Expediente Nº: E/02950/2016

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad LABORATORIO LUCAS NICOLAS, S.L., en virtud de denuncia presentada por la ASOCIACION NACIONAL DE FRANQUICIADOS VITALDENT, y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 12 de abril de 2016, se recibió en esta Agencia un escrito remitido por Don ***A.A.A.***, en representación de la Asociación Nacional de Franquiciados VITALDENT, en el que denuncia que todos los franquiciadas suscriben un contrato de franquicia con la entidad denunciada en el que, entre otros aspectos, se indica que son responsables de los ficheros de sus pacientes. No obstante, con el sistema informático implantado por el franquiciador y su sistema de acceso, impide al franquiciado cumplir con lo establecido en la LOPD.

Asimismo, manifiesta que tras la intervención judicial producida en febrero de 2016, el sistema quedó bloqueado, impidiendo el acceso a los franquiciados, a la totalidad de los datos de los pacientes. Además, con fecha 14/03/2016 se comunicó por Burofax a los franquiciados, la habilitación de un nuevo entorno alternativo, no obstante éste es inoperativo, ya que a través del mismo no puede recopilarse toda la información de los pacientes.

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. Con fecha 4 de octubre de 2016, se realizó inspección en los locales de la entidad Laboratorio Lucas Nicolás, S.L. (VITALDENT), en el transcurso de la cual se puso de manifiesto que:

   1.1. El Objeto social de la entidad LABORATORIO LUCAS NICOLAS, S.L. (en adelante el Franquiciador), es entre otros: *El montaje, instalación, explotación, administración de clínicas médicas, odontológicas y estomatológicas, de cirugía estética y de cualquier otra especialidad médica.*

   1.2. El franquiciador tiene una antigüedad de aproximadamente 25 años y cuenta con 150 clínicas propias y 180 franquicias, aproximadamente.

   1.3. Tanto las empresas que deciden suscribir un contrato de Franquicia, como las clínicas propias utilizan para su funcionamiento una Plataforma centralizada a través de un programa de gestión de pacientes, denominado ULYSES.

   1.4. El acceso a la citada Plataforma se realiza a través de Internet, para ello se realiza una adecuación tecnológica para cada clínica, asignando desde el Proveedor de servicios de internet, una línea cifrada y segura para que se conecte a la Red Privada de la entidad, a través de la cual la información se

transmite cifrada. Mediante esta conexión segura cada clínica accede a la citada Plataforma.

1.5. Desde el Departamento de Sistemas de la entidad se asignan los usuarios y contraseñas a las personas que van a acceder a la Plataforma. Dicha contraseña debe ser modificada la primera vez que entren en la misma. Existen diferentes perfiles de acceso en función del puesto de trabajo que desarrollo cada usuario.

1.6. Con la apertura de una nueva clínica, el Franquiciador imparte un curso de Formación para el manejo de la aplicación, en el que se hace entrega de un Manual de usuario, que contiene toda la información necesaria para el buen uso de la aplicación ULYSES.

1.7. Cuando se producen cambios en la aplicación que suponen una actualización en la versión de ULYSES utilizada por los usuarios, se remite un correo explicativo de dichos cambios y el momento en que se realizará la actualización, siempre en horario nocturno para no interrumpir el funcionamiento de las clínicas.

1.8. Cada clínica tiene que inscribir en el Registro General de Protección de Datos su propio fichero de pacientes, en el que figurara como responsable, la propia clínica y como encargado del tratamiento el Franquiciador, ya que todos los ficheros son incorporados al fichero PACIENTES que tiene inscrito el Franquiciador en el Registro General de Protección de Datos con el código ***CÓD.1, del que es Responsable, y a través del cual se lleva a cabo la gestión de pacientes mediante la aplicación ULYSES.

