Procedimiento Nº PS/00590/2008

RESOLUCIÓN: R/01254/2009

En el procedimiento sancionador **PS/00590/2008**, instruido por la Agencia Española de Protección de Datos a la entidad **FLEUROP INTERFLORA ESPAÑA, S.A**., vista la denuncia presentada por **M.M.M.** y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha de 8/06/2007, tuvo entrada en esta Agencia una denuncia de M.M.M. en la que denuncia a *INTERFLORA (*FLEUROP INTERFLORA ESPAÑA, S.A.,en lo sucesivo la denunciada), por facilitar a un Juzgado de Madrid, un documento conteniendo datos relativos a su identificador de usuario en la página web de solicitud de pedidos, los cuales, además de su clave de usuario, incluían su contraseña de acceso, pudiendo ser visualizado por cualquier persona relacionada con el procedimiento.

Aporta el denunciante una citación judicial expedida por el Juzgado de Instrucción nº 0A de ....., de fecha 12/04/2007, en la que en calidad de denunciado en un juicio de faltas por presunta estafa, se le acompañan dos hojas impresas de la pagina web "*www...X..../..../....."*, fechadas a 6/03/2006, referidas como "*fotocopia de la gestión de Interflora*". Una hoja aportada, denominada "*Gestión de Interflora. Consulta de cliente*", contiene los datos identificativos de registro del cliente, nombre de usuario y contraseña, totalmente visibles, la otra "*Gestión de Interflora. Pedidos de cliente*", contiene datos relativos a un pedido realizado a través de Internet por M.M.M., el 25/07/2005, así como los datos generales asociados al usuario que realizó el pedido.

SEGUNDO: El Director de la Agencia Española de Protección de Datos, tras la recepción de la denuncia, ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento por requerimiento contestado por la denunciada el 4/12/2007, de los siguientes extremos:

1. FLEUROP INTERFLORA ESPAÑA, S.A., es responsable de varios ficheros inscritos en el Registro General de Protección de Datos en los que se almacenan datos de carácter personal relativos al desarrollo de su actividad comercial, entre ellos el denominado "*Gestión de Clientes*", de nivel de seguridad básico, en el que se almacenan los datos de los usuarios que realizan compras a través del sitio web "*http://www...X...*". El fichero fue notificado para su inscripción al Registro General de Protección de Datos el 19/09/2007, figurando descrito como fichero cuya finalidad es "*la gestión de clientes que realizan encargos florales directamente a Fleurop Interflora España S.A., a través de la página web y vía telefónica; mantenimiento de la relación entidad-cliente, alta de cliente y pedido, alta de usuario en la web y gestiones relacionadas con al transmisión y ejecución del encargo floral*."
2. El apartado de datos que se recogen en el fichero son: NIF/DNI, nombres y apellidos, dirección, teléfono, usuario y contraseña.
3. FLEUROP INTERFLORA ESPAÑA, S.A., manifiesta que el 13/12/2006, interpuso demanda judicial frente al denunciante, lo que ocasionó la incoación del Juicio de faltas 363/2007. Junto a la

denuncia, se aportaron distintos documentos, entre ellos "*los datos registrados de D. M.M.M.*". La denunciada manifiesta que "*la totalidad de los documentos aportados al Órgano Jurisdiccional se presentaron al amparo de lo dispuesto en el artículo 24 de la Constitución Española y del artículo 11.2 de la LOPD, al objeto de obtener la tutela judicial efectiva de los Jueces y Tribunales y, en ningún caso, resultó arbitraria, toda vez que de la relación fáctica se deduce una evidente relación de D. M.M.M. con los hechos acaecidos, por lo que esta parte puso a disposición del Juzgado todos los datos de que disponía para el esclarecimiento de los hechos y al objeto de facilitar la labor instructora del Juez".*

4. El anexo nº 28 del Documento de Seguridad aportado por FLEUROP INTERFLORA ESPAÑA, S.A., describe el procedimiento habilitado para la gestión de contraseñas, incluyendo un apartado específico donde se especifican los métodos de almacenamiento de las mismas. En particular, se establece lo siguiente: "*En el caso de aplicaciones de gestión definidas en el presente documento de seguridad, el cifrado de contraseñas será realizado por el sistema gestor de bases de datos o por la propia aplicación*."

5. En la página web: "*www...X...",* constan algunas cláusulas en virtud de la Ley del Servicio de Sociedad de la información y del comercio electrónico, y avisa de la incorporación a un fichero de los datos proporcionados al realizar un pedido, cuyo uso se hará acorde con la política de protección de datos y protección a la intimidad. También consta que "*el pago debe efectuarse mediante tarjeta de crédito de la que el contratante declara ser titular o estar autorizado por el mismo para su utilización. Cualquier uso fraudulento de la misma dará derecho a Fleurop a no tramitar el pedido, sin perjuicio de exigir la indemnización de los daños y perjuicios ocasionados*".

