Procedimiento nº.: PS/00457/2012

ASUNTO: Recurso de Reposición Nº RR/00198/2013

Examinado el recurso de reposición interpuesto por la entidad Seguridad en la Gestión, S.L. contra la resolución dictada por el Director de la Agencia Española de Protección de Datos en el procedimiento sancionador, PS/00457/2012, y de acuerdo con los siguientes,

HECHOS

PRIMERO: Con fecha 15 de febrero de 2013, se dictó resolución por el Director de la Agencia Española de Protección de Datos en el procedimiento sancionador, PS/00457/2012 , en virtud de la cual se imponía a la entidad Seguridad en la Gestión, S.L., una sanción de 6.000 €, 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, .4 y .5 de la citada Ley Orgánica.

Dicha resolución, que fue notificada al recurrente en fecha 19 de febrero de 2013, 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/00457/2012, quedó constancia de los siguientes:

<<PRIMERO: *Con fecha 16 de septiembre de 2011 tiene entrada en esta Agencia un escrito del denunciante en el que declara que la entidad de gestión de cobros Segestión SL le ha enviado por correo postal sobres de reclamación de deuda con la frase "COBRO DE MOROSOS" en letras de tamaño grande y bien visible y que cualquiera que presencie la inserción de la correspondencia puede ver ese texto. (folios 1 a 9)*

SEGUNDO: *Los representantes de Seguridad en la Gestión SL indican que realizan actuaciones de gestión de cobros para la entidad Creditclose Finance S.L. como encargados del tratamiento.*

Los datos personales del afectado, y la información de la deuda pendiente, han sido facilitados por el responsable del fichero Creditclose Finance S.L. (folios 19 a 34)

TERCERO: *Los representantes de Seguridad en la Gestión S.L. aportan copia de uno de los sobres utilizados para remitir los requerimientos de pago en el que figura la frase "COBRO DE MOROSOS" en letras de tamaño grande y bien visible.*

Según consta en la documentación remitida a la Agencia Española de Protección de Datos se han remitido 7 requerimientos de pago al reclamante en este tipo de sobres. (folios 19 a 34)>>

TERCERO: La entidad Seguridad en la Gestión, S.L. ha presentado en fecha 1 de marzo de 2013, en esta Agencia Española de Protección de Datos, recurso de reposición fundamentándolo, básicamente, en los mismos argumentos presentados durante el procedimiento, no obstante manifiesta que no ha negado nunca que los sobres corporativos contenían descripciones de los servicios prestados por la entidad; que la atribución de la condición de dato personal a la descripción de los servicios de la entidad se fundamenta únicamente en función de su tamaño; que la interpretación de los hechos es extensiva, injustificada y contraria a la seguridad jurídica.

Concluye su escrito solicitando se revise la Resolución recurrida, se declare la inexistencia de infracción y se archiven las actuaciones.

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

En relación con las manifestaciones efectuadas por Seguridad en la Gestión, S.L., 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 VIII ambos inclusive, de la Resolución recurrida, tal como se transcribe a continuación:

<<II

Los hechos enjuiciados fueron calificados en el Acuerdo de Inicio de este expediente sancionador como constitutivos de infracción del artículo 10 de la LOPD, tipificada en el artículo 44.2.d) de la citada Ley Orgánica. No obstante, en esta fase del procedimiento, se considera conveniente modificar la calificación jurídica efectuada e imputar a Seguridad en la Gestión, S.L. una infracción del artículo 9 de la Ley Orgánica 15/1999, tipificada en el artículo 44.3.h) de la LOPD.

Respecto a si es o no procedente cambiar en fase de propuesta la calificación jurídica de los hechos objeto de la denuncia que se realizó en el Acuerdo de Inicio y a la incidencia que tal cambio puede tener en el derecho de defensa de la entidad denunciada, conviene señalar que nada impide efectuar esta modificación siempre y cuando, como ahora sucede, permanezcan invariables los hechos en los que se funda la acusación formulada.

El primero de los derechos que el artículo 135 de la LRJPAC reconoce a favor del presunto infractor es el de que le sean notificados los términos de la acusación, que

comprende la información "de los hechos que se le imputen, de las infracciones que tales hechos puedan constituir y de las sanciones que, en su caso, se les pudiera imponer…".

