Procedimiento nº.: PS/00382/2012

ASUNTO: Recurso de Reposición Nº RR/00142/2013

Examinado el recurso de reposición interpuesto por la entidad ***ASOCIACION ESPAÑOLA DE LEASING Y RENTING*** contra la resolución dictada por el Director de la Agencia Española de Protección de Datos en el procedimiento sancionador, PS/00382/2012, y en base a los siguientes,

HECHOS

PRIMERO: Con fecha 17/1/13, se dictó resolución por el Director de la Agencia Española de Protección de Datos en el procedimiento sancionador, PS/00382/2012 , en virtud de la cual se imponía a la entidad **ASOCIACION ESPAÑOLA DE LEASING Y RENTING,** una sanción de 20.000 €, por la vulneración de lo dispuesto en el artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), infracción tipificada como grave en el artículo 44.3.h, de conformidad con lo establecido en el artículo 45.2 de la citada Ley Orgánica.

Dicha resolución, que fue notificada al recurrente en fecha 17/01/17, fue dictada previa la tramitación del correspondiente procedimiento sancionador, de conformidad con lo dispuesto en el artículo 127 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

SEGUNDO: Como hechos probados del citado procedimiento sancionador, PS/00382/2012, quedó constancia de los siguientes:

<<<<< 1º *Consta denuncia presentada por D.* ***A.A.A.*** *manifestando que a través de la consulta de un foro podía enlazar a la página de la Asociación sin ninguna restricción en el acceso. Permitiéndose la consulta del titular de un vehículo introduciendo la matricula o el nº de bastidor y se visualiza el nombre apellidos, nº de bastidor o nº de matrícula, la compañía en la que está asegurado el vehículo y si dicho seguro está en vigor. Aporta a la denuncia fotocopia de la pantalla de visualización en el que aparecen sus datos y los de su vehículo (Fol. 1-3)*

2º *Se ha aportado en la denuncia el enlace a los dos foros a través de los cuales se enlaza con la página de la Asociación*

<http://www.bmwfaq.com.....
<http://www.audisport-iberica.com.....

3º *Consta Acta de Inspección levantada por los inspectores de esta Agencia en la sede de la entidad denunciada, con fecha 14/2/12, poniéndose de manifiesto en el curso de la misma lo siguiente:*

3.1 Que se recogieron las siguientes declaraciones de los representantes de la Asociación:

- La finalidad de la entidad es representar los intereses de empresas que operan en España en el sector del arrendamiento financiero (leasing) y arrendamiento operativo

(renting). Entre sus miembros se encuentran las compañías de todos los sectores de la actividad crediticia sometida a la tutela y supervisión del Banco de España, entre los que se encuentran 28 grupos financieros. Los miembros de las asociación son propietarios (personas jurídicas) de aproximadamente 1.000.000 de vehículos en modalidad de leasing y los que disponen del bien (arrendatarios) son también sociedades o profesionales.

- En el Registro de Bienes Muebles se encuentran inscritos dichos vehículos: nº de bastidor y propietario, siendo este último el responsable del aseguramiento del vehículo y de las posibles responsabilidades sobre las sanciones de tráfico según el Reglamento del seguro obligatorio de responsabilidad civil en la circulación de vehículos a motor, aprobado mediante Real Decreto 1507/2008.. Este procedimiento es el único que las entidades de crédito disponen para cubrir los riesgos de seguro obligatorio tras este Real Decreto sin caer en indefensión. Con esta consulta las entidades de crédito deciden contratar los seguros oportunos en casa de que el obligado (arrendatario) no lo hubiera hecho. Por lo que dicha circunstancia es la causa por la cual los miembros de la AELR requieren conocer la matrícula del vehículo así como el arrendatario que es titular administrativo o razón social que consta en el Registro de Vehículos cuyo responsable es la Dirección General de Tráfico.

- Que la ASOCIACION dispone de acceso al Registro de Vehículos, de la Dirección General de Tráfico de forma telemática (on-line) mediante el procedimiento "service web" o "máquina a máquina", siendo dicha Asociación quién se encarga de proceder a la gestión y control de los usuarios con acceso al fichero y, además, es la que debe implementar las medidas de seguridad necesarias con objeto de que no se produzcan accesos no autorizados.

