Procedimiento Nº: A/00175/2012

RESOLUCIÓN: R/02516/2012

En el procedimiento A/00175/2012, instruido por la Agencia Española de Protección de Datos a D. ***B.B.B.***, vista la denuncia presentada por DÑA. ***C.C.C.***, y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha de 20/12/2011, tuvo entrada en esta Agencia un correo electrónico de Dña. ***C.C.C.*** (en lo sucesivo la denunciante), en el que manifiesta lo siguiente:

1. Al realizar una búsqueda en el buscador Google utilizando como criterio su número de teléfono móvil, el primer resultado consistía en un enlace a la URL " ***A.A.A.***" en el que era accesible en formato Microsoft Word su currículum vitae (CV), con detalle de sus datos identificativos, formación académica, experiencia profesional y fotografía.
2. El sitio web en el que están accesibles los datos corresponde a una empresa de Elche dedicada al entrenamiento y a la fisioterapia, a la que remitió por correo electrónico su currículum, pero a la que nunca autorizó su publicación.

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:

1. El titular del dominio "domopersonal.com" es D. ***B.B.B.*** (en lo sucesivo el denunciado).

2. En el Registro General de Protección de Datos consta inscrito, entre otros, un fichero denominado "CURRICULUM VITAE", cuya finalidad declarada es "GESTION DE LAS PERSONAS INTERESADAS EN LOS PROCESOS DE SELECCION DE LAS OFERTAS" y en el que el denunciado consta como responsable del fichero.

3. Respecto al periodo de publicación de los datos.
   3.1. El 22/12/2011 se constató que el documento que contenía el currículum vitae de la denunciante no era accesible en el sitio web "domopersonal.com", pero el documento era accesible mediante el acceso al servicio de caché proporcionado por el buscador Google (el servicio de caché de Google proporciona acceso temporal a versiones anteriores de las páginas publicadas en Internet así como ha páginas eliminadas. El periodo normal de permanencia de dichas copias depende de la frecuencia de actualización del buscador que, a su vez, depende de la importancia relativa conferida por los programas de búsqueda de Google al sitio web en concreto).
   3.2. El 17/01/2012 se constató que el citado documento no figuraba en los resultados de la búsqueda en el buscador, ni en el sitio web, ni en su servicio de caché.
   3.3. El 17/01/2012 se constato que, si bien el currículum de la denunciante no era accesible a través de la URL citada en los antecedentes, al acceder a la URL "comopersonal.com/cv" se mostraba el contenido de una carpeta del servidor web en el que constaba el currículum de otra persona.

4. En respuesta a la solicitud de información remitida por el inspector actuante, el denunciado remitió un escrito en el que manifiesta lo siguiente:
   4.1. El sitio web fue creado por él mismo, por lo que es el responsable del mismo.
   4.2. La información de que dispone de la denunciante es la proporcionada por ésta en su currículum.
   Aporta copia de un correo electrónico, remitido en fecha 03/06/2011 desde la cuenta "info@domopersonal.com" y dirigido a esa misma cuenta, en el que se notifica el alta de un nuevo currículum ubicado en la URL que se cita en los antecedentes.
   4.3. El mismo día que tuvo conocimiento de los hechos eliminó el currículum de la web e inició los trámites para que Google eliminara la URL correspondiente, trámite que tardó aproximadamente una semana.
   Aporta copia de un correo electrónico remitido por la denunciante el 22/11/2011, en el que esta le informaba que su currículum era accesible a cualquiera a través de un enlace de su sitio web.
   4.4. Como medida destinada a evitar que se reprodujese este problema de nuevo o alguno similar ha eliminado la posibilidad de enviar el currículum a través de la web.

TERCERO: Con fecha 30/08/2012, el Director de la Agencia Española de Protección de Datos, por virtud de lo dispuesto en el artículo 45.6 de la LOPD, acordó someter al denunciado a trámite de audiencia previa al apercibimiento, en relación con la denuncia por infracción de los artículos 9 de la LOPD y 91 y 93 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la citada Ley Orgánica, tipificada como grave en el artículo 44.3.d) de la misma norma.

