Roj: **SAN 4700/2018** - **ECLI:ES:AN:2018:4700**

Id Cendoj: **28079230012018100553**
Órgano: **Audiencia Nacional. Sala de lo Contencioso**
Sede: **Madrid**
Sección: **1**
Fecha: **30/11/2018**
Nº de Recurso: **302/2017**
Nº de Resolución:
Procedimiento: **Procedimiento ordinario**
Ponente: **FERNANDO DE MATEO MENENDEZ**
Tipo de Resolución: **Sentencia**

A U D I E N C I A N A C I O N A L

Sala de lo Contencioso-Administrativo

SECCIÓN PRIMERA

Núm. de Recurso: 0000302 /2017

Tipo de Recurso: **PROCEDIMIENTO ORDINARIO**

Núm. Registro General: **03015/2017**

Demandante: **ASOCIACIÓN DE TÉCNICOS EN INFORMÁTICA**

Procurador: **DOMINGO JOSÉ COLLADO MOLINERO**

Letrado: **JOSEP JOVER PADRÓ**

Demandado: **AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS**

Abogado Del Estado

Ponente Ilmo. Sr.: **D. FERNANDO DE MATEO MENÉNDEZ**

S E N T E N C I A Nº:

Ilmo. Sr. Presidente:

D. EDUARDO MENÉNDEZ REXACH

Ilmos. Sres. Magistrados:

Dª. FELISA ATIENZA RODRIGUEZ

Dª. LOURDES SANZ CALVO

D. FERNANDO DE MATEO MENÉNDEZ

Dª. NIEVES BUISAN GARCÍA

Madrid, a treinta de noviembre de dos mil dieciocho.

Vistos por la Sala, constituida por los Sres. Magistrados relacionados al margen, los autos del recurso contencioso-administrativo número 302/17, interpuesto por el Procurador de los Tribunales don Domingo José Collado Molinero, en nombre y representación de la **ASOCIACIÓN DE TÉCNICOS EN INFORMÁTICA,** contra la resolución de 22 de marzo de 2017, de la Directora de la Agencia Española de **Protección** de **Datos**, por la que se impone una sanción a la asociación recurrente de 45.000 euros por una infracción del art. 33 de la Ley Orgánica 15/1999, de 13 de diciembre, tipificada como infracción muy grave en el art. 44.4.d) de la citada norma, y una sanción de 5.000 euros por la infracción del art. 22.2 de la Ley 34/2002, de Servicios de la Sociedad de la Información y del Comercio Electrónico, tipificada como leve en el art. 38.4.g) de dicha Ley.

Ha sido parte **LA ADMINISTRACIÓN DEL ESTADO**, representada por el Abogado del Estado. La cuantía del recurso quedó fijada en 50.000 euros.

AN TECEDENTES DE HECHO

PRIMERO .- Admitido el recurso y previos los oportunos trámites procedimentales, se confirió traslado a la parte actora para que, en el término de veinte días formalizara la demanda, lo que llevó a efecto mediante escrito presentado el día 7 de octubre de 2017 en el que, tras exponer los hechos y fundamentos de derecho que estimó oportunos, terminó solicitando que se dictara sentencia por la que se acordara:

"A) Proceder a la anulación de las sanciones recibidas por la Asociación de Técnicos en Informática, por los motivos y fundamentos de derecho antes expuestos.

B) Tener por interpuesto el reenvío prejudicial al Tribunal de Justicia de la UE, sugiriendo esta parte las preguntas siguientes

*PRIMERA.- ¿Es el correo de contacto de una asociación de profesionales, correo que han dado un afiliado para que les contacten como profesional, un **dato** de carácter personal según el nuevo REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la **protección** de las personas físicas en lo que respecta al tratamiento de **datos** personales y a la libre circulación de estos **datos** y por el que se deroga la Directiva 95/46/CE (Reglamento general de **protección** de **datos**)?*

*SEGUNDA.- En caso de que la respuesta a la pregunta anterior sea negativa, ¿Habiendo establecido el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la **protección** de las personas físicas en lo que respecta al tratamiento de **datos** personales y a la libre circulación de estos **datos** y por el que se deroga la Directiva 95/46/CE (Reglamento general de **protección** de **datos**) un régimen sancionatorio determinado en el articulado del mismo, puede un estado, una vez en vigor el mismo, establecer otro régimen sancionatorio diferente?*

*TERCERA.- ¿Puede una Agencia de **Protección** de **Datos** Estatal aplicar otro régimen sancionador que no sea el del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la **protección** de las personas físicas en lo que respecta al tratamiento de **datos** personales y a la libre circulación de estos **datos** y por el que se deroga la Directiva 95/46/CE (Reglamento general de **protección** de **datos**) y aplicar sanciones por aquellas infracciones que no están comprendidas en el nuevo Reglamento?*

*CUARTA.- ¿Puede una Agencia de **Protección** de **Datos** Estatal que ha establecido públicamente una moratoria que afecta a la ejecución de una sentencia del TJUE, aplicarla ésta con discrecionalidad? Se vulnera en este caso los arts. 6, 8, 21, 41, 48 y 53 de la Carta de Derechos Fundamentales de los Ciudadanos de la UE.*

C) Subsidiariamente, y valorando la ausencia de mala fe de esta parte y el cúmulo de situaciones sobrevenidas, declaraciones de entidades públicas, de la Unión y del Estado Español, reducir la gravedad y cuantía de la sanción de forma que no le suponga un impacto económico para ATI, que la obligaría a cerrar".

SEGUNDO .- Formalizada la demanda se dio traslado de la misma a la parte demandada para que la contestara en el plazo de veinte días, lo que realizó mediante el pertinente escrito, alegando los hechos y fundamentos jurídicos que estimó pertinentes, solicitando la desestimación del recurso, con expresa imposición de costas a la parte recurrente.

TERCERO .- No habiendo solicitado las partes el recibimiento del recurso a prueba, ni la formulación de conclusiones, quedaron los autos conclusos para sentencia, señalándose para votación y fallo el día 27 de noviembre del presente año, fecha en que tuvo lugar.

SIENDO PONENTEel Magistrado Ilmo. Sr. Don FERNANDO DE MATEO MENÉNDEZ.

FU NDAMENTOS DE DERECHO

PRIMERO .- La parte demandante impugna la resolución de 22 de marzo de 2017, de la Directora de la Agencia Española de **Protección** de **Datos**, por la que se impone una sanción a la asociación recurrente de 45.000 euros por una infracción del art. 33 de la Ley Orgánica 15/1999, de 13 de diciembre (en adelante LOPD), tipificada como infracción muy grave en el art. 44.4.d) de la citada norma, y una sanción de 5.000 euros por la infracción del art. 22.2 de la Ley 34/2002, de Servicios de la Sociedad de la Información y del Comercio Electrónico (en lo sucesivo LSSI), tipificada como leve en el art. 38.4.g) de dicha Ley.

Los hechos por los que ha sido sancionada la asociación recurrente por infringir la LOPD, son por realizar transferencias internacionales de **datos** de carácter personal entre el 20 de octubre de 2015 y el 29 de marzo

de 2016, a la empresa The Rocket Science Group LLC (en adelante TRS), entidad radicada en los Estados Unidos de América, que presta el servicio MailChimp de gestión de envíos de correo electrónico, sin mediar autorización previa de la Directora de la Agencia Española de **Protección** de **Datos**.

Por otro lado, la imposición de la sanción por la infracción del art. 22.2 de la LSSI es por no facilitar, con anterioridad a la realización de los envíos de las campañas, ningún tipo de información a los destinatarios de los correos electrónicos remitidos por la parte actora a través de MailChimp, relativa a la instalación por parte del tercero prestador del citado servicio en dichos envíos, de dispositivos de seguimiento de la actividad de los destinatarios, a fin de controlar la apertura de los correos y la pulsación de los enlaces contenidos en los correos, y poder elaborar con la información recabada, informes de seguimiento de las campañas.

SEGUNDO.- La primera cuestión que se suscita por la parte recurrente es que, los correos electrónicos transferidos pertenecientes a asociados y amigos de la entidad denunciada, no son **datos** de carácter personal, sino de carácter profesional, y, por tanto, excluidos de la aplicación de la LOPD.

