Expediente Nº: E/02402/2018

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante el Colegio Oficial de Médicos de Palencia, en virtud de denuncia presentada por Don ***A.A.A.,*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 20 de abril de 2018, tuvo entrada en esta Agencia un escrito remitido por Don ***A.A.A.*** en el que expone lo siguiente:

Con fecha 24 de marzo de 2018, constata, mediante una búsqueda realizada de su nombre y apellidos en Google, que entre los resultados obtenidos aparece un archivo en formato "pdf" denominado "*C.C.C.– Colegio Oficial de Médicos de Palencia*" al que se puede acceder y que contiene toda la documentación personal y clínica que el denunciante aportó en su día al Colegio Oficial de Médicos de Palencia y que fue presentada al Juzgado de lo Contencioso-Administrativo nº 1 de Palencia en el Procedimiento Abreviado B.B.B./2014 del que el denunciante fue parte demandante.

El citado archivo era accesible a través de internet y en relación con el denunciante contiene los siguientes documentos:

> Oficio de remisión al citado Juzgado de fecha 18 de junio de 2014, con sus datos personales y el índice de documentos que conforman el expediente.
>
> Denuncia formulada el 9 de julio de 2013 frente a una doctora de la Seguridad Social, en la que aparecen además de sus datos personales, información clínica relativa a su estado de salud.
>
> Resolución de alta médica de 26 de octubre de 2012 del INSS, con todos sus datos.
>
> Informe Psiquiátrico, de 19 de octubre de 2012, con sus datos personales y de salud.
>
> Informe Médico, de 29 de octubre de 2012, de la Gerencia de Atención Primaria de Palencia, con sus datos personales y de salud.
>
> Sentencia D.D.D./2013 de 26 de febrero, del Juzgado de Social nº 2 de Palencia, relativa a un procedimiento del que fue parte, con todos sus datos personales, laborales y de salud.
>
> Fotocopia de su D.N.I.
>
> Escrito de alegaciones de fecha 14 de noviembre de 2014, de la doctora de la Seguridad Social, donde constan sus datos de salud.
>
> Informe Jurídico Legal del Asesor Jurídico del Colegio Oficial de Médicos de Palencia, relativo a la reclamación presentada por el denunciante, en el que constan sus datos personales y de salud.

Informe de la Comisión Deontológica del Colegio de Médicos de 18 de diciembre de 2013.

Todos estos documentos que forman parte del citado archivo, han estado accesibles en internet al menos desde el 24 de marzo de 2018; no obstante, desconoce el tiempo durante el que han sido expuestos.

Así mismo, también desde el 24 de marzo de 2018, se puede acceder a 900 carpetas con documentación del Colegio de Médicos de Palencia, en la página web: www.compalencia.org/live que corresponde al citado Colegio. Según manifiesta en la fecha en la que formula la denuncia ya no es posible acceder a ésta información.

El número de archivos PDF encontrados con información del colegio asciende aproximadamente a 3340 archivos, de los que aporta una muestra de 862 archivos, de entre 2012 y 2018. Entre los documentos accesibles se encuentran:

De ciudadanos y pacientes: (reclamaciones, certificados de defunción etc…)

De trabajadores del Colegio Oficial de Médicos de Palencia (ordenes de transferencia bancaria de las nóminas de la totalidad de los trabajadores con sus números de cuenta bancaria.)

De médicos colegiados (certificados, vida laboral, puestos de trabajo ocupados en administración pública, reclamaciones, etc…)

Del propio Colegio Oficial de Médicos, estos documentos suponen alrededor de un 5% de los documentos accesibles, en general no contienen datos personales.

El denunciante aporta un DVD que, según manifiesta, contiene dos carpetas: una denominada " ***C.C.C.***" que contiene los documentos accesibles a través de internet en los que constan sus datos y otra denominada COLMEDICOS-AFECTADOS que contiene las carpetas por años desde el 2012 al 2018 con los documentos que descargo como prueba de su publicación en la citada página web.

Con fecha 16 de mayo de 2018 se examina el contenido del CD aportado por el denunciante, no pudiendo acceder al contenido de la mayoría de los archivos (se accede a uno que contiene la búsqueda realizada en Google del nombre y apellidos del denunciante y del resultado de la misma, donde consta el fichero "PDF" "*C.C.C.– Colegio Oficial de Médicos de Palencia*". También se verifica en esa fecha que en la página web www.compalencia.org/live no se encuentra accesible la documentación que indica el denunciante.

Con fecha 22 de mayo de 2018, se solicita al denunciante que aporte la de nuevo la documentación que contenía el CD aportado, dado que no se podía acceder la mayor parte de su contenido.