Con tal motivo, se concedió al denunciado plazo para formular alegaciones, recibiéndose escrito del mismo en el que declara que, como responsable y encargado del fichero y del tratamiento de los datos, el mismo día en que tuvo conocimiento de los hechos eliminó el currículum en la web e inició los trámites ante Google para eliminar la URL correspondiente, para la eliminación del servicio de cache, que se resolvió en una semana.

Añade que, seguidamente, contrató una empresa informática para verificar que no existiera ninguna carpeta CV ni ningún dato referente a currículums vitae, exceptuando los propios del equipo de la empresa (aporta copia de una facturación emitida por la empresa contratada para llevara a cabo dichas comprobaciones, de fecha 25/09/2012), y ha eliminado la posibilidad de enviar el CV a través de su web.

HECHOS PROBADOS

1. El denunciado es titular del dominio "domopersonal.com".

2. En el Registro General de Protección de Datos consta inscrito un fichero denominado "CURRICULUM VITAE", cuya finalidad declarada es "GESTION DE LAS PERSONAS INTERESADAS EN LOS PROCESOS DE SELECCION DE LAS OFERTAS" y en el que el denunciado figura como responsable del mismo.

3. Con fecha 03/06/2011, a través de la web "domopersonal.com", la denunciante facilitó al denunciado su currículo vitae con detalle de sus datos identificativos, formación académica, experiencia profesional y fotografía. Según consta en el correo electrónico que notifica el alta de este CV, el documento correspondiente se ubicó en la URL " ***A.A.A.***".

4. La denunciante, mediante el buscador de Google, realizó una búsqueda utilizando como criterio su número de teléfono móvil, obteniendo como primer resultado un enlace a la URL " ***A.A.A.***" que permitía el acceso al CV facilitado por la misma al denunciado, en formato Word, reseñado en el Hecho Probado Tercero.

5. Con fecha 22/11/2011, la denunciante remitió al denunciado un correo electrónico comunicando que su CV era accesible a terceros a través de un enlace de su sitio web, con la URL indicada en los Hechos Probados Tercero y Cuarto.

6. Con fecha 22/12/2011, por los Servicios de Inspección de la Agencia Española de Protección de Datos se constató que el documento que contenía el CV de la denunciante no era accesible en el sitio web "domopersonal.com", pero sí lo era mediante el uso del servicio de caché proporcionado por el buscador Google, como resultado de la búsqueda realizada utilizando como criterio el número de línea de telefonía móvil de la denunciante

7. Con fecha 17/01/2011, por los Servicios de Inspección de la Agencia Española de Protección de Datos se constató que el CV de la denunciante no figuraba en los resultados de la búsqueda realizada mediante el buscador de Google, ni en el sitio web "domopersonal.com" ni en el servicio de caché de Google.

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 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).

III

El Titulo VII sobre *Infracciones y sanciones*, 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."

IV

Se imputa al denunciado 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.

Por su parte, el artículo 3.a) de dicha Ley añade que se entenderá por datos de carácter personal *"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 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos profesionales y a la libre circulación de estos datos, que dispone *"toda información sobre una persona física identificada o identificable (el «interesado»); 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".*

Para completar el sistema de protección en lo que a la seguridad afecta, el artículo 44.3.h) de la LOPD tipifica como infracción grave el mantener los ficheros *"...que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".*

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 recabados por el denunciado a través de la web "domopersonal.com", relativos a las personas que utilizan dicho canal para facilitar al mismo su CV, correspondiendo adoptar las calificadas de nivel medio, en atención al tipo de información que contiene, tal como se especifica en los artículos 80 y 81.2 del RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

El artículo 81.1 del citado Reglamento señala que *"Todos los ficheros o tratamiento de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico"*.

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 acceso 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.

En definitiva, el denunciado está obligado a adoptar, de manera efectiva, las medidas técnicas y organizativas necesarias previstas para los ficheros de la naturaleza indicada, y, entre ellas, las dirigidas a impedir el acceso no autorizado por parte de terceros a los datos personales que constan en sus ficheros.