6. FLEUROP fue requerida para que aportara los datos que del denunciante constaran en sus ficheros. Aporta el mismo documento que aportó al Juzgado, confirmándose que en la hoja "*Gestión de INTERFLORA. Consulta de cliente*" se visualiza la contraseña, cuando según su documento de seguridad, estas "*se almacenarán cifradas, y ningún usuario, salvo el administrador del sistema, dispondrá de los mecanismos para descifrarlas*". La misma obligación establece el artículo 11 del Real Decreto 1Real Decreto 994/1999, de 11/06, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personales que se encuentra en vigor en el momento de los hechos, a tenor de lo previsto en la disposición transitoria tercera de la LOPD, al señalar:

   "*1.- El responsable del fichero se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso.*

   2.- 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.

   3.- Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y mientras estén vigentes se almacenarán de forma ininteligible."

TERCERO: Con fecha 9/12/2008, el Director de la Agencia Española de Protección de Datos acordó iniciar, procedimiento sancionador FLEUROP INTERFLORA ESPAÑA, S.A., por presunta infracción del artículo 9.1 de la Ley Orgánica 15/1999, de 13/12, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), tipificada como grave en el artículo 44.3.h) de dicha norma, pudiendo ser sancionada, con multa de 60.101, 21 a 300.506,05 €, de acuerdo con el artículo 45.2 de dicha Ley Orgánica.

CUARTO: Notificado el acuerdo de inicio, se hizo entrega de copia del expediente Al representante de Fleurop el 15/12/2008. FLEUROP INTERFLORA ESPAÑA, S.A. mediante escrito de fecha 26/12/2008 formuló alegaciones, significando:

1) Caducidad de las actuaciones previas por aplicación del artículo 122.4 del Real Decreto 1720/2007, han pasado mas de 18 meses desde la fecha de la denuncia hasta la recepción del acuerdo de inicio.. Además las disposiciones sancionadoras deben producir efecto retroactivo cuando favorezcan al presunto infractor.

2) En este caso, se hicieron unos pedidos vía internet, pagándose con una tarjeta, y realizado el servicio, no se pudo cobrar, por no ser el titular de la tarjeta coincidente con el usuario registrado, folios 24 y 25, interponiendo denuncia ante el Juzgado y aportándose dicho documento por considerarse necesario, en el ejercicio del derecho de defensa.

3) Los datos aportados lo fueron a un procedimiento judicial, los funcionarios y jueces que acceden a este dato lo hacen por el desarrollo profesional, sujetos al deber de secreto

4) El hecho de haber aportado al Juzgado tales contraseñas y usuario no quiere decir que Fleurop no las "*almacene de forma ininteligible*", y "*cifradas*",y "ningún usuario puede descifrar las contraseñas en el almacenamiento en el que se encuentran", pero si puede hacerlo el administrador, pues tiene mecanismos para descifrarlas, así está previsto en el documento de seguridad, y así se hizo para aportarse al Juzgado.

5) Cuando se han dado los datos previo requerimiento de la Agencia del denunciante, se ha hecho igual que cuando se aportaron al Juzgado, siendo el Administrador el que descifra las contraseñas. Este supuesto, junto con el requerimiento del Juzgado y la tutela judicial efectiva entiende Fleurop que son los únicos que justifican la reversión de la contraseña. De este modo, no se acredita la violación del artículo 9 imputado, pues la intención era de forma clara y transparente aportar dicho documento al Juez, y en momento alguno se han "m*antenido*" los ficheros sin seguridad.

6) Ejercía uno de los derechos previstos en el artículo 16.3 de la LOPD, teniendo los datos bloqueados, conservándolos para la atención de posibles responsabilidades nacidas del tratamiento durante el plazo de prescripción".

7) Falta de intencionalidad y de culpabilidad, no se ha acreditado la culpabilidad, debiéndose respetar entonces la presunción de inocencia, no se han causado perjuicios al interesado ni beneficio alguno, razones que deben conducir a la aplicación del artículo 45.5 de la LOPD

QUINTO: Con fecha 15/01/2009 el denunciante solicitó se parte interesada en el procedimiento, indicando que la denuncia que Fleurop le interpuso se halla en el Juzgado 0A de ..... , que conocía de denuncias análogas "*por uso indebido o fraudulento de tarjeta de crédito*"

SEXTO: Con fecha 20/01/2009, se inició el período de práctica de pruebas, dando por reproducidos a efectos probatorios la denuncia y su documentación, los documentos obtenidos y generados por los Servicios de Inspección ante FLEUROP INTERFLORA ESPAÑA, S.A., y el Informe de actuaciones previas de Inspección que forman parte del expediente E/00882/2007, así como las alegaciones presentadas por FLEUROP INTERFLORA ESPAÑA, S.A. y la documentación que a ellas acompaña. Adicionalmente se practicaron las siguientes:

2. A Fleurop que detallase el fichero en el que en el año 2005 y 2006 se almacenaban los datos de los compradores vía web en la página de "*...X...*", ya que el fichero "*Gestión Clientes*" se registró en septiembre 2007. Contestó con escrito de 6/02/2009 que se almacenaban en el fichero "*Bases de datos web*", que figuraba inscrito en el Registro, siendo suprimido el 14/09/2007, traspasándose la información al fichero de "*Gestión de clientes*".