- La comunicación entre la Dirección General de Tráfico y la AELR se realiza a través de Internet y la consulta (aplicativo denominado ATEX) puede efectuarse por el criterio de matrícula o número de bastidor y se facilita el nombre y apellidos o denominación social del titular administrativo (arrendatario habitualmente persona jurídica), fecha de matriculación y la compañía aseguradora y periodo del aseguramiento. Por lo que tienen acceso a la información de cualquier vehículo que consta en el fichero sin ninguna restricción.

***-** Que El certificado digital para el acceso al Registro de Vehículos fue facilitado a la AELR por la Dirección General de Tráfico en el año 2009. Las entidades miembros de la AELR, propietarios civiles, pueden realizar consultas al Registro de Vehículos mediante identificación y autenticación facilitando un código de usuario y contraseña en el portal web de la misma de cualquier matrícula o número de bastidor sin ninguna restricción.*

- Los miembros de la AELR deben solicitar por escrito, mediante correo electrónico, el código de usuario y la contraseña para el acceso al Registro de Vehículos facilitando el nombre, apellidos, NIF y dirección de correo electrónico. Si bien dicha solicitud solamente puede ser efectuada por el representante de la entidad ante la AELR.

- El Administrador del sistema de la AELR procede a dar de alta al usuario y se comunica por correo electrónico al titular de la dirección de correo el código de usuario y la contraseña, que cuando lo desee podrá cambiarla ya que en la actualidad el sistema no obliga a cambiarla, ni en la primera conexión ni posteriormente. Si bien en la

actualidad se están implementando funcionalidades para que sea necesario su cambio de forma periódica.

- En la actualidad se encuentran dados de alta 380 usuarios y en la relación de los mismos consta por cada uno de ellos la siguiente información: nombre de la entidad, nombre, apellidos, NIF, dirección de correo electrónico, usuario y password inteligible de cada uno de los usuarios con acceso autorizado.

- Por otra parte, en octubre de 2011 se implementó un Registro de accesos "log" en el cual se guarda la identificación del usuario, fecha y hora, criterio de acceso nº de matrícula o de bastidor, si ha sido correcta o no se ha podido producir por la existencia de un error. Si bien, hasta la fecha no se han realizado revisiones ni controles sobre dicha información. (Folios 18-20)

3.2 Que las inspectoras de la Agencia solicitaron a los representantes de la AELR que les informen en relación con la habilitación legal para el acceso al Registro de Vehículos por parte de los miembros de dicha Asociación. Ante lo cual manifiestan que la Dirección General de Tráfico les emitió un certificado digital y les facilitó el acceso.

3.3 Que se solicitó a los representantes de la AELR que les faciliten la documentación relativa con el acceso al Registro de Vehículos que han suscrito o que les ha remitido la Dirección General de Tráfico con respecto al procedimiento o normas sobre protección de datos, deber de secreto o medidas de seguridad. Ante lo cual hacen entrega de impresiones de varios correos electrónicos intercambiados entre ambas entidades y el "Manual de usuario: servicio web" de fecha 1 de junio de 2010, adjuntándose copia del mismo (Folios 150-158)

3.4 Se solicitó así mismo, a los representantes de la AELR información en relación con la incidencia acaecida en agosto de 2011 sobre la difusión de información del Registro de Vehículos a través de la página web de la Asociación. Manifestándose por parte de la entidad denunciada lo siguiente::

- El Grupo de Delitos Telemáticos de la Guardia Civil informó a la AELR, el día 16 de agosto de 2011, que a través de su página web estaban accediendo de forma fraudulenta al Registro de Vehículos por lo que procedieron al cierre de la página y a comunicar dichas circunstancias a la Dirección General de Tráfico.