En este caso, los hechos expuestos, en relación con la posibilidad de que por parte de terceros se pudiera acceder sin restricción, a través de Internet, a los datos personales contenidos en la base de datos del denunciado, según el detalle reseñado en los Hechos Probados, sin haber garantizado la seguridad de tales datos personales, suponen la comisión, por parte del mismo, de una infracción del artículo 9.1 de la LOPD, al haberse constatado que utilizando un buscador se obtuvieron resultados, con el número de teléfono de la denunciante como criterio de búsqueda, en el enlace " ***A.A.A.***", que incluye el detalle de los datos identificativos de aquélla, formación académica, experiencia profesional y fotografía, entre otros

Así, los datos personales recabados por el denunciado a través del sitio web "domopersonal.com" resultaron accesibles a terceros, siendo ello consecuencia de una insuficiente o ineficaz implementación de las medidas de seguridad detalladas. Dado que ha existido vulneración del *"principio de seguridad de los datos"*, se considera que el denunciado ha incurrido en la infracción grave descrita.

Tales hechos quedaron acreditados por la documentación aportada por la denunciante, que incluía el detalle de la información accesible a través de la URL " ***A.A.A.***", en la que figura sus datos personales antes citados; y por la constataciones realizadas por los Servicios de Inspección de la Agencia Española de Protección de Datos, que constan reseñadas en los Hechos Probados Sexto y Séptimo.

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 su Sentencia de 11/12/08 (recurso 36/08), fundamento cuarto: *"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".

V

El artículo 44.3.h) de la LOPD, considera infracción grave:

"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".

Dado que ha existido vulneración del *"principio de seguridad de los datos"*, recogido en el artículo 9 de la LOPD, se considera que el denunciado ha incurrido en la infracción grave descrita.

VI

La disposición final quincuagésima sexta de la Ley 2/2011, de 4 de marzo, de Economía Sostenible (BOE 5-3-2011), ha añadido un nuevo apartado 6 al artículo 45 de la LOPD, en lugar del existente hasta su entrada en vigor, del siguiente tenor:

"*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".

A este respecto, procede considerar lo establecido en el artículo 45.4 y 5 de la LOPD, que establece lo siguiente:

"4. La cuantía de las sanciones se graduará atendiendo a los siguientes criterios:

a) El carácter continuado de la infracción.

b) El volumen de los tratamientos efectuados.

c) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.

d) El volumen de negocio o actividad del infractor.

e) Los beneficios obtenidos como consecuencia de la comisión de la infracción.

f) El grado de intencionalidad.

g) La reincidencia por comisión de infracciones de la misma naturaleza.

h) La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.

i) La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia

exigible al infractor.

j) Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:

a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado 4 de este artículo.

b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.

c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.

d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.

e) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente".

En el presente supuesto se cumplen los requisitos recogidos en los apartados a) y b) del citado artículo 45.6 de la LOPD. Junto a ello se constata una cualificada disminución de la culpabilidad de la entidad denunciada por la concurrencia de varios criterios de los enunciados en el artículo 45.4 de la LOPD, concretamente, el grado de intencionalidad apreciado y que no constan beneficios obtenidos como consecuencia de la comisión de la presunta infracción, el volumen de negocio y que no consta vinculación de la actividad del denunciado con la realización de tratamientos de datos de carácter personal.

VII

De acuerdo con las manifestaciones efectuadas por el responsable de la entidad denunciado, y conforme a las constataciones efectuadas por los Servicios de Inspección de la Agencia Española de Protección de Datos, resulta que, en las últimas búsquedas realizadas con fecha 17/01/2012, no se obtuvieron resultados sobre información relativa a la denunciante. Además, consta que el denunciado contrató los servicios de una empresa informática para verificar que no existiera ninguna carpeta CV ni ningún dato referente a currículums vitae accesible a través de Internet, exceptuando los propios del equipo de la empresa, y ha informado que ha sido suprimida la posibilidad de enviar el CV a través de su web.

Por tanto, se entiende que el denunciado ha adoptado las medidas correctoras adecuadas y que no procede requerimiento alguno.

De acuerdo con lo señalado,

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

SE ACUERDA:

1.- APERCIBIR (**A/00175/2012**) a D. ***B.B.B.*** 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, tipificada como grave en el artículo 44.3.h) de la citada Ley Orgánica, respectivamente, y de conformidad con lo establecido en los artículos 36 y 37.a), f) y n) de la LOPD, que atribuye la competencia **al Director de la Agencia Española de Protección de Datos.**

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.

2.- NOTIFICAR el presente Acuerdo a D. ***B.B.B.***.

3.- NOTIFICAR el presente Acuerdo a DÑA. ***C.C.C.***.

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.