadas.

VI

El artículo 45.6 de la LOPD, introducido a través de la reforma operada por la Ley 2/2011, de 4 de marzo, de Economía Sostenible, dispone:

Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:

a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.
b) Que el infractor no hubiese sido sancionado o apercibido con anterioridad.

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento."

Trasladando las consideraciones expuestas al supuesto que nos ocupa, se observa que la infracción de la LOPD de la que se responsabiliza al denunciado es una infracción "grave"; que la denunciada no ha sido sancionada o apercibida por este organismo en ninguna ocasión anterior; y que concurren de manera significativa varias de las circunstancias descritas en el artículo 45.5 de la LOPD, concretamente, la ausencia de beneficios, el volumen de negocio o actividad de la entidad, así como el grado de intencionalidad apreciado y la regularización llevada

a cabo. Todo ello, unido a la naturaleza de los hechos que nos ocupan, justifica que la AEPD **no acuerde la apertura de un procedimiento sancionador y que opte por aplicar el artículo 45.6 de la LOPD.**

Ahora bien, es obligado hacer mención a la Sentencia de la Audiencia Nacional de 29/11/2013, (Rec. 455/2011), Fundamento de Derecho Sexto, que sobre el apercibimiento regulado en el artículo 45.6 de la LOPD y a propósito de su naturaleza jurídica advierte que "*no constituye una sanción*" y que se trata de "*medidas correctoras de cesación de la actividad constitutiva de la infracción*" que *sustituyen* a la sanción. La Sentencia entiende que el artículo 45.6 de la LOPD confiere a la AEPD una "*potestad*" diferente de la sancionadora cuyo ejercicio se condiciona a la concurrencia de las especiales circunstancias descritas en el precepto.

En congruencia con la naturaleza atribuida al apercibimiento como una alternativa a la sanción cuando, atendidas las circunstancias del caso, el sujeto de la infracción no es merecedor de aquella y cuyo objeto es la imposición de medidas correctoras, la SAN citada concluye que cuando éstas ya hubieran sido adoptadas, lo procedente en Derecho es acordar el archivo de las actuaciones.

Como se ha señalado, en el asunto que examinamos la denunciada adoptó con diligencia las medidas correctoras necesarias para adecuar su conducta a las exigencias de la LOPD. En concreto, se cerró el acceso no autorizado detectado, dejando al administrador de la web el acceso a las carpetas donde estaban alojados los CV; se instó a Google la eliminación de la información que pudiera existir en la cache de los motores de búsqueda y adoptó las medidas pertinentes para impedir la indexación de la web por motores de búsqueda, además de revisar los procedimientos de cambio de contraseñas y control de accesos en el documento de seguridad. Finalmente, la entidad BINTERNATIONAL SPAIN advirtió sobre su intención de desarrollar una nueva web con medidas de seguridad más amplias.

Por tanto, a la vista del pronunciamiento recogido en la SAN de 29/11/2013 (Rec. 455/2011) referente a los supuestos en los que **la denunciada ha adoptado las medidas correctoras oportunas,** de acuerdo con lo señalado **se debe proceder al archivo de las actuaciones.**

De acuerdo con lo señalado,

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

SE ACUERDA:

1.- ARCHIVAR el procedimiento **A/00024/2015** seguido contra la entidad BINTERNATIONAL SPAIN, S.R.L., con arreglo a lo dispuesto en el artículo 45.6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en relación con la denuncia por la infracción del artículo 9 de la LOPD.

2.- NOTIFICAR el presente Acuerdo a la entidad BINTERNATIONAL SPAIN, S.R.L. y a D. ***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 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 esta 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