1.9. Desde la clínica se incorporan todos los datos de los pacientes, tanto personales como clínicos y económicos, información a la que el franquiciador tiene acceso. No obstante, cada clínica puede replicar el fichero de pacientes en sus sistemas, pero no se puede hacer desde la aplicación.

1.10. Cada clínica solo tendrá acceso a través de la Plataforma, a los datos de sus pacientes, en ningún momento puede ver datos de pacientes de otras clínicas. En el hipotético caso de que desde una clínica sea necesario ver los datos de un paciente perteneciente a otra, el interesado debe prestar su consentimiento y ha de solicitarse por escrito a la clínica donde se encuentra su historia.

1.11. Las copias de seguridad de la Base de Datos de la Plataforma, solo las puede realizar el Franquiciador, las clínicas no tienen acceso a la realización de copias.

1.12. La Base de Datos que contiene todos los ficheros de pacientes de los franquiciados, se encuentra alojada en una NUBE, ubicada en un Hosting primario denominado ESPACIO RACK y es replicada en tiempo real en un Hosting secundario, denominado GLOBAL SWITCH.

1.13. El Franquiciador tiene contratado los servicios de Hosting con la entidad IAAS365, S.L., el cual ha emitido un certificado de ubicación física de CPD's, que se adjunta a esta Actuaciones de investigación, donde figura que tanto la ubicación del Hosting primario como el de respaldo, se encuentran en la Comunidad de Madrid.

1.14. No obstante, ya que la clínica puede tener en paralelo un fichero generado por ellos a imagen del incluido en la Plataforma, puede hacer sus propias copias de

seguridad, como responsable del fichero de sus pacientes, pero no puede descargarse ni el fichero ni las copias a través de la Plataforma.

1.15. En el caso de que una clínica no cuente con un fichero de pacientes en paralelo y necesite una copia de seguridad, tiene que solicitarla al Franquiciador, éste le hará entrega de la misma, bien vía telemática o en un soporte físico.

1.16. Las clínicas cuentan con un fichero de Historias clínicas en papel, pero el Franquiciador no tiene acceso a la información contenida en el mismo.

1.17. Con fecha 16 de febrero de 2016, se produjo una intervención judicial a VITALDENT (Franquiciador) y se procedió, por parte de la autoridad, al bloqueo de los sistemas informáticos de la misma, de tal manera que las clínicas que no tuvieran duplicado el fichero en sus propios sistemas informáticos, no tendría acceso a la información existente de sus pacientes en la Plataforma.

1.18. En ese momento se empieza a trabajar para proporcionar a las clínicas un sistema alternativo de acceso mediante SFTP (entorno seguro), al que se conectarían con un usuario y contraseña proporcionado por el Franquiciador, para que pudieran tener acceso a las agendas y a la historia clínica.

1.19. No obstante, el bloqueo duró 36 horas, después se pudo acceder a la Plataforma como habitualmente se venía haciendo, hecho que fue comunicado a través de correo electrónico a todas las clínicas. Se adjuntan al Acta de inspección, varios correos relativos a esta información, entre las clínicas y el Franquiciador.

1.20. Con relación al ejercicio de los derechos ARCO por parte los pacientes, éstos pueden ser ejercidos directamente a través de las clínicas o mediante envío a la dirección del Franquiciador. El paciente es informado de este aspecto y de la cesión de los datos al Franquiciador, mediante una cláusula contenida en el documento “Información de diagnóstico”, que ha de cumplimentar cuando acude a la consulta para tratamiento, y que dice literalmente: *Asimismo, y salvo que manifieste lo contrario, usted consiente expresamente que su datos personales sean comunicados, para las finalidades arriba señaladas, a las entidades propias del Grupo Vitaldent, controladas por el franquiciador Laboratorio Lucas Nicolás, S.L., a cuyos ficheros quedaran incorporados sus datos personales. Le informamos que respecto a este tratamiento de datos puede ejercer sus derechos de acceso, rectificación, cancelación y oposición mediante petición por escrito firmada adjuntando copia de su documento nacional de identidad o de cualquier otra documentación que le identifique dirigida a la siguiente dirección; (C/...1)de Madrid.*.

