La Sala Segunda del Tribunal Constitucional, compuesta por el magistrado don Juan Antonio Xiol Ríos, presidente, y los magistrados don Antonio Narváez Rodríguez, don Cándido Conde-Pumpido Tourón, don Ramón Sáez Valcárcel y don Enrique Arnaldo Alcubilla, y la magistrada doña Concepción Espejel Jorquera, ha pronunciado

EN NOMBRE DEL REY

la siguiente

SENTENCIA

En el recurso de amparo núm. 4011-2020, promovido por la Asociación Omnium Cultural, contra el auto de 19 de junio de 2020, dictado por la Sección Primera de la Sala de lo Contencioso-Administrativo del Tribunal Supremo, que inadmitió a trámite el recurso de casación núm. 6960-2019, interpuesto contra la sentencia de 29 de abril de 2019, también impugnada, dictada por la Sección Primera de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, que, a su vez, había desestimado el recurso núm. 397-2017, formalizado contra la resolución R/00326/2017 de la Directora de la Agencia Española de Protección de Datos de 4 de mayo de 2017, dictada en el PS/00391/2016, que confirmó en reposición la resolución R/00325/2017, de 22 de febrero, por la que se impuso a la recurrente una sanción de 90.000 euros por una conducta de incumplimiento de la prohibición prevista en el art. 33 de la Ley Orgánica de Protección de Datos. Ha intervenido el Ministerio Fiscal. Ha sido ponente el magistrado don Antonio Narváez Rodríguez.

I. Antecedentes

1. Mediante escrito, que tuvo entrada en el registro de este Tribunal el día 20 de agosto de 2020, el procurador de los tribunales don Luis Fernando Granados Bravo, en nombre y representación de la asociación Omnium Cultural, defendida por el letrado don Manuel Martínez Ribas, interpuso recurso de amparo contra las resoluciones judiciales que se citan en el encabezamiento, por vulneración de sus derechos fundamentales a la legalidad sancionadora (art. 25.1 CE), en relación con el art. 9.3 CE; a la tutela judicial efectiva (art. 24.1 CE), por falta de

motivación, en relación con el art. 120.3 CE; y a los derechos de asociación (art. 22 CE) y a la propiedad privada (art. 33 CE).

2. La demanda trae causa de los siguientes hechos:

a) En fecha 22 de febrero de 2017, la Agencia Española de Protección de Datos (AEPD) dictó la resolución núm. R/00325/2017, por la que se impuso a la entidad ahora recurrente, Omnium Cultural (OC), y a la entidad Asamblea Nacional Catalana (ANC), una sanción de 90.000 euros a cada una de ellas, por la comisión de una conducta de incumplimiento de la prohibición prevista en el art. 33 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), entonces vigente, que fue calificada como infracción tipificada como muy grave en el art. 44.4.d) LOPD. Esta resolución fue dictada en el marco del expediente sancionador PS/00391/2016, incoado a instancia de dos particulares, y en la que se consideraron acreditados los siguientes hechos:

> "UNO.- En fecha de 10/07/2014 OC y ANC firmaron un contrato con BSD, en calidad de responsables del fichero, cuya ejecución material suponía que un fichero –AHORA ES LA HORA- del que son responsables las citadas entidades, estuviera alojado en los servidores de BSD [Blue State Digital, Inc.] sitos en Estados Unidos.
> DOS.- En el Registro General de Protección de Datos, por parte de ANC y OC se inscribió el fichero AHORA ES LA HORA sin que conste marcado el campo relativo a transferencias internacionales de datos.
> TRES.- La Sentencia del Tribunal de Justicia Europeo número C-362/14 de 6/10/2015, invalida la Decisión de la Comisión 2000/520/CE que considera que las transferencias internacionales de datos a Estados Unidos tenían un nivel adecuado de protección.
> CUATRO.- En fecha de 19/10/2015 se publica en la página web de la Agencia Española de Protección de Datos un comunicado donde se informa que, en relación con las transferencias internacionales de datos realizadas al amparo de la Decisión de la Comisión 2000/520/CE, las Autoridades de Protección de datos investigarán aquellos casos de los que tengan conocimiento a partir de denuncias para ejercer sus poderes con el fin de proteger a las personas, teniendo entrada en esta Agencia dos denuncias de fecha 21/04/2016.
> CINCO.- OC remitió comunicaciones por correo electrónico a BSD donde informa de su voluntad de rescindir el contrato de fecha 10/07/2014, al no ser posible la adhesión de BSD al acuerdo de privacidad –Privacy Shield- siendo la última de fecha 22/08/2016.
> SEIS.- En una comunicación de BSD a OC de fecha 22/08/2016 en contestación a la anterior, se pone de manifiesto que aquella supone la comunicación previa a la rescisión del contrato que surte efecto transcurrido un mes de la misma, por lo que a finales del mes de septiembre de 2016 los datos alojados en los servidores de BSD serían eliminados".

En la resolución se hacía una amplia reseña de los antecedentes, incluyendo las actuaciones inspectoras realizadas, las alegaciones formuladas por OC, la propuesta de resolución, y los hechos declarados probados. En los fundamentos jurídicos se abordaba la competencia de la AEPD, la

normativa aplicable, la desestimación de la solicitud de nulidad formulada por OC, así como las referencias expresas a la responsabilidad, los hechos probados, la conducta típica y antijurídica, la determinación de la cuantía de la sanción a imponer y el análisis del elemento subjetivo. Más en concreto, a efectos de fijar la cuantía de la multa, la AEPD tuvo en cuenta lo dispuesto en el art. 45.5.a) LOPD, que permite imponer las sanciones previstas para las infracciones que precedan inmediatamente en gravedad, por la concurrencia significativa de dos de los criterios previstos en el art. 45.4 LOPD, ya que la entidad OC no tiene como actividad principal el tratamiento de datos personales [art. 45.4.d) LOPD] ni obtuvo beneficio alguno con la conducta sancionada [art. 45.4.e) LOPD]. No obstante, una vez rebajada la sanción a la escala prevista para las infracciones graves (de 40.001 a 300.000 euros, según dispone el art. 45.2 LOPD), se tuvo en cuenta el carácter continuado de la infracción [art. 45.4.a) LOPD]; el grado de intencionalidad [art. 45.4.f) LOPD]; el volumen de los tratamientos efectuados [art. 45.4.b) LOPD], acreditados en 684.952 registros; así como otros criterios [art. 45.4.j) LOPD] tales como la diligencia exigible, el riesgo al que han sido sometidos los datos contenidos en el fichero, la situación de este y la naturaleza de los datos como datos sensibles de ideología.

b) Contra esta decisión, la entidad OC interpuso un recurso de reposición que fue desestimado por la AEPD por medio de la resolución núm. RR/00326/2017, de 4 de mayo.

En su recurso, OC alegó error material en la parte dispositiva, que se habían obviado hechos relevantes para la resolución del expediente, así como la infracción de los siguientes principios y derechos: principios de confianza legítima, culpabilidad y seguridad jurídica; derecho a un procedimiento con todas las garantías y de defensa; principios de responsabilidad y proporcionalidad. La resolución rectifica el error material y desestima el resto de alegaciones, porque no se han aportado nuevos hechos o argumentos que permitan reconsiderar la validez de la decisión impugnada, a la que se remite ampliamente por tratarse –en su mayor parte- de alegaciones que ya habían sido planteadas por la recurrente con anterioridad, durante la tramitación del expediente.

c) Frente a esta resolución, la entidad OC interpuso recurso contencioso administrativo que fue desestimado por la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, en sentencia dictada el 29 de abril de 2019 en el marco del recurso núm. 307/2017. En esta resolución, tras analizar la normativa aplicable, se destaca lo siguiente:

> "[L]as transferencias internacionales de datos llevadas a cabo por la entidad recurrente desde el inicio de la relación contractual el 10 de julio de 2014 con BSD, radicada en los Estados Unidos (EE.UU), se encontraban amparadas en la Decisión de la Comisión 2000/520/CE, que establecía el nivel adecuado de protección de las garantías para las transferencias internacionales de datos desde la Unión Europea a EE.UU ofrecidas por el acuerdo de "Puerto Seguro" (Safe Harbour).

> Situación que cambió con la declaración de invalidez de la Decisión 2000/520/CE, adoptada por la Sentencia del TJUE de 6 de octubre de 2015, C- 362/14, que entendió que el acuerdo de "Puerto Seguro", no proporcionaba un nivel adecuado de protección de las garantías exigidas por la Directiva 95/46/CE para las transferencias internacionales de datos desde la Unión Europea a Estados Unidos.
>
> Por tanto, para las transferencias internacionales o lo que es igual para la conservación de los datos de carácter personal del fichero Ara és l´Hora, del que es responsable Omnium, fuera del territorio nacional, en los servidores de BSD en Estados Unidos, se debió acudir a la norma general del artículo 33 de la LOPD, así como al resto de la normativa de datos, relacionada con la transferencia internacional de datos. Sin embargo, dicha entidad con posterioridad a la citada sentencia, siguió conservando los datos alojados en los servidores de BSD en Estados Unidos hasta el mes de septiembre de 2016 en que se hizo efectiva la resolución del contrato con BSD, sin haber recabado autorización de la Directora de la Agencia Española de Protección de Datos. De hecho, Omnium ni siquiera había comunicado la realización de transferencias internacionales, ni en la inscripción del fichero, al no marcarse dicha opción en la solicitud de inscripción por Omnium del fichero Ahora es la Hora, que figura como activo desde el 8 de agosto de 2014, ni con posterioridad, pese a la exigencia establecida con carácter general para todos los casos por el artículo 66.3 del RLOPD" (FJ tercero)

En los siguientes fundamentos jurídicos se van exponiendo los distintos motivos de impugnación alegados por la entidad OC, procediendo a su análisis y resolución individualizada.

Así, en relación con el principio de confianza legítima, se recuerda la doctrina expuesta en la STS de 3 de marzo de 2016 (Rec. 3012/2014), y se hace una reseña parcial expresa de las comunicaciones y notas de prensa emitidas por la AEPD entre los meses de octubre de 2015 y febrero de 2016. En concreto, en el FJ cuarto se indica lo siguiente:

> "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 de 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. Añadiendo que "*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."*
>
> Por 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 las denuncias presentadas con fecha 26 de abril de 2016, y en ningún momento desde la AEPD se realizó comunicación que permitiera creer a los afectados que su actuación no podría ser sancionable, advirtiéndoles

expresamente de la necesidad de adecuar su actuación a la nueva situación legal creada tras la Sentencia del TJUE.

Prueba de ello es la comunicación enviada a los responsables el 29 de octubre de 2015, donde se indica "*Por ello, en el caso de que tenga previsto continuar transferencias internacionales de datos a Estados Unidos…deberán encontrar legitimación en otros instrumentos como las Cláusulas Contractuales Tipo adoptadas por las decisiones de la Comisión Europea 2001/497/CE, 2004/915/CE y 2010/87/UE y, en su caso, en las excepciones previstas en el artículo 34 de la LOPD que pudieran ser aplicables".*

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."*

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*"*.

Para la sala, esos documentos no permitían crear "la apariencia de que determinadas conductas no serían sancionadas, sino que por el contrario, se advirtió expresamente a las empresas sobre los riesgos que asumían si realizaban dichas transferencias internacionales, indicando también expresamente la posibilidad de realizar actuaciones investigadoras ante la presentación de denuncias, como aquí ha ocurrido, lo que motiva la intervención de la AEPD".

En lo referente a la infracción del derecho a un procedimiento con garantías y de defensa (art. 24.2 CE), por la indebida denegación de una prueba, la sala expone (FJ quinto) la doctrina sobre el derecho a la prueba (SSTC 129/2005 y 22/2008) y la exigencia de una real y efectiva indefensión para que pueda apreciarse la vulneración del derecho reconocido en el art. 24. 2 CE (SSTC 15/1995 y 27/2001). En el presente caso, la diligencia de prueba solicitada en el trámite administrativo consistía en recabar una certificación de la AEPD sobre otros expedientes incoados por hechos similares. La petición no indicaba "la finalidad perseguida" y, aunque la sala admite que la "prueba se inadmitió sin un pronunciamiento expreso", la resolución sancionadora sí ofrece una respuesta fundada a esta pretensión. La diligencia era "irrelevante" y "no pertinente", porque la existencia o no de otros expedientes no afecta o modula la responsabilidad de la entidad recurrente. En cualquier

caso, la parte pudo formular alegaciones e incluso pudo haber propuesto la prueba en la vía jurisdiccional, lo que no hizo, por lo que concluye que no hubo indefensión material alguna.

Por lo que se refiere al principio de responsabilidad, que el recurrente consideraba infringido al no haberse entrado a valorar el régimen de cotitularidad del fichero y sus consecuencias en el régimen de atribución de responsabilidades, la sala se remite al pronunciamiento contenido en la sentencia de 2 de diciembre de 2018 (Rec. 453/2016), dictada en un supuesto que afectaba a las mismas entidades ahora implicadas. De esta forma, en el FJ sexto, con reseña de la normativa aplicable y del Dictamen 1/2010 del GT29 [Grupo de trabajo de carácter consultivo creado por el art. 29 de la Directiva 95/46/CE, que reúne a los representantes de las autoridades de control de datos a nivel europeo], la sala afirma que "cada una [de las entidades] ha realizado individualmente las acciones constitutivas de la infracción, por lo que la responsabilidad es individual y a título personal. (…) [R]ealizaron cada una (…) sendas inscripciones relativas al fichero Ara es l'hora, que es el objeto de la transferencia internacional de datos y en el anexo de privacidad del contrato de servicio de alojamiento con la empresa BSD, figuran ambas entidades como firmantes y en calidad de Data Controller, es decir, responsables del tratamiento".

Finalmente, en cuanto al principio de proporcionalidad, la sala valida el criterio de la AEPD, "atendidas las circunstancias concurrentes", de forma que "la sanción de 90.000 € de multa impuesta resulta ponderada y proporcionada a la gravedad de la infracción cometida y la entidad de los hechos, sin que se aprecien razones que justifiquen su minoración". En el FJ séptimo, la sala desglosa todos los criterios tenidos en cuenta por la AEPD para fijar la cuantía de la multa, confirmando su actuación. Y también descarta la concurrencia de la circunstancia atenuante prevista en el art. 45.5.b) LOPD, alegada por la entidad recurrente, consistente en la regularización diligente de la situación irregular. Para la sala, "difícilmente cabe apreciar la invocada circunstancia (…) cuando los datos se mantienen en los servidores de BSD en Estados Unidos, después de la STJUE de 6 de octubre de 2015 hasta que el 22 de agosto de 2016 se inicia el periodo de preaviso de un mes para resolución del contrato con BSD. Es decir, durante casi un año, hasta septiembre de 2016, se mantienen los datos en un servidor ubicado en un país cuyas transferencias requieren la autorización prevista en el artículo 33 LOPD". Además, "la mera tenencia de los datos en un Estado donde las autoridades podían acceder a los datos personales transferidos y tratarlos de manera incompatibles con las finalidades de la transferencia (apartado 90 de la STJUE de octubre de 2015), constituye en sí mismo un riesgo", de tal forma que "el bloqueo del acceso al fichero por parte de Omnium no impedía que las autoridades gubernativas de ese tercer Estado pudieran acceder y gestionar sin restricción el fichero, en tanto que cualquier ciudadano que quisiera ejercer los derechos previstos en la LOPD difícilmente podrían hacerlo al estar el fichero bloqueado". Por último, "cabe señalar

(…) que Omnium no había comunicado la realización de transferencias internacionales, ni en la inscripción del fichero, ni con posterioridad, pese a la exigencia establecida con carácter general para todos los casos por el artículo 66.3 del RLOPD, lo que, de entrada, pone en entredicho esa esgrimida voluntad de cumplir la normativa de protección de datos".

d) La sentencia de la Audiencia Nacional fue recurrida en casación por la entidad OC. El recurso fue inadmitido por auto de la Sección Primera de la Sala de lo Contencioso-Administrativo del Tribunal Supremo, fechado el 19 de junio de 2020.