- Que la hipótesis de cómo se realizaron los accesos fraudulentos podría haber sido que por parte de un usuario con acceso autorizado se capturó la URL de acceso a la aplicación ATEX, ***<http://atex.ael.es.....>****, que si se tecleaba directamente permitía el acceso sin restricciones y desde el sitio web de la Asociación utilizando el certificado digital emitido por la DGT. Dicha dirección se publicó en diversos foros como <forocepos.com>, <bmwfaq.com>, <audisport-iberica.com> y <forocoches.com>. Subrayan que se trata de una hipótesis.*

- Por parte de la Dirección General de Tráfico se procede a dar de baja al usuario y a revocar el certificado digital de la AELR hasta el mes de octubre de 2011.

- Que el secretario de la AELR presentó denuncia ante la Unidad Central Operativa de Policía Judicial de la Guardia Civil con fecha de 18 de agosto de 2011 en relación a un

posible ataque informático a la página web de la Asociación.

3.5 Se ha incorporado al Acta, en relación a lo anterior, la siguiente documentación:

a) Circular 87/2011 "Suspensión de los servicios de información de la herramienta de Tráfico a través de nuestra web" de 16/8/11 (folio 75)

b) impresión de los correos electrónicos remitidos por cinco personas físicas a la AELR solicitando la cancelación de sus datos personales así como las respuestas al efecto.

*c) Medidas a implementar con objeto de verificar los accesos al Registro de Vehículos a través de su página web, en octubre de 2011, (Folios 110-111**)***

3.6 Que en el periodo comprendido entre el día 12 y el día 16 de agosto de 2011, fechas en las ocurrieron los hechos, se efectuaron un total de 141.474 consultas a través de la página web de la Asociación de Leasing y durante el resto del año 2011 se realizaron un total de 95.598 consultas,

*3.7 Se ha verificado por parte de la Inspección de Datos, en las instalaciones de la Dirección General de Tráfico, que durante los días 13 al 16 se realizaron consultas al Registro de Vehículos por nº de matricula: "*****MATRÍCULA.1**", "*****MATRÍCULA.2**", "*****MATRÍCULA.3**" y "*****MATRÍCULA.4**", a través de la Asociación (*************) cuyo titular es el afectado,*

*3.8 Se ha verificado por parte de la Inspección de Datos, en las instalaciones de la Asociación de Leasing, que a través de la página web <http://atex.ael.es> se tiene acceso al Registro de Vehículos realizándose ocho consultas por nº de bastidor de vehículos cuyo propietario son entidades financieras, comprobándose que los titulares que constan en dicho Registro son personas jurídicas a excepción de uno de ellos que es **persona física**.*

*3.9 También, se han realizado seis consultas por nº de matricula **"***MATRÍCULA.5"**, **"***MATRÍCULA.6"**, **"***MATRÍCULA.3"**, **"***MATRÍCULA.2"**, **"***MATRÍCULA.4"** y **"***MATRÍCULA.1"** verificándose que se visualiza el titular (**persona física**), nº bastidor, entidad aseguradora y periodo de cobertura, siendo titular de las dos últimas el afectado.*

*3.10 La Asociación ha confirmado que el documento aportado por el denunciante de la consulta realizada por nº de matrícula **"***MATRÍCULA.7"**, descrita en el apartado primero del presente informe, coincide el formato y contenido del documento con las consultas realizadas a través su página web entre el día 12 y 16 de agosto de 2011*

4- Que por parte de la entidad denunciada se ha implementado un procedimiento para la asignación de claves y confidencialidad >>>>>

TERCERO: La ***ASOCIACION ESPAÑOLA DE LEASING Y RENTING*** (AELR) ha presentado en fecha 12/02/13 en esta Agencia Española de Protección de Datos, recurso de reposición fundamentándolo, básicamente,

- Nulidad de la resolución sancionadora
- Indefensión

- Resolución notificada no firmada por el Director
- Caducidad del Procedimiento
- Inexistencia de responsabilidad
- Principio de proporcionalidad

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el presente recurso el Director de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto 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 (en lo sucesivo LRJPAC).