El concepto de **dato** de carácter personal aparece definido en el art. 3.a) de la LOPD, como *"cualquier información referente a personas físicas identificadas o identificables"*.

Por su parte, el art. 5 del Reglamento de desarrollo de la citada Ley, aprobado por Real Decreto 1.720/2007, de 21 de diciembre, define en su apartado 1.f) los **datos** de carácter personal, como *"cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier tipo concerniente a personas físicas identificadas o identificables"*. Y en el apartado 1.o) se define persona identificable, como *"toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier comunicación referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados"*.

Por otro lado, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la **protección** de las personas físicas en lo que respecta al tratamiento de **datos** personales y a la libre circulación de estos **datos**, y por el que se deroga la Directiva 95/46/CE (Reglamento general de **protección** de **datos**), define "**datos** personales", como *"toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, **datos** de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona"*.

En cuanto a la dirección de correo electrónico, en nuestra Sentencia de 15 de enero de 2015 -recurso nº. 297/2010-, dijimos: <<*... esta Sala ha considerado en las SSAN, Sec. 1ª, de 23 de marzo 2006 (Rec. 911/2003) y de 25 de mayo de 2006 (Rec. 536/2004), que la dirección de correo electrónico de la que es titular una persona física, constituye una información que le concierne, que le afecta, y que forma parte del ámbito de su privacidad protegido por la Ley de **Protección** de **Datos**, siéndole plenamente aplicable su régimen jurídico.*

*En dichos procedimientos se argumentaba que en los supuestos a los que se referían la dirección de correo electrónico no recogía el nombre y apellidos de su titular y no tenía vinculación con su identidad, por lo que no debería considerarse como **dato** de carácter personal, pero ello fue desestimado por las citadas sentencias. En concreto, la SAN de 25 de mayo de 2006 especificaba que la dirección de correo electrónico de que es titular una persona física constituye un **dato** personal porque "con independencia de que la denominación de la dirección corresponda o no con el nombre y apellido de su titular, país o empresa en la que trabaja, lo cierto es que se puede mediante una operación nada difícil, identificar perfectamente a una persona física, ya que esa dirección de correo electrónico aparecerá vinculada a un dominio concreto, por lo que sólo será necesario consultar al servidor en que se gestione dicho servicio. Es más esta Sala, en un caso como el número del Documento Nacional de Identidad, que en principio no tiene aparente relación externa con el nombre y apellido de su titular, ha entendido que es un **dato** de carácter personal amparado por la LOPD en la sentencia de 27 de octubre de 2004 (Rec. 1112/2002)".*

*Por tanto, la dirección de correo electrónico de una persona física, en la medida que permite identificar a su titular sin plazos ni actividades desproporcionadas, constituye un **dato** personal y su tratamiento en casos como el presente, y sin perjuicio de las previsiones específicas establecidas por la Ley de Servicios de Sociedad de la Información para otros supuestos, está sometido a las previsiones de la LOPD*>>.

Pues bien, en el caso que nos ocupa, en el fichero "Asociados" cuyo responsable es la parte actora, junto a los correos electrónicos de los asociados, aparece la siguiente información de carácter personal de los mismos: DNI, nombre y apellidos, dirección del asociado.

Por tanto, conforme a lo expuesto, los correos electrónicos son **datos** de carácter personal, pues permiten identificar fácilmente a personas físicas vinculadas al sector de las Tecnologías de la Información y de la Comunicación.

TERCERO.- Así las cosas, una vez determinada la condición de **datos** de carácter personal de los correos electrónicos, objeto de tratamiento por la asociación demandante, resulta necesario determinar si al tratamiento efectuado por dicha asociación, con la reseñada información, le pudiera resultar de aplicación lo dispuesto en los apartados 2 y 3 del art. 2 del Real Decreto 1.720/2007, de 21 de diciembre, que establecen: *"2. Este reglamento no será aplicable a los tratamientos de **datos** referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los **datos** de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.*

*3. Asimismo, los **datos** relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la **protección** de **datos** de carácter personal".*

Como hemos declarado en la reciente Sentencia de 2 de noviembre de 2018 -recurso nº. 50/2017-: *<<... en el derecho a la **protección** de **datos** de carácter personal quedan incluidos **datos** de los profesionales individuales, como se deriva del art. 2 del Real Decreto 1.720/2007, de 21 de diciembre , y así se puso de manifiesto por el Tribunal Supremo en la Sentencia de 20 de febrero de 2007 -recurso nº. 732/2003 -.*

*Como decíamos al respecto en nuestra Sentencia de 12 de mayo de 2011 -recurso nº. 31/2010 -, se trata del problema de la aplicación o no de la normativa sobre **protección** de **datos** a aquellos supuestos en que los **datos** se refieran a personas físicas, pero que lleven a cabo una actividad mercantil o profesional. Se añadía que: <<Para ello es imprescindible recordar algunas de las consideraciones de la STC 292/2000, de 30 de noviembre , que establece que (FJ 6º) el objeto de **protección** del derecho fundamental a la **protección** de **datos** no se reduce solo a los **datos** íntimos de la persona sino a cualquier tipo de **datos** personales, sean o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está el art. 18.1 CE (6), sino los **datos** de carácter personal. Por consiguiente, también alcanza a aquellos **datos** personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado, porque así lo garantiza su derecho a la **protección** de **datos** (pues) los **datos** amparados son todos aquellos que identifiquen o permitan la identificación de la persona pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituye una amenaza para el individuo.*

*No puede concluirse, por tanto, que los empresarios individuales y profesionales estén en su conjunto excluidos del ámbito de **protección** de la LOPD, sino que se hace necesario diferenciar (y la línea divisoria es confusa y difusa) cuando un **dato** del empresario o profesional, se refiere a la vida privada de la persona y cuando a la empresa o profesión, pues solo en el primer caso cabe aplicar la **protección** de la LO 15/1999. Labor de diferenciación que puede basarse en dos criterios distintos y complementarios:*

*Uno, el criterio objetivo de la clase y la naturaleza de los **datos** tratados, según estén en conexión y se refieran a una esfera (la íntima y personal) o a otra (la profesional) de la actividad. Otro, el de la finalidad del tratamiento y circunstancias en que éste se desarrolla, criterio éste que operaría en aquellos casos en que alguno de los **datos** profesionales coincida con los particulares (por ej. coincidencia de domicilio privado con el de la empresa, o cuando no se pueda acreditar si una deuda es de la empresa o si es personal del interesado)>>.*

*Acorde con lo expuesto, y haciendo hincapié en que la LOPD tiene por objeto garantizar y proteger los **datos** personales entendiendo por tales, art. 3.a) de dicha Ley "cualquier información concerniente a persona física identificadas o identificables", esta Sala ha considerado, en ocasiones anteriores en que se ha planteado la misma controversia, que bajo determinadas circunstancias dicha Ley sí ampara los **datos** personales de los profesionales en tanto que no dejaban por ello de ser personas físicas. Así, ha ocurrido en nuestra Sentencia de 21 de noviembre de 2002 -recurso nº. 881/2000 -, en relación **datos** personales de arquitectos en el mercado de la construcción; en la Sentencia de 25 de junio de 2003 -recurso nº. 1.099/2000 -, en relación con **datos** personales de promotores en la construcción de su propia vivienda, y en la Sentencia de 11 de febrero de 2004 -recurso nº.119/2002 -, y ya bajo la vigencia de la actual LOPD, hemos entendido que el **dato** del afectado, aunque se refería al lugar de ejercicio de su profesión, concretamente un despacho de abogados, era un **dato** de una persona física con una actividad profesional cuya **protección** caía en la órbita de la Ley Orgánica 15/1999*

*En el mismo sentido, tal y como nos recuerda la Sentencia de 9 de junio de 2011 -recurso nº. 147/2010 -, precisábamos en nuestra Sentencia de 14 de febrero de 2007 -recurso nº. 186/2005 -, que: "Si cualquier persona física tiene derecho a la **protección** de los **datos** personales, no parece que puedan ser excluidos de tal **protección***

*los **datos** personales de todas aquellas personas físicas que, obviamente conservando tal condición, también tengan la condición de profesionales, pues la adicción de esta circunstancia no les priva de sus derechos como ciudadanos, salvo que estos profesionales organicen su actividad bajo fórmulas mercantiles y que se acredite que los **datos** eran ajenos a su esfera privada y ostentaban una clara vinculación con la actividad mercantil"...*

Finalmente, hemos reiterado la doctrina expuesta en las de Sentencias de 15 de julio de 2016 - recurso nº. 225/2014-, de 19 de junio de 2104 - recurso nº. 253/2013 -, y de 25 de octubre de 2013 - recurso nº. 145/2012 -, en la que se cita como precedentes, entre otros, nuestras Sentencias de 12 de mayo de 2011 - recurso nº. 31/2010-, de 10 de septiembre de 2009 - recurso nº. 89/2008 -, y de 29 de marzo de 2006 - recurso nº. 348/2004 ->>.