3. Se solicitó a FLEUROP, que aportase copia de la demanda y documentación que presentó junto a la demanda por estafa contra el denunciante, autos ****/****, específicamente del documento folio 6, en el que se visualizase la fecha de presentación, así como situación procesal actual del procedimiento o en su caso de la Sentencia e indique si es firme, aportando copia de esta o sede del Juzgado que la tramita.

Con fecha 6/02/2009, aporta copia de la demanda presentada en el Juzgado Decano de (…..) el 13/12/2006. La demanda indica que los pagos electrónicos con tarjeta de crédito con los que se pagan los encargos, son remitidos vía terminal de pago electrónico a BBVA, quien a través de VISA solicita la autorización de pago al banco emisor de la tarjeta, quien acepta o deniega el pago. Señala que "*se han venido utilizando nombres y abonando con tarjetas de crédito que de acuerdo con las retrocesiones efectuadas*", "*no eran de titularidad del contratante*", causando perjuicio a Fleurop. En el relato de las al menos tres compras de encargos florales, a lo largo de 2006, señala que aparece como contratante una usuaria registrada que en distintas fechas realiza pedidos florales con **distintos nombres de usuarios**, siendo la contraseña en las tres ocasiones la misma, y constando como datos personales asociados los de la misma persona y domicilio, que se corresponde con la titular de la tarjeta de crédito, pero que manifiesta que no consintió las operaciones. Esta persona, según Fleurop en la demanda, interpuso denuncia ante el Juzgado de Instrucción 0C de la .... , diligencias previas número xxx/xxxx por no haber consentido pago ni uso de su tarjeta. Finaliza manifestando que el 25/07/20005, se contrató un pedido por el usuario M.M.M., con datos personales asociados M.M.M., su domicilio, teléfono y correo, y que contrató el envío a la persona física cuyos datos coincidían con la titular de la tarjeta y cuyos datos resultaban asociados por los usuarios registrados en los pedidos de 2006. Señala Fleurop que esta última operación no fue "*retrocedida*", y que la titular refiere que es "*el autor de la presunta estafa*".Por ello solicitan de M.M.M. las cantidades que fueron retrocedidas en el año 2006. Fleurop aporta copia de la hoja que entregó al Juzgado, denominada "Gestión de Interflora" "*Consulta de cliente*", que reúne todos los datos del usuario registrado, incluida la "*contraseña*". Esta hoja se obtuvo por Interflora en http://www...X.../...../...../.....,..., portando la fecha 6/03/2006.

4. Se solicitó a Fleurop, que en relación con la ventana que existe en su página para darse de alta para poder usar el servicio de enviar pedidos, en los que hay que seleccionar persona física/empresa, e-mail y NIF, y adjunto la casilla de enviar, detalle mediante impresión de pantallas de un alta ficticia el procedimiento que continua una vez remitidos los datos con la tecla de enviar, si se remite alguna confirmación al correo que se incluye y se efectúa alguna confirmación.

Contestó Fleurop que para cumplimentar la casilla en la que en el apartado "*Regístrate*", aparecen dos recuadros el superior "*Email",* y el de debajo "*Clave"*. Al registrarse se han de cumplimentar los datos, e-mail y DNI, la máquina comprueba que no consten ya registrados, pues si se introduce el DNI que ya existiera, saldría un mensaje. Si no existe, el cliente queda "*logado*" para poder hacer pedidos. En el momento del alta del cliente que se registra, "*no se envía ningún correo de confirmación a dicho correo*". El usuario al hacer cualquier envío remite los datos al servidor de Interflora.

5. Se solicitó a Fleurop que informase, y acreditase a ser posible, la fecha en que quedó bloqueado el acceso a los datos del denunciante a través del servicio de pedidos en la página web "*...X..."* de su contraseña y usuario. Contestó que el 2/01/2007 los datos del denunciante fueron bloqueados fecha

en la que comenzó a funcionar la nueva web, que nació sin contenido de datos, ya que "*no existió*" migración de datos de la antigua a la nueva.

6. Se solicitó a Fleurop NTERFLORA que informase sobre el modo de almacenamiento de la contraseña una vez se da de alta el cliente. Contestó Fleurop que la clave de acceso a la aplicación del cliente "***se guarda encriptada en la base de datos*** *"generando un hash con el criptosistema SHA-1, y luego aplicando una codificación Base64. Dicha clave no se puede desencriptar, sino que la clave que introduce el cliente en la autenticación se encripta y se compara con la que hay almacenada. Con esto se consigue que solo el cliente pueda conocer la clave*".7

7. Se incorporó como prueba una diligencia efectuada por el Instructor el día 21/01/2009, referente a la información que porta la página "*...X..."*, sobre protección de datos e información de pedidos, y los datos a rellenar en la casilla de registro de clientes.