II

Debe contestarse en primer lugar la alegación formulada relativa a la nulidad de la resolución de esta Agencia de fecha 17/01/13. Tal como se desprende de la misma dicho documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003 de firma electrónica, constando el siguiente código seguro de verificación: apdpf327e3d2b7c9dbe275c80-93766, en consecuencia ya que dicha firma está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control. Puede deducirse, tal como dispone el art. 3.4 que la misma "tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Tampoco se ha producido indefensión puesto que se notificó a la entidad sancionada el Acuerdo de Inicio del procedimiento sancionador, el trámite de práctica de pruebas, y la propuesta de resolución donde figuraban la determinación inicial de los hechos, la posible calificación y las sanciones imponibles. Estando el expediente administrativo a disposición de la recurrente para ser consultado en cualquier momento del procedimiento o solicitar copia del mismo

Se ha alegado la existencia de vulneración del principio de igualdad en la aplicación del derecho, ya que existen otros procedimientos sancionadores en que la Agencia ha terminado dictando resolución por la que se imponía un apercibimiento en lugar de sanción. Dicha manifestación no puede tener favorable acogida pues si bien se ha añadido un nuevo apartado 6 al artículo 45 de la LOPD que permite apercibir al sujeto responsable (para que acredite la adopción de las medidas correctoras que en cada caso resulten pertinentes), dicha posibilidad tiene un carácter excepcional que debe atender a la naturaleza de los hechos, situación que no se ha producido en el presente caso en base a los hechos probados en el procedimiento sancionador recurrido.

III

En cuanto al resto las manifestaciones efectuadas por AELR reiterándose básicamente, en las alegaciones ya presentadas a lo largo del procedimiento sancionador, debe señalarse que todas ellas ya fueron analizadas y desestimadas en los Fundamentos de Derecho del II al VII ambos inclusive, de la Resolución recurrida, tal como se transcribe a continuación:

<<<<< II

El capítulo primero del Título IV de la Ley Orgánica de Protección de Datos de carácter personal (LOPD) regula los ficheros de titularidad pública. En concreto el art. 20.1 se dispone que:

"1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente"

2. Las disposiciones de creación o de modificación de ficheros deberán indicar:
a) La finalidad del fichero y los usos previstos para el mismo.
b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
c) El procedimiento de recogida de los datos de carácter personal.
d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
f) Los órganos de las Administraciones responsables del fichero.
g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

Con objeto de adecuar sus ficheros informáticos a la normativa de protección de datos por parte de Ministerio de Interior se dictó la Orden (INT/3764/2004, de 11 de noviembre). En la misma aparece el fichero: "Registro de vehículos" cuyo responsable es la Dirección General de Tráfico. Estableciéndose la siguiente estructura y contenido:

<<<<. Nombre del fichero: Registro de vehículos Finalidad: Registro de Vehículos. Usos previstos: Gestión de las competencias propias. Información a interesados legítimos y terceros interesados. Elaboración de estadísticas BOE núm. 277 Miércoles 17 noviembre 2004 38005 internas y públicas. Anotación a instancia de otros Órganos, Registros y Entidades, con trascendencia para este registro de vehículos. Personas o colectivos de los que se obtienen los datos o que resulten obligados a suministrarlos: Titulares de vehículos, Registro de Bienes Muebles, Consorcio de Compensación de Seguros, Ministerio de Ciencia y Tecnología, Concesionarios de vehículos, Estaciones de Inspección Técnica de Vehículos, Fabricantes de Automóviles, Camiones y Autobuses. Procedimiento de recogida de los datos: Impresos cumplimentados por los interesados, transmisión electrónica y fuentes accesibles al público.

Estructura básica del fichero y descripción de los datos recogidos: Comprende datos de vehículos, con su identificación, matrícula y número de bastidor, datos de titularidad (nombre, apellidos y DNI o NIE), domicilio, datos técnicos, trámites, inspecciones técnicas, precintos, limitaciones y cargas, eventuales poseedores y seguro.