Por consiguiente, la información contenida en los apartados 2 y 3 del art. 2 del Real Decreto 1.720/2007, de 21 de diciembre, anteriormente reseñada, en el fichero en el que se encuentran registrados los correos electrónicos, de los que son usuarios o titulares los socios y amigos de la parte actora, no incluyen esta información como un medio para contactar con las personas jurídicas en la que éstos pudieran prestar servicios, tal y como se exige en el citado art. 2.2.

Por otro lado, en el fichero se incluyen también el DNI y fecha de nacimiento de los afectados, así como **datos** bancarios de los mismos, información que, evidentemente, excede de la detallada en art. 2 del Real Decreto 1.720/2007, de 21 de diciembre.

Además, no se ha probado por la asociación recurrente que los socios y amigos, que recibieron los correos electrónicos remitida desde el servicio MailChimp, fueran únicamente empresarios individuales en los términos del mencionado precepto. Es más, a tenor de las campañas remitidas por la parte actora, tanto con anterioridad como con posterioridad a la Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) de 6 de octubre de 2015, éstas no iban destinadas exclusivamente a comerciantes. En este sentido, basta poner de manifiesto las campañas sobre los asuntos: *"Novedades de diciembre de nuestro colaborador Ediciones ENI, editorial especializada en libros de informática"*, *"Pídenos tu invitación para la Semana de la educación AULA en Madrid"*, *" Convocatoria de Elecciones a la Junta Directiva General de ATI"*, *"TECHNO-LUNCH CTECNO. Vine a dinar amb en Dídac Lee. Descompte pels socis de l'ATI"*, *"Estudio sobre privacidad de **datos** en el entorno sanitario"*, *"Webinar Gratuito 28 Octubre-Algunas claves para la informatización de un archivo hospitalario"*, y *"Presentación de Novática y entrega de Premio Novatica 2015"*.

Finalmente, según la página web de la asociación recurrente, ésta cuenta "socios de número", "Jubilados", socios "Adheridos", y socios "Invitados". Es decir, el tratamiento efectuado se dirige tanto a personas físicas identificadas que están, o estuvieron, vinculadas profesionalmente con el sector informático, como a personas que no son profesionales informáticos, pero están interesados en participar en las actividades desarrolladas por la parte actora dentro del sector de la informática.

Por tanto, a tenor de lo expuesto, los **datos** transferidos por la parte actora, son **datos** de carácter personal que se encuentran bajo la aplicación de la LOPD.

***CUARTO*.-** La infracción imputada a la parte actora de la LOPD es la vulneración de los arts. 33, no concurriendo las excepciones de los apartados e) y k) del art 34.

El art. 33 dispone: *"1. No podrán realizarse transferencias temporales ni definitivas de **datos** de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de **protección** equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de **Protección** de **Datos**, que sólo podrá otorgarla si se obtienen garantías adecuadas.*

*2. El carácter adecuado del nivel de **protección** que ofrece el país de destino se evaluará por la Agencia de **Protección** de **Datos** atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de **datos**. En particular, se tomará en consideración la naturaleza de los **datos**, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países"*.

Mientras que los anteriormente citados apartados del art. 34 establecen que, no será de aplicación lo dispuesto en el artículo anterior cuando: *"e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista. (...)*

*k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de **protección** adecuado"*.

Por su parte, en el Real Decreto 1.720/2007, de 21 de diciembre, las transferencias internacionales de **datos**, se encuentran recogidas en los artículos 65 a 70, que se reproducen a continuación, con la excepción del art. 69, que hace referencia a la suspensión temporal de transferencias.

Artículo 65. *"Cumplimiento de las disposiciones de la Ley Orgánica 15/1999 , de 13 de diciembre. La transferencia internacional de **datos** no excluye en ningún caso la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento".*

Artículo 66. *"Autorización y notificación. 1. Para que la transferencia internacional de **datos** pueda considerarse conforme a lo dispuesto en la Ley Orgánica 15/1999 , de 13 de diciembre, y en el presente Reglamento será necesaria la autorización del Director de la Agencia Española de **Protección** de **Datos**, que se otorgará en caso de que el exportador aporte las garantías a las que se refiere el artículo 70 del presente reglamento.*

La autorización se otorgará conforme al procedimiento establecido en la sección primera del capítulo V del título IX de este reglamento.

2. La autorización no será necesaria:

*a) Cuando el Estado en el que se encontrase el importador ofrezca un nivel adecuado de **protección** conforme a lo previsto en el capítulo II de este título.*

b) Cuando la transferencia se encuentre en uno de los supuestos contemplados en los apartados a) a j) del artículo 34 de la Ley Orgánica 15/1999 , de 13 de diciembre.

*3. En todo caso, la transferencia internacional de **datos** deberá ser notificada a fin de proceder a su inscripción en el Registro General de **Protección** de **Datos**, conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento".*

Artículo 67. *"Nivel adecuado de **protección** acordado por la Agencia Española de **Protección** de **Datos**.*

*1. No será precisa autorización del Director de la Agencia Española de **Protección** de **Datos** a una transferencia internacional de **datos** cuando las normas aplicables al Estado en que se encontrase el importador ofrezcan dicho nivel adecuado de **protección** a juicio del Director de la Agencia Española de **Protección** de **Datos**.*

*El carácter adecuado del nivel de **protección** que ofrece el país de destino se evaluará atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de **datos**. En particular, se tomará en consideración la naturaleza de los **datos**, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.*

*Las resoluciones del Director de la Agencia Española de **Protección** de **Datos** por las que se acordase que un determinado país proporciona un nivel adecuado de **protección** de **datos** serán publicadas en el "Boletín Oficial del Estado".*

Artículo 68. *"Nivel adecuado de **protección** declarado por Decisión de la Comisión Europea.*

*No será necesaria la autorización del Director de la Agencia Española de **Protección** de **Datos** para la realización de una transferencia internacional de **datos** que tuvieran por importador una persona o entidad, pública o privada, situada en el territorio de un Estado respecto del que se haya declarado por la Comisión Europea la existencia de un nivel adecuado de **protección**".*

Artículo 70. *"Transferencias sujetas a autorización del Director de la Agencia Española de **Protección** de **Datos**.*

*1. Cuando la transferencia tenga por destino un Estado respecto del que no se haya declarado por la Comisión Europea o no se haya considerado por el Director de la Agencia Española de **Protección** de **Datos** que existe un nivel adecuado de **protección**, será necesario recabar la autorización del Director de la Agencia Española de **Protección** de **Datos**. La autorización de la transferencia se tramitará conforme al procedimiento establecido en la sección primera del capítulo V del título IX del presente reglamento.*

*2. La autorización podrá ser otorgada en caso de que el responsable del fichero o tratamiento aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la **protección** de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.*

A tal efecto, se considerará que establecen las adecuadas garantías los contratos que se celebren de acuerdo con lo previsto en las Decisiones de la Comisión Europea 2001/497/CE, de 15 de Junio de 2001, 2002/16/CE, de

27 de diciembre de 2001, y 2004/915/CE, de 27 de diciembre de 2004 o de lo que dispongan las Decisiones de la Comisión que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE ".