Como motivos de casación, la entidad OC planteó los siguientes: i) infracción de los arts. 3.1 de la Ley 30/92, 9.3 y 25 CE, en relación con el art. 49 LOPD y demás normativa de desarrollo, todo ello en relación con el art. 127 de la Ley 30/92 (principio de legalidad de la potestad sancionadora) y con los principios de confianza legítima, seguridad jurídica y buena fe; ii) infracción del art. 45 LOPD, en relación con los arts. 129 y 131 de la Ley 30/92 y los arts. 9.3 y 25 CE, puestos en relación con la infracción del principio de proporcionalidad; y iii) infracción de los arts. 24.1 y 120.3 CE, 130.3 de la Ley 30/92, en base a definiciones de la normativa sobre protección de datos, por falta de motivación sobre la individualización de responsabilidades de las entidades sancionadas.

El Tribunal Supremo inadmitió el recurso de casación por entender que carecía manifiestamente de interés casacional objetivo. Para ello, razona que existe sobrada jurisprudencia sobre el principio de confianza legítima, responsabilidad y proporcionalidad, y que la entidad recurrente ha planteado cuestiones que "no supera[n] el ámbito estrictamente casuístico", o que constituyen "elementos circunstanciales del pleito", sin proyección general o extensibles a otros casos. No obstante, sobre el primer motivo de casación, la Sala Tercera expone que "la entidad recurrente ciñe en muy buena parte su escrito de preparación a la infracción de este principio [de confianza legítima], sin haber cuestionado, en buena lógica con tal alegación, la tipificación de los hechos realizada por la Administración y confirmada por la Sala de instancia, pues concurriría, según alega, una suerte de exclusión de la antijuridicidad de la conducta basada precisamente en la confianza creada por la Administración, a partir de las comunicaciones emitidas por la Agencia Estatal de Protección de Datos de que los hechos no serían sancionados. En efecto, a pesar de que en su preparación invoca la asimilación del bloqueo del fichero con la suspensión temporal de transferencias, no cuestiona la parte en su escrito la tipificación de los hechos consistentes en la conservación de datos alojados en un servidor de Estados Unidos, pertenecientes a la entidad Blue State Digital (BSD), con posterioridad a la sentencia del Tribunal de Justicia de la Unión Europea (TJUE), de 6 de octubre de 2015, que declaró la invalidez de la Decisión de la Comisión 2000/520/CE, sin autorización de la AEPD ni amparo legal alguno, conforme establece el artículo 33 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y ello sobre la base de

la consideración de que la mera conservación de los datos constituye una modalidad de tratamiento de datos por parte del responsable del fichero establecido en territorio español, que queda englobado dentro del concepto de transferencia internacional que recoge el artículo 5.1.s) del Reglamento de la Ley Orgánica de Protección de Datos".

3. La demanda de amparo identifica las resoluciones judiciales impugnadas y fundamenta el recurso en una serie de hechos y argumentos que se exponen a continuación.

a) En primer lugar, la demanda formula un extenso relato de hechos que, al mismo tiempo, constituye la base de su recurso. Así, se dice que en "el marco de la campaña 'Ara és l'hora' organizada conjuntamente por OC y ANC (…), ambas entidades, de forma conjunta y coordinada, inscribieron sendos ficheros en el Registro General de Protección de Datos", y que los formularios existentes no permitían la "posibilidad de declarar la inscripción conjunta como corresponsables". Que "en el desarrollo [de esa iniciativa] se iban a recoger datos de carácter personal", para lo que la entidad OC "suscribió el 10 de julio de 2014 un contrato de prestación de servicios con la empresa norteamericana Blue State Digital, Inc. (en adelante, "BSD") para la elaboración de una web y su lanzamiento, consultoría estratégica y el uso del software BSD Tools". Esa empresa estaba "adherida a los principios de Safe Harbour, recogidos en la Decisión de la Comisión 2000/520/CE de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo". Como quiera que en "la ejecución del mencionado contrato BSD iba a acceder a los datos de carácter personal incorporados en el fichero (…) ambas asociaciones suscribieron un contrato el 1 de septiembre de 2014 para regular dicho acceso, de forma que se cumpliera con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) para los encargos del tratamiento". Tras dictarse la sentencia del TJUE en el asunto C-362/14, se produjo la "pérdida de una base legal para realizar transferencias internacionales de la Unión Europea a empresas norteamericanas sujetas al mismo", como era el "caso de BSD". Esta situación generó la actuación de las autoridades europeas y nacionales de protección de datos, a través de comunicados y notas de prensa emitidos entre los meses de octubre de 2015 y febrero de 2016, que se transcriben parcialmente. En la demanda se destaca, en particular, una nota de la AEPD emitida el mes de diciembre de 2015, con el siguiente tenor literal:

> *"a) 'Desde la AEPD no se ha dado ningún ultimátum a las empresas españolas'.*
>
> *b) 'La Agencia en ningún caso ha requerido a los responsables para que dejen de utilizar determinados servicios de almacenamiento en la nube. Las acciones de la Agencia no están orientadas a la prohibición de utilizar herramientas concretas sino a informar a los responsables para que requieran a su proveedor de servicios, si es necesario, que les ofrezca una respuesta adaptada a la sentencia del TJUE.'*

c) '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 las transferencias.'

d) 'La Agencia, junto con las Autoridades europeas de protección de datos, apuesta por encontrar soluciones sostenibles para aplicar la sentencia del TJUE e insiste en el llamamiento realizado a las Instituciones de la UE, los Estados miembros y las empresas para encontrar un camino que permita el cumplimiento de la sentencia del Tribunal.'"

Ante esta situación, la demanda señala que la entidad OC mantuvo diversos contactos con la empresa BSD, entre los meses de noviembre de 2015 y agosto de 2016, con la finalidad de adaptar el contrato a los nuevos requerimientos derivados de la STJUE ya citada. En el contexto de estas comunicaciones, en el mes de enero de 2016 la entidad OC solicitó a BSD el "bloqueo" del "acceso al programa".

En el mes de abril de 2016 se presentó ante la AEPD una denuncia contra ANC y OC, suscrita por dos particulares, lo que motivó una actuación de dos inspectores que, en fecha 26 de abril de 2016, se personaron en la sede de OC. En la demanda se pone de manifiesto que, "ante la imposibilidad de que los inspectores pudieran acceder al programa [por la situación de bloqueo ya descrita] se solicitó en la misma inspección a los representantes de OC que aportaran en diez días documentación acreditativa del estado de los ficheros alojados en BSD y de haber regresado el fichero a su estado de bloqueo anterior".

Finalmente, ante las dificultades de BSD para adaptarse a la nueva normativa derivada de la Decisión 2016/1250, de 12 de julio (denominada "Privacy Shield", o "Escudo de privacidad"), la entidad OC solicitó la rescisión del contrato con BSD en fecha 22 de agosto de 2016.

El resto del relato se centra en las resoluciones administrativas y judiciales impugnadas.

b) En segundo lugar, la demanda desarrolla los fundamentos jurídicos alegados como motivos de amparo, que se pueden resumir de la siguiente manera:

(i) Vulneración del derecho a la legalidad sancionadora (art. 25.1 CE), en relación con el art. 9.3 CE y los principios de seguridad jurídica y de confianza legítima.

Tras hacer una reseña de la doctrina jurisprudencial sobre los derechos y principios invocados, con cita expresa, entre otras, de las SSTC 121/2016 y 181/2016, así como de la STS de 22 de febrero de 2016 (recurso núm. 4948/2013), la demanda fundamenta su alegación en este punto en dos tipos de elementos: por un lado, las comunicaciones del GT29 y de la AEPD, de

octubre y diciembre de 2015, que extracta parcialmente; y por otro, la propia normativa de protección de datos y, señaladamente, el art. 37.1.f) LOPD y los arts. 49 y 69.1.b) RLOPD. De este conjunto de factores concluye que la actuación administrativa y judicial resultó imprevisible. En primer lugar, la entidad recurrente realizó las gestiones indicadas por el GT29 y la AEPD, a fin de adaptar la relación contractual con su proveedor de servicios norteamericano a las nuevas condiciones impuestas por la STJUE. Y, en segundo lugar, su decisión de acordar el "bloqueo" de los ficheros era equivalente a las medidas de "suspensión" o de "inmovilización" que, según la normativa sobre protección de datos, podría haber adoptado la AEPD. A su juicio, de las normas citadas se deduce: "(i) que la AEPD tiene potestad para adoptar medidas necesarias para adecuar los tratamientos a la Ley; (ii) que en el ejercicio de dicha potestad, podrá acordar la suspensión de transferencias hacia un tercer país; (iii) que cuando el responsable haya desatendido dicho acuerdo de suspensión de transferencias, la AEPD podrá ejercer su potestad sancionadora y requerir el cese en la utilización o cesión de ilícita de datos; y que (iv) desatendido el requerimiento, podrá la AEPD inmovilizar los ficheros. Consecuentemente, es legítimo confiar en que el bloqueo del fichero supone el cese en la utilización o cesión ilícita de datos y que, por tanto, la actuación de OC, en la medida que alcanza idénticos efectos materiales que la suspensión de transferencias o la inmovilización de fichero, no puede ser tipificada como una infracción del art. 33 LOPD, ante la ausencia de la transferencia misma". Precisamente por este motivo, no se comunicó la continuidad de las transferencias de datos en la "confianza legítima (…) [de] que (…) habían sido suspendidas mediante el bloqueo del fichero". Confianza que se vio reforzada por el hecho de que los inspectores de la AEPD solicitaron no solo el desbloqueo de los datos para comprobar su estado sino la "documentación acreditativa de haber regresado el fichero a su estado de bloqueo anterior". Situación que ahora se ve confirmada con la vigente redacción del art. 69 de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales que, según el recurrente, utiliza la expresión "bloqueo de datos" como medida adecuada para la "inmovilización" de ficheros.

(ii) Vulneración del derecho a la tutela judicial efectiva sin indefensión (art. 24 CE) y motivación de las sentencias (art. 120.3 CE), en relación con el art. 9.3 CE y los principios de legalidad, responsabilidad e interdicción de la arbitrariedad de los poderes públicos.

En este apartado de la demanda se hace una extensa reseña de la doctrina jurisprudencial sobre los derechos alegados y, más en concreto, sobre el derecho a una resolución motivada y fundada en Derecho. Para la entidad recurrente, la sentencia de la Audiencia Nacional se basó en un razonamiento arbitrario, irracional e ilógico, al ratificar la decisión administrativa de sancionar a cada una de las dos entidades responsables de los ficheros como autoras de sendas infracciones,

en vez de sancionarlas como responsables solidarias de una sola infracción. Se trataba de una campaña conjunta, el fichero era compartido y las dos entidades habían suscrito el anexo del contrato de servicios con BSD. A pesar de ello, y aunque la Audiencia expone la doctrina general sobre la determinación del grado de responsabilidad, no la aplica al caso enjuiciado mediante la concreción de las operaciones de cada entidad y su grado de control sobre estas. Por el contrario, el órgano judicial afirmó que cada una de las entidades había realizado individualmente las acciones constitutivas de la infracción, sobre la base de que cada asociación había realizado su propia inscripción en el registro correspondiente, y ambas figuraban como responsables del tratamiento. Se considera que este razonamiento es contrario al derecho a la tutela judicial efectiva.

Otro tanto se alega sobre la resolución del Tribunal Supremo. En la demanda se hace un amplio resumen de los motivos de casación invocados y de los fundamentos ofrecidos por el auto del TS, que el recurrente considera ilógicos y arbitrarios. A su juicio, era evidente la necesidad de un pronunciamiento interpretativo de las normas contenidas en los arts. 49 LOPD y 69 RLOPD, a fin de definir el alcance de la suspensión temporal de transferencias en relación a los efectos que produce el bloqueo de datos. Y lo mismo sucede con el sistema de graduación de sanciones (art. 45, apartados 4 y 5 LOPD), en su relación con el principio de proporcionalidad; o con el principio de responsabilidad solidaria. La decisión del TS supone una aplicación errónea de los requisitos procesales para el acceso al recurso de casación, lo que implica la "denegación (…) de su derecho de acceso a la justicia y a la tutela judicial efectiva".

(iii) Vulneración del derecho de asociación (art. 22 CE) y del derecho de propiedad (art. 33 CE), sobre la base del derecho a la legalidad sancionadora y del principio de proporcionalidad (art. 25 CE).

Para el recurrente, la doctrina constitucional sobre el derecho de asociación, que extracta ampliamente, se ha visto vulnerada en el presente caso. La injerencia en este derecho solo es admisible si está prevista en la ley y ésta resulta previsible, de forma que los interesados puedan conocer anticipadamente las consecuencias de sus actos. Además, esa injerencia ha de estar orientada a un fin legítimo y ser adecuada, necesaria y proporcionada desde la perspectiva de una sociedad democrática. En el presente supuesto, la sanción impuesta era imprevisible, citando como referencia la STC 76/2019, sobre la inconstitucionalidad del art. 58.1 bis LOREG, a lo que se añade la falta de práctica aplicativa de este tipo de sanciones. Se impuso a la entidad OC una sanción por una conducta cuyos efectos no son más perjudiciales que los derivados del ejercicio de las potestades que se conceden a la AEPD en la normativa vigente. Los datos estaban cifrados y, en todo caso, el posible acceso de las autoridades norteamericanas tampoco podría evitarse

mediante la suspensión temporal de la transferencia o la inmovilización de ficheros, equivalentes al bloqueo dispuesto por OC. Además, la sanción fue desproporcionada, en comparación con la impuesta a la única otra asociación sancionada por la AEPD por la infracción del art. 33 LOPD, a la que se impuso una multa de 45.000 euros; así como a las establecidas en otros países, que se han situado en torno a los 10.000 euros. Para la recurrente, estos hechos pueden "comprometer seriamente su existencia y actividades a causa de un hostigamiento judicial y administrativo dirigido contra OC, (…) en el contexto político y social de conflicto y confrontación entre la voluntad de autodeterminación que defiende, entre otros, OC y la voluntad de preservar la integridad territorial por parte de los poderes públicos del Estado".

Finalmente, con cita de la STEDH de 15 de noviembre de 2008 (asunto *Togrul c. Bulgaria*), considera que la imposición de una multa constituye una injerencia en el derecho de propiedad (art. 33 CE) que solo puede entenderse justificada si está prevista en la ley y resulta proporcional a la finalidad pretendida, lo que no concurre en este caso por los motivos ya expuestos.

c) La demanda contiene un apartado dedicado específicamente a la justificación de la especial trascendencia constitucional del recurso. En apretada síntesis, se puede señalar que se invocan dos motivos a estos efectos. Por un lado, la "concurrencia de cuestiones jurídicas relevantes y de evidente repercusión social y económica, con consecuencias políticas de carácter general", lo que nos conduce a la causa prevista en el FJ 2, g) de la STC 155/2009; y por otro, la "concurrencia de cuestiones sobre las que no hay doctrina del Tribunal Constitucional", es decir la causa prevista en el FJ 2, a) de la STC 155/2009. En el primer caso, se argumenta que la cuestión planteada afecta a un número muy importante de empresas, europeas y norteamericanas, con una "altísima cuota de mercado" y con "importantísimas implicaciones financieras en prácticamente todos los sectores económicos", que supone en términos comerciales una cifra aproximada de "7,1 billones de dólares", debido al "volumen de datos personales involucrados". A ello se añade la grave situación de inseguridad jurídica creada con las SSTJUE, y la consiguiente falta de previsibilidad de la normativa sancionadora. En relación con el derecho de asociación, además de destacar su significación como derecho de ejercicio colectivo, que le dota de especial repercusión social, la demanda incide en la relevancia de la entidad OC desde el punto de vista de su grado de implantación y de su representatividad y reconocimiento nacional e internacional, así como su papel en lo que denomina como "conflicto actual entre la voluntad de autodeterminación de una parte significativa de la sociedad catalana y los poderes públicos del estado que busca preservar la integridad territorial".