Cesiones de datos previstas: Se trata de un registro público, de conformidad con lo establecido en el art. 2 del Reglamento General de Vehículos, aprobado por Real Decreto 2822/1998, de 23 de diciembre. Se prevén cesiones a la Administración Tributaria, Administración de la Seguridad Social, Ayuntamientos, Diputaciones y Cabildos, Fuerzas y Cuerpos de Seguridad, Juzgados, Ministerio de Fomento, Ministerio de Industria, Turismo y Comercio y Consejerías de Industria de Comunidades Autónomas, Defensor del Pueblo, Ministerio Fiscal, Tribunales y Tribunal de Cuentas.

Órgano responsable del fichero: Dirección General de Tráfico. Órgano ante el que puede ejercitarse los derechos de rectificación, cancelación y oposición: Dirección General de Tráfico C/ Josefa Valcarcel28, 28071-Madrid. Medidas de seguridad: Nivel medio. Medidas de seguridad: Nivel medio..>>>>

Hay que tener en cuenta que la Sentencia del Tribunal Supremo de 31/10/2000, sala tercera, (rec. 6188/96) manifestó, en relación a los datos que figuran en este fichero, que los datos de vehículos registrados a nombre de persona física en dicho fichero. son datos de carácter personal pero no son datos accesibles al público, en consecuencia el acceso al mismo está condicionado a que exista un interés habilitante.

III

El Reglamento General de Vehículos, aprobado por Real decreto 2822/98 de 23 de diciembre, establece, en su artículo 2, y en relación al Registro de Vehículos. lo siguiente:

<<<< 1. La Jefatura Central de Tráfico llevará un Registro de todos los vehículos matriculados, que adoptará para su funcionamiento medios informáticos y en el que figurarán, al menos, los datos que deben ser consignados obligatoriamente en el permiso o licencia de circulación, así como cuantas vicisitudes sufran posteriormente aquéllos o su titularidad.

Estará encaminado preferentemente a la identificación del titular del vehículo, al conocimiento de las características técnicas del mismo y de su aptitud para circular, a la comprobación de las inspecciones realizadas, de tener concertado el seguro obligatorio de automóviles y del cumplimiento de otras obligaciones legales, a la constatación del Parque de Vehículos y su distribución, y a otros fines estadísticos.

El Registro de Vehículos tendrá carácter puramente administrativo, será público para los interesados y terceros que tengan interés legítimo y directo, mediante simples notas informativas o certificaciones, y los datos que figuren en él no prejuzgarán las cuestiones de propiedad, cumplimientos de contratos y, en general, cuantas de naturaleza civil o mercantil puedan suscitarse respecto a los vehículos.

Tendrá también una función coadyuvante de las distintas Administraciones públicas, Órganos judiciales y Registros civiles o mercantiles con los que se relaciona. El funcionamiento del Registro, la forma y efectos de sus anotaciones, así como el alcance de su publicidad se ajustará, además, a la reglamentación que se recoge en el anexo I.>>>>

El Real Decreto 1507/2008, de 12 de septiembre, por el que se aprueba el Reglamento

del seguro obligatorio de responsabilidad civil en la circulación de vehículos a motor dispone:

"Artículo 11. Contenido de la solicitud y de la proposición del seguro obligatorio.
La solicitud del seguro obligatorio dirigida por el tomador del seguro a la entidad aseguradora, o la proposición del seguro obligatorio hecha por el asegurador al tomador, deberá contener, como mínimo, las siguientes indicaciones:

a) Las de identificación del propietario del vehículo, del conductor habitual y del tomador del seguro, debiendo constar su domicilio a efectos de notificaciones. Si el tomador no fuese el propietario del vehículo, habrá de indicarse el concepto en que contrata.
b) Las de identificación del vehículo, marca, modelo, características y matrícula o signo distintivo análogo.
c) Las garantías solicitadas u ofrecidas, que en ningún caso podrán ser inferiores a las del seguro obligatorio.
d) La identificación clara y destacada de que se trata de una proposición o de una solicitud de seguro.
e) El período de cobertura mínimo, con indicación del día y hora de su cómputo inicial.

IV

El artículo 9 de la LOPD, que 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 art. 44.3.h) de la LOPD tipifica como infracción grave el mantener los ficheros "...que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".