QUINTO- Así las cosas, las transferencias internacionales de **datos** llevadas a cabo por la parte actora desde el inicio de la relación contractual, el 14 de junio de 2014, a la empresa TRS, radicada en los EE.UU, hasta el 6 de octubre de 2015, se encontraban amparadas en la Decisión de la Comisión 2000/520/CE, que consideraba que el acuerdo de "Puerto Seguro", ofrecía un nivel adecuado de **protección** para las transferencias internacionales de **datos** desde la Unión Europea a Estados Unidos de América.

Pero dicha situación cambió, con la declaración de invalidez de la Decisión 2000/520/CE, adoptada por la Sentencia C-362/14 del TJUE de 6 de octubre de 2015, que entendió que el acuerdo de "Puerto Seguro" (Safe Harbour), no proporcionaba un nivel adecuado de **protección** de las garantías para la realización de transferencias de **datos** desde la Unión Europea a EE.UU. Por tanto, para las transferencias internacionales, la asociación recurrente debió acudir a la norma general del art. 33 de la LOPD respecto del movimiento internacional de **datos**, así como al resto de preceptos de la normativa de **protección** de **datos**, relacionados con el régimen de transferencias internacionales de **datos**.

Según la parte asociación demandante, la Agencia Española de **Protección** de **Datos**, y la figura de su Directora, mediante cartas a las empresas, discursos e incluso colgándolo en la propia página web, concedió un periodo de transitoriedad hasta el 30 de enero de 2016, mientras que el 2 de febrero de 2016, la Unión Europea anunció el "Escudo de Privacidad" (Privacy Shield). Por lo que únicamente, podría resultar reprochable el espacio existente entre ambas fechas, no habiéndose acreditado que se hubiese enviado ninguna comunicación entre las mismas, aludiéndose a la teoría de los actos propios.

En relación con la doctrina de los actos propios resulta de interés lo declarado en las Sentencias del Tribunal Supremo de 28 de diciembre 2012 -recurso nº. 273/2009- y 3 julio 2013 -recurso nº. 2.511/2011-, entre otras, que tratan sobre la infracción del principio de vinculación por actos propios, doctrina, surgida originariamente en el ámbito del derecho privado, que significa la vinculación del autor de una declaración de voluntad al sentido objetivo de la misma y la imposibilidad de adoptar después un comportamiento contradictorio, encontrándose la misma doctrina estrechamente ligada al principio de buena fe y de **protección** de la confianza legítima, que estaba en el art. 3.1 de la Ley 30/1992, de 26 de noviembre, y actualmente, en el art. 3.1.e) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y que ha sido acogida igualmente por la jurisprudencia del Tribunal Supremo (SS.TS. de 1 de febrero de 1990; 13 de febrero y 4 de junio de 1992; 28 de julio de 1997). En consecuencia, tal doctrina, indican las citadas Sentencias, supone que la actuación de las Administraciones Públicas no puede ser alterada arbitrariamente, y añaden: < *<En concreto, en la STS de esta Sala de 26 de febrero de 2001, RC 5453/1995 dijimos que "Tanto la doctrina del Tribunal Constitucional como la Jurisprudencia de este Alto Tribunal (STS de 1 de febrero de 1999) considera que el principio de buena fe protege la confianza que fundadamente se puede haber depositado en el comportamiento ajeno e impone el deber de coherencia en el comportamiento propio. Lo que es tanto como decir que dicho principio implica la exigencia de un deber de comportamiento que consiste en la necesidad de observar de cara al futuro la conducta que los actos anteriores hacían prever y aceptar las consecuencias vinculantes que se desprenden de los propios actos, constituyendo un supuesto de lesión a la confianza legítima de las partes "venire contra factum propium". Ahora bien, este principio no puede invocarse para crear, mantener o extender, en el ámbito del Derecho público, situaciones contrarias al ordenamiento jurídico, o cuando del acto precedente resulta una contradicción con el fin o interés tutelado por una norma jurídica que, por su naturaleza, no es susceptible de amparar una conducta discrecional por la Administración que suponga el reconocimiento de unos derechos y/u obligaciones que dimanen de actos propios de la misma. O, dicho en otros términos, la doctrina invocada de los "actos propios" sin la limitación que acaba de exponerse podría introducir en el ámbito de las relaciones de Derecho público el principio de la autonomía de la voluntad como método ordenador de materias reguladas por normas de naturaleza imperativa, en las que prevalece el interés público salvaguardado por el principio de legalidad; principio que resultaría conculcado si se diera validez a una actuación de la Administración contraria al ordenamiento jurídico por el solo hecho de que así se ha decidido por la Administración o porque responde a un precedente de ésta>>.*

En la resolución sancionadora se declara lo siguiente, sobre la cuestión que estamos analizando: *<<Sobre este particular, en primer lugar señalar que los comunicados realizados desde el Grupo de Trabajo del Artículo 29, así como las notas de prensa o publicaciones realizadas desde la Agencia Española de **Protección** de **datos**, en nada modifican la responsabilidad que se atribuye a ATI en la comisión de la infracción que ahora se analiza. Así, en la nota de prensa de fecha 19 de octubre de 2015, referente a la publicación de una declaración conjunta de las Autoridades Europeas de **Protección** de **Datos** en relación con la aplicación se la sentencia del TJUE sobre Puerto Seguro, se advierte claramente que durante el período que se buscan soluciones políticas, jurídicas y técnicas que permitan transferencias de **datos** al territorio de EEUU respetando los derechos fundamentales, "las Autoridades de **protección** de **datos** consideran que las Cláusulas Contractuales Tipo y las Normas Corporativas Vinculantes*

*(BCRs) pueden seguir utilizándose. En cualquier caso, esto no impedirá que las Autoridades de **protección** de **datos** investiguen casos particulares, por ejemplo a partir de denuncias, y ejerzan sus poderes con el fin de proteger a las personas".*

*También en dicha nota, tras precisar que "las transferencias que aún se estén llevando a cabo bajo la Decisión Puerto Seguro tras la sentencia del TJUE son ilegales.", se indica que "Con el fin de garantizar que todos los actores están suficientemente informados, las Autoridades de **protección** de **datos** de la UE van a poner en marcha campañas de información adecuadas en sus respectivos países. Esto puede incluir información directa a todas las empresas respecto de las que conste que utilizaban la Decisión de Puerto Seguro, así como mensajes generales en los sitios web de las Autoridades."*

En dicha comunicación, por lo tanto, se advertía la posibilidad de iniciar actuaciones de investigación en caso de denuncia, tal y como ha ocurrido en este caso a raíz de la denuncia presentada con fecha 29 de enero de 2016 por un afectado, ya que en ningún caso la AEPD puede hacer dejación de sus funciones y competencias.

*Posteriormente en la comunicación de fecha 9 de diciembre de 2015, sobre la aplicación de la sentencia de Puerto Seguro, la AEPD señalaba que "El marco temporal definido por las Autoridades europeas de **protección** de **datos** se concreta, en el caso de España, en que los responsables informen al Registro General de **Protección** de **Datos** de la AEPD antes de finales de enero sobre la continuidad de las transferencias y sobre su adecuación a la normativa de **protección** de **datos**. La Agencia en ningún momento ha anunciado su intención de iniciar procedimientos sancionadores por defecto contra las empresas. En la comunicación enviada a los responsables, la AEPD sólo indica que, de no modificarse la base legal para la realización de transferencias, la Agencia podrá iniciar el procedimiento para acordar, en su caso, la suspensión temporal de transferencias."*

*En cuanto a la nota de prensa de 3 de febrero de 2016, se trata de una información facilitada por la AEPD "con el objetivo de ofrecer información a los responsables que realizan transferencias de **datos** a EEUU" que se limita a señalar que la Comisión Europea y EEUU anuncian un nuevo marco para la realización de transferencias internacionales, advirtiendo, además, que la "CE ha anunciado que en las próximas semanas prepara un borrador de "Decisión de adecuación". Por lo que dicha nota de prensa no modifica en modo alguno la situación anterior, ni exime del cumplimiento a los responsables del tratamiento de obtener la autorización a la que se refiere el artículo 33 de la LOPD .*