En cuanto a la segunda causa, la demanda señala que "existe doctrina sobre la intervención de los poderes públicos dentro de la organización interna de una asociación para asegurar y preservar los valores democráticos del derecho de asociación", pero no sobre la dimensión que plantea este recurso, consistente en que se ha producido una "injerencia de los poderes públicos (…) con la sanción de 90.000 euros [que] tiene como objeto (…) limitar de manera ilegítima la actividad" de la asociación recurrente, incurriendo en una "desviación de poder y [en un] hostigamiento administrativo y judicial" a la entidad recurrente, que "representa posiciones ideológicas antagónicas a los poderes públicos del Estado".

4. Por medio de providencia de 10 de mayo de 2021, la Sección Cuarta de la Sala Segunda de este Tribunal acordó admitir a trámite el recurso de amparo apreciando que en el mismo concurre una especial trascendencia constitucional (art. 50.1 LOTC), "porque el recurso plantea un problema o afecta a una faceta de un derecho fundamental sobre el que no hay doctrina de este Tribunal [STC 155/2009, FJ 2, a)], y porque el asunto suscitado trasciende del caso concreto porque plantea una cuestión jurídica de relevante y general repercusión social o económica [STC 155/2009, FJ 2, g)]".

En la misma providencia se ordenaba remitir atenta comunicación a las Salas de lo Contencioso-Administrativo del Tribunal Supremo y de la Audiencia Nacional, a fin de que, en el plazo de diez días, remitieran certificación o fotocopia adverada de las actuaciones correspondientes al recurso de casación núm. 6960-2019, y al recurso contencioso administrativo núm. 397-2017, respectivamente. Del mismo modo, se debía emplazar a quienes hubieran sido parte en el procedimiento, excepto la parte recurrente en amparo, para que, en el plazo de diez días, pudieran comparecer en el recurso de amparo.

5. En fecha 26 de mayo de 2021 tuvo entrada en el registro de este Tribunal escrito presentado por el abogado del Estado, solicitando que se le tuviera por comparecido y parte en las actuaciones.

6. Por diligencia de ordenación de 16 de junio de 2021, la secretaría de justicia de la Sala Segunda tuvo "por personado y parte en el procedimiento al abogado del Estado, acordándose entender con él las sucesivas actuaciones". Asimismo, de conformidad con lo dispuesto en el art. 52.1 LOTC, se dispuso dar vista de las actuaciones a las partes personadas y al Ministerio Fiscal, por plazo común de 20 días, para que pudieran presentar las alegaciones que estimaran pertinentes.

7. En fecha 16 de julio de 2021, el abogado del Estado presentó su escrito de alegaciones, en el que solicitó la inadmisión del recurso de amparo y, subsidiariamente, su desestimación.

Una vez expuestos los antecedentes que estimó de interés, comienza la argumentación poniendo de manifiesto que, a su juicio, la demanda utiliza el recurso de amparo como un recurso más, pretendiendo una nueva valoración de la prueba o una revisión del criterio jurídico aplicado por la jurisdicción ordinaria. Con cita y reseña parcial de diversas resoluciones de este Tribunal, considera que el recurrente obvia el carácter subsidiario del amparo y su naturaleza de recurso autónomo, es decir, no integrado como una fase dentro del procedimiento judicial de origen. El recurrente pretende encubrir su mera disconformidad con la decisión del Tribunal Supremo sobre la inadmisión del recurso de casación, como si fuera una vulneración del derecho a la tutela judicial efectiva cuando, en realidad, la resolución judicial satisface el canon constitucional de razonabilidad propio del derecho de acceso al recurso como un derecho de configuración legal. La pretensión del recurrente, en definitiva, sería volver a plantear las mismas cuestiones de legalidad ordinaria ya resueltas en la vía jurisdiccional correspondiente.

Por otro lado, considera que tampoco concurre vulneración alguna del derecho a la legalidad sancionadora ni a los principios de seguridad jurídica y de confianza legítima. Para ello, se remite íntegramente a los hechos consignados en las resoluciones de la AEPD, y hace un amplio resumen de los fundamentos jurídicos de la sentencia dictada por la Audiencia Nacional. Y, a continuación, destaca los siguientes elementos fácticos y jurídicos:

i) La transferencia internacional de datos presenta un elemento dinámico (la propia "comunicación/transmisión/cesión de datos personales del exportador al importador") y otro estático, consistente en la "finalidad del flujo (…), el tratamiento a que los datos (…) van a ser sometidos", que puede ser "la mera 'conservación' (hosting) (…), dada la amplitud del concepto de tratamiento del art. 5.2.t) RLOPD". El responsable del tratamiento ha de cumplir con las normas establecidas para la exportación de los datos, pero también ha de hacerse responsable de que las garantías sobre protección de datos sean equiparables en el lugar de importación. Es decir, su responsabilidad abarca los dos elementos que integran la transferencia de los datos. En este contexto, la suspensión temporal de la transferencia y la inmovilización de ficheros serían medidas que afectarían a los datos "que no hubieran sido ya exportados", resultando de "utilidad escasa o nula" respecto de los datos que estuviesen alojados en el país tercero.

ii) La mera lectura de la regulación sobre la inmovilización de ficheros (art. 49 LOPD) pone de manifiesto su compatibilidad con el ejercicio de la potestad sancionadora, por lo que la entidad recurrente "podía prever razonablemente" la actuación administrativa, al margen de que el principio de confianza legítima "sólo puede alcanzar la actuación que se cree lícita y no sobre

el tipo de procedimiento o ejercicio de potestad que el organismo de control pudiera llevar a cabo". De hecho, la demanda pone de manifiesto que la entidad recurrente fue consciente de que, al menos desde el mes de enero de 2016 había finalizado el denominado "periodo de gracia" para la regularización de su fichero y, sin embargo, "no es hasta finales de septiembre de ese mismo año cuando se entiende resuelto el contrato con BSD".

iii) El alegado bloqueo de los datos no produce los mismos efectos que la suspensión temporal de la transferencia internacional ni la inmovilización de los ficheros. En el presente caso, los "datos no se encontraban bloqueados de acuerdo con la definición de bloqueo que hacía la LOPD y el RDLOPD, sino que lo que se solicitó y así se hizo fue bloquear el acceso a través de la cuenta de usuario de OC en la aplicación BSD Tools. Es decir, los datos seguían siendo accesibles y utilizables por parte del importador de datos". Por lo tanto, "es obvio" que la transferencia internacional "seguía existiendo". Para la abogacía del Estado, la definición normativa de "bloqueo de datos" viene derivada de la noción de "cancelación" recogida en el art. 5.1.b RDLOPD, y supone la "identificación y reserva [de los datos] con el fin de impedir su tratamiento". De manera que, "mientras no se rescinda el contrato y se ejecute la eliminación o devolución de los datos, éstos siguen fuera del Espacio Económico Europeo". El bloqueo del acceso de la entidad OC a su base de datos "en ningún caso serviría para evitar los riesgos de realizar transferencias internacionales a EEUU, pues los riesgos que derivan de la propia legislación de [ese] país es una de las causas por las que se invalidó la (…) Decisión sobre *Safe Harbour*". Concluye este punto señalando que "ni de la interpretación de las comunicaciones de la AEPD, ni de los artículos 69.1 (ni del art. 70.3) RDLOPD, o 37.1.f) y 49 de la LOPD, OC podía formarse la convicción de que su actuación era conforme a derecho y que, por tanto, no daría lugar al ejercicio de la potestad sancionadora por parte de la AEPD".

Descartada la vulneración del derecho reconocido en el art. 25.1 CE, considera que "el solo principio de seguridad jurídica (art. 9.3 de la CE) sin conexión íntima o inmediata con una supuesta vulneración de un derecho [fundamental] (…) no sería susceptible de amparo, en la medida en que no puede fundarse (…) en la hipotética vulneración de un principio", citando las SSTC 8/1981 y 10/1985.

En lo relativo a la responsabilidad solidaria invocada en la demanda, el abogado del Estado sostiene que, aunque la STC 76/1990 no la excluye en el ámbito administrativo sancionador, tampoco la configura como obligatoria, sino que está sujeta a una "decisión del legislador", mediante una "disposición legal que contemple de modo expreso dicho cumplimiento conjunto". Cuestión distinta es que pueda apreciarse una responsabilidad "independiente" o individualizada, que es lo que ha ocurrido en este caso, tras hacer una amplia reseña de la

sentencia dictada por la Audiencia Nacional. Por lo tanto, considera que nos encontramos ante una "apreciación de los hechos y su calificación desde la perspectiva de la legalidad ordinaria aplicable al caso (…), respecto de la que no se atisba ninguna vulneración de un derecho fundamental".

Respecto de la alegación sobre la desproporción de la sanción impuesta, el abogado del Estado se remite al extenso fundamento jurídico séptimo de la sentencia de la Audiencia Nacional, considerando que se hace una aplicación motivada y no incursa en arbitrariedad, error patente o irrazonabilidad de la legislación vigente, lo que conduce de nuevo "al campo de la legalidad ordinaria".

En cuanto al derecho de asociación, se remite a la doctrina constitucional sobre sus facetas o vertientes (SSTC 218/1988; 113/1994 y 48/2003), para descartar que se haya visto afectada en este "caso: ni se le ha impedido crear una asociación, ni se le ha impuesto a nadie un deber de adscripción, ni la sujeción a una determinada categoría de organización, ni con veto o autorización previa administrativa de funcionamiento". A su juicio, el recurrente "no puede pretender vulnerado el derecho del art. 22 de la CE porque haya sido sancionada por infringir una norma establecida en el ámbito sectorial correspondiente", lo que supondría "un ámbito de impunidad frente a los órganos del Estado encargados de la aplicación de la ley".

Y en lo referente al derecho de propiedad (art. 33 CE), señala que "no es un derecho susceptible de invocación en amparo".

El escrito de alegaciones finaliza señalando la falta de especial trascendencia constitucional del amparo, porque considera que la demanda no ha motivado "en modo alguno" esa supuesta "relevancia y general repercusión social o económica" o las "consecuencias políticas generales", al margen de su mera discrepancia con la actuación administrativa y judicial ahora impugnada.

En virtud de lo anterior, interesa la inadmisión del recurso "por pretender la estimación de aspectos de legalidad ordinaria y [por] falta de trascendencia constitucional del mismo" y, "subsidiariamente", su desestimación.

8. En fecha 22 de julio de 2021, el fiscal ante el Tribunal Constitucional presentó su escrito de alegaciones, en el que solicitó la inadmisión del recurso en relación con el motivo de amparo imputado a la resolución del Tribunal Supremo, y la estimación parcial del recurso de amparo por la vulneración del derecho a la tutela judicial efectiva, achacable a la sentencia dictada por la Audiencia Nacional.

El escrito incluye una amplia reseña de los antecedentes que se consideraron de interés, así como de las resoluciones impugnadas, para abordar seguidamente el óbice procesal que, a su juicio, concurre respecto de la alegación sobre una eventual vulneración del derecho a la tutela judicial efectiva (art. 24.1 CE) atribuida a la resolución dictada por el Tribunal Supremo. Para el fiscal, se trataría de una lesión autónoma e independiente de las demás, lo que habría exigido el agotamiento de la vía judicial previa, mediante la oportuna promoción del incidente de nulidad de actuaciones (art. 241 LOPJ). Al no hacerse así, se estaría incurriendo en la causa de inadmisión prevista en el art. 50.1.a) LOTC, en relación con el art. 44.1.a) LOTC.

A continuación, el Ministerio Fiscal expone la doctrina jurisprudencial sobre los derechos fundamentales invocados en la demanda. En particular, sobre el principio de legalidad sancionadora, con cita de la STC 70/2012, y sobre el principio de confianza legítima, con amplia reseña de la STS de 30 de octubre de 2012 (recurso núm. 1657/2010) y de la normativa administrativa aplicable.

Entrando en las diversas cuestiones de fondo planteadas por el recurrente, el fiscal aborda, en primer lugar, la alegación sobre la vulneración del principio de confianza legítima y de seguridad jurídica. A tal efecto, tras extractar la respuesta ofrecida por la sentencia de la Audiencia Nacional, concluye que "el comportamiento de OC" no pudo estar "determinado por el seguimiento de las directrices o instrucciones de la AEPD", ya que "nunca cumplió (…) con sus obligaciones más elementales (…) en materia de transferencia internacional de datos". En concreto, no llegó a comunicar la realización de las propias transferencias y tampoco solicitó la autorización de la AEPD, por lo que no podía entenderse que las comunicaciones de la AEPD estuvieran dirigidas a entidades como OC. En cualquier caso, aunque fuera cierto que la conducta de la recurrente se hubiera ajustado a las directrices de la AEPD, eso no supondría la atipicidad de la conducta sino la ausencia o disminución de la culpabilidad.

En cuanto al derecho a la tutela judicial efectiva (art. 24.1 CE), en su modalidad de resolución motivada, el fiscal considera que la sentencia de la Audiencia Nacional recoge los elementos de juicio que fueron tenidos en cuenta para resolver la controversia planteada. Sin embargo, esta vulneración aparece directamente vinculada a la cuestión de la determinación de la responsabilidad por la infracción cometida y, en este punto, el fiscal considera que la resolución judicial no fue "debidamente motivada". A su juicio, la sala no tuvo en cuenta algunas de las alegaciones formuladas por la entidad recurrente, tales como: que la actividad había sido organizada conjuntamente por dos asociaciones; que ambas notificaron la existencia de un único fichero; que no pudieron registrar la corresponsabilidad porque los formularios de inscripción no admitían esa posibilidad; o que se distribuyeron los gastos derivados de la campaña, lo que explica que fuera OC la que figurara en el contrato de prestación de servicios con BSD, pero que aparecieran ambas

entidades como responsables del tratamiento en el anexo de privacidad de ese contrato. Para el fiscal, la falta de referencia o de apreciación de estas circunstancias determinó un "déficit motivacional (…) que afecta a uno de los elementos esenciales de la pretensión", como era que "se declarara la existencia de una sola infracción (…) con dos autores diferentes" que, a su vez, era el "cauce necesario para el reconocimiento (…) de una responsabilidad solidaria". En consecuencia, propone la estimación del recurso por este motivo.

En lo relativo al derecho de asociación (art. 22 CE) y al derecho de propiedad (art. 33 CE), se recoge extensamente el fundamento jurídico séptimo de la sentencia de la Audiencia Nacional, así como la doctrina constitucional sobre el principio de proporcionalidad de las penas (STC 133/2021), a lo que se añade una amplia reseña de la STC 292/2000, sobre el derecho a la protección de datos (art. 18.4 CE). De este conjunto doctrinal se deduce que "el bien jurídico protegido por la norma aplicada y los fines inmediatos y mediatos de protección de esa norma [el derecho de protección de datos] son, sin ningún género de dudas, suficientemente relevantes. Además, puede afirmarse que la medida era idónea y necesaria para alcanzar los fines de protección que constituyen el objetivo del precepto en cuestión. Finalmente, resulta que la sentencia ahora impugnada ha argumentado en su FJ 7 de forma extensa sobre la proporcionalidad de la sanción impuesta a la entidad recurrente, en términos que han de ser considerados completamente razonables". Por lo tanto, el hecho de que la sanción impuesta no pueda ser considerada como desproporcionada implica que "deban decaer los argumentos (…) para sostener que, como derivación (…), resultaron afectados los derechos fundamentales" invocados.

9. En fecha 27 de julio de 2021, la representación del recurrente presentó su escrito de alegaciones, en el que se remite a lo expuesto en la demanda así como en el posterior escrito de 1 de marzo de 2021, por el que se aportó información complementaria.

10. Por providencia de 17 de marzo de 2022, se señaló para deliberación y votación de la presente sentencia el día 21 del mismo mes y año.