El citado 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 sean los accesos que la Ley pretende evitar exigiendo las pertinentes medidas de seguridad es preciso acudir a las definiciones de "fichero" y "tratamiento" contenidas en la LOPD.

En lo que respecta a los ficheros el art. 3.a) los define como "todo conjunto organizado de datos de carácter personal" con independencia de la modalidad de acceso al mismo.

Por su parte la letra c) del mismo artículo permite considerar tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente expediente, la "comunicación" o "consulta" de los datos personales tanto si las operaciones o procedimientos de acceso a los datos son automatizados como si no lo son.

Sintetizando las previsiones legales puede afirmarse que:

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

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

c) La LOPD impone la adopción de medidas de seguridad, cuyo detalle se remite a normas reglamentarias, que eviten accesos no autorizados, ya provengan de la acción humana o del medio físico o natural.

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

El artículo 81.a del RLOPD establece que: "Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico"

En el caso que nos ocupa los hechos denunciados derivan del acceso por terceros (no miembros de la Asociación) a la información sobre la titularidad de los vehículos y del aseguramiento a partir de la matrícula o número de bastidor a través de la Web de la misma. Probablemente capturando la URL de acceso a la aplicación ATEX, permitiendo entonces el acceso sin restricciones y desde fuera del sitio web de la Asociación, utilizando el certificado digital emitido por la DGT a aquella. Con la consecuencia que durante los días 12 al 17 de agosto de 2011 se realizaron más de 140.000 consultas al Registro de Vehículos que pudieron estar no autorizadas.

Para valorar dichos hechos deben tenerse en cuenta las previsiones establecidas en el RLOPD en particular a lo que hace relación al control de acceso (art. 91) e identificación y autenticación (art. 93)

En el artículo 91 se desarrollan las previsiones que deberán establecerse para garantizar que los usuarios con acceso a datos personales o recursos sólo podrán acceder a dichos datos y recursos cuando así se precise para el desempeño de sus funciones. Para ello es necesario que previamente se hayan concedido las autorizaciones pertinentes a los mismos para la utilización de los diversos recursos, y deben también incluirse las autorizaciones o funciones que tenga atribuidas un usuario

por delegación del responsable del fichero. En este supuesto la entidad denunciada dispone de acceso al Registro de Vehículos de forma telemática, mediante el procedimiento "service web", siendo dicha entidad quien se encarga de proceder a la gestión y control de los usuarios con acceso al fichero. La comunicación entre la responsable del fichero (DGT) y la asociación se realiza a través de internet y la consulta (por el aplicativo denominado ATEX) se puede efectuarse por el criterio de matrícula o el número de bastidor.

Además de la implementación de mecanismos que impidan el acceso no autorizado deberán estar definidos procedimientos que establezcan los criterios a seguir para conceder o anular la autorización de los accesos.

Por otro lado el art. 93 del Reglamento establece la obligación de adoptar las medidas de seguridad que garanticen la correcta identificación y autenticación de las personas que accedan o traten datos personales. Así mismo, es de obligado cumplimiento realizar la comprobación de la existencia de la autorización exigida relativa al control de acceso, con un proceso de verificación de la identidad de la persona (autenticación) implicando un mecanismo que en función de la identificación ya autenticada permita acceder a datos y recursos

El proceso de autenticación y control en el acceso es distinto con el proceso de autorización: es decir, los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones que deberán ser autorizados por el responsable del fichero). La relación de identidades personales deberá estar asociada normalmente con un perfil de seguridad (perfil de usuario), roles y permisos concedidos. Lo que se pretende por tanto en la norma reglamentaria es la obligación de implantar un mecanismo que permita que la identificación de los usuarios sea inequívoca y personalizada, no permitiéndose el uso de usuarios genéricos en ningún acceso o tratamiento debiendo quedar registrados todos y cada uno de los intentos de acceso al sistema de información. También se ha establecido la periodicidad de la contraseña, obligando a que exista un procedimiento de asignación, distribución y almacenamiento de las contraseñas que garantice su confidencialidad e integridad.