El Tribunal Constitucional ha venido señalando que "el contenido esencial del derecho constitucional a ser informado de la acusación se refiere a los hechos considerados punibles que se imputan al acusado" (STC 95/1995). Por el contrario, y a diferencia de lo que acontece con los hechos, el TC, en Sentencia 145/1993 advierte que la comunicación al presunto infractor de la calificación jurídica y de la eventual sanción a imponer no integra el contenido esencial del derecho a ser informado de la acusación. Hasta tal punto es importante la puesta en conocimiento de los hechos constitutivos de la infracción administrativa, que el T.C. ha declarado que las exigencias del artículo 24.2 de la CE se satisfacen fundamentalmente con la sola comunicación de los hechos imputados para poder defenderse sobre los mismos (STC 2/1987 y 190/1987). En esta línea el Tribunal Supremo, Sentencia de 3 de marzo de 2004, señala que "la finalidad primordial del acuerdo de inicio es informar sobre los hechos imputados y no sobre la calificación jurídica, de lo que se encargará la propuesta de resolución". (El subrayado es de la AEPD).

III

El artículo 7 del Convenio Nº 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, establece:

"Seguridad de los datos:

Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados."

El artículo 17.1 de la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, establece:

"Seguridad del tratamiento:

1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse"

IV

La LOPD traspuso al ordenamiento interno el contenido de la Directiva 95/46, y en su artículo 1 dispone que "la presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".

El artículo 2.1 de la misma Ley Orgánica establece: "La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento y a toda modalidad de uso posterior de estos datos por los sectores públicos y privados".

El artículo. 3 de la LOPD establece las definiciones de responsable de fichero o tratamiento, de encargado de tratamiento y de cesión de datos:

"d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

g) Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

i) Cesión o comunicación de datos: toda revelación de datos realizada a la persona distinta del interesado."

V

Se imputa a la entidad Seguridad en la Gestión, S.L. el incumplimiento del principio de seguridad de los datos personales que constan en sus ficheros. A este respecto, el artículo 9 de la LOPD, dispone:

"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 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 dicha seguridad, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el "acceso no autorizado" por parte de terceros.

Para poder delimitar cuáles son los accesos que la LOPD 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 artículo 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 3 permite considerar tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente expediente, la "conservación" o "consulta" de los datos personales, tanto si las operaciones o procedimientos de acceso a los datos son automatizados como si no lo son.

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

Sintetizando las previsiones legales puede afirmarse que:

a) Las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso –la conservación 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.

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.

Es necesario analizar las previsiones que el R. D. 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, prevé para garantizar que no se produzcan accesos no autorizados a los ficheros.

El citado Reglamento define en su artículo 5.2 ñ) el "Soporte" como el "objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos".

Por su parte, en el artículo 81.1 del mismo Reglamento se establece 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 88.3, referido al documento de seguridad, establece lo siguiente:

"El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos".

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.

El Reglamento citado, distingue entre medidas de seguridad aplicables a ficheros y tratamientos automatizados (Capítulo III Sección 2ª del Título VIII) y las medidas de seguridad aplicables a los ficheros y tratamientos no automatizados (Capítulo IV Sección 2ª del Título VIII).

Igualmente el citado Reglamento regula:

"Artículo 91. Control de acceso.

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Artículo 92. Gestión de soportes y documentos.

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento

de seguridad.

3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas."

Así, Seguridad en la Gestión, S.L. está obligado a adoptar, de manera efectiva, las medidas técnicas y organizativas necesarias previstas para los ficheros de la naturaleza indicada, y, entre ellas, las dirigidas a impedir el acceso no autorizado por parte de terceros a los datos personales que constan en sus ficheros. Sin embargo, ha quedado acreditado que la citada entidad incumplió esta obligación, al establecer un sistema de notificaciones de sus reclamaciones y requerimientos de deuda a los deudores de su cliente, Creditclose Finance, sistema que no impidió de manera fidedigna que los datos personales de los deudores: nombre, apellidos y domicilio completo, pudieran ser accesibles por terceros, asociados a su situación de deudor moroso.