En contestación a la solicitud, el denunciante aporta en su escrito, de fecha 1 de junio de 2018, copia de casi 900 documentos que, según manifiesta, fueron descargados de la página web www.compalencia.org en marzo de 2018, y que contienen datos personales de profesionales médicos, pacientes, etc… de los años 2012, 2014 y 2016. Entre los documentos del año 2014 se encuentran los relativos al denunciante. Así mismo, aporta un dispositivo de memoria USB que contiene, según manifiesta, la documentación impresa así como varios programas que pueden facilitar el acceso a los ficheros que contiene.

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:

Con fecha 16 de mayo de 2018, se realiza una búsqueda en Google del nombre y apellidos del denunciante, no obteniendo como resultado ningún fichero con sus datos personales publicado en la página web del Colegio de Médicos de Palencia www.compalencia.org.

Así mismo, con esa fecha, se realiza una búsqueda en Google de la página web www.compalencia.org/live/data, verificando que en los resultados que ofrece figuran algunos ficheros en formato "pdf", pero no se puede acceder al contenido de ninguno de ellos, dado que la página devuelve un mensaje de error al intentar abrirlos.

Con fecha 5 de julio de 2018, EL ILUSTRE COLEGIO DE MEDICOS DE PALENCIA (en adelante el Colegio), ha remitido a esta Agencia la siguiente información en relación con los hechos denunciados:

1. Con fecha 5 de marzo de 2018, se actualizó el motor de la web www.compalencia.org, que está desarrollada en un CMS (Programa de Sistema de Gestión de Contenidos) propio que se actualiza regularmente con parches de seguridad y otras mejoras.

2. Con fecha 24 de marzo de 2018, según consta en la denuncia, a través de la dirección www.compalencia.org/live se tenía acceso a un número de archivos situados en las carpetas que se detallan en la misma.

3. El acceso a dichos archivos era posible a través de un protocolo de conexión segura (https), donde como consecuencia de un script (programa), subido por un usuario malintencionado al directorio de la página web, se activó la función "directoryIndex" del servidor. El origen del ataque (hackeo) es desconocido. El fichero con el programa fue subido con fecha aproximada de 20 de marzo.

   "*Según la información obtenida en internet, la directiva "directoryIndex" establece la lista de recursos que se deben buscar cuando el cliente solicita el índice de un directorio del sitio. La URL que se especifica a continuación es relativa al directorio solicitado (por lo general, se trata del nombre de un archivo dentro del mismo) DirectoryIndex permite que se especifiquen varias URLs, haciendo que el servidor devuelva la primera que encuentre. En el caso de ninguna de las URLs exista y que esté seteada la opción Indexes, se devolverá un listado del directorio*."

4. El servidor donde se encuentra alojada la página web del Colegio dispone de un antivirus que no detecto el programa como un virus por lo que el hackeo pasó desapercibido ante todas las medidas de seguridad del servidor.

5. Con fecha 3 de abril de 2018, una colegiada dio aviso al Colegio, mediante una llamada de teléfono, de que un usuario de la página había localizado su número de teléfono en el buscador Google, dentro de una ficha de inscripción a un curso, la ficha estaba alojada en la página web del Colegio.

6. Con esa misma fecha, el Colegio traslada la incidencia a la empresa NDS (Net Design Estudio) encargada del mantenimiento de la página web.

7. La empresa detecta que la página web ha sufrido un ataque (hackeo) que consiste en que un usuario ha insertado un programa en el directorio de la página con el que se puede acceder a todas las carpetas del servidor y a los documentos que contienen, incluso modificarlos o eliminarlos.
8. El mismo día 3 de abril, se corrige la incidencia de seguridad siguiendo los siguientes pasos:
    a. Se elimina el programa dañino.
    b. Se elimina la función "directoryIndex"
    c. Se reconfigura el servidor eliminando las posibles vulnerabilidades insertadas con el programa.
    d. Se compara el resultado con una copia de seguridad por si existiera algún otro fichero modificado pero no se encuentra ninguno.
    e. Se examina la vulnerabilidad por la que un usuario hubiera podido insertar el programa maligno, comprobando que en el formulario de altas de colegiados existente en la web se podían adjuntar ficheros (documentación y certificados necesarios para colegiación). Se elimina el formulario y se desactiva.
    f. Se detecta que Google ha indexado alguna de las carpetas privadas a las que se tenía acceso y se solicita al buscador que elimine todos los contenidos indexados (aunque ya no son accesibles) pero que pueden haber quedado guardados en la memoria "caché) del buscador.
9. Respecto a la posible utilización por terceros de los datos personales obtenidos como consecuencia del ataque: Según manifiestan, no existen registros de acceso a los directorios donde se encontraban los documentos, al haber transcurrido más de un mes; no obstante, no tienen constancia de que se hayan utilizado datos personales por terceros, excepto lo que consta en la denuncia.
10. Aportan copia del Registro de Incidencias, donde consta la comunicación de la misma con fecha 3 de abril de 2018 y su resolución con esa misma fecha. Así mismo, se detallan todas las acciones realizadas para su resolución.
11. Por último manifiestan que el denunciante que detecto la vulnerabilidad, con fecha 24 de marzo de 2018, no comunicó la misma al Colegio, lo que impidió que se pudiera resolver la incidencia de forma inmediata, tampoco comunicó la incidencia a la Agencia hasta el 16 de abril, cuando ya se había resuelto.