SÉPTIMO: Con fecha 6/05/2009 se emitió propuesta de resolución al Director de la Agencia, proponiendo la imposición de una multa a Fleurop Interflora España, S.A. de 12.000 €, por la infracción del artículo 9.1 de la LOPD, tipificada como grave en el artículo 44.3.h) de dicha norma, teniendo en cuenta el artículo 45.2, 4 y 5 de dicha Ley Orgánica.

Frente a dicha propuesta, alega el 25/05/2009:

1) Reitera lo ya argumentado con anterioridad

2) El artículo 16.3 de la LOPD se refiere a la cancelación mediante bloqueo, y prevé su conservación únicamente a disposición de las Administraciones públicas. Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas."El 11 de la LOPD prevé su uso "Cuando la comunicación que deba efectuarse tenga por destinatario…Jueces o Tribunales en el ejercicio de las funciones que tienen atribuidas". De ello deduce la posibilidad de acceso a los datos por el administrador del sistema para ponerlos a disposición de los sujetos mencionados

3) Solicita que se aplique la cuantía mínima en la sanción, ya que su conducta se realizó pensando que era una actuación correcta, no se ha causado daño alguno al denunciante, existe buena fe, no se ha buscado directa ni indirectamente, ningún beneficio, y ha faltado la nota de voluntariedad y de culpabilidad. Ha podido surgir una diferencia de matiz interpretativo sobre la posibilidad de acceso del administrador del sistema a descifrar las contraseñas.

HECHOS PROBADOS

1) *La entidad Fleurop Interflora España S.A. almacena datos de carácter personal de usuarios que realizan compras a través del sitio www....X.... (folio 24). Dichos datos se almacenan en el fichero "Gestión de Clientes", de nivel de seguridad básico, que figura inscrito en el* Registro General de Protección de datos *(folio 24 y 15)*

2) El usuario se registra por primera vez en la web insertando un e mail y una clave, además del NIF (folios 192, y 231) y le debe dar a "*enviar*" La petición del usuario de cada pedido o encargo floral supone antes su identificación y autenticación a través de usuario y contraseña. Los datos del usuario son enviados con su navegador al servidor de Interflora, hallándose encriptados, de modo que no es posible conocer su clave. Igualmente, cuando el usuario introduce su clave, aparece esta sin poder ser visualizada (folios 23, 231 y 232).

3) Fleurop manifestó que "La clave de acceso a la aplicación del cliente se guarda encriptada en Base de datos generando un hash con el criptosistema SHA-1 y luego aplicando una codificación Base64. Dicha clave no se puede desencriptar, sino que la clave que introduce el cliente en la autentificación se encripta y se compara con la que hay almacenada"(folio 234).

4) El documento de seguridad de Fleurop señala que las claves o contraseñas se almacenarán cifradas(folio 53). Cuando el usuario se conecta a la web para hacer un pedido, la clave encriptada y almacenada por parte de Fleurop, se contrasta con la que en el momento de conectarse se introduce desde el otro lado. Las contraseñas se almacenarán, según el documento de seguridad, en forma ininteligible (folios 117), cifradas (folio 53).

*5) Fleurop presentó una demanda judicial en la que se siguió juicio de faltas ante el Juzgado de Instrucción 0A de ...., ****/**** (folios 209 a 213) contra M.M.M., aportando la hoja "*Gestión de INterflora*" "Consulta de cliente", en la que se visualiza claramente la contraseña" de dicho usuario /(.....). M.M.M. tuvo conocimiento de que su clave era visible cuando se le envió la citación con la copia de dicha hoja, el 12/04/2007 por el Juzgado de Instrucción 0A de .... (folio 4 a 6).*

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

En lo que respecta a la caducidad de las actuaciones**,** referentes a que se debe aplicar el artículo 122 del Real Decreto 1720/2007, de 21/12, por el que se aprueba el reglamento de desarrollo de la ley Orgánica 15/1999, de 13712, de protección de datos de carácter personal, que decreta la caducidad de las actuaciones, que en su punto 4 refiere:

"*4. Estas actuaciones previas tendrán una duración máxima de doce meses a contar desde la fecha en la que la denuncia o petición razonada a las que se refiere el apartado 2 hubieran tenido entrada en la Agencia Española de Protección de Datos o, en caso de no existir aquéllas, desde que el Director de la Agencia acordase la realización de dichas actuaciones.*

*El vencimiento del plazo sin que haya sido dictado y notificado acuerdo de inicio de procedimiento sancionador producirá la caducidad de las actuaciones previa*s."

Teniendo en cuenta que la transitoria quinta señala:

"*A las actuaciones previas iniciadas con anterioridad a la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.*

El presente real decreto se aplicará a las actuaciones previas que se inicien después de su entrada en vigor."

Aparte del tenor literal que excluye a hechos producidos antes de la entrada en vigor del Reglamento, 19/04/2008 la aplicación de dicha resolución, y además se debe manifestar que dicha disposición no regula sanciones, no tipifica infracciones, sino que regula procedimiento, por lo que esta alegación no puede ser estimada.