*En cuanto a la nota de prensa de la AEPD de 29 de junio de 2016 trata de la inauguración de la 8ª Sesión Anual Abierta de la AEPD por el ministro de Justicia en funciones, refiriéndose básicamente a los retos de asumir el nuevo Reglamento General de **Protección** de **Datos**...*

*Además, tampoco consta que ATI con posterioridad a la Sentencia de 6 de octubre de 2015 procediese a notificar la modificación del fichero "Asociados" a fin de regularizar la falta de inscripción previa en el fichero Registro General de **Protección** de **Datos** de la AEPD de las transferencias internacionales de **datos** que venía realizando con las cuentas de correo registradas en dicho fichero desde que en junio de 2014 contrató el servicio MailChimp de TRS, ...*

*Igualmente, en el período posterior a la reseñada STJUE, en el que consta que ATI continuó realizando transferencias internacionales de **datos** a EEUU, dicha Asociación no solicitó la iniciación de procedimiento de autorización de transferencias internacionales de **datos** de conformidad con lo dispuesto en el artículo 137.1 del RLOPD...*

En todo caso, la afiliación de TRS al mecanismo "Privacy Shield" o "Escudo de Privacidad" con fecha 21 de noviembre de 2016 resulta irrelevante a los efectos que nos ocupan, ya que dicha circunstancia se produce meses después de haber finalizado la relación contractual existente entre ambas partes>>.

Por tanto, a tenor de lo relatado, de las citadas notas de prensa o comunicaciones no se desprende el reconocimiento por la Agencia Española de **Protección** de **Datos**, la existencia de un período de transitoriedad como pretende la parte actora, y, en todo caso, debe prevalecer el interés público salvaguardado por el principio de legalidad. Por lo que no ha resultado conculcado la doctrina de los actos propios.

SEXTO.- Por otro lado, aduce la asociación recurrente, que resulta de aplicación el Reglamento General de **Protección** de **Datos**, de conformidad con el art. 128 de la Ley 30/1992, de 26 de noviembre, aludiéndose al expositivo 51 y a los art. 9 y 3.3 del citado Reglamento.

De conformidad con los arts. 94 y 99 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la **protección** de las personas físicas en lo que respecta al tratamiento de **datos** personales y a la libre circulación de estos **datos**, y por el que se deroga la Directiva 95/46/CE (Reglamento general de **protección** de **datos**) -en lo sucesivo RGPD-, si bien entró en vigor el 25 de mayo de 2016, no comenzó

a aplicarse hasta el 25 de mayo de 2018, por lo que en el momento de dictarse la resolución sancionadora no resultaba de aplicación, tal y como se razona en la misma. Pero en cambio, si lo sería en esta vía judicial.

El art. 26.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, aplicable a la sazón, establece, en el mismo sentido que el art. 28 de la Ley 30/1992, de 26 de noviembre, invocado por la parte actora, que: *"Las disposiciones sancionadoras producirán efecto retroactivo en cuanto favorezcan al presunto infractor o al infractor, tanto en lo referido a la tipificación de la infracción como a la sanción y a sus plazos de prescripción, incluso respecto de las sanciones pendientes de cumplimiento al entrar en vigor la nueva disposición"*.

La Sentencia del Tribunal Supremo de 30 de octubre de 2012 -recurso nº. 964/2010- declara al respecto: *<< Esta Sala ha señalado en sentencias de 24 de enero de 2006 (recurso 419/2002), 31 de enero de 2007 (recurso 8873/2003) y 13 de febrero de 2008 (recurso 2110/2004), que el principio de retroactividad de las normas administrativas sancionadoras obliga a aplicar retroactivamente dichas normas en todo aquello que pudiera ser más beneficioso para el presunto infractor, y "...tal aplicación debe llevarse a cabo en cualquier instancia administrativa o judicial donde se encuentre pendiente de enjuiciamiento o ejecución una resolución sancionadora, ya que no tendría sentido confirmar judicialmente la legalidad de una resolución administrativa, según la normativa vigente cuando fue dictada, para que la Administración proceda a dictar seguidamente otra que aplique retroactivamente la nueva norma sancionadora más favorable, resolución esta última que podría ser objeto de un nuevo recurso judicial">>.*

Por tanto, si fuese más favorable lo recogido sobre la cuestión que estamos tratando lo establecido en el RGPD, sería aplicable, pues nos movemos en el ámbito sancionador.

Así las cosas, las trasferencias de **datos** personales a terceros países u organizaciones internacionales, se recogen en el Capítulo V del RGPD, arts. 44 a 50. Los tres primeros artículos establecen:

Artículo 44: *"Principio general de las transferencias.*

*Solo se realizarán transferencias de **datos** personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de **datos** personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de **protección** de las personas físicas garantizado por el presente Reglamento no se vea menoscabado"*.

Artículo 45: *"Transferencias basadas en una decisión de adecuación.*

*1. Podrá realizarse una transferencia de **datos** personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de **protección** adecuado. Dicha transferencia no requerirá ninguna autorización específica.*

*2. Al evaluar la adecuación del nivel de **protección**, la Comisión tendrá en cuenta, en particular, los siguientes elementos:*

*a. el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los **datos** personales, así como la aplicación de dicha legislación, las normas de **protección** de **datos**, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de **datos** personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos **datos** personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;*

*b. la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de **protección** de **datos**, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y*

*c. los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la **protección** de los **datos** personales.*

*3. La Comisión, tras haber evaluado la adecuación del nivel de **protección**, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de **protección** adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 93 (Procedimiento de comité), apartado 2.*

4. La Comisión supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las decisiones adoptadas con arreglo al apartado 3 del presente artículo y de las decisiones adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE .

*5. Cuando la información disponible, en particular tras la revisión a que se refiere el apartado 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de **protección** adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el apartado 3 del presente artículo. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen a que se refiere el artículo 93 (Procedimiento de comité), apartado 2. Por razones imperiosas de urgencia debidamente justificadas, la Comisión adoptará actos de ejecución inmediatamente aplicables de conformidad con el procedimiento a que se refiere el artículo 93 (Procedimiento de comité), apartado 3.*

6. La Comisión entablará consultas con el tercer país u organización internacional con vistas a poner remedio a la situación que dé lugar a la decisión adoptada de conformidad con el apartado 5.

*7. Toda decisión de conformidad con el apartado 5 del presente artículo se entenderá sin perjuicio de las transferencias de **datos** personales al tercer país, a un territorio o uno o varios sectores específicos de ese tercer país, o a la organización internacional de que se trate en virtud de los artículos 46 a 49 (Sobre transferencias de **datos** con terceros países).*

*8. La Comisión publicará en el Diario Oficial de la Unión Europea y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de **protección** adecuado.*

9. Las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión adoptada de conformidad con los apartados 3 o 5 del presente artículo".

Artículo 46: *"Transferencias mediante garantías adecuadas.*

*1. A falta de decisión con arreglo al artículo (Transferencias basadas en una decisión de adecuación), apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir **datos** personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.*

2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:

a. un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;

b. normas corporativas vinculantes de conformidad con el artículo 47 (Transferencias basadas en una decisión de adecuación);

*c. cláusulas tipo de **protección** de **datos** adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93 (Procedimiento de comité), apartado 2;*

*d. cláusulas tipo de **protección** de **datos** adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93 (Procedimiento de comité), apartado 2;*

e. un código de conducta aprobado con arreglo al artículo 40 (Códigos de conducta), junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o

f. un mecanismo de certificación aprobado con arreglo al artículo 42 (Certificación), junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.

3. Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante:

a. cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los **datos** *personales en el tercer país u organización internacional, o*

b. disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

4. La autoridad de control aplicará el mecanismo de coherencia a que se refiere el artículo 63 en los casos indicados en el apartado 3 del presente artículo.

5. Las autorizaciones otorgadas por un Estado miembro o una autoridad de control de conformidad con el artículo 26 apartado 2, de la Directiva 95/46/CE seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por dicha autoridad de control. Las decisiones adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas, en caso necesario, por una decisión de la Comisión adoptada de conformidad con el apartado 2 del presente artículo".