1.21. No obstante, desde las clínicas, mediante acceso a la aplicación, pueden dar cumplimiento al derecho de acceso y al de rectificación de datos del paciente.

1.22. El Franquiciador cuenta con contratos marco con diferentes financieras para facilitar a los pacientes la financiación de los servicios de odontología. Cuando un paciente está interesado en la financiación, desde la clínica se realiza la tramitación de la solicitud, para lo cual se le hace entrega de un cuestionario que debe cumplimentar, éste es remitido a la financiera la cual debe decir la documentación, en su caso que debe aportar. La documentación es entregada en la clínica para que la haga llegar a la financiera correspondiente, no obstante no queda en poder de la clínica ninguno de los documentos. El franquiciador no tiene acceso a esta información y documentación.

1.23. Cuando una clínica resuelve el contrato y se da de baja, puede ocurrir que, el franquiciado decida ejercer la actividad por su cuenta y como excepción a las cláusulas contractuales, se le hace entrega de la Base de Datos en formato exportable, y se regula en un documento suscrito por ambas partes. No obstante los datos de los pacientes de esa clínica no se borran del fichero PACIENTES que se gestiona en la Plataforma.

1.24. En el caso de que se resuelva el contrato y existan pacientes en activo, éstos son informados mediante carta conjunta de la clínica y el Franquiciador, comunicándole el cierre de la clínica y la opción de cesión de su historial a una nueva clínica.

Una representante del Administrador Judicial, que actúa en los locales donde se realiza la inspección, manifiesta que desde el Juzgado se les ha dado traslado de una denuncia presentada por la Asociación Nacional de Franquiciados de Vitaldent, haciendo entrega de las alegaciones presentadas desde esta Administración Judicial con relación a estos mismos hechos denunciados, entre las que se encuentran las siguientes:

Con relación a la denuncia ante la Agencia de Protección de Datos adjunta a la citada denuncia ante el Juzgado manifiestan que:

- La denuncia ante la Agencia, parece que tiene como finalidad generar cierta preocupación al Juzgado haciendo creer que estos hechos están provocando un problema de salud pública. Cuestión que niegan rotundamente.

- Ningún franquiciado ha dejado de realizar intervenciones con causa en la no disposición de historia clínica, si bien la actividad del Grupo VITALDENT, se vio gravemente afectada por el impacto mediático de la intervención Judicial.

De la supuesta privación del libre acceso a la base da datos de los pacientes integrados en el sistema informático ULYSES:

- La privación del acceso fue un hecho puntual. No obstante, esta interrupción duro 48 horas, ya que el sistema fue interrumpido por orden del Juzgado al intervenir la UDEF las oficinas del franquiciador el día 16 de febrero de 2016. Una vez finalizada dicha intervención policial, el sistema ULYSES fue restablecido y hasta el momento ha continuado funcionado con total normalidad.

De las medidas ya adoptadas para salvaguardar la información ante posibles eventualidades:

- Como consecuencia de la interrupción del sistema ULYSES durante el breve espacio de tiempo descrito, desde el Departamento de sistemas se ha creado un entorno seguro (SFTP) independiente de la red corporativa, al que se puede acceder desde cualquier punto, que contiene los datos clínicos de los pacientes. Así en el futuro, ante cualquier eventualidad ninguna clínica se encontraría privada de la información clínica de sus pacientes. Por lo tanto, los franquiciados han tenido y tienen, actualmente, acceso a los datos clínicos de sus pacientes. Dicho lo cual, esa parte niega cualquier tipo de incumplimiento del contrato de franquicia..

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

En primer lugar, y en referencia a los contratos de franquicia y la posición, desde la perspectiva de la normativa de protección de datos, del franquiciador y del franquiciado, recogemos en este Fundamento, las consideraciones de un informe del Gabinete Jurídico de esta Agencia, en el que se señala lo siguiente:

<<En el presente supuesto debe tomarse como punto de partida que tal y como señala el artículo 62.1 de la Ley 7/1996, de 15 enero, de Ordenación del Comercio Minorista "la actividad comercial en régimen de franquicia es la que se lleva a efecto en virtud de un acuerdo o contrato por el que una empresa, denominada franquiciadora, cede a otra, denominada franquiciada, el derecho a la explotación de un sistema propio de comercialización de productos o servicios".

Del mencionado concepto se desprende, obviamente, la distinta personalidad jurídica de las partes intervinientes en el contrato, así como el hecho de la absoluta independencia de las mismas en lo que al régimen de personal y clientela se refiere, siendo así que el único elemento puesto en común es el relacionado con el sistema de comercialización de la franquiciadora, que es cedido a la entidad franquiciada

Por este motivo, al existir esa completa independencia, cada una de las entidades resultará obligada independiente y separadamente al cumplimiento de sus correspondientes obligaciones legales, constituyendo cualquier intercambio de datos entre ambas empresas una auténtica cesión de datos de carácter personal, definida por el artículo 3 i) de la Ley Orgánica 15/1999 como "toda revelación de datos realizada a una persona distinta del interesado".

Tal cesión debe sujetarse al régimen general de comunicación de datos de carácter personal establecido en el artículo el artículo 11 de la misma Ley, donde se establece que la misma solo puede verificarse para el cumplimiento de fines directamente relacionados con las funciones legitimas del cedente y cesionario y exige, para que pueda tener lugar, el consentimiento del interesado (artículo 11.1), otorgado con carácter previo a la cesión y suficientemente informado de la finalidad a que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar (artículo 11.3), y que debe recabar el cedente como responsable del fichero que contiene los datos que se pretenden ceder. De la obligación de obtener el consentimiento del interesado quedan solamente exceptuados determinados supuestos recogidos en el artículo 11.2 que no resultan de aplicación al caso que nos ocupa.

Asimismo, debe recordarse, teniendo en cuenta que el consultante es una clínica y por consiguiente trata datos de salud de sus clientes, que los datos relativos a la salud quedan sometidos al régimen específico establecido por el artículo 7.3 de la Ley Orgánica 15/1999, a cuyo tenor "Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente".

En este sentido, la Agencia Española de Protección de Datos ha puesto reiteradamente de manifiesto que la aplicación del artículo 7.3 implica, por mor del principio de especialidad, la imposible aplicación a los datos referidos en el mismo de cualquiera de las causas legitimadoras de cesión inconsentida previstas en el artículo 11.2 de la Ley Orgánica, quedando limitados los supuestos habilitantes del tratamiento y cesión de estos datos a los establecidos en la norma especial o a aquéllos en los que la norma general se refiere expresamente a tales datos (como sucede en relación con los datos de salud en el artículo 11.2 f) de la Ley Orgánica 15/1999).

En particular, en cuanto a la cesión de datos relacionados con la historia clínica debe acudirse a lo previsto en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, cuyo artículo 16 regula los posibles accesos a la historia clínica, disponiendo en sus apartados 2 a 5 lo siguiente:

"2. Cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten.

3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y en la Ley 14/1986, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

4. El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones.

5. El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria."

De lo señalado en el precepto que acaba de analizarse se desprende que la cesión de datos relacionados con la salud de sus clientes no se encuentra amparada en lo previsto por la legislación reguladora del tratamiento de datos en las historias clínicas, dado que el artículo 16.3 no la contempla.

En consecuencia, la empresa consultante será responsable de los ficheros por ella creados para el cumplimiento de sus fines, configurándose el acceso por parte de otra empresa a los datos obrantes en sus ficheros, con independencia de la existencia de un contrato de franquicia entre ambas, como una cesión de datos personales que, si no es consentida por el interesado en los términos vistos o se encuentra amparada en alguno de los supuestos en que la Ley lo permite, sean los contemplados en el artículo 11 de la Ley Orgánica 15/1999 con carácter general o los señalados por el artículo 7.3 de la misma Ley cuando se trata de datos relacionados con la salud, constituirá una

vulneración de la citada Ley, vulneración agravada cuando se trate de éstos últimos.

II

En cuanto a la relación que se establece entre el consultante y la empresa que presta el servicio informático cabe señalar que se adjunta a la consulta un contrato celebrado con ésta el que se afirma que dicha empresa ostenta la condición de encargado del tratamiento.

La figura del encargado del tratamiento responde a la necesidad de dar respuesta a fenómenos como el de la externalización de servicios, de manera que en aquellos supuestos en que el responsable del tratamiento encomiende a un tercero la prestación de un servicio que requiera el acceso a datos de carácter personal por éste, dicho acceso no pueda considerarse como una cesión de datos. Es así que el artículo 12.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, establece que "no se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento"

En este sentido, tendrá la condición de encargado del tratamiento, conforme al artículo 3.g de Ley Orgánica 15/1999 "La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento" por contraposición a la figura del responsable al que, conforme al artículo del mismo texto legal le corresponde decidir "sobre la finalidad, contenido y uso del tratamiento."

Para que la relación entre responsable y encargado del tratamiento pueda darse y se ajuste a la Ley, es preciso que se cumplan los requisitos expresados en el artículo 12 de la Ley Orgánica 15/1999, considerando los siguientes aspectos:

En primer lugar, es preciso que el acceso a los datos por el tercero se efectúe con la exclusiva finalidad de prestar un servicio al responsable del fichero, y que dicha relación de servicios se encuentre contractualmente establecida. En lo que atañe a los requisitos formales de este tipo de contratos, el artículo 12.2 de la Ley Orgánica 15/1999 impone que "la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas".

El hecho de que la relación derivada del contrato sea la existente entre un responsable y un encargado del tratamiento implicará que al término de la relación sea aplicable lo establecido en el artículo 12.3 de la misma Ley, de forma que "una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento".

El incumplimiento de esta previsión llevará aparejada la consecuencia, prevista en el artículo 12.4 de la Ley Orgánica 15/1999, de que "En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido

personalmente".

En consecuencia, desde el punto de vista de la normativa de protección de datos existe una relación entre el responsable del fichero, en el presente supuesto el consultante, y el encargado del tratamiento que obliga a éste a seguir las instrucciones del responsable del fichero o ficheros, de modo que el encargado será responsable de la vulneración de lo previsto en la Ley Orgánica 15/1999 si se produce un acceso indebido a los datos que no obedezca a las órdenes recibidas del responsable del fichero.

Entre las obligaciones del responsable del fichero se encuentran las de adoptar las correspondientes medidas de seguridad. En cuanto a las medidas de seguridad que hayan de ser adoptadas por quienes realicen trabajos de tratamiento de datos por cuenta de tercero, habrán de ser, en principio, las mismas que las impuestas al responsable del fichero, tal y como se desprende de lo previsto en los artículo 9 y 12.2 de la Ley Orgánica 15/1999, dichas medidas deberá venir especificadas en el contrato que se firme con el encargado del tratamiento.

Prevé así el citado artículo 9 en su número primero que "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 estén expuestos, ya provengan de la acción humana o del medio físico o natural."

En el número segundo de dicho artículo 11 se establece que "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" constituyendo una infracción tipificada en la Ley Orgánica 15/1999 el mantenimiento de los ficheros, locales, programas o equipos sin las debidas condiciones de seguridad.