III

El artículo 9.1 de la LOPD , no viene sino a trasponer el *artículo 17 de la Directiva 9546 /*CE, dispone "*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 evite 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 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 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 aquélla, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el *"acceso no autorizado".*

Para poder delimitar cuáles son 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 art. 3.b) los define como *"todo conjunto organizado de datos de carácter personal, cualesquiera que fuera la forma o modalidad de su creación, almacenamiento, organización y acceso".*

Por su parte, la letra c) del mismo artículo define tratamiento de datos como *"operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".*

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 refiere a normas reglamentarias, que eviten accesos no autorizados.

Deben analizarse a continuación las previsiones que el Reglamento de Medidas de Seguridad, prevé para garantizar que no se produzcan accesos no autorizados a los ficheros.

El Real Decreto 994/1999, de 11/06, regula el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal, realiza las siguientes definiciones:

"***4.- Accesos autorizados:*** *Autorizaciones concedidas a un usuario para la utilización de los diversos recursos.*

5.- Identificación*: Procedimiento de reconocimiento de la identidad de un usuario.*

6.- Autenticación*: Procedimiento de comprobación de la identidad de un usuario.*

7.- Control del acceso*: Mecanismo que en función a la identificación ya autenticada permite acceder a datos o recursos.*

8.- Contraseña*: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.*

9.- Incidencia*: Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos*."

El artículo 11.2 del Real Decreto 994/1999, de 11/06 señala que "*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*", y que "*Las contraseñas se cambiaran con la periodicidad que se determine en el documento de seguridad y mientras estén vigentes se almacenaran de forma ininteligible*".

En el presente supuesto, la password, palabra clave o PIN cuando se refiere a números resulta inteligible y ello es lo que provoca la apertura del presente procedimiento.

Debe tenerse en cuenta que la finalidad del PIN o contraseña que tiene la que figura en el registro de clientes de INTERFLORA va precedida de la identificación que se efectúa mediante el registro del "*usuario*", siendo la clave, contraseña o palabra de acceso o paso, la que permite operar al usuario. En el presente supuesto, pese a que no existe inconveniente en aportar a Juzgados y Tribunales cualquier documentación que estime conveniente para su derecho de defensa, se aprecia que aunque puede aportar la clave de registro del denunciante, se está vulnerando ya de antes la LOPD, también con su aportación al mismo Juzgado, al constar visible la contraseña. No es que se aporte en abierto para que el Juzgado pueda visualizarla, que también es sancionable, sino que previamente se hallaba visible. No solo se está contribuyendo a la transparencia por aportar dicha clave al Juzgado, sino que se está infringiendo la LOPD por ello. El fin que tiene la contraseña es permitir que mediante su introducción por el cliente o usuario, la otra parte sea capaz de desvelar la misma mediante la comprobación el acceso al espacio que hablita dicho acceso. El establecimiento de contraseñas seguras para la organización puede ayudar a impedir que se pueda suplantar a los usuarios y, así, evitar la pérdida, exposición o daños en la información confidencial. La autenticación es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. En un web, "*autenticación*" es un modo de asegurar que los usuarios son quién ellos dicen que ellos son - que el usuario que intenta realizar funciones en un sistema es de hecho el usuario que tiene la autorización para hacer así, quedando identificado en su caso al acceso a determinados recursos del sistema.

Los sistemas de autenticación se basan en la introducción de una clave por el usuario que es enviada al servidor de la página web, distinguiéndose en el proceso general de autenticación los siguientes pasos:

1. El usuario solicita acceso a un sistema.

2. El sistema solicita al usuario que se autentique.

3. El usuario aporta las credenciales que le identifican y permiten verificar la autenticidad de la identificación.

4. El sistema valida según sus reglas si las credenciales aportadas son suficientes para dar acceso al usuario o no.

El funcionamiento del método de autenticación se basa en que siempre que el usuario introduce la clave o contraseña, la aplicación que los está leyendo, los confronta con los guardados en una base de datos para el usuario que la persona dice ser. Uno de los requisitos es que la entidad no tenga visible o disponible o almacenada en claro la contraseña introducida, pues una de las características que debe reunir la contraseña es la confidencialidad y el ser secreta. Este duo de clave de usuario y contraseña es similar al funcionamiento de la tarjeta de crédito y el PIN que posibilita extraer dinero en los cajeros. Cuando se hace visible la contraseña, se está posibilitando que cualquier persona sea o no de la organización, acceda con la clave al sistema.

En el presente supuesto se menciona por parte de Fleurop que la clave que introduce el usuario se guarda encriptada en BBDD generando un hash con el criptosistema SHA-1, y dicha clave no se puede desencriptar, sino que la clave que introduce el cliente en la autenticación se encripta y se compara con la que hay almacenada, conociendo solo el cliente la clave. Es decir el usuario introduce su clave de usuario y una contraseña que se almacena en la base de datos del servidor de que dispone Fleurop. No obstante, al enviar la contraseña, se almacena en un modo resumen o "*hash*", es decir unos algoritmos que son asignados por la máquina, y que permite a la postre que cuando se introduzca la siguiente ocasión la contraseña, la clave almacenada en el servidor, en su modo de hash, comprueba que se corresponde con dicha contraseña, permitiendo el acceso al sistema. Si así fuera, solo conociendo el hash, no sería posible desencriptar y revertir el proceso adivinando la clave introducida. Cuando se alega que el administrador posee las herramientas y llevó a cabo dicho proceso, carece de acreditación, siendo no obstante dicho proceso contrario a lo que determina el Reglamento de Medidas de Seguridad que prevé el almacenamiento de forma "ininteligible".