Es decir, conforme a lo expuesto, en los supuestos de transferencias de **datos** internacionales, cuando no nos encontremos ante transferencias basadas en una decisión de adecuación, se viene a limitar la autorización administrativa, a diferencia de lo previsto en el art. 33 de la LOPD. Así, se necesitará autorización de la Agencia Española de **Protección** de **Datos**, cuando las garantías adecuadas se aporten mediante: a) cláusulas contractuales entre el responsable o el encargado y el responsable, y el encargado o destinatario de los **datos** personales en el tercer país u organización internacional, que no hayan sido adoptadas por la Comisión Europea o, b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

En este sentido, el Proyecto de Ley Orgánica de **Protección** de **Datos** Personales y Garantía de los Derechos Digitales, aprobado por las Cortes Generales, pendiente de su publicación en el B.O.E., en relación con las transferencias internacionales de **datos**, establece en el Título VI, arts. 40 a 43, lo siguiente:

Artículo 40. *"Régimen de las transferencias internacionales de* ***datos****.*

Las transferencias internacionales de ***datos*** *se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica y sus normas de desarrollo aprobadas por el Gobierno, y en las circulares de la Agencia Española de* ***Protección*** *de* ***Datos*** *y de las autoridades autonómicas de* ***protección*** *de* ***datos****, en el ámbito de sus respectivas competencias.*

En todo caso se aplicarán a los tratamientos en que consista la propia transferencia las disposiciones contenidas en dichas normas, en particular las que regulan los principios de ***protección*** *de* ***datos****".*

Artículo 41. *"Supuestos de adopción por la Agencia Española de* ***Protección*** *de* ***Datos****.*

1. La Agencia Española de ***Protección*** *de* ***Datos*** *y las autoridades autonómicas de* ***protección*** *de* ***datos*** *podrán adoptar, conforme a lo dispuesto en el artículo 46.2.c) del Reglamento (UE) 2016/679, cláusulas contractuales tipo para la realización de transferencias internacionales de* ***datos****, que se someterán previamente al dictamen del Comité Europeo de* ***Protección*** *de* ***Datos*** *previsto en el artículo 64 del citado reglamento.*

2. La Agencia Española de ***Protección*** *de* ***Datos*** *y las autoridades autonómicas de* ***protección*** *de* ***datos*** *podrán aprobar normas corporativas vinculantes de acuerdo con lo previsto en el artículo 47 del Reglamento (UE) 2016/679.*

El procedimiento se iniciará a instancia de una entidad situada en España y tendrá una duración máxima de nueve meses. Quedará suspendido como consecuencia de la remisión del expediente al Comité Europeo de ***Protección*** *de* ***Datos*** *para que emita el dictamen al que se refiere el artículo 64.1.f) del Reglamento (UF) 2016/679, y continuará tras su notificación a la Agencia Española de* ***Protección*** *de* ***Datos*** *o a la autoridad autonómica de* ***protección*** *de* ***datos*** *competente".*

Artículo 42. *"Supuestos sometidos a autorización previa de las autoridades de* ***protección*** *de* ***datos****.*

1. Las transferencias internacionales de ***datos*** *a países u organizaciones internacionales que no cuenten con decisión de adecuación aprobada por la Comisión o que no se amparen en alguna de las garantías previstas en el artículo anterior y en el artículo 46.2 del Reglamento (UE) 2016/679, requerirán una previa autorización de la*

*Agencia Española de **Protección** de **Datos** o, en su caso, autoridades autonómicas de **protección** de **datos**, que podrá otorgarse en los siguientes supuestos:*

a) Cuando la transferencia pretenda fundamentarse en la aportación de garantías adecuadas con fundamento en cláusulas contractuales que no correspondan a las cláusulas tipo previstas en el artículo 46.2, letras c) y d), del Reglamento (UE) 2016/679.

b) Cuando la transferencia se lleve a cabo por alguno de los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica y se funde en disposiciones incorporadas a acuerdos internacionales no normativos con otras autoridades u organismos públicos de terceros Estados, que incorporen derechos efectivos y exigibles para los afectados, incluidos los memorandos de entendimiento.

El procedimiento tendrá una duración máxima de seis meses.

*2. La autorización quedará sometida a la emisión por el Comité Europeo de **Protección** de **Datos** del dictamen al que se refieren los artículos 64.1.e), 64.1.f) y 65.1.c) del Reglamento (UE) 2016/679. La remisión del expediente al citado comité implicará la suspensión del procedimiento hasta que el dictamen sea notificado a la Agencia Española de **Protección** de **Datos** o, por conducto de la misma, a la autoridad de control competente, en su caso".*

Artículo 43. *"Supuestos sometidos a información previa a la autoridad de **protección** de **datos** competente.*

*Los responsables del tratamiento deberán informar a la Agencia Española de **Protección** de **Datos** o, en su caso, a las autoridades autonómicas de **protección** de **datos**, de cualquier transferencia internacional de **datos** que pretendan llevar a cabo sobre la base de su necesidad para fines relacionados con intereses legítimos imperiosos perseguidos por aquéllos y la concurrencia del resto de los requisitos previstos en el último párrafo del artículo 49.1 del Reglamento (UE) 2016/679. Asimismo, informarán a los afectados de la transferencia y de los intereses legítimos imperiosos perseguidos. Esta información deberá facilitarse con carácter previo a la realización de la transferencia. Lo dispuesto en este artículo no será de aplicación a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos, de acuerdo con el artículo 49.3 del Reglamento (UE) 2016/679".*

SÉPTIMO.- Así las cosas, en la Sentencia de 6 de octubre de 2015 del TJUE (C362/14), Maximillian Schrems/ Data Protection Commissioner-, si bien se invalidó la Decisión de la Comisión 2000/520/CE, que establecía el nivel adecuado de **protección** de las garantías para las transferencias internaciones de **datos** a EE.UU ofrecidas por el acuerdo de "Puerto Seguro", publicado por su Departamento de Estado, el Tribunal consideró que ello no implicaba que las Autoridades de **Protección** de **Datos** no pudieran apreciar, con toda independencia, si la transferencia cumplía con las exigencias de la Directiva 95/46 (apartado 57 de la Sentencia). Lo que se exige en la indicada Sentencia, es que el tercer país u organización internacional *"garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de **protección** de las libertades y derechos fundamentales sustancialmente equivalente al garantizado"* en la Unión Europea. Por otra parte, a raíz de la citada Sentencia, se acordó la Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la **protección** conferida por el Escudo de la privacidad UE-EE.UU. Conforme a la indicada decisión de adecuación, la evaluación de la adecuación del nivel de **protección** de **datos** corresponde a la Comisión Europea que, a través de una decisión, que es un acto de ejecución, constatará que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de **protección** adecuado.

Pues bien, las situaciones durante el periodo por el que ha sido sancionada la parte actora, por las transferencias internacionales de correos electrónicos registrados en su fichero de "Asociados" a TRS, que era el importador de **datos** personales, con sede en EE.UU, y el periodo actual, son distintas. Así, después de la Sentencia 6 de octubre de 2015 del TJUE, el acuerdo de "Puerto Seguro" con el citado país, se estimó que no reunía las condiciones adecuadas para las transferencias internacionales de **datos**, cosa que cambió con la adopción del "Escudo de Privacidad" el 12 de julio de 2016, en que se consideró que EE.UU tenía un nivel adecuado de **protección**, decisión de adecuación que sigue siendo válida después del RGPD. Y es durante dicho período, por el que ha sido objeto de sanción la parte actora, por las transferencias de **datos** a terceros países realizadas que, al no haber un nivel adecuado de **protección** en EE.UU, le correspondía a la Agencia Española de **Protección** de **Datos**, apreciar, con toda independencia, si dichas transferencias de **datos** cumplían con las exigencias de la Directiva 95/46/CE, y por ello, era necesario un control por parte de dicha Agencia. Y debido a que la falta de un nivel adecuado de **protección** en relación con EE.UU, había sido apreciada por la repetida Sentencia del TJUE, resultaba necesaria una autorización previa por parte del Director de la Agencia Española de **Protección** de **Datos**.