En conclusión de los hechos acreditados en este procedimiento se puede establecer la existencia de elementos de culpabilidad en la entidad denunciada al no aplicar en su página web las medidas de seguridad necesarias de cara a impedir accesos indebidos al Registro de Vehículos. Se deduce pues que, pese a tener implementado en el momento de los hechos un sistema de control de los usuarios autorizados para realizar consultas al Fichero (facilitándose un código de usuario y contraseña), se produjeron accesos no autorizados al registro de vehículos, durante los días 12 al 16 de agosto de 2011. Presentándose como hipótesis más probable para la explicación de este hecho, tal como se recoge en el Acta de Inspección E/3817/11 que por parte de un usuario autorizado se capturase la URL de acceso a la aplicación ATEX, permitiéndose teclearla directamente fuera del sitio web y publicándose en diversos foros.

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

"Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen."

Dado que ha existido una vulneración en las medidas de seguridad se considera que la citada entidad ha incurrido en la infracción grave descrita.

V

El artículo 10 de la LOPD establece que: "El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo".

El deber de confidencialidad obliga no sólo al responsable del fichero sino a todo aquel que intervenga en cualquier fase del tratamiento. Dado el contenido del precepto, ha de entenderse que el mismo tiene como finalidad evitar que por parte de quienes están en contacto con los datos personales almacenados en ficheros se realicen filtraciones de los datos no consentidas por los titulares de los mismos. Así el Tribunal Superior de Justicia de Madrid ha declarado en su Sentencia de 19 de julio de 2001: "El deber de guardar secreto del artículo 10 queda definido por el carácter personal del dato integrado en el fichero, de cuyo secreto sólo tiene facultad de disposición el sujeto afectado, pues no en vano el derecho a la intimidad es un derecho individual y no colectivo. Por ello es igualmente ilícita la comunicación a cualquier tercero, con independencia de la relación que mantenga con él la persona a que se refiera la información (...)".

En este sentido, la sentencia de la Audiencia Nacional de fecha 18 de enero de 2002, recoge en su Fundamento de Derecho Segundo, y tercer párrafo: "El deber de secreto profesional que incumbe a los responsables de ficheros automatizados, recogido en el artículo 10 de la Ley Orgánica 15/1999, comporta que el responsable –en este caso, la entidad bancaria recurrente- de los datos almacenados –en este caso, los asociados a la denunciante- no puede revelar ni dar a conocer su contenido teniendo el "deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo" (artículo 10 citado). Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la STC 292/2000, y por lo que ahora interesa, comporta que los datos tratados automatizadamente no pueden ser conocidos por ninguna persona o entidad, pues en eso consiste precisamente el secreto.

Este deber de sigilo resulta esencial en las sociedades actuales cada vez más complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la CE. En efecto, este precepto contiene un "instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos" (STC 292/2000). Este derecho fundamental a la protección de los datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino" (STC 292/2000) que impida que se produzcan situaciones atentatorias con la dignidad de la persona, "es decir, el poder de resguardar su vida privada de una publicidad no querida"

En el caso que nos ocupa al permitirse el acceso de usuarios no autorizados, a través de la página web de la entidad denunciada, al Fichero de Vehículos ha existido una omisión del deber de secreto, produciéndose una ausencia de confidencialidad, por lo que se considera que se ha cometido una infracción del transcrito artículo 10 de la LOPD.

El artículo 44.3.g) de la LOPD, califica como infracción grave:

"La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo"

VI

El hecho constatado de la difusión de datos personales establece la base de facto para fundamentar la imputación de las infracciones de los artículos 9 y 10 de la LOPD.

No obstante, nos encontramos ante un supuesto en el que un mismo hecho deriva en dos infracciones, dándose la circunstancia que la comisión de una implica necesariamente la comisión de la otra. Esto es, si un documento interno que contiene información sobre datos personales sale del ámbito de la entidad responsable de su confidencialidad, se está produciendo un incumplimiento de las medidas de seguridad exigidas a dicho responsable que, a su vez, deriva en una vulneración del deber de secreto.