En este sentido se pronuncia la Audiencia Nacional, en Sentencia de 07/05/2009, en la que se declara lo siguiente: "En el presente caso la Sala no aprecia que se haya producido la revelación de secretos que se imputa a AAA, por varias razones:

Por un lado, porque no ha resultado acreditado que los datos personales de D... respecto de los que hubiera deber de secreto profesional por parte de AAA, hayan sido revelados a persona alguna. La infracción tipificada en el art. 44.3.g) es una infracción de resultado que exige que los datos personales sobre los que exista un deber de secreto profesional –como aquí ocurre en relación con el número de la cuenta corriente- se hayan puesto de manifiesto a un tercero, sin que pueda presumirse que tal revelación se ha producido. Efectivamente, la Agencia Española de Protección de Datos en su resolución se limita a poner de manifiesto que el sistema de cierre, mediante ventanilla transparente, de los sobres utilizados por el Banco para realizar determinadas comunicaciones a sus clientes pudiera dar lugar a que determinados datos personales contenidos en esas comunicaciones puedan ser conocidas por terceras personas respecto de las que deba mantenerse el secreto. No prueba sin embargo que los datos fueran efectivamente conocidos por dichos terceros. Estaríamos, por tanto, como sostiene el recurrente, ante una posible infracción de medidas de seguridad -que es una infracción de actividad- pero no ante la infracción que se le imputa que exige la puesta en conocimiento de un tercero de los datos personales".

Aplicando la anterior doctrina, la Audiencia Nacional, en varias sentencias, entre otras las de fechas 14 de febrero y 20 de septiembre de 2002 y 13 de abril de 2005, exige a las entidades que operan en el mercado de datos una especial diligencia a la hora de llevar a cabo el uso o tratamiento de tales datos o su cesión a terceros, visto que se trata de la protección de un derecho fundamental de las personas a las que se refieren los datos, por lo que los depositarios de éstos deben ser especialmente diligentes y cuidadosos a la hora de realizar operaciones con los mismos y deben optar

siempre por la interpretación más favorable a la protección de los bienes jurídicos protegidos por la norma.

VI

SEGESTION ha alegado que en el presente caso las indicaciones de cobro de morosos y vía judicial que pueden aparecer en los sobres de la entidad, no pueden interpretarse como datos personales del destinatario que deban protegerse y sobre los que deban aplicarse medidas de seguridad y, que en el caso de los sobres personalizados, es práctica común su envío en todas las empresas.

Sin embargo, tal alegato no puede ser aceptado.

En primer lugar, es cierto, como manifiesta la representación de la denunciada que las citadas expresiones no pueden ser interpretados, por si solas, como datos personales. No obstante, lo que es objeto de valoración en el presente caso es la vinculación de las expresiones que figuran en el sobre con los datos del denunciante. Los sobres que se utilizan por la entidad denunciada para requerir a los deudores la satisfacción de la deuda a sus empresas clientes, en este caso Creditclose Finance SL, presentan el literal "COBRO DE MOROSOS" en grandes letras, lo que unido a los datos del denunciante que figuran en la ventanilla del sobre, nombre y apellidos y domicilio, permite la asociación de ambas informaciones y la posibilidad de que terceras personas puedan acceder a ellos. Esta forma de comunicación impide salvaguardar la confidencialidad de la correspondencia pues asocia las expresiones cuestionadas con los datos personales del destinatario.

En segundo lugar, se le informa a la representación de la denunciada que la razón de ser del requerimiento de pago como previo a la inclusión de los datos en los ficheros de morosidad correspondientes, tiene como objeto que el deudor conozca la existencia de la deuda y la posibilidad de ser incluido en un fichero de morosos en el supuesto de no hacerla efectiva, sin necesidad de acudir a formulas tan discutibles como la que estamos analizando en el presente caso.

VII

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

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

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

VIII

El artículo 45 de la LOPD, establece, en sus apartados 1 a 5, lo siguiente:

"1. Las infracciones leves serán sancionadas con multa de 900 a 40.000 euros.

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.»

El citado apartado 45.5 de la LOPD deriva del principio de proporcionalidad de la sanción y permite establecer " 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", pero para ello es necesario la concurrencia de, o bien una cualificada disminución de la culpabilidad el imputado, o bien de la antijuridicidad del hecho, o bien de alguna otra de las circunstancias que el mismo precepto cita.