A lo que debemos añadir, que la afiliación de la entidad TRS al mecanismo "Escudo de Privacidad", el 21 de noviembre de 2016, resulta irrelevante a los efectos que nos ocupan, ya que dicha circunstancia se produce meses después de haber finalizado la relación contractual existente con la asociación demandante.

En consecuencia, no se puede considerar más favorables para el supuesto que nos ocupa, los preceptos del RGPD relativos las trasferencias de **datos** personales a terceros países u organizaciones internacionales.

Por otro lado, respecto a los preceptos del RGPD que, según la parte actora resultarían aplicables, arts. 1.3 y 9.2.d) y e), el primero de ellos se refiere a " *la libre circulación de los **datos** personales en la Unión*", mientras que el objeto de la sanción que estamos analizando, son transferencias de **datos** a terceros países. Por su parte, las excepciones contempladas en los apartados d) y e) del citado art. 9.2, precepto relacionado con el Considerando 51, invocado igualmente por la parte actora, se refieren a categorías especiales de **datos** personales, entre las que no se encuentran las direcciones de correo electrónico de los afiliados y amigos de la asociación recurrente objeto de tratamiento, a lo que tenemos que añadir, que dicha asociación no responde a una finalidad política, filosófica, religiosa o sindical.

También la asociación recurrente alega que, en la propia redacción de la sanción se abren las responsabilidades que corresponde al mal funcionamiento de las Instituciones Europeas, por vulneración de los arts. 6, 8, 21, 41, 48 y 53 de la Carta de Derechos Fundamentales de los Ciudadanos de la UE. Dicho motivo de impugnación procede desestimarlo sin más, pues la parte recurrente se limita a reseñar los citados preceptos, sin justificar el modo concreto en que se hayan podido ver conculcados los derechos a la libertad y a la seguridad, a la **protección** de **datos** de carácter personal, a la prohibición de toda discriminación, a una buena administración, a la presunción de inocencia y a un nivel de **protección** que dichos artículos recogen.

Por tanto, en virtud de lo expuesto, cabe apreciar la vulneración del art. 33 de la LOPD por la asociación demandante.

OCTAVO.- El art. 44.4.e) de la LOPD tipifica como infracción muy grave: *"La transferencia internacional de **datos** de carácter personal con destino a países que no proporcionen un nivel de **protección** equiparable sin autorización del Director de la Agencia Española de **Protección** de **Datos** salvo en los supuestos en los que conforme a esta Ley y sus disposiciones de desarrollo dicha autorización no resulta necesaria"*.

Así las cosas, en el caso que nos ocupa, ha quedado acreditado que desde el 6 de octubre de 2015, la parte actora realizó un total de once transferencias internacionales de **datos** a los Estados Unidos de América, país que no proporcionaba un nivel de **protección** adecuado, con motivo de las campañas de fechas 20, 21, 22 de octubre de 2015 y 2, 4, 5, 6 de noviembre de 2015, 11 de enero, 8 y 29 de marzo de 2016, en las que la parte recurrente remitió, respectivamente, un total de 3328, 1471, 3324, 3323, 1468, 739, 71, 3321, 3315, 696 y 696 emails utilizando el servicio MailChimp. Y dichas transferencias internacionales de **datos** de los correos electrónicos, no contaban con autorización previa de la Directora de la Agencia Española de **Protección** de **Datos**, habiendo existido una falta de diligencia de la parte actora en orden a adoptar medidas tendentes a obtener la autorización de la citada Directora, para la realización de las transferencias internacionales de los **datos** objeto de la sanción.

Por último, en el suplico de la demanda, se solicita por la entidad recurrente, la reducción de la cuantía de la sanción, para que no le supusiera a aquella un impacto económico que la obligara a cerrar, con la argumentación de la ausencia de mala fe y el cúmulo de situaciones sobrevenidas, declaraciones de entidades públicas, de la Unión Europea y del Estado Español.

La resolución sancionadora, aplica el apartado 5.a) del art 45 de la LOPD, por la concurrencia significativa de los criterios de los apartados d) y e) del art. 45.4, al tratarse de una asociación sin ánimo de lucro, que desarrolla su actividad en beneficio de los asociados generando un volumen de negocio que no tiene carácter lucrativo, no constando que, a raíz de la comisión de la infracción descrita, la parte demandante hubiese obtenido beneficios económicos o de otra naturaleza.

En cuanto a la determinación de la sanción de 45.000 euros, dentro del intervalo de las infracciones graves, la Agencia considera que operan como agravantes a los efectos de dicha graduación, la concurrencia de los criterios a), b) y j) del apartado 4 del art. 45 de la LOPD.

Respecto al criterio a), carácter continuado de la infracción, ya que de lo actuado se desprende que, con posterioridad a la anulación por el TJUE de la Decisión de la Comisión 2000/50/CE, la asociación recurrente continuó transfiriendo los **datos** de los correos electrónicos de los socios y amigos de aquélla a la empresa estadounidense prestadora del servicio MailChimp, para la realización de once campañas durante el 20 de octubre de 2015 y el 29 de marzo de 2016, sin mediar autorización previa de la Directora de la Agencia Española de **Protección** de **Datos** para ello, ni haber acreditado durante la tramitación del expediente que los titulares

de los **datos** afectados por las transferencias hubieran dado su consentimiento inequívoco a las mismas con esa finalidad.

Por lo que respecta al criterio b), volumen de los tratamientos efectuados, se destaca el elevado número de correos electrónicos registrados en el fichero "Asociados", cuyo tratamiento se vio afectado en cada una de las once campañas descritas.

Y, en relación con el criterio j), la conducta poco colaboradora mostrada por la parte actora con la labor inspectora de la Agencia Española de **Protección** de **Datos**, *"en tanto que con fecha 30 de marzo de 2016 ATI solicitó posponer la visita de inspección inicialmente prevista para el 5 de abril de 2016 por motivos de agenda del asesor jurídico de la Asociación que iba a estar presente en la actuación, fijándose, finalmente la realización de la visita para el día 12 de abril de 2016, fecha en la que pudo comprobarse que la suspensión del servicio "MailChimp" se produjo cuatro días después de que ATI tuviera conocimiento de que iba a realizarse una inspección presencial en sus instalaciones relacionada con la utilización del mencionado servicio de correo electrónico. De esta forma, con la suspensión del servicio los inspectores actuantes no pudieron realizar en la cuenta de usuario de MailChimp de ATI comprobaciones sobre aspectos relevantes para la investigación al estar suspendido el servicio desde el 4 de abril de 2016"*.

Así las cosas, el principio de proporcionalidad de las sanciones comporta, según reiterada jurisprudencia del Tribunal Supremo, como la Sentencia de 12 de abril de 2012 - recurso nº. 5149/2009-, entre otras, que debe existir una debida adecuación entre la gravedad del hecho constitutivo de la infracción y la sanción aplicada, como dispone el número 3 del art. 29 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Dicho principio no puede sustraerse al control jurisdiccional, pues el margen de apreciación que se otorga a la Administración en la imposición de sanciones dentro de los límites legalmente previstos, debe ser desarrollado ponderando en todo caso las circunstancias concurrentes, al objeto de alcanzar la necesaria y debida proporción entre los hechos imputados y la responsabilidad exigida, dado que toda sanción debe determinarse en congruencia con la entidad de la infracción cometida, y según un criterio de proporcionalidad en relación con las circunstancias del hecho. De modo que, la proporcionalidad constituye un principio normativo que se impone a la Administración y que reduce el ámbito de sus potestades sancionadoras.

Pues bien, de conformidad con lo expuesto, estima la Sala que la resolución sancionadora no ha infringido el principio de proporcionalidad en la determinación de la sanción que estamos examinando, que resulta ponderada y proporcionada a la gravedad de la infracción cometida y a la entidad de los hechos, sin que se aprecien razones que justifiquen su minoración. Debemos añadir que, la asociación recurrente realiza una actividad que por su naturaleza, alcance, volumen de **datos** personales en sus ficheros, y su habitualidad en el manejo, hacen que deba de extremarse el cuidado en la actualización y rectificación ajustando su práctica a las previsiones legales, pues, está en juego la salvaguarda de un derecho fundamental.