Por lo tanto, aplicando el artículo 4.4 del Real Decreto 1398/1993, de 4 de agosto, por el que se aprueba el Reglamento del procedimiento para el ejercicio de la potestad sancionadora que señala que "en defecto de regulación específica establecida en la norma correspondiente, cuando de la comisión de una infracción derive necesariamente la comisión de otra u otras, se deberá imponer únicamente la sanción correspondiente a la infracción más grave cometida", procede subsumir ambas infracciones en una. Dado que, en este caso, se ha producido una vulneración de las medidas de seguridad, calificada como grave por el artículo 44.3.h) de la LOPD y también un incumplimiento del deber de guardar secreto, calificado como grave en el artículo 44.3.g) de la misma

norma, procede imponer únicamente la sanción correspondiente a la infracción del artículo 9 de la LOPD.

VII

El artículo 45 de la LOPD, en sus aparatados 2 a 5, establece, según también la nueva redacción dada por la Ley 2/2011, que:

«2. Las infracciones graves serán sancionadas con multa de 40.001 a 300.000 euros.

3. Las infracciones muy graves serán sancionadas con multa de 300.001 a 600.000 euros.

4. La cuantía de las sanciones se graduará atendiendo a los siguientes criterios:
a) El carácter continuado de la infracción.
b) El volumen de los tratamientos efectuados.
c) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.
d) El volumen de negocio o actividad del infractor.
e) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
f) El grado de intencionalidad.
g) La reincidencia por comisión de infracciones de la misma naturaleza.
h) La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.
i) La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.
j) Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

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

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

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

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

d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.

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

Debe analizarse para este caso, en primer lugar, si operan algunos de los supuestos contemplados en el art. 45.5 y puede aplicarse, para la cuantía de la sanción, la que preceda inmediatamente en gravedad a aquella. Entendiéndose que analizados los hechos acreditados operan dichas circunstancias. En concreto que existían antes del acceso fraudulento unas medidas adoptadas para la identificación de los usuarios; que el 31 de agosto se remite a la Dirección General de Tráfico un documento con una serie de medidas adoptadas para evitar los accesos fraudulentos, en especial estableciendo un log para realizar un seguimiento de quien accede a la aplicación; Que en octubre de 2011 se implementaron una serie de medidas de seguridad: inclusión de login y password en el acceso, controles en el flujo del proceso e inclusión de una log para que imposibilite los accesos desde fuera de la web con comprobaciones relativas a la validez del usuario.

Por otra parte, durante el periodo de práctica de prueba se solicitó de la entidad denunciada la remisión de un informe relativo a la asignación, comunicación al usuario y el almacenamiento de las contraseñas, así como el procedimiento y periodicidad para ser cambiadas por el usuario, remitiéndose el informe solicitado con fecha 10/10/12 relativo a las medidas de seguridad implementadas, las circulares que se han remitido a los asociados así como la cláusula de confindencialidad y condiciones de utilización de la página web de la asociación.

Las citadas circunstancias permiten apreciar la existencia de motivos para la aplicación de la facultad contemplada en el artículo 45.5, En el presente caso, de acuerdo a los criterios de graduación de las sanciones establecidos en el art. 45.4 de la LOPD se estima procedente fijar la cuantía de la multa en 20.000 euros.>>>>>

IV

Por lo tanto, en el presente recurso de reposición, ***ASOCIACION ESPAÑOLA DE LEASING Y RENTING*** no ha aportado nuevos hechos o argumentos jurídicos que permitan reconsiderar la validez de la resolución impugnada.

Vistos los preceptos citados y demás de general aplicación,

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

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por ***ASOCIACION ESPAÑOLA DE LEASING Y RENTING*** contra la Resolución de esta Agencia Española de Protección de Datos dictada con fecha 17 de enero de 2013, en el procedimiento sancionador PS/00382/2012.

SEGUNDO: NOTIFICAR la presente resolución a la entidad ***ASOCIACION ESPAÑOLA DE LEASING Y RENTING***.

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, se podrá interponer 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 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, 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 del referido texto legal.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos