LA RESPONSABILIDAD CIVIL Y SU FUNCIÓN DE TUTELA DEL DERECHO A LA PROTECCIÓN DE LOS DATOS PERSONALES: UNA VISIÓN DESDE EL DERECHO DE LA UNIÓN EUROPEA

CIVIL LIABILITY AND ITS FUNCTION OF GUARDING THE RIGHT TO THE PROTECTION OF PERSONAL DATA: A VISION FROM THE LAW OF THE EUROPEAN UNION

JOSÉ MANUEL BUSTO LAGO *

RESUMO[1]

Nesse trabalho, o autor investiga a função e a responsabilidade civil adjacente à tutela da Proteção de Dados Pessoais a partir do Direito Comunitário Europeu, debatendo questões de ordem material e processual no marco normativo vigente. Seu desenvolvimento tem em consideração, também, a Lei Geral de Proteção de Dados brasileira. Trata-se de estudo abrangente, repercutindo debates em torno de temas amplos como os ligados à legitimidade, aos serviços digitais e aos processos e procedimentos de indenização e ressarcimento quando da prática de atos de violação.

Palavras-chave: Proteção de Dados Pessoais. Responsabilidade Civil. Direito da União Europeia.

ABSTRACT[2]

In this work, the author investigates the role and civil liability adjacent to the protection of Personal Data Protection based on European Community Law, debating material and procedural issues within the current regulatory framework. Its development also considers the Brazilian General Data Protection Law. It is a comprehensive study, echoing debates around broad themes such as those related to legitimacy, digital services and indemnification and reimbursement processes and procedures when acts of violation are committed.

Keywords: Protection of Personal Data. Civil responsability. European Union Law.

* Professor Catedrático de Direito Civil da Universidade da Coruña (UDC).
Doutor em Direito Civil pela UDC
jose.busto.lago@udc.es

Recebido em 10-1-2022 | Aprovado em 10-1-2022[3]

[1] Elaborado pelos Editores.

[2] Elaborado pelos Editores.

[3] Artigo convidado. **Nota do autor:** este estudio es una reelaboración de la ponencia titulada «Protección de datos personales y responsabilidad civil», impartida en el *V Congreso Internacional sobre el Derecho de Daños* celebrado en Madrid los días 12 y 13 de marzo de 2020 y publicada en *Derecho de Daños 2020,* Ed. Lefebvre, Madrid, 2020, pgs. 443 a 512; incluyendo algunas referencias comparadas con la vigente regulación de la materia

SUMÁRIO

1. EL MARCO NORMATIVO DE LA RESPONSABILIDAD CIVIL EXTRACONTRACTUAL COMO MECANISMO DE PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL; 2. LA RESPONSABILIDAD CIVIL DEL RESPONSABLE Y DEL ENCARGADO DE TRATAMIENTO Y EL DERECHO A LA INDEMNIZACIÓN DEL TITULAR PERJUDICADO EN EL RGPD; 3. LEGITIMACIÓN ACTIVA: EL TITULAR DE LOS DATOS PERSONALES QUE HA EXPERIMENTADO EL DAÑO O PERJUICIO: 3.1. Acciones indemnizatorias individuales. 3.2. La legitimación para la tutela post mortem». 3.3. Acciones indemnizatorias colectivas; 4. LEGITIMACIÓN PASIVA: 4.1. El responsable del tratamiento. 4.2. El encargado del tratamiento. 4.3. Las relaciones jurídicas entre el responsable y el encargado de tratamiento y su incidencia en la imputación de la responsabilidad civil. 4.4. El delegado de protección de datos. 4.5. El representante en la UE del responsable o del encargado de tratamiento. 4.6. Responsables y encargados de tratamiento que sean autoridades o Administraciones Públicas; 5. SUPUESTOS DE PLURALIDAD DE RESPONSABLES; 6. PRESUPUESTO OBJETIVO: INFRACCIÓN DE LAS NORMAS QUE REGULAN EL TRATAMIENTO DE DATOS PERSONALES (LA CONDUCTA ANTIJURÍDICA); 7. LA NATURALEZA JURÍDICA DE LA RESPONSABILIDAD CIVIL: LOS SUPUESTOS DE EXENCIÓN DE RESPONSABILIDAD CIVIL DE LOS RESPONSABLES Y DE LOS ENCARGADOS DE TRATAMIENTO: 7.1. La naturaleza extracontractual de la responsabilidad civil del responsable y del encargado de tratamiento. 7.2. Naturaleza subjetiva de la responsabilidad civil del responsable y del encargado de tratamiento: 7.2.1. La naturaleza de la responsabilidad civil en la LOPDCP. 7.2.2. La naturaleza de la responsabilidad civil en el artículo 82 del RGPD; 8. LA NO APLICACIÓN DEL RGPD A LOS PRESTADORES DE SERVICIOS DE INTERMEDIACIÓN EN INTERNET (ISPs); 9. TIPOLOGÍA DE DAÑOS RESARCIBLES: SUPUESTOS PARTICULARES DE TRATAMIENTOS DE DATOS PERSONALES ILÍCITOS QUE GENERAN DAÑOS Y PERJUICIOS RESARCIBLES AL TITULAR DE LOS DATOS: 9.1. Consideración general. 9.2. Daños materiales o patrimoniales. 9.3. Daños morales o extrapatrimoniales: lesiones del derecho al honor. 9.4. El llamado derecho al olvido y las consecuencias jurídicas de su infracción; 10. LA INDEMNIZACIÓN DEL TITULAR DE LOS DATOS PERSONALES QUE HA RESULTADO DAÑADO O PERJUDICADO: 10.1. Precisiones generales sobre la acción ejercitando el derecho a la indemnización por el interesado perjudicado. 10.2. Criterios jurisprudenciales sobre el derecho a la indemnización; 11. PROCEDIMIENTO ADMINISTRATIVO SANCIONADOR Y ACCIÓN INDEMNIZATORIA. CONCLUSIONES. BIBLIOGRAFÍA.

1 EL MARCO NORMATIVO DE LA RESPONSABILIDAD CIVIL EXTRACONTRACTUAL COMO MECANISMO DE PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL

Uno de los derechos que las normas reguladoras de la protección de datos personales reconocen a los titulares de los mismos cuando éstos son objeto de tratamiento ilícito -entendiendo como tal cualquier tratamiento que vulnere alguno de los derechos de los interesados en su protección y, en particular, el propio derecho a la protección de los datos personales[4],

que constituye su objeto en la *Lei núm. 13.709/2018, Geral de Proteção de Dados* [**Nota dos Editores:** a última referência do autor se refere à LGPD brasileira].

[4] La STC, Pleno, 292/2000, de 30 de noviembre, en su F.J. 7º, declara que *«el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales,*

conforme a la previsiones de la norma de la UE o de la norma nacional, en su caso-, causando daños o perjuicios a los titulares de aquellos es el derecho a la indemnización. Se erige así la responsabilidad civil extracontractual como instrumento o mecanismo de tutela también en este ámbito, junto con la protección dispensada por las normas administrativas y también las penales para aquellos supuestos de actuaciones ilícitas imputables al responsable o al encargado del tratamiento merecedoras de un mayo reproche por el Derecho y que hayan sido objeto de tipificación expresa. Este mecanismo de protección de los datos personales frente a conductas de vulneración del correlativo derecho subjetivo se contempla también en los arts. 42 a 45 de la *Lei* (brasileña) *núm. 13.709/2018, Geral de Proteção de Dados* (en adelante, LGPD), cuya regulación se inspira en la regulación de los datos personales realizada por la Unión Europea (en adelante, UE).

En virtud del derecho a indemnización, el interesado, cuyos datos personales son objeto de tratamiento, que haya sufrido daños y perjuicios patrimoniales o morales (extrapatrimoniales) como consecuencia de una infracción del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, *relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE* (en adelante, *Reglamento General de Protección de Datos* o RGPD)[5], o de la Ley Orgánica (española) 3/2018, de 5 de diciembre, *de Protección de Datos Personales y garantía de los derechos digitales* (en adelante, LOPD-PGDD)[6]- y de otras normas de rango legal complementarias, como es el caso del art. 96 del *Texto Refundido de la Ley General de Defensa de Consumidores y Usuarios* (en adelante, TRLGDCU) en relación con las comunicaciones comerciales destinadas a consumidores y usuarios-, tiene derecho a recibir una indemnización por los daños y perjuicios que haya sufrido y que el perjudicado podrá hacer valer a través del ejercicio de la acción de responsabilidad civil

que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular». Este pronunciamiento es reiterado en el F.J. 5º de la STC 76/2019, de 22 de mayo, que declaró la inconstitucionalidad del apartado 1 del art. 58.*bis* de la LO 5/1985, de 19 de junio, *del régimen electoral general,* incorporado a esta por la disposición final tercera, apartado dos, de la LO 3/2018, de 5 de diciembre, *de protección de datos personales y garantía de los derechos digitales*.

[5] DOUE de 4 de mayo de 2016, L 119/1. El RGPD entró en vigor a partir de los veinte días de su publicación en el DOUE, siendo aplicable en todos los Estados miembro a partir del día 25 de mayo de 2018 (*ex* art. 99 del RGPD). La ya citada STC 76/2019, de 22 de mayo, respecto del valor normativo del RGP, recuerda que sin perjuicio de su valor interpretativo a los efectos del art. 10.2 de la CE, de la misma forma que en el pasado el TC se lo atribuía a la Directiva 95/46/CE que ha sido sustituida por aquel (*v.gr.,* SSTC 94/1998, de 4 de mayo [RTC 1998, 94], FJ 4; 144/1999, de 22 de julio [RTC 1999, 144], FJ 8; 202/1999, de 8 de noviembre [RTC 1999, 202], FJ 5; 70/2009, de 23 de marzo [RTC 2009, 70], FJ 2; y 29/2013, de 11 de febrero [RTC 2013, 29], FJ 5), la eficacia jurídica del RGPD no se agota, desde luego, en el valor hermenéutico que despliega a los efectos del art. 10.2 de la CE, esto es, en el plano de la constitucionalidad, pues en el seno de nuestro Ordenamiento jurídico representa sobre todo un acto jurídico *"obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro",* como luce al final del texto, con las características inherentes al Derecho de la UE.

[6] BOE núm. 294, de 6 de diciembre de 2018. La LOPDPGDD entró en vigor al día siguiente de su publicación en el BOE (*ex* DF 16ª) y derogó de manera expresa la LO 15/1999, de 13 de diciembre, *de Protección de Datos de Carácter Personal*; así como el RD-Ley 5/2018, de 27 de julio, *de medidas urgentes para la adaptación al Derecho español a la normativa de la UE en materia de protección de datos*; y cuantas disposiciones de igual o inferior rango contradigan, se opongan, o resulten incompatibles con lo dispuesto en el Reglamento (UE) 2016/679 y en la propia LOPDPGDD (*ex* DD Única).

extracontractual, ejercitada en el procedimiento civil o, en su caso, de manera acumulada al ejercicio de la acción penal.

El RGPD sitúa el epicentro de la responsabilidad en la protección de la integridad de los derechos de los titulares de datos personales sobre el llamado responsable de tratamiento y sobre el encargado de tratamiento, que responden de manera conjunta de cualquier infracción o vulneración de las normas aplicables en orden a la protección de los datos personales, conforme resulta de la previsión de su art. 24. En efecto, tanto el responsable, como el encargado de tratamiento, durante todo el periodo temporal que se mantenga el tratamiento de datos personales están coobligados a asegurar o garantizar, de conformidad con las obligaciones impuestas por el RGPD, la adopción de las medidas de seguridad técnicas y organizativas adecuadas para evitar cualquier infracción o vulneración de sus normas (*ex* art. 32 del RGPD). Es el conocido como principio de *accountability»,* que constituye el principio rector de la regulación del RGP, conforme a la lógica propia de la *compliance»*[7]: ser responsable de la conformidad y dar cuenta de esta conformidad. A estos efectos, en el RGPD se prevén instrumentos preordenados a asegurar la adecuación del tratamiento de datos a este principio una vez los datos personales son recogidos, tratados y conservados (*v.gr.,* previsión de registros de conformidad para documentar las acciones realizadas –arts. 30 y 35 del RGPD-), en su caso con la colaboración del llamado delegado de protección de datos (arts. 35 y 37 del RGPD). Tomando en consideración este principio angular de la regulación del RGPD, el responsable y el encargado de tratamiento deben estar, en todo momento, en situación de poder acreditar, ante las autoridades administrativas nacionales competentes (la AEPD o, en su caso, la Autoridad Catalana de Protección de Datos[8] o la Agencia Vasca de Protección de Datos[9]; estas dos últimas con sus competencias circunscritas al tratamiento de dato personales llevado a cabo por Administraciones y organismos públicos), el cumplimiento de todas las normas que rigen el tratamiento de datos personales.

La previsión expresa del derecho del titular de datos personales a la indemnización en caso de tratamiento ilícito no es algo novedoso que haya introducido el RGPD, sino que ya que estaba previsto en la derogada Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de

[7] BIURRUM, F.J.: «*"Accountability"* o responsabilidad activa en el Reglamento General de Protección de Datos», *AJA*, núm. 927, 25 de febrero de 2017, pg. 28.
Este principio se acoge también en el Derecho de Brasil. En particular, a tenor del inciso X del art. 6 de la LGPD, no es suficiente con cumplir con los artículos de la Ley, sino que es necesario, además, demostrar la adopción de medidas eficaces y capaces de comprobar la observancia y el cumplimiento de las normas de protección de datos personales, así como la eficacia de estas medidas, de manera que no incumplir la Ley no es suficiente para que los agentes de tratamiento de datos personales no puedan incurrir en infracciones de naturaleza administrativa o en supuestos de responsabilidad civil. En este sentido, se pronuncian, *v.gr.*, BODIN DE MORAES, MªC.; DE QUEIROZ, J.Q.: «Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD», en *Cadernos Adenauer*, Vol. 3 (*Proteção de dados pessoais: privacidade versus avanço tecnológico*), Ed. Fundação Konrad Adenauer, Rio de Janeiro, 2019, pg. 129 (en donde hablan de la vinculación de la responsabilidad de los agentes de tratamiento de datos con el conceto de *«prestação de contas»*); y, siguiendo a los anteriores, DA SILVA LIMA, H.: «Responsabilidade civil objetiva, subjetiva ou proativa? Pela Lei Geral de Proteção de Dados e suas implicações: contexto brasileiro», *Revista Jurídica de Daños,* núm. 24, diciembre de 2021, expresamente la pg. 6.

[8] Ley, Generalitat de Cataluña, 32/2010, de 1 de octubre, *de la Autoridad Catalana de Protección de Datos* (DOGC núm. 5731, de 8 de octubre de 2010).

[9] Ley, Parlamento de Euskadi, 2/2004, de 25 de febrero, *de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos*; desarrollada, por lo que se refiere a la propia Agencia, por el Decreto 309/2005, de 18 de octubre, *por el que se aprueba el Estatuto de la Agencia Vasca de Protección de Datos.*

24 de octubre de 1995, *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*. En particular, el Considerando 55 de esta Directiva 95/46/CE preconizaba que las legislaciones nacionales debían prever un recurso judicial para los casos en los que el responsable del tratamiento de datos no respetase los derechos de los interesados; al tiempo que señalaba que los daños que pueden sufrir las personas a raíz de un tratamiento ilícito de su datos responsables habrían de ser reparados por el responsable del tratamiento de datos; al tiempo que en el apartado 1 de su art. 23, rubricado *responsabilidad»,* preveía que los Estados miembro dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido. A su vez, el art. 19.1 de la derogada LO 15/1999, de 13 de diciembre, *de Protección de Datos de Carácter Personal*[10] -inmediatamente después de que los artículos precedentes estableciesen y regulasen los derechos de acceso, de consulta al Registro General de Protección de Datos, de rectificación, de oposición y de cancelación, así como el procedimiento para ejercitarlos- y en términos similares a los previstos en el art. 17.3 de la por ella derogada LO 5/1992, de 29 de octubre, *de regulación del tratamiento automatizado de datos personales* –si bien, de una forma técnicamente más correcta, al individualizar el derecho a la indemnización frente a la protección de carácter administrativo dispensada por la Agencia de Protección de Datos (AEPD) y extender la legitimación pasiva al encargado del tratamiento-, bajo la rúbrica *derecho a indemnización»,* establecía que:

> *Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados».*

Con este precepto, el legislador español daba respuesta a la exigencia que se derivaba de la previsión contenida en el referido art. 23 de la Directiva 95/46/CE.

2 LA RESPONSABILIDAD CIVIL DEL RESPONSABLE Y DEL ENCARGADO DE TRATAMIENTO Y EL DERECHO A LA INDEMNIZACIÓN DEL TITULAR PERJUDICADO EN EL RGPD

La vigente LOPDPGDD no contiene previsión específica alguna en relación con la responsabilidad civil en la que pueden incurrir, como consecuencia de la causación de daños y/o perjuicios a los titulares de datos personales objeto de tratamiento, los responsables o los encargados de su tratamiento, de manera que ha de estarse a la previsión contenida en el art. 82 del RGPD, directamente aplicable para regular la cuestión que nos ocupa, haciéndolo de una manera uniforme en todos los Estados miembro de la UE, al tratarse de una norma de aplicación directa, frente la divergencia de las normas nacionales dictadas con ocasión de la transposición de las previsiones del art. 23.1 de la Directiva 95/46/CE. Ha de tenerse en cuenta que el art. 82 del RGPD no es la única norma del Derecho derivado de la UE que contempla el

[10] BOE núm. 298, 14 diciembre 1999.

derecho del titular de datos personales que ha sufrido un daño o un perjuicio como consecuencia de un tratamiento ilícito a ser resarcido. Es el caso del art. 56 -*Derecho a la indemnización»*- de la Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo*[11], a tenor del cual, *los Estados miembros dispondrán que toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una operación de tratamiento ilícito o de cualquier acto que vulnere las disposiciones nacionales adoptadas con arreglo a la presente Directiva tenga derecho a recibir una indemnización del responsable o de cualquier autoridad competente en virtud del Derecho del Estado miembro por los daños y perjuicios sufridos».*

La regulación del derecho a la protección de datos vigente, el derecho de indemnización del titular o interesado perjudicado y la consiguiente responsabilidad civil del responsable y del encargado de tratamiento está contemplada en el art. 82 del RGPD. Como se expone en los epígrafes que siguen, esta nueva regulación uniforme para el conjunto de los Estados de la UE solventa alguna de las cuestiones no resueltas, al menos de manera expresa, por el derogado art. 19 de LOPD. En su apartado 1º, este precepto establece que toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del propio Reglamento tendrá derecho a recibir del responsable o del encargado del tratamiento una indemnización por los daños y perjuicios sufridos; y, en particular, en su apartado 6º, este mismo artículo indica que las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes con arreglo al Derecho del Estado miembro que se indica en el art. 79, apartado 2. Este artículo, al que remite expresamente el art. 82.6 del RGPD, hace referencia a que, con carácter general, las acciones deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento, si bien alternativamente podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos.

La estimación de una acción indemnizatoria fundada en el art. 82 del RGPD exige que el actor, en su condición de perjudicado pruebe la concurrencia de los siguientes presupuestos: la infracción de las normas sobre protección de datos personales previstas en el propio RGPD o en la LOPDPGDD, la imputación de esta infracción al responsable o al encargado de

[11] DOUE de 4 de mayo de 2016, L 119/89. En la *Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE* (Reglamento sobre la privacidad y las comunicaciones electrónicas) [COM/2017/010 final - 2017/03 (COD)] se prevé la introducción de un art. 22, rubricado «*Derecho a indemnización y responsabilidad»* del siguiente tenor: *«Todos los usuarios finales de servicios de comunicaciones electrónicas que hayan sufrido perjuicios materiales o morales como consecuencia de una infracción del presente Reglamento tendrán derecho a recibir una indemnización del infractor por los perjuicios sufridos, a menos que el infractor demuestre que no es en modo alguno responsable del hecho que haya dado lugar al perjuicio de conformidad con el artículo 82 del Reglamento (UE) 2016/679».*

tratamiento de los datos personales, la existencia de un daño o de un perjuicio cuyo resarcimiento se pretende, así como la existencia de una relación causal entre el tratamiento ilícito y el daño o perjuicio cuyo resarcimiento se pretende.

3 LEGITIMACIÓN ACTIVA: EL TITULAR DE LOS DATOS PERSONALES QUE HA EXPERIMENTADO EL DAÑO O PERJUICIO

3.1. Acciones indemnizatorias individuales

El art. 82.1 del RGPD atribuye el derecho a recibir una indemnización de daños y perjuicios a *toda persona»* que los haya sufrido como consecuencia de una infracción de las previsiones contenidas en el propio Reglamento. El amplio tenor literal del precepto podría conducir a admitir la legitimación activa de cualquier persona, física o jurídica, que haya sufrido un daño o un perjuicio como consecuencia de la referida conducta imputable a un responsable o a un encargado de tratamiento de datos personales, con independencia de la condición de aquélla de titular de los datos personales objeto de tratamiento y cuyo tratamiento ilícito, precisamente ha determinado la causación de los daños y perjuicios cuyo resarcimiento se pretende. Sin embargo, no parece que esta interpretación amplia resulte amparada por la interpretación sistemática de la norma, debiendo restringirse la legitimación activa a aquellas personas físicas cuyos datos son objeto de tratamiento y ello por cuanto[12]: 1º) El RGPD se refiere exclusivamente a las personas físicas como titulares de datos personales (art. 1.1 y 2), lo que determina la exclusión de las personas jurídicas de su ámbito subjetivo de aplicación[13].

[12] Comparto así expresamente el parecer expresado por RUBÍ PUIG, A.: «Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD», *Revista de Derecho Civil*, Vol. V, núm. 4, octubre-diciembre de 2018, pg. 60.

[13] En particular, la STS, Sala de lo Civil, 68/2016, de 16 de febrero [RJ 2016\563], en relación con un supuesto de pretendida lesión del derecho al honor de una persona jurídica por cesión de sus datos a un fichero de morosos, declara que la normativa sobre la protección de datos de carácter personal sólo es aplicable a las personas físicas. En cuanto al reconocimiento del derecho al honor de las personas jurídicas –que carecen de los otros dos derechos fundamentales reconocidos en el art. 18 de la CE (intimidad y propia imagen)- no ha sido una cuestión pacífica. En, efecto, en un primer momento la jurisprudencia limitó su titularidad a las personas físicas, de manera que los mecanismos de tutela de las posibles injerencias en su ámbito (en esencia, la acción de responsabilidad civil fundada en la LO 1/1982, de 5 de mayo) propio no resultaban de aplicación a las personas jurídicas. Sin embargo, a partir de las SSTC 214/1991, 139/1995, de 26 de septiembre y 183/1995, de 11 de noviembre (también parte de esta premisa, *v.gr.*, la STC 79/2014, de 28 de mayo), aquella doctrina inicial ha mudado a favor de su reconocimiento definitivo y expreso (*v.gr.* STS, Civil, 861/1997, de 9 de octubre), si bien su ámbito se ha limitado por el TS a las personas jurídicas privadas, rechazando el Tribunal Supremo que las personas jurídicas públicas sean titulares del derecho fundamental al honor (STS núm. 408/2016, de 15 de junio, que considera que su dignidad, el prestigio y la autoridad moral *«son valores que merecen la protección penal que les dispense el legislador, pero que no son exactamente identificables con el honor*»). Se produce así la extensión de la protección y garantía del derecho al honor a las personas jurídicas respecto a los ataques injustificados que afecten a su prestigio profesional y social, que conforman integración de su patrimonio, moral, con repercusión en el patrimonial, por su pérdida reputacional en el mercado –y en el conjunto de la sociedad-, sus resultados negativos y que puede traducirse en una pérdida de confianza de la clientela, de proveedores y concurrentes comerciales o de rechazo o minoración en el mercado de forma general y todo ello, como consecuencia de que también las personas jurídicas ostentan la titularidad del derecho al honor, con protección constitucional, pues no se puede prescindir totalmente del mismo, en su versión de prestigio y reputación

Sin perjuicio de ello, el art. 78.1 del RGPD sí admite la legitimación activa de las personas jurídicas en relación con el ejercicio del derecho a la tutela judicial efectiva frente a una autoridad nacional de control y ello por cuanto, se trata de procedimientos en los que estarán habitualmente involucrados responsables y encargados de tratamiento –e, incluso, delegados de protección de datos- que, con frecuencia, tendrán la naturaleza jurídica de personas jurídicas; al tiempo que la legitimación activa de determinadas personas jurídicas se admite en relación con el ejercicio de acciones colectivas de tutela de conformidad con las previsiones del art. 80 del RGPD y en el caso de que tengan amparo en las previsiones de los Derechos procesales nacionales, como seguidamente se expone. 2º) Los arts. 77 y 79 del RGPD se refieren exclusivamente a los *interesados»* al regular, respectivamente, los derechos a presentar una reclamación ante una autoridad de control y a la tutela judicial efectiva frente a un responsable o a un encargado de tratamiento y lo hacen en línea con la previsión del Considerando 146 del propio RGPD que alude al derecho de los *interesados»* a recibir una indemnización total y efectiva de los daños sufridos.

En relación con el concepto de *interesado»* en el RGPD, hemos de estar a la previsión de su art. 4.1, a tenor del cual, *interesado»* es una *persona física identificada o identificable»*, respecto de la que se produzca el tratamiento de cualquier información considerada como datos personales, precisando que se considerará como persona física identificable *toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona»*. Lo cierto es que el término *interesado»* utilizado en la versión en español del RGPD, similar al *interessato»* de la versión italiana y a los de *personne concernée»* y *betroffene Person»* de las versiones francesa y alemana respectivamente, no son los técnicamente más correctos, debiendo haberse utilizado la expresión titular de los datos personales, de manera concordante con el término *data subject»* de la versión en inglés del Reglamento y *titular dos dados»* de su versión en portugués.

3.2. La legitimación para la tutela *post mortem»*

Sin perjuicio de los supuestos de sucesión procesal que se rigen de conformidad con las previsiones del art. 16 de la LECiv, merece una particular consideración la cuestión atinente

profesional, necesarios para el desarrollo de sus objetivos sociales y cumplimiento de los fines para los que fueron constituidas, con un componente de personas individuales, que siempre resultan identificables y a las que también les afecta, en mayor o menor medida, el desprestigio del ente en que están integradas.

La consecuencia fundamental del reconocimiento del derecho al honor de las personas jurídicas radica en que, en el caso de ser vulnerado, están legitimadas activamente para acudir a los mecanismos de tutela previstos a estos efectos, como acontece con la LO 1/1982, de 5 de mayo, *de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*; y también con el procedimiento especial contencioso-administrativo de tutela de los derechos fundamentales contemplado en los arts. 115 y ss. de la LJC**A** que tiene una tramitación de carácter de preferente y urgente. La cuestión dudosa que se plantea en el caso que nos ocupa radica en que el objeto de este procedimiento especial lo constituyen los actos de las Administraciones Publicas, sujetas al Derecho administrativo en cuanto afecte a los derechos fundamentales que señala el art. 53.2 de la Constitución (entre los que está el derecho al honor); es decir, podrán hacerse valer en este proceso las pretensiones a que se refieren los artículos 31 y 32 CE, siempre que tengan como finalidad la de restablecer o preservar los derechos o libertades por razón de los cuales el recurso hubiere sido formulado, siendo su plazo de interposición de 10 días.

a la legitimación activa para el ejercicio de acciones de protección de los derechos sobre datos personales de personas físicas tras el fallecimiento de éstas y, en particular, la determinación de la posibilidad de su tutela *post mortem»* y de identificación de las personas que gozan de legitimación activa en estos supuestos, en particular para el ejercicio de las acciones indemnizatorias. A tenor de la doctrina que resulta de las SSTC 43/2004, de 23 de maro y 51/2008, de 14 de abril, la muerte de la persona que conlleva la extinción de la personalidad, entendida como idoneidad para ser titular de derechos subjetivos (capacidad jurídica), es compatible con la subsistencia, derivada del principio de la inviolabilidad de la dignidad de la persona (*ex* art. 10.1 de la CE), de un derecho al respeto de los derechos existenciales de la persona, de los que disfruta en vida, incluso tras su fallecimiento (derecho al respeto de la personalidad pretérita). Por otra parte, ha de tenerse en cuenta que, cada vez son más los contenidos digitales, ordinariamente de naturaleza extrapatrimonial, vinculados a datos personales, que son transmisibles *mortis causa»*, aun cuando, con frecuencia, los prestadores de los servicios de la sociedad de la información (*v.gr., Google, Facebook, Amazon,* etc.) pretendan limitar contractualmente la referida transmisibilidad, planteándose la cuestión relativa la transmisión de su titularidad y, vinculada a ella, la legitimación del ejercicio de los derechos derivados de la misma, habiendo recibido alguna respuesta expresa en leyes autonómicas, como es el caso de la Ley 10/2017, de 27 de junio, *de las voluntades digitales y de modificación de los libros segundo y cuarto del CC de Cataluña*[14]. El art. 96.4 de la LOPDPGDD expresamente dispone la aplicación preferente de las normas de Derecho civil propio de las CCAA en el caso de que existan en relación con las propias previsiones del referido precepto, si bien refiere su ámbito de subjetivo de aplicación, de manera técnicamente incorrecta, a las *personas fallecidas en las comunidades autónomas con Derecho civil, foral o especial, propio»,* cuando debería referirlo a las personas fallecidas con una vecindad civil correspondientes a una CA con un Derecho civil propio (al ser éste el criterio que ha de tomarse en consideración para determinar el Derecho aplicable).

Respecto de la cuestión que se ha planteado no existe previsión expresa alguna en el RGPD, pero sí en la LOPDPGDD, en cuyo art. 96 se contiene una previsión sobre el denominado derecho al testamento digital[15], en el que se regula el acceso a los contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas, atribuyendo legitimación para realizar aquel acceso a las personas vinculadas por el fallecido por razones familiares o de hecho, así como a sus herederos y, en su caso al albacea testamentario. Fuera de este supuesto, teniendo en cuenta la naturaleza de los derechos protegidos, concurren razones suficientes para argumentar, sobre la *eadem ratio»* existente en ambos supuestos, la aplicación analógica, de las previsiones expresas contenidas en el art. 6 de la LO 1/1982, de 5 de mayo, *de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*, que extiende la legitimación activa de las personas que, de acuerdo

[14] *Vid.* OTERO CRESPO, M.: «La sucesión en los "bienes digitales". La respuesta plurilegislativa española», *Revista de Derecho Civil*, Vol. VI, núm. 4, octubre-diciembre de 2019, pgs. 89 a 133; DÍAZ ALABART, S.: *La protección de los datos y contenidos digitales de las personas fallecidas*, Ed. Reus, Madrid, 2020; MARTÍNEZ MARTÍNEZ, N.: «Reflexiones en torno a la protección *post mortem* de los datos personales y la gestión de la transmisión *mortis causa* del patrimonio digital tras la aprobación de la LOPDGDD», *DPyC*, núm. 35, 2019, pgs. 169 a 212.

[15] En el Derecho italiano el art.2–*terdecies* fruto del Decreto legislativo n. 101/2018, de 10 agosto de 2018, que reformó el *Codice della Privacy* DLgs. 196/2003 (que ha entrado en vigor el 19 de septiembre de 2018), regula el denominado *«diritto all'eredità del dato in caso di decesso: I diritti riferiti a persone decedute possono essere esercitati da chi ha un interesse proprio o agisce a tutela dell'interessato, in qualità di suo mandatario o per ragioni familiari meritevoli di protezione».*

con su art. 4 (la designada en testamento, el cónyuge, los ascendientes, los descendientes, los hermanos y, en su caso, Ministerio Fiscal) la tienen para promover la defensa de la memoria de la persona fallecida, a los supuestos de lesiones producidas en vida del titular de los derechos de la personalidad, permitiéndoles el ejercicio de las acciones que la persona que ha padecido la intromisión ilegítima no haya podido ejercitar antes de su fallecimiento (por sí o por su representante legal), por las circunstancias en que la lesión se produjo (párrafo 1º), y para la continuación en las acciones que ya hubiera entablado (párrafo 2º)[16]. En ambos supuestos (a diferencia de lo que sucede en la defensa de la reputación de una persona fallecida) con el ejercicio o con la continuación de las acciones se pretende la tutela frente a las intromisiones ilegítimas sufridas en vida por el titular de los derechos y se previene el destino que ha de darse a la reparación de los daños que con ellas se le han causado en vida, a cuyos efectos, el inciso final del art. 9.4 de a LO 1/82 dispone que la indemnización que, en su caso, se establezca para resarcir el daño causado al titular de derecho lesionado, se entenderá comprendida en la herencia del perjudicado.

Si se admiten las premisas precedentes, la legitimación activa para el ejercicio de las acciones para la protección de los derechos derivados de la necesaria tutela de los datos personales de la persona fallecida corresponderá a la persona que el fallecido haya designado, a los familiares (y no a los herederos), con fundamento en el *deber recíproco de protección existente entre los miembros de la familia»*[17]*,* y, en defecto de todos ellos, al Ministerio Fiscal. Estas personas ejercitarán la acción frente a las intromisiones o lesiones producidas *post mortem»,* porque ostentan una legitimación *ope legis»,* vinculada a un derecho, la dignidad protegida de la personalidad pretérita, cuya tutela pretenden con el proceso, apreciándose la independencia de la cualidad de legitimado con la de beneficiario de la indemnización que, en su caso, proceda por la lesión del derecho a la tutela de los datos personales, en tanto que las personas legitimadas, por la voluntad del fallecido o por disposición de la ley, no son, en atención a esta cualidad, destinatarios de la indemnización que, en su caso, se conceda.