II. Fundamentos jurídicos

1. *Objeto del recurso y pretensiones de las partes.*

El presente recurso de amparo tiene por objeto la impugnación de dos resoluciones judiciales. Por un lado, el auto de 19 de junio de 2020, dictado por la Sección Primera de la Sala de

lo Contencioso-Administrativo del Tribunal Supremo (TS), por el que se inadmite a trámite el recurso de casación núm. 6960-2019 interpuesto contra la sentencia de 29 de abril de 2019, también impugnada, dictada por la Sección Primera de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional (AN), en el recurso núm. 397-2017. La demanda se interpone por la vía del art. 44 LOTC. No obstante, la mayor parte de los motivos de impugnación tienen su origen en dos resoluciones de la Directora de la Agencia Española de Protección de Datos (AEPD). En concreto, la resolución RR/00326/2017 de 4 de mayo de 2017, dictada en el PS/00391/2016, que confirmó en reposición la resolución R/00325/2017, de 22 de febrero, por la que se impuso una sanción de 90.000 euros a la asociación ahora recurrente, por la comisión de una conducta infractora de incumplimiento de la prohibición prevista en el art. 33 de la L.O. 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). Esto determinaría la ubicación sistemática del recurso en el art. 43 LOTC, de manera que las resoluciones judiciales habrían incurrido en las lesiones invocadas en la medida en que no habrían reparado las vulneraciones atribuidas a las resoluciones administrativas. Sin embargo, el recurso debemos considerarlo como un recurso de amparo mixto, toda vez que, además de lo expuesto, la demanda impugna específicamente, la resolución del Tribunal Supremo que inadmitió a trámite el recurso de casación, así como la ya citada sentencia de la Audiencia Nacional, alegando la vulneración del derecho a la tutela judicial efectiva (art. 24.1 CE).

Por tanto, como se ha expuesto con más detalle en los antecedentes de hecho, el recurso considera que las resoluciones impugnadas vulneran: i) el derecho a la legalidad sancionadora (art. 25.1 CE), en relación con el art. 9.3 CE (principios de seguridad jurídica y de confianza legítima), dado que la aplicación administrativa y judicial del régimen sancionador en materia de protección de datos resultaba imprevisible; ii) los derechos de asociación (art. 22 CE) y de propiedad (art. 33 CE), por la desproporción de la sanción impuesta; iii) el derecho a la tutela judicial efectiva (art. 24.1 CE), en su vertiente de derecho a obtener una resolución motivada, por la insuficiente justificación de la imposición de una sanción individualizada a la entidad recurrente, como autora de una infracción, en vez de haber apreciado la coautoría y la consiguiente responsabilidad solidaria, mediante la imposición de una sola sanción a las dos entidades corresponsables del tratamiento de datos; y iv) la vulneración del derecho a la tutela judicial efectiva (art. 24. 1 CE), por la irrazonabilidad de los argumentos tenidos en cuenta para inadmitir a trámite el recurso de casación.

Las dos primeras quejas se imputan directamente a las resoluciones administrativas y no habrían sido reparadas por las posteriores decisiones judiciales; la tercera queja se formula contra la sentencia de la Audiencia Nacional y la última se imputa específicamente al auto del Tribunal Supremo.

Por su parte, el abogado del Estado plantea la concurrencia de un óbice procesal que afectaría a toda la demanda, consistente en la falta de especial trascendencia constitucional del recurso [art. 50.1.b) LOTC, *sensu contrario*], dado que no se ha justificado suficientemente este presupuesto procesal y, en todo caso, por plantear aspectos de mera legalidad ordinaria. Subsidiariamente, se interesa la desestimación del recurso, al entender que no concurre vulneración alguna de un derecho fundamental.

Por último, el Ministerio Fiscal interesa, por un lado, la inadmisión del recurso en relación con la lesión atribuida a la resolución dictada por el TS, por falta de agotamiento de la vía judicial previa, al no haberse promovido el correspondiente incidente de nulidad de actuaciones (art. 24.1 LOPJ), de conformidad con lo dispuesto en el art. 50.1.a) LOTC, *sensu contrario*, en relación con el art. 44.1.a) LOTC. Por otro lado, interesa la estimación parcial del recurso, por entender que la sentencia de la AN habría vulnerado el derecho a la tutela judicial efectiva (art. 24.1 CE), en su vertiente de derecho a obtener una resolución motivada, por no haber dado respuesta suficiente a algunas de las cuestiones sustanciales alegadas por el recurrente en la vía judicial previa.

Planteado el recurso en estos términos, nuestro orden de enjuiciamiento comenzará con el análisis de los óbices procesales alegados para, en su caso, exponer la doctrina jurisprudencial sobre los derechos fundamentales invocados y realizar el enjuiciamiento que proceda.

2. *Óbices procesales. Delimitación del objeto de este recurso de amparo.*

Tanto la Abogacía del Estado como el Ministerio Fiscal han alegado la concurrencia de óbices procesales que determinarían la inadmisión, total o parcial, del presente recurso de amparo, que han de ser abordados con carácter preliminar. De entre los óbices expuestos, procede analizar, en primer lugar, aquellos que afectan a la demanda en su conjunto ya que, de ser admitidos, excluirían la necesidad de proseguir nuestro enjuiciamiento constitucional.

a) El abogado del Estado argumenta que la demanda incurre en falta de especial trascendencia constitucional [arts. 49.1 y 50.1.b) LOTC]. Como es conocido, este presupuesto procesal fue introducido por la reforma de la LOTC llevada a cabo por la LO 6/2007, de 24 de mayo.

Conforme señala la STC 155/2009, de 25 de junio (FJ 2), este "requisito sustantivo o de fondo" determina que "para la admisión del recurso de amparo no [sea] suficiente la mera lesión de un derecho fundamental o libertad pública del recurrente tutelable en amparo [arts. 53.2 y 161.1 b) CE y 41 LOTC]", sino que es necesario que su contenido "justifique una decisión de fondo" de este Tribunal (FJ 2). Para ello, "es preciso que 'en la demanda se disocie adecuadamente la argumentación tendente a evidenciar la existencia de la lesión de un derecho fundamental —que

sigue siendo, obviamente, un presupuesto inexcusable en cualquier demanda de amparo— y los razonamientos específicamente dirigidos a justificar que el recurso presenta especial trascendencia constitucional' (STC 17/2011, de 28 de febrero, FJ 2)" [STC 118/2014, de 8 de julio (FJ 2.c)]. Se trata de que la parte realice un "esfuerzo argumental" [ATC 154/2010, de 15 de noviembre (FJ 4)] que "permita advertir 'por qué el contenido del recurso de amparo justifica una decisión sobre el fondo en atención a su importancia para la interpretación, aplicación o general eficacia de la Constitución o para la determinación del contenido y alcance de los derechos fundamentales' que se aleguen en la demanda (STC 69/2011, de 16 de mayo, FJ 3, citando el ATC 187/2010, de 29 de noviembre, FJ único)" [STC 118/2014, de 8 de julio (FJ 2.c)]. El "carácter notablemente abierto e indeterminado, tanto de la noción de 'especial trascendencia constitucional', como de los criterios legalmente establecidos para su apreciación, confieren a este Tribunal un amplio margen decisorio para estimar" que concurre este requisito; unos criterios que fueron delimitados, esencialmente, en el fundamento jurídico 2 de la ya citada STC 155/2009, de 25 de junio. En cualquier caso, la "decisión liminar de admisión a trámite del recurso al apreciar el cumplimiento del citado requisito no limita las facultades del Tribunal sobre la decisión final en relación con el fondo del asunto" [STC 155/2009, de 25 de junio, (FJ 2)].

En el presente caso, por medio de providencia de 10 de mayo de 2021, la Sección Cuarta de la Sala Segunda de este Tribunal acordó admitir a trámite el recurso de amparo apreciando que en el mismo concurre una especial trascendencia constitucional (art. 50.1 LOTC), "porque el recurso plantea un problema o afecta a una faceta de un derecho fundamental sobre el que no hay doctrina de este Tribunal [STC 155/2009, FJ 2, a)], y porque el asunto suscitado trasciende del caso concreto porque plantea una cuestión jurídica de relevante y general repercusión social o económica [STC 155/2009, FJ 2, g)]". El abogado del Estado considera que no concurre ninguna de estas causas, por falta de suficiente justificación y por plantear cuestiones de mera legalidad ordinaria. Sin embargo, este Tribunal entiende que, tal y como estaba planteada la demanda, era posible apreciar la existencia de este presupuesto procesal.

En efecto, el recurso de amparo plantea una faceta específica del derecho fundamental del art. 18.4 CE, en relación con el art. 25.1 CE, hasta ahora no abordada por nuestra jurisprudencia, como es la del régimen sancionador en el ámbito de la protección de datos personales recogidos en ficheros transferidos internacionalmente a servidores ubicados en un Estado no perteneciente a la UE. En concreto, la cuestión de la previsibilidad de la aplicación de un determinado tipo infractor en relación con las transferencias internacionales de datos y los efectos que, respecto del citado derecho fundamental, puede ocasionar un pronunciamiento del TJUE que anule una Decisión de la Comisión que, con anterioridad, hubiera reconocido un nivel adecuado de protección de servidores

instalados en un Estado no perteneciente a la UE. La sentencia del TJUE de 6 de octubre de 2015 (asunto C-362/14), que anuló la Decisión de la Comisión 2000/520/CE, de 26 de julio, da ocasión a este Tribunal para el enjuiciamiento de la problemática que suscita esta cuestión, desde la denunciada vulneración del derecho fundamental del art. 18.4 CE.

Por otro lado, es un hecho público y notorio que la progresiva informatización de una realidad cada vez más globalizada implica que cualquier decisión sobre transferencia de datos personales pueda afectar a un número muy significativo de ciudadanos, empresas y administraciones, tanto a nivel nacional como internacional.

En definitiva, la demanda realizó un adecuado esfuerzo argumental disociativo entre las lesiones invocadas y las razones que justificarían un pronunciamiento de este Tribunal y la providencia que acordó la admisión a trámite, así lo ha estimado, por lo que procede rechazar el óbice opuesto por el abogado del Estado al conjunto de las vulneraciones de derechos fundamentales denunciadas por la demanda.

b) El Ministerio Fiscal considera que concurre el óbice de falta de agotamiento de la vía judicial previa, respecto de las vulneraciones que la demanda atribuye a la resolución del TS.

Tiene razón el fiscal. La parte recurrente ha alegado diversas lesiones de derechos fundamentales que, en lo esencial, se imputan a las resoluciones de la AEPD y, por extensión, a las resoluciones judiciales que no las repararon, señaladamente, la sentencia de la AN. Sin embargo, también se atribuye específicamente al auto de 19 de junio de 2020, dictado por la Sección Primera de la Sala de lo Contencioso-Administrativo del TS, la vulneración del derecho a la tutela judicial efectiva (art. 24.1 CE), que el recurrente sitúa en su vertiente de "acceso a la justicia", y que más propiamente habría que encuadrar en la del "acceso al recurso". Alega, a tal efecto, la irrazonabilidad de los argumentos tenidos en cuenta para inadmitir a trámite el recurso de casación interpuesto contra la sentencia de la AN.

La demanda incurre en el requisito de no procedibilidad de falta de agotamiento de la vía judicial previa [art. 44.1.a) LOTC, en relación con el art. 50.1.a) LOTC, *sensu contrario*]. Frente a esa concreta resolución impugnada, el auto del TS, no se ha interpuesto el correspondiente incidente de nulidad de actuaciones previsto en el art. 241 LOPJ.

Este incidente está previsto para los casos en que la vulneración no haya podido denunciarse antes de recaer resolución que ponga fin al proceso y siempre que dicha resolución no sea susceptible de recurso ordinario ni extraordinario. De esta forma, el incidente excepcional de nulidad de actuaciones "constituye 'el remedio procesal idóneo' para obtener la reparación [del derecho fundamental de que se trate]. En tales casos, antes de acudir en amparo, debe solicitarse en la vía ordinaria el referido incidente de nulidad 'sin cuyo requisito la demanda de amparo devendrá

inadmisible, conforme a los arts. 44.1 a) y 50.1 a) LOTC, por falta de agotamiento de todos los recursos utilizables dentro de la vía judicial' (SSTC 228/2001, de 26 de noviembre, FJ 3; 74/2003, de 23 de abril, FJ 2; y 237/2006, de 17 de julio, entre otras muchas)" (STC 126/2011, de 18 de julio).

En el supuesto que nos ocupa, el órgano judicial (TS) no ha tenido la oportunidad de reparar la concreta vulneración que se le atribuye, lo que solo podría haberse efectuado mediante el planteamiento de un incidente de nulidad de actuaciones, ya que el auto dictado no podía ser objeto de recurso alguno. Al no hacerse así, se considera que no se ha agotado la vía judicial previa, imprescindible para respetar el carácter subsidiario del recurso de amparo, ya que, como recordaba la ya citada STC 155/2009, de 25 de junio (FJ 2), el legislador ha "encomendado a los Jueces y Tribunales como guardianes naturales y primeros de [los derechos fundamentales] (STC 227/1999, de 13 de diciembre, FJ 1), a los que confiere un mayor protagonismo en su protección (…), culminado por el Tribunal Constitucional que, además de garante último, es su máximo intérprete (arts. 53.2 y 123 CE y 1.1 LOTC)".

Procede, pues, estimar el óbice alegado por el Ministerio Fiscal.

c) Con independencia de lo anterior, y como es conocido [STC 154/2016, de 22 de septiembre (FJ 2), y más recientemente en STC 130/2018, de 12 de diciembre (FFJJ 3 a 5)], los defectos insubsanables de que pudiera estar afectado el recurso de amparo no resultan reparados porque haya sido inicialmente admitido a trámite [por todas, SSTC 18/2002, de 28 de enero (FJ 3), y 158/2002, de 16 de septiembre (FJ 2)]. De esta manera, la comprobación de los presupuestos procesales para la viabilidad de la acción puede volverse a abordar o reconsiderar en la sentencia, de oficio o a instancia de parte, dando lugar a un pronunciamiento de inadmisión por falta de tales presupuestos, sin que para ello constituya obstáculo el carácter tasado de los pronunciamientos previstos en el art. 53 LOTC [por todas, STC 69/2004, de 19 de abril (FJ 3); 89/2011, de 6 de junio (FJ 2); y 174/2011 de 7 de noviembre (FJ 2)].

En el presente caso, un análisis detallado de la documentación obrante en autos pone de manifiesto que también concurre el óbice procesal de falta de invocación previa de la lesión alegada [art. 44.1.c) LOTC, en relación con el art. 50.1.a) LOTC, *sensu contrario*], con respecto a los derechos de asociación (art. 22 CE) y de propiedad (art. 33 CE).

Nos encontramos ante el mismo supuesto que el planteado en el recurso de amparo núm. 2058-2020, promovido por la misma entidad ahora recurrente, y que fue inadmitido a trámite por medio del ATC 75/2021, de 22 de julio, a cuyo FJ 3 nos remitimos expresamente. Como ocurriera en aquel caso, las quejas sobre la posible vulneración del derecho de asociación y del derecho a la propiedad no fueron alegadas en la vía judicial previa, tan pronto como fue posible. De esta forma,

se vuelve a ignorar que el recurso de amparo es un mecanismo subsidiario de protección de derechos fundamentales.

El agotamiento de la vía judicial previa "no resulta un mero formalismo retórico o inútil, pues tiene por finalidad, por una parte, que los órganos judiciales tengan la oportunidad de pronunciarse sobre la violación constitucional, haciendo posible el respeto y el restablecimiento del derecho constitucional en sede jurisdiccional ordinaria y, por otra, preservar el carácter subsidiario de la jurisdicción constitucional de amparo" [STC 128/2014, FJ 2.a)]. Conforme a esa misma doctrina, se trata, en todo caso, de un requisito que ha de ser "interpretado de manera flexible y con un criterio finalista", lo que supone obviar el puro formalismo de la mera cita de un precepto, para atender a la exposición de un "marco de alegaciones que permita al Tribunal ordinario cumplir con su función de tutelar los derechos fundamentales". Este planteamiento encuentra también su fundamento en la jurisprudencia europea que, para entender agotados los recursos judiciales internos del país de origen de la demanda, considera bastante que la lesión se haya invocado "al menos en sustancia (STEDH 26 de mayo de 2020, parágrafo 30)" [ATC 75/2021 (FJ 3)].

En el presente caso, tanto en la vía administrativa como en la posterior vía jurisdiccional, la parte ahora recurrente no alegó en momento alguno la posible vulneración de los derechos de asociación y de propiedad. Toda su argumentación estuvo orientada a discutir la concurrencia de la infracción administrativa sobre protección de datos, su responsabilidad, la concreta sanción impuesta, o la efectividad de su derecho de defensa. No es que no se mencionaran esos derechos, sino que ni siquiera podía deducirse su mera alegación. Incluso, al invocar la falta de proporcionalidad de la sanción fijada por la AEPD, no se relacionó con la imposibilidad o grave afectación para el ejercicio de tales derechos, sino con la concurrencia o no de circunstancias atenuantes o agravantes, es decir, sobre cuestiones de legalidad ordinaria.

De forma coherente, las resoluciones judiciales impugnadas se pronunciaron sobre las cuestiones planteadas y no entraron a valorar las alegaciones que ahora plantea la entidad recurrente. Por lo tanto, no se "suministró ese mínimo marco de alegaciones que permitiera a los jueces ordinarios, en este caso la Audiencia Nacional en instancia y el Tribunal Supremo en casación, cumplir su función de tutelar los derechos fundamentales y preservar la subsidiariedad del recurso de amparo" [ATC 75/2021 (FJ 3)].

Por lo demás, resulta manifiesto que el derecho a la propiedad no es un derecho tutelable en esta vía de amparo, al no estar comprendido entre los arts. 14 a 30 CE, de conformidad con lo dispuesto en el art. 41.1 LOTC, *sensu contrario*, lo que hubiera determinado en todo caso la inadmisión de cualquier alegación sobre este derecho reconocido en el art. 33 CE.

d) En virtud de todo lo anterior, el presente recurso de amparo ha de quedar limitado al análisis de las vulneraciones invocadas sobre los derechos a la legalidad sancionadora (art. 25. 1 CE) y a la tutela judicial efectiva (art. 24.1 CE), y sobre el principio de seguridad jurídica (art. 9.3 CE), en su dimensión de la confianza legítima, específicamente atribuidas a las resoluciones de la AEPD y a la sentencia de la AN.

3. *Doctrina jurisprudencial sobre el derecho a la legalidad sancionadora administrativa; sobre el principio de seguridad jurídica, en su dimensión de confianza legítima; y sobre el derecho a la tutela judicial efectiva, en su vertiente de derecho a obtener una resolución motivada y fundada en Derecho.*

A) *Legalidad sancionadora administrativa.*

La doctrina de este Tribunal sobre el derecho a la legalidad sancionadora administrativa ha sido expuesta en la STC 14/2021, de 28 de enero (FJ 2), con cita de otras anteriores. Así, se recuerda que "el principio de legalidad penal recogido en el art. 25.1 CE (…) también 'es de aplicación al ordenamiento sancionador administrativo', y es esencialmente una concreción de diversos aspectos del Estado de Derecho en el ámbito del Derecho estatal sancionador (STC 133/1987, de 21 de julio, FJ 4). Se vincula, ante todo, con el imperio de la ley como presupuesto de la actuación del Estado sobre bienes jurídicos de los ciudadanos, pero también con el derecho de los ciudadanos a la seguridad, previsto en la Constitución como derecho fundamental de mayor alcance, así como la prohibición de la arbitrariedad y el derecho a la objetividad e imparcialidad del juicio de los tribunales, que garantizan el artículo 24.2 y el artículo 117.1 CE e implica, al menos, tres exigencias: la existencia de una ley (*lex scripta*); que la ley sea anterior al hecho sancionado (*lex praevia*), y que la ley describa un supuesto de hecho estrictamente determinado (*lex certa*).

La garantía constitucional de *lex certa*, como faceta específica del derecho a la legalidad sancionadora, se desenvuelve, en nuestra doctrina (vid, por todas, las SSTC 146/2015, de 25 de junio, FJ 2; 219/2016, de 19 de diciembre, FJ 5, y 220/2016, de 19 de diciembre, FJ 5), en dos ámbitos distintos:

a) *Ámbito normativo*. De un lado, la garantía de certeza puede resultar vulnerada por la insuficiente determinación *ex ante* de la conducta sancionable, como defecto inmanente a la redacción legal del precepto sancionador objeto de escrutinio; vulneración que afectaría a la calidad de la ley, esto es, a la accesibilidad y previsibilidad del alcance de la norma en el ámbito penal o sancionador (SSTC 184/2003, de 23 de octubre, FJ 3, y 261/2015, de 14 de diciembre, FJ 5).

b) *Ámbito aplicativo*. En cambio, aun cuando la redacción de la norma sancionadora resulta suficientemente precisa, la garantía de *lex certa* puede verse afectada por la aplicación irrazonable de dicha norma, vertiente que se desdobla, a su vez, en dos planos, (i) el de la indebida interpretación *ad casum* del alcance semántico del precepto, más allá de su sentido literal posible (analogía *in malam partem*), y (ii) el de la subsunción irrazonable, en el precepto ya interpretado, de la conducta que ha sido considerada probada. En estos casos, pese a la 'calidad' de la ley, su aplicación irrazonable se proyecta sobre la exigencia de previsibilidad del alcance de su aplicación (STC 220/2016, de 19 de diciembre, FJ 5). Así, en efecto, una vez que el autor de la norma, el legislador, ha cumplido suficientemente con el mandato al dar una redacción precisa al precepto sancionador, la garantía de certeza exige igualmente de los órganos sancionadores que están llamados a aplicarlo 'no solo la sujeción […] a los dictados de las leyes que describen ilícitos e imponen sanciones, sino la sujeción estricta, impidiendo la sanción de comportamientos no previstos en la norma correspondiente pero similares a los que sí contempla' (SSTC 137/1997, de 21 de julio, FJ 6, y 146/2015, de 25 de junio, FJ 2). Por tanto, tal y como hemos señalado en nuestra doctrina, el derecho fundamental a la legalidad penal, reconocido en el art. 25.1 CE, ha de reputarse vulnerado cuando la conducta que ha sido declarada probada en la sentencia 'es subsumida de un modo irrazonable en el tipo' [sancionador correspondiente] (SSTC 91/2009, de 20 de abril, FJ 6; 153/2011, de 17 de octubre, FJ 8, y 196/2013, de 2 de diciembre, FJ 5)". Esta doctrina ha sido reiterada en la más reciente STC 133/2021, de 24 de junio [FJ 6.B.b)], con cita de otras anteriores como las SSTC 137/1997, de 21 de julio (FJ 6); 151/1997, de 29 de septiembre (FJ 7); 146/2015, de 25 de junio (FJ 2); y 184/2014, de 6 de noviembre (FJ 8); a las que cabe añadir la STC 145/2013, de 11 de julio (FJ 4). Conforme a lo expuesto en la STC 133/2021, de 24 de junio [FJ 6.B.b)], los criterios de razonabilidad serían: "(i) 'respeto al tenor literal de la norma', lo que implica que la subsunción del supuesto de hecho en el tipo penal aplicable no debe ser ajeno al significado posible de los términos de la norma aplicada; (ii) razonabilidad del discurso lógico, que 'habrá de ser analizada desde las pautas axiológicas que informan nuestro texto constitucional […] y desde modelos de argumentación aceptados por la propia comunidad jurídica'; (iii) Finalmente, '[s]on también constitucionalmente rechazables aquellas aplicaciones que por su soporte metodológico —una argumentación ilógica o indiscutiblemente extravagante— o axiológico —una base valorativa ajena a los criterios que informan nuestro ordenamiento constitucional— conduzcan a soluciones esencialmente opuestas a la orientación material de la norma y, por ello, imprevisibles para sus destinatarios'; [mientras que la labor de este Tribunal se ha de limitar a] verificar un juicio externo sobre la compatibilidad de la interpretación realizada con el tenor literal de la norma y sobre su razonabilidad metodológica y axiológica"**.**

B) *Seguridad jurídica y confianza legítima.*

La demanda invoca el principio de seguridad jurídica (art. 9.3 CE), en su dimensión de la confianza legítima. Como es conocido, la alegación sobre una vulneración de lo dispuesto en el art. 9.3 CE no se encuentra protegida por el recurso de amparo [STC 144/1987, de 23 de septiembre (FJ 2)]. No obstante, este Tribunal ha tenido la ocasión de pronunciarse en reiteradas ocasiones sobre este principio. Así, puede citarse la STC 181/2016, de 20 de octubre (FJ 4), sobre la ausencia de un derecho o garantía a la inmutabilidad del ordenamiento jurídico, que proteja frente a los cambios normativos; o la STC 51/2018, de 10 de mayo (FJ 5), sobre las limitaciones impuestas a la acción del legislador, en una doctrina que, inicialmente elaborada para las normas tributarias (a partir de la STC 126/1987, de 16 de julio), con posterioridad ha sido aplicada a cualquier ámbito normativo, lo que requiere una valoración casuística (ver, en esta línea, SSTC 182/1997, de 28 de octubre; 270/2015, de 17 de noviembre; o la ya citada STC 181/2016, de 20 de octubre).

Fuera del ámbito de las modificaciones normativas, este Tribunal se ha pronunciado en diversas resoluciones. Así, en la STC 6/2019, de 17 de enero [FJ 6.d)] se hacía referencia a otras vertientes de este principio. A tal efecto, se puede citar la que "deriva, (…) en el terreno jurisdiccional, de las actuaciones precedentes de un órgano de justicia en el mismo proceso o en otros similares, susceptibles de configurar un criterio previsible de proceder, el cual sin embargo deja de seguirse sin razón que lo justifique y con menoscabo de la posición de una de las partes, lo que también hemos reputado como una quiebra de aquel principio, con vulneración de un derecho fundamental (entre otras, SSTC 58/2000, de 28 de febrero, FJ 4; 135/2008, de 27 de octubre, FJ 4, y 13/2017, de 30 de enero, FJ 2)". O la que se refiere a una "aplicación razonable de las normas jurídicas procesales otorgantes de derechos, obligaciones y cargas a las partes, cuya inobservancia determina la lesión del derecho a la tutela judicial efectiva (art. 24.1 CE), puesto que entonces 'sufre la confianza legítima generada por los términos en que fue conformada la realidad jurídica en el proceso' (…)". Del mismo modo, en la STC 179/2015, de 7 de septiembre (FJ 2), como reiteración de lo expuesto en otras anteriores (SSTC 75/2015, 76/2015 o 78/2015) se resaltaba que la evolución de la jurisprudencia no es en sí contraria a este principio. Finalmente, en la STC 70/2018, de 21 de junio (FJ 10), se abordaba la aplicación del principio de confianza legítima en el supuesto concreto del silencio positivo en materia de autorizaciones administrativas.

Un recorrido por la doctrina expuesta permite llegar a la conclusión de que el principio de seguridad jurídica, se ha centrado fundamentalmente en el ámbito de los cambios normativos

(singularmente, en la aplicación retroactiva de las normas tributarias o en las que afectan a las actividades económicas sujetas a intervención administrativa) y jurisprudenciales.

Conforme a lo expuesto en la STC 14/2021, de 28 de enero (FJ 2), con cita de las SSTC 136/2011, de 13 de septiembre (FJ 9); 2006/2013, de 5 de diciembre (FJ 8) y 81/2020, de 15 de julio, FJ 14 b)]; la seguridad jurídica ha de entenderse como la "certeza sobre el ordenamiento jurídico aplicable y los intereses jurídicamente tutelados" (STC 156/1986, de 31 de enero, FJ 1), procurando "la claridad y no la confusión normativa" (STC 46/1990, de 15 de marzo, FJ 4), así como "la expectativa razonablemente fundada del ciudadano en cuál ha de ser la actuación del poder en la aplicación del Derecho" (STC 36/1991, de 14 de febrero, FJ 5). En definitiva, "solo si en el ordenamiento jurídico en que se insertan, y teniendo en cuenta las reglas de interpretación admisibles en Derecho, el contenido o las omisiones de un texto normativo produjeran confusión o dudas que generaran en sus destinatarios una incertidumbre razonablemente insuperable acerca de la conducta exigible para su cumplimiento o sobre la previsibilidad de sus efectos, podría concluirse que la norma infringe el principio de seguridad jurídica" (SSTC 96/2002, de 25 de abril, FJ 5; 93/2013, de 23 de abril, FJ 10, y 161/2019, de 12 de diciembre, FJ 4, por todas).

Una vertiente de la seguridad jurídica es el denominado principio de confianza legítima, que cuenta con respaldo normativo expreso en el art. 3.1.e) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP), como principio general de actuación de las administraciones públicas. En sus orígenes fue una creación jurisprudencial, de la que se encuentran numerosas referencias en la doctrina del Tribunal Supremo (ver, en tal sentido, la sentencia de su Sala Tercera de 30 de octubre de 2012, dictada en el recurso núm. 1657/2020, con reseña de otras muchas anteriores, citada en el informe del Ministerio Fiscal). Este reconocimiento normativo y jurisprudencial no puede desconocer, sin embargo, su profundo anclaje constitucional, bajo el principio de seguridad jurídica consagrado en el art. 9.3 CE y, en lo que ahora interesa, también en relación con el principio de legalidad sancionadora (art. 25.1 CE), como garantía de previsibilidad de la norma y de su aplicación.

La seguridad jurídica puede entenderse en este ámbito como el conjunto de facultades y obligaciones que deben presidir las relaciones entre la administración y los ciudadanos, y que permite a éstos conducirse en su actividad con garantía de certeza sobre los límites y las consecuencias de sus propios actos.

Desde la perspectiva que es propia de este Tribunal, el principio de confianza legítima, como expresión o vertiente de los principios más generales de seguridad jurídica y de legalidad sancionadora, habilita al ciudadano para realizar una conducta legítima bajo el amparo de una previa y consolidada actuación de la administración pública, con apariencia de licitud, y le protege frente a

cambios relevantes no justificados de los criterios de actuación administrativa que le hayan generado un perjuicio para sus legítimos derechos e intereses que no tenga la obligación de soportar. En consecuencia, los elementos necesarios para poder acogerse al principio de confianza legítima serían los siguientes:

a) Conducta legítima del ciudadano. La confianza legítima no puede ser alegada cuando la conducta ciudadana no encuentra amparo alguno en el ordenamiento jurídico, es decir, cuando se trata de una conducta notoriamente ilegal. No se puede invocar la seguridad jurídica, que es el fundamento del principio de confianza legítima, respecto de conductas que sean antijurídicas.

b) Conducta basada en una previa y consolidada actuación administrativa. El ciudadano ha de desarrollar su conducta sobre la base de hechos externos concluyentes, que revelen de forma inequívoca un determinado criterio de actuación administrativo. No puede tratarse de meras suposiciones o deducciones implícitas de la actividad o inactividad administrativa, ni tampoco de meras opiniones o interpretaciones divergentes del ordenamiento jurídico, que tienen su cauce normal de resolución en la vía jurisdiccional correspondiente.

c) Apariencia de licitud de la actuación administrativa. El ciudadano ha de realizar su conducta con la creencia racional y fundada de que es adecuada a Derecho. El principio de confianza legítima solo protege frente a una actuación administrativa que, precisamente por su apariencia de legitimidad, ha motivado la conducta ciudadana. El ciudadano no debe adecuar su conducta a las actuaciones administrativas manifiestamente ilegales.

d) Quebrantamiento de la confianza depositada en la actuación administrativa. La esencia de este principio se pone de manifiesto ante una modificación relevante de los criterios de actuación consolidados previamente, sin justificación alguna. De esta forma, se defrauda la confianza del ciudadano que, hasta entonces, había guiado su actuación conforme a los parámetros establecidos por la administración. La modificación ha de referirse a elementos relevantes de la actuación administrativa, es decir, que produzcan efectos en la esfera de bienes y derechos del ciudadano, y que no ofrezcan una justificación suficiente basada, por ejemplo, en hechos imprevisibles o causas de fuerza mayor o de prevalencia del interés público.

e) Perjuicio para el ciudadano que no tenga la obligación de soportar. El principio de confianza legítima solo puede tener virtualidad en los casos en que, como consecuencia del cambio de actuación administrativa, se ha producido un perjuicio para el ciudadano, no necesariamente económico o patrimonial. Además, debe tratarse de un perjuicio que el ciudadano no esté obligado a soportar, de forma que las causas imprevisibles, de fuerza mayor o de prevalencia del interés público podrían justificar un cambio en la actuación administrativa.

f) Protección frente a la actuación administrativa. El principio de confianza legítima protege al ciudadano ante una modificación injustificada de la actuación administrativa, mediante su declaración de nulidad y el consiguiente restablecimiento de sus derechos e intereses. Eso no impide una eventual indemnización de daños y perjuicios, pero no estaría basada en el principio de confianza legítima, sino que habría de ajustarse a los requisitos previstos en la normativa vigente para la protección de otros derechos como el de propiedad (Ley de 16 de diciembre de 1954, sobre expropiación forzosa) o para la declaración de responsabilidad patrimonial de las administraciones públicas (arts. 32 y siguientes LRJSP).

g) El principio de confianza legítima es predicable respecto de la actividad discrecional de la administración, pero no puede entrar en juego cuando se trata de una actividad reglada, porque entonces la conducta administrativa y la del ciudadano solo pueden adecuarse a lo dispuesto en el ordenamiento jurídico, y su eventual incumplimiento dará lugar a las acciones legales correspondientes. El principio de confianza legítima no puede superponerse a lo dispuesto en la propia legalidad, que es la máxima expresión de la seguridad jurídica.

C) *Tutela judicial efectiva: Motivación.*

Finalmente, la doctrina jurisprudencial sobre el derecho a la tutela judicial efectiva (art. 24.1 CE), en su vertiente de derecho a obtener una resolución motivada y fundada en Derecho, ha sido reiteradamente expuesta por este Tribunal. Entre los pronunciamientos más recientes, y en lo que ahora interesa, la STC 61/2021, de 15 de marzo (FJ 4), recuerda lo siguiente:

> "Hemos afirmado que el derecho fundamental a la tutela judicial efectiva 'exige que las resoluciones judiciales al decidir los litigios sean fundadas en Derecho' (SSTC 99/2000, de 10 de abril, FJ 6, y 144/2003, de 14 de julio, FJ 2), lo que significa, como hemos advertido en la STC 184/1992, de 16 de noviembre, FJ 2, reiterando consolidada doctrina de este tribunal, que 'una aplicación de la legalidad que sea arbitraria, manifiestamente irrazonada o irrazonable no puede considerarse fundada en Derecho y lesiona, por ello, el derecho a la tutela judicial (SSTC 23/1987, 24/1990 y 25/1990)'.
>
> Según consolidada y unánime doctrina constitucional, el derecho a obtener la tutela judicial efectiva garantizado en el art. 24.1 CE, comprende el derecho a obtener de los jueces y tribunales una resolución motivada y fundada en Derecho sobre el fondo de las pretensiones oportunamente deducidas por las partes en el proceso (por todas, STC 38/2011, de 28 de marzo, FJ 3). Lo que significa, en primer lugar, que la resolución judicial ha de estar motivada, es decir, debe contener los elementos y razones de juicio que permitan conocer cuáles han sido los criterios jurídicos que fundamentan la decisión; y en segundo lugar, su motivación debe estar fundada en Derecho (SSTC 276/2006, de 25 de septiembre, FJ 2, y 64/2010, de 18 de octubre; FJ 3) o, lo que es lo mismo, que sea consecuencia de una exégesis racional del ordenamiento y no fruto de un error patente o de la arbitrariedad (por todas, STC 146/2005, de 6 de junio, FJ 7). En resumidas cuentas, el art. 24.1 CE impone a los órganos judiciales 'no sólo la obligación de ofrecer una respuesta motivada a las

> pretensiones deducidas, sino que, además, esta ha de tener contenido jurídico y no resultar arbitraria' (STC 8/2005, de 17 de enero, FJ 3).
>
> Conviene no obstante recordar que en esa misma doctrina constitucional está igualmente dicho que el derecho a la tutela judicial efectiva del art. 24.1 CE 'no incluye un pretendido derecho al acierto judicial en la selección, interpretación y aplicación de las disposiciones legales, salvo que afecte al contenido de otros derechos constitucionales distintos al de tutela judicial efectiva' (recientemente, entre otras, SSTC 3/2011, de 14 de febrero, FFJJ 3 y 5, y 183/2011, de 21 de noviembre, FFJJ 5 y 7). Y que la simple discrepancia de las partes con una resolución judicial, aun fundada en otra interpretación posible de la legalidad aplicada, incluso por plausible que esta resulte, no convierte el correspondiente razonamiento judicial en arbitrario o manifiestamente irrazonable ni, menos aún, obliga a este tribunal a elegir entre las interpretaciones posibles cuál es la que debe prevalecer (SSTC 59/2003, de 24 de marzo, FJ 3; 221/2003, de 15 de diciembre, FJ 4; 140/2005, de 6 de junio; FJ 5, y 221/2005, de 12 de septiembre, FJ 5)".

4. *Enjuiciamiento del caso.*

Como ya se ha expuesto, el objeto de este recurso de amparo ha quedado circunscrito a las alegaciones sobre la vulneración del derecho a la legalidad sancionadora (art. 25.1 CE), en su vertiente de previsibilidad de la actuación administrativa y judicial, que ha de ponerse en relación, también, con el principio de seguridad jurídica (art. 9.3 CE), en su dimensión del quebrantamiento de la confianza legítima; y de la tutela judicial efectiva (art. 24.1 CE), en su vertiente del derecho a obtener una resolución motivada y fundada en Derecho.

El enjuiciamiento de las cuestiones planteadas exige, en primer lugar, una somera descripción de la regulación vigente en el momento de los hechos, en sus elementos esenciales aplicables al caso; y, en segundo lugar, determinar si, a la vista de esa regulación, la actuación administrativa y judicial era razonablemente previsible y estuvo suficientemente motivada.

4.1 Descripción del régimen administrativo sancionador aplicable al caso.

En el momento de suceder los hechos objeto de enjuiciamiento, estaba vigente la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD), en la redacción llevada a cabo, en lo que ahora interesa, por la disposición final quincuagésima sexta de la Ley 2/2011, de 4 de marzo; así como el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprobó el Reglamento de desarrollo de la citada ley orgánica (RLOPD).

a) Conforme a esa normativa, los preceptos que configuraban el régimen jurídico del tratamiento de datos, con la descripción de su concepto, de la delimitación del responsable del fichero o del tratamiento, así como de la definición de lo que había de entenderse por transferencia

internacional de datos, así como del cuadro de infracciones y sanciones a las conductas que incumplieran esta última modalidad de actuaciones en materia de protección de datos, podemos sintetizarla en los siguientes aspectos, que son relevantes para la resolución del caso:

(i) El concepto de tratamiento de datos quedaba definido en el art. 3 c) LOPD como "las "operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".

(ii) El art. 3 d) LOPD consideraba como responsable del fichero o tratamiento a la "persona física o jurídica, de naturaleza pública o privada u órgano administrativo que decid[ier]a sobre la finalidad, contenido y uso del tratamiento".

(iii) El art. 33. 1 LOPD prohibía la realización de transferencias temporales o definitivas de datos de carácter personal que hubieran "sido objeto de tratamiento o [hubieran] sido recogidos para someterlos a dicho tratamiento con destino a países que no [proporcionaran] un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se [obtuviera] autorización previa del Director de la Agencia de Protección de Datos, que sólo [podía] otorgarla si se [habían obtenido] garantías adecuadas". El régimen de prohibición de este precepto venía complementado por un cuadro de excepciones, recogido en el art. 34 LOPD, de tal manera que, lo dispuesto en el precepto anterior no sería de aplicación en una serie de supuestos que, en lo que concierne al caso presente, se reconducen a dos: "e) [c]uando el afectado [hubiera] dado su consentimiento inequívoco a la transferencia prevista. (…) k) [c]uando la transferencia [tuviera] 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, [hubiera] declarado que garantiza un nivel de protección adecuado".

(iv) La infracción impuesta a la entidad recurrente estaba tipificada, como muy grave, en el art. 44.4.d) LOPD, y consistía en la "transferencia internacional de datos de carácter personal con destino a países que no [proporcionaran] 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 [resultara] necesaria".

(v) En lo que ahora es de interés, el art. 37.1 LOPD disponía que la Agencia Española de Protección de Datos (AEPD) tenía atribuidas, entre otras, las siguientes funciones: "f) [r]equerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se

[ajustara] a sus disposiciones". Y g) [e]jercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley".

(vi) El art. 45 LOPD regulaba las sanciones imponibles. En sus tres primeros apartados establecía la horquilla en la que se podía mover la AEPD para imponer las sanciones, en función del tipo de infracción cometida (leve, grave o muy grave, respectivamente). El apartado 4 señalaba que la "cuantía de las sanciones se graduará atendiendo" a una serie de criterios, mientras que el apartado 5 indicaba que 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 una serie de supuestos que también se describen en la norma. En concreto, uno de esos supuestos es que "a) (…) 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" precisamente, "en el apartado 4" de ese precepto.

(vii) Finalmente, el art. 49 LOPD señalaba que: "[e]n los supuestos constitutivos de infracción grave o muy grave en que la persistencia en el tratamiento de los datos de carácter personal o su comunicación o transferencia internacional posterior pudiera suponer un grave menoscabo de los derechos fundamentales de los afectados y, en particular, de su derecho a la protección de datos de carácter personal, el órgano sancionador podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, el órgano sancionador podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas".

b) Por otro lado, la normativa sobre transferencia internacional de datos venía desarrollada en el Título VI (arts. 56 a 70) del RLOPD, en términos similares a lo dispuesto en la LOPD. En lo que ahora tiene interés, los arts. 69 y 70 hacían referencia a la "suspensión temporal de la transferencia" como una medida aplicable en el ejercicio de la potestad reconocida a la AEPD en el art. 37.1.f) LOPD.

c) El marco normativo expuesto no ha sido objeto de impugnación en el recurso de amparo. Desde la perspectiva del derecho a la legalidad sancionadora, la entidad recurrente no discute la cualidad de *lex certa* de la norma, sino la previsibilidad de su aplicación. No obstante, ambas vertientes aparecen íntimamente ligadas, ya que cuanto más concreta y precisa sea una norma, más previsible habrá de ser su aplicación.

En el caso que nos ocupa, la asociación recurrente considera que el ejercicio de la potestad sancionadora de la AEPD resultaba imprevisible en tres aspectos concretos: i) por la actuación previa

de la AEPD y la consiguiente quiebra del principio de confianza legítima; ii) porque la concreta sanción impuesta no era necesaria ni proporcionada a las circunstancias del caso; iii) porque se impuso una responsabilidad individual, en vez de una corresponsabilidad y la consiguiente responsabilidad solidaria entre las dos entidades titulares del fichero. La ulterior actuación judicial habría incurrido en la misma vulneración, al no haber reparado la lesión invocada.

4.2 La previsibilidad de la actuación administrativa y judicial.

La demanda alega que se ha vulnerado el derecho a la legalidad sancionadora reconocido en el art. 25.1 CE, ya que la actuación administrativa y judicial no resultaba previsible en función de las circunstancias del caso. Como se ha expuesto, esta falta de previsibilidad se concreta en tres aspectos que, a efectos de ordenación sistemática, serán analizados de forma individualizada, sin perjuicio de la evidente interrelación entre algunos de ellos.

A) La vulneración del principio de confianza legítima.

La entidad recurrente considera que la AEPD ha quebrantado el principio de confianza legítima, fundamentalmente por dos motivos: i) las comunicaciones previas de la AEPD no permitían deducir la aplicación del régimen administrativo sancionador; y ii) la medida de "bloqueo" adoptada por la asociación había sido aceptada por la AEPD y era sustancialmente idéntica a las que la AEPD podía adoptar en un supuesto como el que nos ocupa.

a) Sobre las comunicaciones previas de la AEPD

La demanda hace una reseña parcial de las comunicaciones remitidas por la AEPD entre los meses de octubre de 2015 y febrero de 2016, a raíz de la STJUE de 6 de octubre de 2015. Esta resolución invalidó la Decisión 2000/520/CE, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América. Esa Decisión había declarado que la normativa de los Estados Unidos de América ofrecía una garantía de nivel de protección adecuada a la normativa de la Unión Europea. Sin embargo, para el TJUE, la normativa estadounidense no garantiza el mismo grado de protección que la europea. "En particular, se debe considerar que una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto a la vida privada

garantizado en el artículo 7 de la Carta" (parágrafo 94); del mismo modo, "una normativa que no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconocer el art. 47 de la Carta" (parágrafo 95).

Tras esta decisión del TJUE, las transferencias internacionales de datos desde Europa hacia EEUU quedaban sin respaldo normativo expreso, ya que se dejaba sin efecto el supuesto de hecho previsto en el art. 34.k) LOPD. A partir de ese momento, y ante la lógica situación de incertidumbre generada, las autoridades europeas de protección de datos, de forma coordinada, procedieron a informar sobre la estrategia a seguir a los que figuraban como responsables de este tipo de ficheros o bases de datos. Ese es el contexto de las comunicaciones de la AEPD.

La recurrente alega que las comunicaciones no hacían referencia al ejercicio de acciones sancionadoras y que, por lo tanto, su aplicación resultaba imprevisible, quebrantando con ello el principio de confianza legítima. Sin embargo, una lectura detenida de esas comunicaciones pone de manifiesto que la interpretación ofrecida en la demanda debe considerarse como parcial y, por lo tanto, necesariamente sesgada, ya que no tiene en cuenta ni el presupuesto de hecho ni las condiciones establecidas para alcanzar esa eventual conclusión.

En efecto, la comunicación de 19 de octubre de 2015, publicada en la página web de la AEPD, estaba dirigida a los que figuraban como responsables de ficheros que realizaban transferencias internacionales de datos. Su tenor literal es el siguiente:

> "Con fecha 6 de octubre del presente año, el Tribunal de Justicia de la Unión Europea (TJUE) ha declarado inválida la Decisión de la Comisión 2000/520/CE, que establece el nivel adecuado de protección de las garantías para las transferencias internacionales de datos a EEUU ofrecidas por el acuerdo de Puerto Seguro, por lo que las transferencias no pueden ampararse en esa base legal.
>
> Por ello, en el caso de que se tenga previsto continuar realizando transferencias internacionales de datos a Estados Unidos, país que no proporciona un nivel de protección equivalente al que presta la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), deberán encontrar legitimación en otros instrumentos como las Cláusulas Contractuales Tipo adoptadas por las Decisiones de la Comisión Europea 2001/497/CE, 2004/915/CE y 2010/87/UE y, en su caso, en las excepciones previstas en al artículo 34 de la LOPD que pudieran ser aplicables.
>
> En consecuencia, en el ejercicio de las competencias de esta Agencia, se le requiere para que, a la mayor brevedad, y en todo caso antes del 29 de enero de 2016, informe al Registro General de Protección de Datos sobre la continuidad de las transferencias y, en su caso, sobre su adecuación a la normativa de protección de datos.
>
> De no recibirse contestación a este requerimiento ni, en su caso, la notificación de modificación de las transferencias internacionales contenidas en el/los fichero/s en el plazo indicado, es preciso recordarle que, conforme a lo dispuesto en el Reglamento de

> la LOPD, la Agencia podrá iniciar el procedimiento para acordar, en su caso, la suspensión temporal de las transferencias".

Esta comunicación no estaba dirigida a cualquier responsable de fichero, sino a los que ya figuraban en el Registro General de Protección de Datos como responsables de ficheros que realizaban transferencias internacionales de datos. No se puede interpretar de otra forma la expresión "en el caso de que se tenga previsto continuar realizando transferencias internacionales de datos a Estados Unidos", o el requerimiento para que se informe al registro "sobre la continuidad de las transferencias". No se puede continuar lo que no se ha hecho con anterioridad, ni se puede requerir a un desconocido que no figura en el registro como responsable de un fichero de este tipo.

La segunda comunicación de la AEPD, emitida en diciembre de 2015, a la que se hace expresa referencia en la demanda, exponía literalmente lo siguiente:

> "Con el objetivo de informar de forma directa a los responsables que realizan transferencias internacionales de datos a EEUU y ante la inquietud generada por la noticia titulada 'Ultimátum de la AEPD a empresas españolas: prohibido usar Dropbox o Google Apps', la Agencia Española de Protección de Datos (AEPD) quiere puntualizar lo siguiente:
> •Desde la AEPD no se ha dado ningún ultimátum a las empresas españolas. El Tribunal de Justicia de la Unión Europea (TJUE) hizo pública una sentencia el pasado 6 de octubre que implica que las transferencias desde la Unión Europea a EEUU no pueden seguir realizándose bajo la base legal de la Decisión de Puerto Seguro (Safe Harbour).
> •La Agencia ya anunció de forma pública el pasado 29 de octubre que, en el marco de una actuación conjunta de las Autoridades europeas de protección de datos, iba a establecer contacto con todas las empresas de las que tuviera constancia que utilizaban Puerto Seguro para la realización de transferencias internacionales. Ese mismo día, la AEPD comenzó a enviar una comunicación a esas empresas con el objetivo de facilitar la comunicación directa con los responsables, poniendo a su servicio canales de información adecuados.
> •La Agencia en ningún caso ha requerido a los responsables para que dejen de utilizar determinados servicios de almacenamiento en la nube. Las acciones de la Agencia no están orientadas a la prohibición de utilizar herramientas concretas sino a informar a los responsables para que requieran a su proveedor de servicios, si es necesario, que les ofrezca una respuesta adaptada a la sentencia del TJUE.
> •La sentencia del TJUE está orientada a responsables, no a los ciudadanos que hacen uso doméstico de los datos personales que pudieran almacenar en la nube.
> •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 las transferencias.

> •La Agencia, junto con las Autoridades europeas de protección de datos, apuesta por encontrar soluciones sostenibles para aplicar la sentencia del TJUE e insiste en el llamamiento realizado a las Instituciones de la UE, los Estados miembros y las empresas para encontrar un camino que permita el cumplimiento de la sentencia del Tribunal.
> En cualquier caso, los responsables que tengan dudas pueden plantear sus preguntas a través de la Sede electrónica de la AEPD".

De los términos de esta segunda comunicación se deduce su finalidad informativa y aclaratoria, pretendiendo salir al paso de determinadas informaciones que distorsionaban el contenido y la finalidad de la primera comunicación que, en todo caso, se mantenía en sus elementos esenciales. Así, parece claro que, a partir de la STJUE, la AEPD había iniciado una relación con aquellas empresas que figuraban como responsables de ficheros que realizaban transferencias internacionales de datos, a las que se concedía un periodo transitorio, fijado a nivel europeo hasta finales de enero de 2016, para que comunicaran la eventual continuación de las transferencias e informaran, en su caso, sobre las gestiones realizadas para adaptar su relación con las empresas norteamericanas a la nueva situación derivada de la STJUE. Es cierto que esta segunda comunicación señalaba expresamente que la AEPD no había anunciado en ningún momento su intención de iniciar "procedimientos sancionadores por defecto contra las empresas". Pero, del contexto se infiere que lo que se descartaba era una incoación de oficio de forma masiva o generalizada que, en cualquier caso, solo podría afectar a los responsables que se encontraran en la situación o presupuesto de hecho de estas comunicaciones, es decir, a los que hubieran declarado previamente la transferencia internacional de datos. Lo que no se deduce de estas comunicaciones es que la AEPD renunciara a exigir las responsabilidades procedentes a quienes, sin haber comunicado la realización de las transferencias, ni solicitado la correspondiente autorización a la AEPD, continuaran realizando la conducta prohibida por la norma, es decir, la realización de transferencias internacionales de datos a EEUU, que no garantizaba el estándar europeo de protección de los datos personales, según la sentencia del TJUE, tantas veces repetida.

b) Sobre la medida de "bloqueo" adoptada por la entidad recurrente.

Un segundo motivo esgrimido en la demanda para considerar aplicable el principio de confianza legítima es que la medida de "bloqueo" acordada por OC era equivalente a las medidas de "suspensión temporal de las transferencias" y a la "inmovilización de ficheros", que eran las únicas que la AEPD anunció que podía y debía adoptar, y que fueron validadas por la actuación de los inspectores de la AEPD, por lo que, a juicio de la recurrente, la aplicación del régimen sancionador le resultaba igualmente imprevisible.

No corresponde a este Tribunal realizar una interpretación de la legalidad ordinaria, sobre todo en un ámbito en el que confluyen, no solo conceptos jurídicos sino también técnicos. Sin embargo, desde el plano jurídico-constitucional, se puede constatar que la transferencia internacional de datos se realiza con finalidad de tratamiento (art. 33.1 LOPD), y dentro de la definición de tratamiento se incluye la mera "conservación" así como "las cesiones de datos que resulten de (…) transferencias" [art. 3.c) LOPD]. De esta forma, el "bloqueo" no podía impedir el tratamiento de los datos ya transferidos, en el sentido de que los datos estaban siendo, al menos, "conservados" en los servidores ubicados en EEUU, con el consiguiente riesgo para los titulares del derecho fundamental a la protección de datos personales derivado del art. 18.4 CE, que no era la entidad OC sino las personas que se habían sumado a la iniciativa "Ahora es la hora", y que carecían de los mecanismos eficaces, reconocidos en la legislación europea, frente a las posibles injerencias llevadas a cabo conforme a la normativa de EEUU. Es decir, aun admitiendo como hipótesis que el "bloqueo" impidiera nuevas transferencias de datos, lo cierto es que no podía oponerse como obstáculo al tratamiento indebido de los datos ya transferidos, que estaban siendo conservados en los servidores de EEUU, sin las garantías debidas. En realidad, no puede deslindarse completamente la transferencia y el tratamiento de los datos, porque la transferencia se hace con finalidad de tratamiento y, en todo caso, la mera cesión de los datos a través de una transferencia ya supone un tratamiento [art. 3.c), *in fine* LOPD], cuyos efectos se mantienen en el tiempo con su mera conservación.

Por otro lado, la actuación de los inspectores de la AEPD, al requerir el desbloqueo de los ficheros para facilitar la información solicitada en el marco de las actuaciones de investigación, y la vuelta a la situación de bloqueo una vez obtenidos los datos, no implica una validación expresa de esa medida, ni tampoco una declaración sobre su equivalencia con el contenido, significación o efectos de una suspensión temporal de las transferencias o una inmovilización de los ficheros.

En todo caso, el análisis conjunto de los arts. 37.1.f) y 49 LOPD y de los arts. 69 y 70 RLOPD permite concluir que, aunque con terminología parcialmente equivalente, las medidas de "cesación" o "suspensión" de las transferencias y de "inmovilización" o "cancelación" de los ficheros presentan una inequívoca naturaleza de medios de restauración de la legalidad, pero no impiden el ejercicio de la potestad sancionadora correspondiente. Se trata de medidas que se mueven en planos distintos, ya que la suspensión e inmovilización pretenden impedir la continuación de una conducta ilegal, mientras que la potestad sancionadora supone una penalización por la conducta ya realizada, prevista expresamente como infracción en el ordenamiento jurídico. En ambos casos, se ejercen potestades públicas, pero diferenciadas en dos apartados de la norma [art. 37.1, letras f) y g)

LOPD] y perfectamente compatibles entre sí, como expresamente se declara en el propio art. 49 LOPD.

Desde la perspectiva del juicio externo de razonabilidad que nos corresponde, la interpretación y aplicación del régimen sancionador resultaba previsible, conforme al tenor literal de la norma y a las pautas metodológicas y axiológicas comúnmente admitidas en Derecho.

c) Desestimación de la queja.

Expuestos los argumentos que, según la entidad recurrente, justificarían la aplicación del principio de confianza legítima, este Tribunal debe rechazar esta pretensión. Como ya se indicó, este principio permite a los ciudadanos realizar una conducta legítima bajo el amparo de una previa y consolidada actuación de la administración pública, con apariencia de licitud, y le protege frente a cambios relevantes no justificados de los criterios de actuación administrativa que le hayan generado un perjuicio para sus legítimos derechos e intereses que no tenga la obligación de soportar. En el presente caso, no concurren algunos de los presupuestos necesarios para la aplicación de este principio, por los siguientes motivos:

i) La actuación de la AEPD no implicó cambio alguno de criterio, porque sus comunicaciones no permitían deducir la inaplicación del régimen administrativo sancionador. Por lo tanto, el ejercicio de la potestad sancionadora no produjo quiebra alguna de la confianza depositada en una previa y consolidada actuación administrativa.

ii) La actuación de OC no puede considerarse como una conducta legítima. Esta entidad no comunicó a la AEPD que estaba realizando transferencias internacionales de datos a los EEUU; y tampoco comunicó su intención de continuar realizando esas transferencias, ni solicitó autorización alguna para hacerlo. En estas condiciones, no puede acogerse al principio de confianza legítima, que solo protege a quien realiza conductas no prohibidas expresamente por la norma. Tampoco se puede invocar este principio sobre la base de una determinada interpretación de la legalidad realizada por el propio interesado, como ocurre en este caso con la posible equivalencia entre las medidas de "bloqueo", "suspensión" o "inmovilización", cuando un somero análisis del régimen vigente permite diferenciar sus fundamentos, contenido y finalidad.

iii) La potestad sancionadora es una actividad reglada, sobre todo en un caso como éste, en que la incoación del procedimiento se produjo a instancia de parte. Se trataba de una conducta exigible para la AEPD, sobre la que no opera el principio de confianza legítima.

iv) La aplicación del régimen sancionador no puede considerarse como un perjuicio no soportable. Quien incumple un régimen legal de prohibiciones, que aparece tipificado como

infracción y castigado con una sanción (en este caso, de multa), está obligado a soportar las consecuencias de sus actos.

B) La necesidad y proporcionalidad de la sanción impuesta.

Aunque se trata de alegaciones que estaban íntimamente ligadas al motivo de amparo fundado en la eventual vulneración del derecho de asociación (art. 22 CE), que ha sido inadmitido a trámite, encuentran también su enlace con el principio de legalidad sancionadora (art. 25.1 CE), única perspectiva que será objeto de enjuiciamiento.

La demanda no discute la condición de *lex certa* de la normativa sancionadora, en el sentido de que no cuestiona la constitucionalidad de la tipicidad de la conducta ni la proporcionalidad, en abstracto, de las sanciones establecidas. Lo que se impugna es el grado de previsibilidad de una actuación administrativa y judicial en la concreta aplicación del régimen administrativo sancionador en materia de protección de datos, susceptible de generar una vulneración del derecho a la legalidad sancionadora (art. 25.1 CE). La tacha de imprevisibilidad que ahora se examina en este apartado se centra en dos aspectos concretos: por un lado, el régimen sancionador era innecesario porque la medida de "bloqueo" adoptada por la propia entidad recurrente implicaba una adecuación a la norma y, por lo tanto, la atipicidad de la conducta; y por otro, la concreta sanción impuesta era desproporcionada, en función de las circunstancias del caso.

En realidad, la demanda reproduce en este punto las razones que ha venido alegando en la vía administrativa y judicial previa, de forma que, revestidas ahora de una supuesta falta de previsibilidad, lo que hace es mostrar su discrepancia con la actuación de la AEPD y de la AN, en su labor de interpretación y aplicación concreta de un determinado régimen sancionador.

Este Tribunal no tiene entre sus funciones la de revisar una resolución administrativa o judicial por motivos de legalidad ordinaria, es decir, no nos corresponde realizar una interpretación o aplicación directa de una norma, función asignada a los integrantes del Poder Judicial (*ex* art. 117 CE). Por ello, desde la perspectiva del control de constitucionalidad que nos corresponde, nuestro objeto de enjuiciamiento se debe centrar en determinar si, a la vista del régimen vigente ya expuesto, la actuación administrativa y judicial resultaba razonablemente previsible y se ajustó a su tenor literal y a los parámetros metodológicos y axiológicos de general conocimiento.

Un somero examen de la regulación vigente permite concluir que el régimen sancionador en materia de protección de datos ofrecía base suficiente para considerar como previsible su aplicación en este caso concreto. El juego conjunto de los arts. 33.1 y 44.4.d) LOPD identificaba de forma clara y precisa la conducta sancionable. En lo que ahora interesa, una transferencia

internacional de datos solo era lícita en dos supuestos: si el país de destino proporcionaba garantías de protección equiparables a las europeas o si se obtenía autorización de la AEPD. En este caso, EEUU no ofrecían garantías de adecuación, según la STJUE de 6 de octubre de 2015; y la entidad recurrente no solicitó la autorización correspondiente a la AEPD, manteniendo los datos ya transferidos en poder de los servidores ubicados en EEUU, en condiciones potencialmente perjudiciales para los titulares de esos datos, al menos entre los meses de febrero y septiembre de 2016. Nos remitimos en este punto a lo expuesto en el FJ 4.2.A).b).

Ante la constatación de una infracción del régimen sancionador, la actuación administrativa y judicial devenía necesaria y respondía a una finalidad legítima, como era la protección de los datos personales de los terceros.

Por otro lado, la sanción se ajustó al rango punitivo legalmente permitido, sin desproporción alguna. Como se expone con todo detalle en las resoluciones impugnadas (señaladamente, en sus respectivos fundamentos de derecho séptimos, a los que nos remitimos), y se recoge en el antecedente 2.a) de esta sentencia, se aplicó el rango penológico asignado a las infracciones graves, a pesar de tratarse de una infracción muy grave [art. 44.4.d) LOPD], por aplicación de lo dispuesto en el art. 45.5.a), en relación con el art. 45.4, apartados d) y e), LOPD. De esta forma, una vez tipificada la infracción y establecido el marco general penológico, se individualizó la cuantía en función de los criterios fijados en el art. 45.4 LOPD, más en concreto, en sus apartados a), b), f) y j) LOPD y las circunstancias concurrentes en el caso, apreciadas por la AEPD.

Conforme a este esquema metodológico, la operación de subsunción de la infracción y de determinación de la cuantía de la sanción supera el juicio de razonabilidad que corresponde a esta jurisdicción constitucional, al basarse en el texto de la norma y guiarse por parámetros aplicativos comúnmente aceptados en Derecho.

C) Principio de responsabilidad y tutela judicial efectiva.

La tercera tacha de imprevisibilidad en la actuación administrativa y judicial se basa en la indebida aplicación del principio de responsabilidad individual que la parte recurrente atribuye a las resoluciones impugnadas. A su juicio, estas resoluciones le han impuesto una sanción como autora de una infracción, cuando de las circunstancias del caso se deducía una coautoría y, en consecuencia, una responsabilidad solidaria entre las dos entidades sociales que lideraron la iniciativa “Ahora es la hora”, OC y ANC. Ambas eran responsables del tratamiento de los datos y, por lo tanto, realizaron las transferencias internacionales, por lo que ambas debían ser sancionadas como coautoras de una

única infracción. Esta pretensión es la que aparece más claramente ligada a la eventual vulneración del derecho a la tutela judicial efectiva (art. 24.1 CE), en su vertiente de derecho a obtener una resolución motivada y fundada en Derecho, por lo que procederá su análisis conjunto.

En efecto, la entidad recurrente alega que las resoluciones impugnadas, muy particularmente, la sentencia de la AN, vulneran su derecho a la tutela judicial efectiva, porque no han dado una respuesta motivada y fundada en Derecho a la concreta pretensión de que se declarara una corresponsabilidad de la infracción y la consiguiente responsabilidad solidaria de las entidades responsables del fichero. A juicio de la recurrente, se le ha impuesto una sanción como autora de una infracción cuando, de las circunstancias del caso, se deducía una coautoría y, en consecuencia, una responsabilidad solidaria entre las dos entidades sociales que lideraron la iniciativa "ahora es la hora" (Omnium Cultural y Asamblea Nacional Catalana). Sostiene la demanda que ambas eras responsables del tratamiento de los datos y, por lo tanto, realizaron las transferencias internacionales, por lo que ambas deberían, en su caso, haber sido sancionadas como coautoras de una única infracción.

Como ya se expuso, el canon de enjuiciamiento constitucional del derecho a la tutela judicial efectiva implica un juicio externo o de razonabilidad, que no puede sustituir a los órganos administrativos y judiciales competentes para la interpretación y aplicación de la normativa sancionadora correspondiente. Ese juicio consiste en una doble verificación: por un lado, que se haya ofrecido una respuesta motivada, es decir, que las resoluciones hayan expuesto los elementos que se han tenido en cuenta para resolver la pretensión planteada; y por otro, que la respuesta esté fundada en Derecho, es decir, que esté basada en una exégesis de la norma que no sea irracional, arbitraria o incursa en error patente.

Las resoluciones de la AEPD denegaron esta concreta pretensión de la recurrente por dos motivos. En primer lugar, se descartó la referencia jurisprudencial aportada por la entidad OC, ya que analizaba un supuesto urbanístico que se consideró sustancialmente diferente al que nos ocupa. En segundo lugar, porque las dos entidades denunciadas (OC y ANC) figuraban como responsables del fichero y, por lo tanto, susceptibles de generar responsabilidad por el incumplimiento de los preceptos de la LOPD. Para la autoridad administrativa, "la propuesta de resolución determina la comisión de una única infracción -tal como aducen las denunciadas-, y la imposición de sanción a cada entidad deriva precisamente de su condición de responsable del fichero y de las obligaciones que el ordenamiento jurídico les atribuye derivadas de dicha condición. El principio de personalidad y de responsabilidad solidaria que establece la LRJPAC, determina que para el caso de que se haya incumplido una obligación que corresponda a varias personas conjuntamente (art. 130.3) todos los infractores pueden ser sancionados por una única infracción -siendo esa posibilidad la que puede

revestirse de ‘solidaria’-. Por lo que debe confirmarse la propuesta de resolución en el sentido de determinar la imposición de una sanción a cada entidad por la infracción del art. 33 de la LOPD, en su calidad de responsables del fichero”.

Impugnada esta resolución, la sentencia de la Audiencia Nacional validó este criterio en su fundamento de derecho sexto. En lo que ahora interesa, la resolución judicial se remite a la argumentación expuesta en la sentencia de 2 de diciembre de 2018, dictada por la misma sala y sección, en el recurso núm. 453/2016, interpuesto por las mismas entidades frente a otras resoluciones sancionadoras de la AEPD impuestas en relación con el mismo fichero “Ara es l’hora”. Tras hacer una reseña literal de esa argumentación, considera que es aplicable el mismo criterio, ya que “ambas entidades no sólo han decidido conjuntamente, sino que cada una de ellas ha realizado individualmente las acciones constitutivas de la infracción, por lo que la responsabilidad es individual y a título personal. Así resulta que ANC y OC realizaron cada una en el Registro General de Protección de Datos, sendas inscripciones relativas al fichero Ara és l´Hora, que es el objeto de la transferencia internacional de datos y en el anexo de privacidad del contrato de servicio de alojamiento con la empresa BSD, figuran ambas entidades como firmantes y en calidad de Data Controller, es decir, responsables del tratamiento”.

El análisis de ambas resoluciones permite afirmar que ofrecieron una respuesta motivada y fundada en Derecho a la cuestión planteada.

La reciente STC 31/2022, de 7 de marzo, ha declarado:

> “Para dar respuesta a esta queja debe tenerse en cuenta que la sentencia impugnada, razona, en su fundamento jurídico noveno, que ‘el art. 2 d) de la Directiva 95/46/CE, al definir la figura de responsable del fichero o tratamiento, alude a que la determinación de los fines y los medios del tratamiento de datos personales se puede hacer «solo o conjuntamente con otros» […] Es dicho poder de decisión sobre la finalidad y uso del tratamiento donde radica la esencia de la figura del responsable de fichero o tratamiento, responsable que puede venir constituido, a tenor de la normativa expuesta, bien por una persona o bien por varias personas. A este respecto resulta esclarecedor el Dictamen 1/2010 del GT29, que indica que «[…] la definición de tratamiento contenida en el art 2.b) de la Directiva no excluye la posibilidad de que distintos agentes estén implicados en diferentes operaciones o conjuntos de operaciones en materia de datos personales. Estas operaciones pueden producirse simultáneamente o en distintas fases». Y se concluye que «la participación de las partes en la determinación de los fines y los medios del tratamiento en el contexto del control conjunto puede revestir distintas formas y el reparto no tiene que ser necesariamente a partes iguales ... Los distintos grados de control pueden dar lugar a distintos grados de responsabilidad, y desde luego no cabe presumir que haya una responsabilidad solidaria en todos los casos’.
>
> Toda la argumentación de la sentencia gira en torno a la figura jurídica del responsable del tratamiento que determina los fines y los medios del tratamiento conjuntamente con otros, categoría normativa que el vigente Reglamento (UE) 2016/1979 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD), 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 también denomina corresponsable del tratamiento (art. 26). Se trata de un concepto autónomo y específico de la legislación de protección de datos personales, que ha sido interpretado en sus líneas principales por el Tribunal de Justicia de la Unión Europea, sobre todo en las sentencias de 5 de junio de 2018, asunto Wirtschaftsakademie Schleswig-Holstein, C-210/16; de 10 de julio de 2018, asunto Jehovan todistajat, C-25/17; y de 29 de julio de 2019, asunto Fashion ID, C-40/17.

No es impertinente recordar al respecto que, aunque el Derecho de la Unión Europea no pueda considerarse canon de constitucionalidad, sí cabe otorgarle un valor hermenéutico, con fundamento en el art. 10.2 CE, incluyendo tanto los tratados constitutivos y sus sucesivas reformas, como el Derecho derivado (entre otras, SSTC 292/2000, de 30 de noviembre, FJ 3; 136/2011, de 13 de septiembre, FJ 2; 13/2017, de 30 de enero, FJ 6, y 76/2019, de 22 de mayo, FJ 3); así como la interpretación que de tales normas realiza el Tribunal de Justicia de la Unión Europea (SSTC 61/2013, de 14 de marzo, FJ 5; 66/2015, de 13 de abril, FJ 3; 140/2016, de 21 de julio, FJ 5; 3/2018, de 22 de enero, FJ 4; 32/2019, de 28 de febrero, FJ 6; y 156/2021, de 26 de septiembre, FJ 2, por todas). En particular en la materia que nos ocupa, toda vez que el desarrollo legislativo del derecho a la protección de datos personales 'se halla en la actualidad parcialmente determinado por el Derecho de la Unión Europea' (STC 76/2019, de 22 de mayo, FJ 3).

Pues bien, la primera de las citadas sentencias del Tribunal de Justicia de la Unión Europea sienta (§§ 26 a 29) los principios informadores de este concepto legal de corresponsable del tratamiento, que se reiteran en las demás (sentencias de 10 de julio de 2018, asunto Jehovan todistajat, § 65; y de 29 de julio de 2019, asunto Fashion ID, § 67). Se afirma en los referidos apartados de la sentencia de 5 de junio de 2018, asunto Wirtschaftsakademie Schleswig-Holstein que la 'Directiva 95/46 tiene por objeto garantizar un nivel elevado de protección de las libertades y los derechos fundamentales de las personas físicas, sobre todo de su vida privada, en relación con el tratamiento de datos personales (sentencia de 11 de diciembre de 2014, Ryneš, C-212/13, § 27). Conforme a este objetivo, el art 2, letra d), de dicha Directiva define de manera amplia el concepto de «responsable del tratamiento», refiriéndose a la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales. En efecto, tal como ya ha declarado el Tribunal de Justicia, el objetivo de esta disposición consiste en garantizar, mediante una definición amplia del concepto de «responsable», una protección eficaz y completa de los interesados (sentencia de 13 de mayo de 2014, Google Spain y Google, C-131/12, § 34). Además, puesto que, tal como prevé expresamente el art 2, letra d), de la Directiva 95/46, el concepto de «responsable del tratamiento» se refiere al organismo que «solo o conjuntamente con otros» determine los fines y los medios del tratamiento de datos personales, dicho concepto no se remite necesariamente a una única entidad, sino que puede aludir a varios actores que participen en ese tratamiento, cada uno de los cuales estará por tanto sujeto a las disposiciones aplicables en materia de protección de datos'.

En la sentencia de 29 de julio de 2019, asunto Fashion ID, se abordaba una situación en que una empresa de comercio electrónico dedicada a la venta de prendas de vestir (Fashion ID) insertó en su sitio de Internet el módulo social 'me gusta' de Facebook. Simplemente con accionar esa función se transmitían ciertos datos personales del usuario a Facebook, que a su vez decide de un modo exclusivo cuáles eran los fines de tratamiento de esos datos. El Tribunal de Justicia de la Unión Europea resuelve en este caso que 'una persona física o jurídica únicamente puede ser responsable, en el sentido del art 2, letra d), de la Directiva 95/46, conjuntamente con otros, de las operaciones de tratamiento de datos personales cuyos fines y medios determine conjuntamente. En cambio, y sin perjuicio de

una eventual responsabilidad civil prevista en el Derecho nacional al respecto, dicha persona física o jurídica no puede ser considerada responsable, en el sentido de dicha disposición, de las operaciones anteriores o posteriores de la cadena de tratamiento respecto de las que no determine los fines ni los medios' (§ 74). Queda claro, por tanto, que cuando se distinguen varias fases del tratamiento o varios conjuntos de operaciones de tratamiento no se está haciendo referencia a las distintas actividades de ejecución material del tratamiento sino a la existencia de fases del tratamiento con diferente diseño (donde qué datos personales se tratarán, con qué fines y en virtud de qué medios difiere). La empresa en cuestión era corresponsable del tratamiento en cuanto a la transmisión de los datos personales derivada del uso del módulo social de Facebook, pero ninguna capacidad de influencia tenía respecto del diseño del tratamiento que Facebook realizaba una vez recibidos los datos personales de quien accionaba la función 'me gusta'. No tiene sentido, en conclusión, que la condición de corresponsable del tratamiento de la empresa se proyecte sobre esa segunda fase del tratamiento, en cuyo diseño no participa.

Este planteamiento, conforme al cual las distintas fases o conjuntos de operaciones de tratamiento se refieren a su diseño y no a su ejecución material, ya había quedado apuntada en la citada sentencia de 10 de julio de 2018, asunto Jehovan todistajat. En ella se examina un caso en que los miembros de la comunidad de los Testigos de Jehová realizaban, en el ámbito de su actividad de predicación puerta a puerta, anotaciones sobre las visitas efectuadas a personas que ni ellos mismos ni la comunidad conocían previamente. El Tribunal de Justicia de la Unión Europea entendió que la comunidad de los Testigos de Jehová, a pesar de que no participara en la ejecución del tratamiento de datos, era corresponsable, en la medida en que tenía capacidad de influir en cómo se organizaba la actividad de predicación y, por tanto, en qué datos recogían sus miembros y con qué finalidad. Dicha sentencia, en su § 69, razonó en concreto que 'la responsabilidad conjunta de varios agentes respecto a un mismo tratamiento en virtud de dicho precepto [art 2, letra d), de la Directiva 95/46] no supone que cada uno de ellos tenga acceso a los datos personales en cuestión (véase, en este sentido, la sentencia de 5 de junio de 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, § 38)'.

De todo lo anterior se desprende que los 'diferentes conjuntos de operaciones' o 'distintos grados de responsabilidad' a que alude el 'Dictamen 1/2010 del GT29' que cita la sentencia impugnada (el GT29 es el grupo de trabajo independiente, creado al amparo del art. 29 de la Directiva 95/46/CE, que se ha ocupado de cuestiones relacionadas con la protección de la privacidad y los datos personales hasta la entrada en aplicación del RGPD, el 25 de mayo de 2018), no se determinan en función de la mayor o menor participación en las actividades de ejecución del tratamiento de datos personales, sino de la mayor o menor participación en el diseño del mismo. Por este motivo, la sentencia impugnada no incurre en ningún defecto de motivación lesivo del derecho a la tutela judicial efectiva por no precisar qué concretas actividades del tratamiento de datos que nos ocupa ejecutó la entidad" recurrente. "Ello es irrelevante para determinar si esta entidad es responsable del tratamiento y en qué medida lo es. Lo decisivo es, como señala la sentencia impugnada, el 'poder de decisión sobre la finalidad y uso del tratamiento' y resulta acreditado, como se razona en la sentencia, que el poder de decisión" de la entidad OC se proyectó sobre todo el tratamiento de datos personales asociado a la iniciativa "Ahora es la hora".

El otro elemento interpretativo que resulta relevante para resolver la presente queja es que la jurisprudencia del Tribunal de Justicia de la Unión Europea antes reseñada ha interpretado que "el sentido de la figura del corresponsable es que en los tratamientos de datos complejos la presencia de varios responsables no haga resentir el nivel elevado de protección que garantiza el régimen previsto en la Directiva 95/46/CE, de modo que cada uno de los actores que participen en ese tratamiento estará por tanto sujeto a las

> disposiciones aplicables en materia de protección de datos. Este propósito de garantía de un alto nivel de protección es el que resalta la argumentación de la sentencia impugnada que ha sido transcrita, en particular al citar el 'Dictamen 1/2010 del GT29' en la parte que afirma que '[…] la definición de tratamiento contenida en el art 2.b) de la Directiva no excluye la posibilidad de que distintos agentes estén implicados en diferentes operaciones o conjuntos de operaciones en materia de datos personales'.
>
> Con este razonamiento la sentencia impugnada viene a destacar que las entidades ANC y OC, al determinar conjuntamente los fines y los medios del tratamiento de datos personales […], están cada una de ellas sujetas a las disposiciones aplicables en materia de protección de datos, criterio jurisprudencial sobre la funcionalidad del concepto de corresponsable del tratamiento que ha venido a ratificar el vigente art. 26.3 RGPD ('Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables')" (FJ 5).

En conclusión, como también dijimos en nuestra STC 31/2022, "la sentencia impugnada, al resolver que los varios actores que participan en el diseño de un tratamiento de datos personales están sujetos cada uno de ellos a las disposiciones aplicables en materia de protección de datos, está necesariamente rechazando todos los distintos argumentos que la entidad recurrente hizo valer para instar que se declarase una responsabilidad solidaria de ambas entidades. No se advierte, por tanto, que la sentencia impugnada haya incurrido en deficiencias de motivación lesivas del derecho a la tutela judicial efectiva, por lo que procede desestimar también esta concreta queja de la recurrente" (FJ 5).

FALLO

En atención a todo lo expuesto, el Tribunal Constitucional, por la autoridad que le confiere la Constitución de la Nación española, ha decidido desestimar el recurso de amparo interpuesto por la Asociación Omnium Cultural contra las resoluciones de la Agencia Española de Protección de Datos de 22 de febrero y 4 de mayo de 2017, recaídas en el procedimiento sancionador PS/00391/2016; así como contra la sentencia de 29 de abril de 2019 de la Sección Primera de la Sala de lo Contencioso-administrativo de la Audiencia Nacional, dictada en el recurso núm. 397-2017 y contra el auto de 19 de junio de 2020 de la Sección Primera de la Sala de lo Contencioso-administrativo del Tribunal Supremo, que inadmitió a trámite el recurso de casación formalizado contra aquella sentencia.

Publíquese esta Sentencia en el "Boletín Oficial del Estado".

Dada en Madrid, a veintiuno de marzo de dos mil veintidós.