    Desde el 24 de marzo, hasta el 3 de abril (fecha en que se resuelve la incidencia), el denunciante ha tenido acceso y se ha descargado multitud de documentación de naturaleza confidencial, desconociendo si han podido tener acceso a la misma terceras personas.

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

Teniendo en cuenta la fecha en la que se produjeron los hechos denunciados, entre el 24 de marzo y el 3 de abril de 2018, resultan de aplicación las previsiones contenidas en la LOPD, al no resultar aplicable, en este caso, el Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos, aunque en vigor desde mayo de 2018.

III

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.

El Colegio tiene como actividad la realización de servicios de gestión y administración relacionados con los colegiados, lo que conlleva, entre otras, el tratamiento de los datos personales relativos a las personas que se relacionan y encargan dichas actividades.

En el presente caso, el denunciante ha manifestado que tras realizar una búsqueda de su nombre y apellidos en Google, entre los resultados obtenidos aparece un archivo en formato "pdf" denominado "*C.C.C.– Colegio Oficial de Médicos de Palencia*" al que se puede acceder y que contiene toda la documentación personal y clínica que había aportado en su día al Colegio Oficial de Médicos de Palencia y que fue presentada al Juzgado de lo Contencioso-Administrativo nº 1 de Palencia en el Procedimiento Abreviado B.B.B./2014 del que el denunciante fue parte demandante.

De la información aportada al expediente y de la recabada por los servicios de inspección de este centro directivo durante la fase de actuaciones previas, consta acreditado que e acceso a dichos archivos era posible a través de un protocolo de conexión segura (https), donde como consecuencia de un script (programa), subido

por un usuario malintencionado al directorio de la página web, se activó la función "directoryIndex" del servidor. El origen del ataque (hackeo) es desconocido. El fichero con el programa fue subido con fecha aproximada de 20 de marzo.

> "*Según la información obtenida en internet, la directiva "directoryIndex" establece la lista de recursos que se deben buscar cuando el cliente solicita el índice de un directorio del sitio. La URL que se especifica a continuación es relativa al directorio solicitado (por lo general, se trata del nombre de un archivo dentro del mismo) DirectoryIndex permite que se especifiquen varias URLs, haciendo que el servidor devuelva la primera que encuentre. En el caso de ninguna de las URLs exista y que esté seteada la opción Indexes, se devolverá un listado del directorio*."

Según las comprobaciones realizadas, el acceso a los datos registrados en los sistemas de JALD fue perpetrado por parte de terceros desconocidos con importantes conocimientos técnicos, no habiendo sido posible determinar su autoría. El servidor está alojado en una página web del Colegio con antivirus.

Esta circunstancia, en sí misma, no es suficiente para exonerar de responsabilidad al Colegio; es necesario que el acceso indebido no se aprovechara de vulnerabilidades del sistema atacado que tuvieran causa en una falta de medidas de seguridad adecuadas o en una ineficaz implantación de las mismas.

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 este caso, no se ha constatado que la denunciada haya incumplido la obligación de adoptar de manera efectiva las medidas dirigidas a impedir el acceso no autorizado por parte de terceros a los datos personales, visibles a través del buscador Google, desconociéndose la causa por la que los documentos fueron indexados por lo que no cabe entender infringido el artículo 9 de la LOPD.

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, señaló 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..., 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 19D.D.D./246), señaló que la culpabilidad constituye un principio básico del Derecho administrativo sancionador. Culpabilidad, que no concurre en la conducta analizada de xxx".

En el presente caso, resulta destacable la diligencia observada por parte de la entidad tras detectarse el acceso indebido a la información para minimizar los riesgos y asegurar sus sistemas; el mismo día se corrige la incidencia, eliminando el programa dañino; se elimina la función “directoryIndex”; se reconfigura el servidor eliminando las posibles vulnerabilidades insertadas con el programa; se compara el resultado con una copia de seguridad por si existiera algún otro fichero modificado; se examina la vulnerabilidad por la que un usuario hubiera podido insertar el programa maligno, comprobando que en el formulario de altas de colegiados existente en la web se podían adjuntar ficheros (documentación y certificados necesarios para colegiación). Se elimina el formulario y se desactiva; se detecta que Google ha indexado alguna de las carpetas privadas a las que se tenía acceso y se solicita al buscador que elimine todos los contenidos indexados (aunque ya no son accesibles) pero que pueden haber quedado guardados en la memoria “caché) del buscador.

IV

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.”

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 al Colegio Oficial de Médicos de Palencia, y a Don ***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 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