Por tanto, la Sala comparte los razonamientos efectuados en relación con los apartados 4 y 5 del art. 45 de la LOPD por la Agencia de **Protección** de **Datos**, considerándolos respetuosos con el principio de proporcionalidad, por lo que se justifica sobradamente la imposición de la sanción en la cuantía impuesta, muy próxima al grado mínimo prevista para las infracciones graves.

Sin que se considere por la Sala necesario el planteamiento ante al TJUE de una cuestión prejudicial, pues en primer lugar, hay que poner de relieve que, siendo la presente sentencia susceptible de ser recurrida en casación ante el Tribunal Supremo, esta Sala de la Audiencia Nacional no estaría obligada a plantear cuestión de prejudicialidad ante el TJUE, según el art. 267 del Tratado de Funcionamiento de la Unión Europea, lo que bastaría para contestar a la solicitud formulada de planteamiento de la cuestión prejudicial. Pero, además, no se considera que existan en el caso concreto motivos para plantear la cuestión prejudicial, pues no se aprecia ningún aspecto que se oponga a la normativa comunitaria.

En consecuencia, procede declarar conforme a derecho la sanción que hemos analizado.

NOVENO.- La segunda infracción por la que ha sido sancionada la asociación recurrente, con la cantidad de 5.000 euros, se encuentra recogida en el art. 38.4.g) de la LSSI, que establece como infracción leve: *"Utilizar dispositivos de almacenamiento y recuperación de **datos** cuando no se hubiera facilitado la información u obtenido el consentimiento del destinatario del servicio en los términos exigidos por el artículo 22.2"*.

Por su parte, el art. 22.2 de la LSSI dispone: *"Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de **datos** en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los **datos**, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de **protección** de **datos** de carácter personal.*

Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los ***datos*** *podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones.*

Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario".

Los hechos en que se basa la resolución sancionadora, es que la parte actora no facilitó, con anterioridad a la realización de los envíos de las campañas, ningún tipo de información a los destinatarios de los correos electrónicos (socios y amigos de la asociación recurrente), remitidos por dicha asociación a través de MailChimp, servicio de envío de correo electrónico gestionado por TRS, relativa a la instalación por parte del tercero prestador del citado servicio en dichos envíos de dispositivos de seguimiento de la actividad de los destinatarios, a fin de controlar la apertura de los correos y la pulsación de los enlaces contenidos en los correos, y poder elaborar con la información recabada informes de seguimiento de las campañas.

DÉCIMO.- Frente a la anteriormente reseñada infracción, la asociación demandante se limita a reseñar que no es un prestador de servicios de la sociedad de información, y entiende, además que se castiga el mismo hecho dos veces.

El Anexo de la LSSI define en su apartado c) al prestador de servicios como la " *persona física o jurídica que proporciona un servicio de la sociedad de la información*". Y por servicio de la sociedad de la información, el apartado a) entiende, *"todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario*.

El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios.

Son servicios de la sociedad de la información, entre otros y siempre que representen una actividad económica, los siguientes:

1.º La contratación de bienes o servicios por vía electrónica.

2.º La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.

3.º La gestión de compras en la red por grupos de personas.

4.º El envío de comunicaciones comerciales.

5.º El suministro de información por vía telemática. No tendrán la consideración de servicios de la sociedad de la información los que no reúnan las características señaladas en el primer párrafo de este apartado y, en particular, los siguientes...".

Así las cosas, se debe considerar a la sociedad recurrente como prestadores de servicios, en su condición de titular del sitio web www.ati.es, y responsable de la remisión de los correos electrónicos en los que se incluían dispositivos de seguimiento de la actividad de los destinatarios de tales envíos. No podemos olvidar que el fichero "Asociados", cuyo responsable es la parte actora, tiene como finalidad, entre otras, la prestación de los servicios de formación, asesoramiento profesional, envío de publicaciones, asesoramiento laboral, y envío de ofertas y promociones relacionados con el sector de la informática. Y, en la página web www.ati.es, se informa que la parte actora *"tiene como objetivo la defensa, promoción y desarrollo de la actividad de quienes ejercen como técnicos y profesionales en el campo de las tecnologías de información, facilitando a sus socios el intercambio de experiencias, la formación y la información sobre dichas tecnologías, a la vez que contribuye a la promoción, y el desarrollo delas mismas, estudiando su impacto en la Sociedad y los ciudadanos, y potenciando las relaciones con su entorno social y Económico, colaborando con otras entidades profesionales informáticas, implantadas tanto en nuestro país como fuera de él"*.

En consecuencia, la parte actora no facilitó, con anterioridad a la realización de los envíos de las campañas, cuestión ésta que no se discute en la demanda, ningún tipo de información a los destinatarios de los correos electrónicos remitidos por aquella a través de MailChimp, de que el acceso a los mismos conllevaba la instalación de dispositivos, ficheros o archivos que posibilitaban la recogida actualizada y continuada de **datos** relacionados con su comportamiento.

Finalmente, la parte recurrente alega que se castiga el mismo hecho dos veces, por lo que con ello, se está haciendo referencia al principio *non bis in idem.* Dicho motivo de impugnación procede desestimarlo, pues se han sancionado dos conductas distintas, perfectamente distinguidas en los hechos y fundamentos de la resolución, que vulneran dos bienes jurídicos diferentes: la realización de transferencias internacionales

de **datos** de carácter personal a la empresa TRS, entidad radicada en los Estados Unidos de América, sin mediar autorización previa de la Directora de la Agencia Española de **Protección** de **Datos**, y el no facilitar, con anterioridad a la realización de los envíos de las campañas, ningún tipo de información a los destinatarios de los correos electrónicos remitidos por la asociación demandante a través de MailChimp, relativa a la instalación por parte del tercero prestador del citado servicio en dichos envíos de dispositivos de seguimiento de la actividad de los destinatarios, a fin de controlar la apertura de los correos y la pulsación de los enlaces contenidos en los correos, y poder elaborar con la información recabada informes de seguimiento de las campañas.

Por tanto, la citada infracción que estamos analizado es conforme a derecho, siendo la cuantía de la sanción impuesta de 5.000 euros, acorde con el principio de proporcionalidad, teniendo en cuenta los hechos imputados, y que las infracciones leves conforme a lo establecido en el art. 39.1.c) de la LSSI, pueden ser sancionadas con multa de hasta 30.000 euros.

En consecuencia, en virtud de lo expuesto, el recurso contencioso-administrativo debe ser desestimado.

UNDÉCIMO.- De conformidad con el art. 139.1 de la Ley de la Jurisdicción procede imponer las cotas procesales a la parte actora.

VISTOS los artículos citados, y demás de general y pertinente aplicación.

FALLAMOS:

Que desestimando el recurso contencioso-administrativo interpuesto por el Procurador de los Tribunales don Domingo José Collado Molinero, en nombre y representación de la **ASOCIACIÓN DE TÉCNICOS EN INFORMÁTICA,** contra la resolución de 22 de marzo de 2017, de la Directora de la Agencia Española de **Protección** de **Datos**, por la que se impone una sanción a la asociación recurrente de 45.000 euros por una infracción del art. 33 de la Ley Orgánica 15/1999, de 13 de diciembre, tipificada como infracción muy grave en el art. 44.4.d) de la citada norma, y una sanción de 5.000 euros por la infracción del art. 22.2 de la Ley 34/2002, de Servicios de la Sociedad de la Información y del Comercio Electrónico, tipificada como leve en el art. 38.4.g) de dicha Ley, declaramos la citada resolución conforme a derecho; con expresa imposición de las costas procesales a la parte actora.

La presente sentencia es susceptible de recurso de casación, que deberá prepararse ante esta Sala en el plazo de 30 días contados desde el siguiente al de su notificación; en el escrito de preparación del recurso deberá acreditarse el cumplimiento de los requisitos establecidos en el art. 89.2 de la Ley de la Jurisdicción justificando el interés casacional objetivo que presenta.

Así, por esta nuestra Sentencia, lo pronunciamos, mandamos y firmamos.

PUBLICACIÓN.- Dada, leída y publicada fue la anterior Sentencia en Audiencia Pública. Doy fe.

Madrid a

LA LETRADA DE LA ADMINISTRACIÓN DE JUSTICIA