En el caso examinado, de las actuaciones practicadas ha quedado acreditado que SEGURIDAD EN LA GESTION vulneró el artículo 9 de la LOPD, en relación con el artículo 92 del Reglamento de desarrollo de la LOPD, al enviar sobres con la expresión "Cobro de Morosos" en caracteres bien visibles permitiendo la vinculación de esta

información con los datos personales del denunciante. No obstante, teniendo en cuenta las circunstancias que concurren en el presente caso, permiten apreciar la existencia de motivos para la aplicación de la facultad contemplada en el artículo 45.5, apartado b), debido a la diligencia desplegada por la entidad, puesto que desde el momento en que dicha actuación fue puesta en cuestión, no ha vuelto a usar el empleo de tales expresiones en los sobres y manifestando su total disposición a colaborar en la AEPD para que este tipo de actuaciones no vuelvan a producirse, lo que permite establecer una sanción de "la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate".

Por otra parte, se advierten otras circunstancias que operan como agravantes de la conducta de la entidad que ahora se enjuicia. Así, concurren las agravantes previstas en los apartados a) y c) del artículo 45.4 de la LOPD: a) El carácter continuado de la infracción, ya que no hubo un solo envío sino varios y, c) la vinculación de su actividad con la realización de tratamientos de datos de carácter personal, pues es evidente que en el desarrollo de la actividad empresarial que desempeñan se ven obligadas a un continuo tratamiento de datos personales tanto de los clientes como de terceros.

En el presente caso, valorados los criterios de graduación de las sanciones establecidos en el artículo 45.4, en particular el carácter continuado de la infracción y la vinculación de la actividad de la entidad denunciada con la realización de tratamientos de datos de carácter personal, se establece la imposición de una multa de 6.000 € por la infracción del artículo 9 de la LOPD, en relación con el artículo 92 del Reglamento de la LOPD, de la que SEGURIDAD EN LA GESTION debe responder.>>

III

El recurrente ha alegado que no ha negado nunca que los sobres corporativos contenían descripciones de los servicios prestados por la entidad; que la mención cobro de morosos que figura en los sobres se fundamenta únicamente en función de su tamaño y que la interpretación de los hechos es extensiva, injustificada y contraria a la seguridad jurídica.

Sin embargo, tales manifestaciones no pueden ser admitidas. En el supuesto que nos ocupa es un hecho contrastado que el recurrente envió al denunciante requerimientos de pago acerca de una deuda y que en los sobres enviados se hacía constar tanto en el anverso como en el reverso el literal *COBRO DE MOROSOS*, incumpliendo las pertinentes medidas de seguridad concernientes al ensobrado en la comunicación dirigida al deudor; obligación que recae en el responsable del fichero que debe adoptar las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos.

Es evidente que el soporte utilizado para el traslado de la información debe incluir y contener necesariamente los datos relativos al denunciante para que la citada comunicación permita ser recepcionada por el mismo. Sin embargo, en el citato soporte se ha incorporado una expresión, tanto en el anverso como en el reverso, el literal *COBRO DE MOROSOS*, que con independencia de su tamaño y de que se refiera a la descripción de la actividad de la recurrente, está ofreciendo una información que vulnera lo señalado en el artículo 9.1 de la LOPD, en relación con el artículo 92.3 del Reglamento de desarrollo de la LOPD, vinculándola y asociándola necesariamente con los datos de carácter personal que figuran en la ventanilla transparente, posibilitando deducir la condición de su destinatario, información que debería estar vedada a terceros,

para salvaguardar la confidencialidad del contenido de la comunicación.

En la resolución recurrida ya se informaba a la recurrente que la razón del requerimiento de pago como previo a la inclusión de los datos en los ficheros de morosidad correspondiente, tenía como objeto que el deudor conociera la existencia de la deuda y la posibilidad de ser incluido en un fichero de morosos en el supuesto de no hacerla efectiva, sin necesidad de acudir a formulas tan discutibles e intimidatorias como la que es analizada en el presente caso.

La vulneración de las medidas de seguridad, acción típica, se halla previsto en el articulo 44.3.h) que 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",* por lo que contrariamente a lo alegado por el recurrente se ha respetado la legalidad no existiendo interpretación extensiva, ni injustificada, ni contraria a la seguridad jurídica.

IV

Por lo tanto, en el presente recurso de reposición, Seguridad en la Gestión, S.L. 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 Seguridad en la Gestión, S.L. contra la Resolución de esta Agencia Española de Protección de Datos dictada con fecha 15 de febrero de 2013, en el procedimiento sancionador PS/00457/2012.

SEGUNDO: NOTIFICAR la presente resolución a la entidad Seguridad en la Gestión, S.L.

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