En el presente supuesto, parecen derivarse dos consecuencias de la hoja que se aportó al sistema:

1) La hoja que se aporta no desvela la relación exclusiva entre usuario y contraseña, sino que lo que se aporta es una caja que contiene los principales datos de cuando el usuario se registra, esto es la consulta del cliente, en la que figura la contraseña, y además el resto de los datos. De ello se deriva que la reversión de la contraseña que manifiesta Fleurop haber efectuado para aportar la citada hoja al Juzgado no es tal, sino que la contraseña ya se hallaba visible, por lo que aportándola al Juzgado como si se hubiera aportado a cualquier otro órgano o meramente hecho visible mediante su exteriorización se hubiese vulnerado en igual medida la LOPD.

2) El sistema de autenticación no es solicitado por el Juzgado, sino que es aportado por Fleurop creyendo que así contribuiría a la clarificación de su denuncia y al ejercicio de su derecho de defensa, pero obviando que las contraseñas sirven para confirmar el acceso, no identifican plenamente a la persona porque el que conozca dicha clave puede acceder.

3) Se manifiesta por Fleurop que el administrador dispone de las herramientas para poder descifrar las contraseñas, y solo las usa cuando esté previsto o habilitado en la norma, como en este caso para ser aportadas para su propia defensa.

Queda pues acreditado que Fleurop disponía de sus sistemas de registro de usuario y contraseña con las contraseñas visibles, vulnerando el artículo 9 de la LOPD. El hecho de que se aportasen al Juzgado para su plena defensa no legitima sino su dación al juicio, que no debió acompañarse de la contraseña, pues esta debe almacenarse de modo ininteligible para que confrontándola con la que inserte el usuario, deje paso a operar en el sistema, debiéndose garantizar su confidencialidad.

IV

Por su parte el *artículo 44.3. h) LOPD* tipifica como 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.*"

Se efectúa así una remisión al desarrollo reglamentario. Dicha regulación reglamentaria esta constituida por el *Real Decreto 994/1999, de 11/06* , que aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal, que ha mantenido su vigencia con la LOPD, según la *Disposición Transitoria Tercera* , hasta que se dicte la normativa de desarrollo de la misma.

Las medidas de seguridad se clasifican en el artículo 3 del Reglamento*, que recibe el título "niveles de seguridad", en tres* niveles: básico, medio y alto. Como indica el precepto dichos niveles se establecen atendiendo a la naturaleza de la información tratada (naturaleza de los datos), en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información. El *Art. 4, con el título "aplicación de los niveles de seguridad" regula cuando son aplicables cada uno* de los diversos niveles, básico (apartado 1), medio (apartado 2) y alto (apartado 3), pero también se refiere a los ficheros que permitan obtener una evaluación de la personalidad del individuo (apartado 4) y termina señalando que cada uno de dichos niveles tiene el carácter de mínimo (apartado 5).

El nivel de seguridad de Fleurop en su fichero “Gestión de clientes” era el básico, por lo tanto le resulta aplicable el artículo 11 “Identificación y autenticación”, que declara que si el sistema de autenticación se basa en existencia de contraseñas, existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad, y mientras estén vigentes, se almacenarán de forma ininteligible.

Fleurop ha incurrido en la violación de este precepto, al manifestarse que las contraseñas se guardaban de modo visible.

V

Se alega por Fleurop que el Administrador revertió la contraseña, de modo que la clave permanecía encriptada, y con unas herramientas y un procedimiento que no indica, consiguió desde la clave encriptada que figuraba en la base de datos, retrotraer y conseguir la clave o contraseña del usuario. Aparte de la falta de credibilidad de dichas manifestaciones que no resultan en modo alguno probadas, se debe tener en cuenta que la hoja aportada al Juzgado no es una hoja específica que desvele solo el PIN o contraseña, pudiendo tener sentido si lo que se hubiera aportado constara el usuario y la contraseña exclusivamente, y aparte los demás datos personales, pero lo que se aportó fue una ficha resumen, consulta de pedido del cliente que auna todos los datos almacenados de este, de lo que se deduce que este dato de la contraseña se almacenaba en abierto, de modo visible. El

documento de seguridad refiere en el anexo 22, folio 110 que durante el registro de usuarios en la página web, se permite seleccionar la contraseña al usuario, "*que permanece encriptada"* en base de datos, y "*no puede ser visualizada ni siquiera durante su introducción durante el logado"*·, incluso si olvida la misma existe un proceso automático que consiste en la introducción del e mail y el NIF, recibiendo un correo que resetea la contraseña anterior.

Asimismo el anexo 28 refiere el procedimiento de gestión de contraseñas, cambio periódico, que incluso la introducción por el usuario en pantalla será en formato ininteligible. En el caso de sistema operativo y red, las contraseñas se almacenarán cifradas por sus propias herramientas de seguridad. En el caso de las aplicaciones de gestión definidas en el presente documento de seguridad, el cifrado de contraseñas será realizado por el sistema gestor de bases de datos o por la propia aplicación (anexo 28). NO figura en el documento que el administrador de sistemas deba acceder a las contraseñas ni el procedimiento y ocasiones en que lo pueda hacer. Ello iría en contra del sentido y tenor del Reglamento de Medidas de Seguridad antecitado.

En lo referente a las alegaciones formuladas relativas a que se disponían de los datos y se pusieron a disposición del Juez, se debe indicar que el artículo 11.2.d) se refiere al supuesto en que el Juez requiere envío de datos en el desarrollo de sus funciones, diferente al que se produce aquí en el que concurren, se aportan motu propio, lo cual es legítimo, sin embargo, al aportarse se comprueba por este mero hecho, que no se custodia adecuadamente la contraseña, que no debía estar visible.

Además, en este supuesto, tampoco guarda relación con cancelación de datos y bloqueo de los mismos, pues no consta que el dato contraseña se hallara en dicha situación y la obligación de conservación pese a que puede obedecer a la defensa de derechos a ejercitar, en este supuesto se trata de un dato visible que no tenía que poder ser visualizado.

VI

Alega Fleurop que cumple el tenor del artículo 16.3 de la LOPD, que determina:

"*3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión*."

El bloqueo se refiere a los datos de que se disponga, no pudiendo estar bloqueado un dato que no debiera figurar en abierto, en modo visible o que permita acceder por el mero hecho de ser conocido. El dato de la clave, contraseña o PIN es aquí un dato asociado a los datos personales de usuario, que permite de algún modo identificar al titular de los datos personales. Sin embargo este dato PIN no tenía que mostrarse, y por tanto no podría haber estado nunca bloqueado. La finalidad de dicho dato es meramente la de contrastar con el almacenado en forma de algoritmo por Fleurop para permitir el acceso, no permanecer en abierto para que de ese modo sea de cualquier modo revelado, suponiendo un riesgo para la seguridad de los datos de su titular.

Por otro lado, en esta dación del documento que contiene el PIN al Juzgado, no resultó requerido por la autoridad judicial, sino aportado por Fleurop, en aras según manifestó a una completa identificación de todos los datos. No obstante se debe señalar que la configuración en abierto de dicho PIN supone una violación de la LOPD.

VII

En lo referente a la falta de culpabilidad alegada por Fleurop, se debe señalar que el ilícito administrativo previsto en el *artículo 44.3.h) de la LOPD* se consuma, como suele ser la norma general en las infracciones administrativas, por la concurrencia de una culpa leve. En efecto, el principio de **culpabilidad** previsto en el *artículo* 130.1 de la LRJPAC dispone que solo pueden ser sancionadas por hechos constitutivos de infracción administrativa los responsables de los mismos, aún a titulo de simple inobservancia. Esta simple inobservancia no puede ser entendida como la admisión en el derecho administrativo sancionador de la responsabilidad objetiva, pues la jurisprudencia mayoritaria de nuestro Tribunal Supremo (a partir de sus sentencias de 24 y 25 de enero y 9 de mayo de 1983) y la doctrina del Tribunal Constitucional (después de su STC 76/1990), destacan que el principio de **culpabilidad**, aún sin reconocimiento explícito en la Constitución, se infiere de los principios de legalidad y prohibición de exceso *(artículo 25.1 CE*), o de la exigencias inherentes a un Estado de Derecho, y requieren la existencia de dolo o culpa.

En la valoración del grado de inobservancia ha de ponderarse la profesionalidad o no del sujeto, y no cabe duda que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto. En este sentido la STS de 5 de junio de 1998 exige a los profesionales del sector "*un deber de conocer especialmente las normas aplicables*", y en similares términos se pronuncian, entre otras, las SSTS de 2 de marzo de 1999 y 17 de septiembre de 1999

Pues bien, la conducta que configura el ilícito administrativo aplicado en este caso -*artículo 44.3*.h) citado- requiere la existencia de culpa, que se concreta, por lo que ahora interesa, en la falta de diligencia observada por la entidad recurrente para asegurarse de que los datos y en concreto el de la contraseña o PIN ha sido recogido en sus bases de datos, sin hacerse ininteligible como determinan las medidas de seguridad, como lo demuestra el hecho de que fue aportado al Juzgado motu propio, con dicha clave visible, lo que revela el incumplimiento de dicha medida.

Además la Audiencia Nacional sobre la implementación de medidas de seguridad señala que "*No basta, entonces, 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. Así, de nada sirve que se aprueben unas Instrucciones detalladas sobre el modo de proceder para la recogida y destrucción de documentos que contengan datos personales, si luego no se exige a los empleados del banco la observancia de aquellas instrucciones*". "Se impone, en consecuencia, 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) debe asegurarse de que dichas medidas o mecanismos se implementen de manera efectiva en la práctica sin que, bajo ningún concepto, datos bancarios o cualesquiera otros datos de carácter personal puedan llegar a manos de terceras personas. En definitiva, y puesto que la entidad bancaria es una deudora de seguridad en materia de datos, debe por tanto dar una explicación adecuada y razonable de cómo los datos personales de sus clientes se hallaban a disposición y se podían encontrar por el afectado (en el lapso temporal en que aconteció el incidente) al acceder éste a la información telemática de sus datos bancarios, siendo insuficiente, según se desprende de la doctrina de la Sala que se acaba de exponer, con acreditar que se adoptaron una serie de medidas, pues dicha entidad bancaria también es responsable de que las mismas se cumplan y ejecuten con rigor*".

VIII

El artículo 45. 2. 4. y 5 de la LOPD establece lo siguiente:

"*2. Las infracciones graves serán sancionadas con multa de 60.101,21 € a 300.506,05 €."*

"*4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora****."***

"*5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, 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***."***

Alega Fleurop que se imponga la multa mínima dentro ya de la aplicación del artículo 45.5 en base a que actuó de buena fé, en la creencia de que al ejercitar un derecho podía aportar la contraseña del denunciante ya que no se han irrogado perjuicios al denunciante**.**

La Sentencia de 21/01/2004 de la Audiencia Nacional, en su recurso 1939/2001*, señaló que* dicho precepto <<…*no es sino manifestación del llamado principio de proporcionalidad (artículo 131.1 de la LRJPAC), incluido en el más general del prohibición de exceso, reconocido por la jurisprudencia como principio general del Derecho. Ahora bien, la presente regla debe aplicarse con exquisita ponderación y sólo en los casos en los que la culpabilidad y la antijuridicidad resulten sustancialmente atenuadas, atendidas las circunstancias del caso concreto. Lo cual insistimos puede darse, por excepción, en casos muy extremos (de aquí la expresión "especialmente cualificada") y concretos*.

En lo que respecta a la falta de perjuicios causados a la denunciante, la Audiencia Nacional, en Sentencia de 19/10/2005, declara que "*Los perjuicios directamente causados o beneficios obtenidos por la entidad recurrente son circunstancias que no admiten ser incluidas dentro de los que deben ser objeto de valoración al amparo de lo previsto por el artículo 45.5 de la LO 15/1999"*.

Se debe partir que lo que se ha incumplido, la obligación de mantener el PIN secreto, se ha manifestado con ocasión de la entrega de documentos al Juzgado, es decir con motivo del ejercicio de un derecho, si bien dicha clave no debía estar visible. Además, se debe tener en cuenta que Fleurop manifiesta que cuando comenzó a funcionar la nueva web, los datos del denunciante fueron bloqueados, sin que existiera migración de datos de la antigua a la nueva aplicación. Por lo demás, la entidad tenía los ficheros inscritos, y disponía de documento de seguridad. El PIN o contraseña no obstante, no ha salido al exterior, ni su conocimiento vino motivado por un acceso indebido de terceros propiciado por su visibilidad, o ha resultado perdido o extraviado los documentos que lo contenían y en los que constase dicha clave. Tampoco se constata que por el hecho de que figure en actuaciones judiciales, haya sido conocido por los empleados de los Juzgados, pues en su función diaria tienen una serie de deberes profesionales, frente a los que en este caso no se presupone violado el secreto con la aportación a los autos del proceso. A ello, se debe unir la falta de intencionalidad de incumplir la norma, que fue interpretada a favor del ejercicio de sus derechos, creyendo dar transparencia a la defensa de su derecho. Estas razones permiten la aplicación del artículo 45.5 de la LOPD.

Teniendo en cuenta los criterios de graduación de las sanciones previstos en el artículo 45. 4 y 5 de la LOPD y, en especial, la falta de intencionalidad, el ámbito en el que se entiende vulnerada la medida de seguridad, procede que se imponga una sanción en la cuantía de 1.000 €.

Vistos los preceptos citados y demás de general aplicación,

El Director de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: **IMPONER** a la entidad FLEUROP INTERFLORA ESPAÑA, S.A., por una infracción del artículo 9.1 de la LOPD, tipificada como grave en el artículo 44.3.h) de dicha norma, una multa de 1.000 € de conformidad con lo establecido en el artículo 45.2, 4 y 5 de la citada Ley Orgánica.

SEGUNDO: **NOTIFICAR** la presente resolución a FLEUROP INTERFLORA ESPAÑA, S.A. y a M.M.M..

TERCERO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva en el plazo de pago voluntario que señala el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso en la cuenta restringida nº 0000 0000 00 00000000000 abierta a nombre de la Agencia Española de Protección de Datos en el Banco Bilbao Vizcaya Argentaria, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo. Si recibe la notificación entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si recibe la notificación entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Madrid, 4 de junio de 2009

EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: Artemi Rallo Lombarte