En este sentido el artículo 20.2 del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, dispone que "Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento." Dicha previsión introduce un poder de supervisión sobre el encargado del tratamiento que se traduce en que el responsable del fichero o tratamiento estará legitimado para realizar controles durante el período de vigencia del contrato para verificar el cumplimiento de las medidas de seguridad establecidas y adoptar las medidas correctoras oportunas.

El Reglamento de desarrollo de la Ley Orgánica 15/1999, constituye en la actualidad la normativa vigente en materia de medidas de seguridad aplicables a los tratamientos de datos de carácter personal. El artículo 80 de esta norma clasifica las medidas de seguridad aplicables a los ficheros o tratamientos de datos en tres niveles, debiendo adoptarse según la naturaleza de los datos a tratar el nivel correspondiente. Debe tenerse presente, además, que dichas medidas tienen un carácter acumulativo, de forma que las establecidas para cada nivel exigen incorporar las previstas para los niveles inferiores.

Cuando se trata de datos relativos a la salud de las personas el artículo 81.2 del

citado Reglamento establece, respecto de la aplicación de los niveles de seguridad, que "Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual."

Dichas medidas, abarcan, desde las de nivel básico relativas a las obligaciones de identificación y autenticación de usuarios, a las de registro de cada intento de acceso previstas para los ficheros que deban adoptar medidas de seguridad de nivel alto. Las medidas a adoptar deberán constar en el documento de seguridad que elaborará el responsable del fichero tal y como establece el artículo 88.1 del Reglamento de desarrollo de la Ley Orgánica 15/1999, según el cual "El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información."

No obstante, dispone el número 6 del artículo 88 que "En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.">>

III

La denuncia se concreta en la imposibilidad que han tenido los franquiciados de Vital Dent, S.L., de acceder a las historias clínicas de sus pacientes durante unas horas.

El artículo 9 de la LOPD 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 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."

El transcrito artículo 9 de la LOPD establece el principio de seguridad de los datos, imponiendo al responsable del fichero la obligación de adoptar las medidas de índole técnica y organizativa que garanticen tal seguridad, así como para impedir el acceso no autorizado a los mismos por ningún tercero.

Sintetizando las previsiones legales citadas 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, regulado en normas reglamentarias.

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 del artículo 9 de la LOPD tipificada como grave en el artículo 44.3.h) de la citada Ley.

El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, en su artículo 81.1 señala que "*Todos los ficheros o tratamientos 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. El artículo 88, en su punto 3, se refiere al documento de seguridad.

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. En el caso que nos ocupa, como establece el artículo 81.3.a) del Reglamento de desarrollo de la LOPD, además de las medidas de nivel básico y medio, deberán adoptarse las medidas de nivel alto a los ficheros o tratamientos de datos de carácter personal que se refieran a datos de salud.

En consecuencia, cada franquiciado debería garantizar la integridad de la historia clínica de sus pacientes, para lo cual es obligado, entre otros aspectos, la realización de copias periódicas de seguridad.

Como se ha recogido en los Antecedentes de esta Resolución, el franquiciador firma un contrato de prestación de servicios con los franquiciados (que son responsables de sus ficheros de pacientes). El Franquiciador facilita el acceso a una Plataforma centralizada a través de un programa de gestión de pacientes. Cada franquiciado accede a su propio fichero. De acuerdo con este contrato de franquicia, es el Franquiciador quien realiza las copias periódicas de seguridad.

El problema denunciado fue puntual debido a la intervención judicial al Franquiciador que llevó a que la autoridad bloquease los sistemas informáticos. Situación que se solventó en unas horas.

A pesar de que los contratos de Franquicias son de adhesión en muchas ocasiones, los franquiciados deben velar porque se cumpla escrupulosamente todas las exigencias en materia de protección de datos, ya que ellos, como responsables de los ficheros, responderían de sus incumplimientos.

Por lo tanto, de acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a LABORATORIO LUCAS NICOLAS, S.L. y a la ASOCIACION NACIONAL DE FRANQUICIADOS VITALDENT.

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