3.3. Acciones indemnizatorias colectivas

El art. 80 del RGPD contempla la posibilidad de que, conforme a las disposiciones de los Derechos nacionales, los titulares de datos personales otorguen mandato a entidades, organizaciones y asociaciones sin ánimo de lucro cuyos objetivos estatutarios sean de interés público y actúen en el ámbito de la protección de los derechos y libertades de aquellos interesados en materia de protección de sus datos personales, en orden a que presenten, en su nombre, la reclamación y ejerzan, también en su nombre, los derechos contemplados en los

[16] Sobre esta cuestión, *vid.*, ampliamente, HUALDE SÁNCHEZ, J.J.: «La protección *post mortem*» de los derechos de la personalidad y la defensa de la memoria del fallecido», en *Bienes de la Personalidad. XII Jornadas de la APDC,* Servicio de Publicaciones de la Universidad de Murcia, Murcia, 2008, pgs. 108 y ss.

En relación con la argumentación de la identidad de razón entre ambos supuestos, acaso resulte procedente señalar que, *v.gr.*, en el art. 151-4 de la *Propuesta de CC* elaborada por la APDC (publicada por la Ed. Tecnos, Madrid, 2018), se califica como intromisión ilegítima en la vida de una persona *«la revelación de datos privados de una persona o familia que se hayan conocido a través de la actividad profesional u oficial de quien los revele»,* lo que permite ejercitar las acciones de tutela enunciadas en el art. 151-7 del misma *Propuesta de CC*, entre las que se haya la acción indemnizatoria de daños y perjuicios.

[17] IGARTUA ARREGUI, F.: «La protección de los aspectos personales y patrimoniales de los bienes de la personalidad tras la muerte de la persona», *La Ley*, 1999-1, pg. 1068.

arts. 77 (presentar reclamaciones ante las autoridades de control), 78 (tutela judicial efectiva contra una autoridad de control), 79 (tutela judicial efectiva contra un responsable o encargado de tratamiento) y el derecho a la indemnización en los términos del art. 82 del RGPD. El apartado 2º de este mismo art. 80 del RGPD prevé también que los Derechos nacionales puedan prever que cualquiera de las referidas entidades -entidades, organizaciones y asociaciones sin ánimo de lucro cuyos objetivos estatutarios sean de interés público y actúen en el ámbito de la protección de los derechos y libertades de aquellos interesados en materia de protección de sus datos personales-, con independencia de la existencia de un mandato del interesado, tengan legitimación para presentar, en ese Estado miembro, una reclamación ante la autoridad de control competente en virtud del art. 77 del RGPD y a ejercer los derechos contemplados en los arts. 78 y 79, si consideran que los derechos del interesado reconocidos en el propio RGPD han resultado vulnerados como consecuencia del tratamiento realizado. Lo más llamativo de las previsiones del art. 80 del RGPD radica en que para que las entidades a las que se refiere puedan tener atribuida legitimación activa para el ejercicio de la acción indemnizatoria del art. 82 del RGPD se exige la concurrencia de un mandamiento expreso conferido por el interesado a favor de la entidad que ejercite, de manera colectiva, la acción que nos ocupa. La pregunta que, de manera evidente e inmediata surge, es la que sigue: ¿significa el distinto ámbito objetivo de los apartados 1 y 2 del art. 80 del RGPD que los Estados nacionales no pueden prever en sus Derechos internos acciones colectivas de naturaleza indemnizatoria o resarcitoria para el caso de lesiones dañosas en materia de tratamiento de datos personales? La respuesta, a mi juicio, es evidentemente negativa, sin perjuicio de la criticable exclusión de la previsión expresa de la acción indemnizatoria o de daños en el apartado 2 del citado art. 80 del RGPD.

No se ha previsto por el legislador español una acción colectiva de naturaleza indemnizatoria o resarcitoria para los casos de daños o perjuicios causados a una pluralidad de sujetos como consecuencia del tratamiento ilícito de datos personales, al margen de las acciones colectivas de tutela de daños ocasionados a consumidores y usuarios reguladas en los arts. 11.2 y 3 de la LECiv[18] y ello a diferencia de lo que sucede, *v.gr.*, en el Derecho francés, tras la reforma del art. 37 de la *Loi núm. 78-17, du 6 janvier 1978, relative à l'informatique, aux*

[18] *Vid.*, entre otros, REGLERO CAMPOS, L.F: «Cap. I. Conceptos generales y elementos de delimitación», en *Tratado de Responsabilidad Civil*, T. I, Ed. Aranzadi, Cizur Menor, 2014 (5ª edic.), pgs. 243 y ss.; LLAMAS POMBO, E.: «Acciones colectivas contra daños», en *Práctica Derecho de daños: Revista de Responsabilidad Civil y Seguros*, núm. 60, 2008, pgs. 5 a 36. Para el caso específico de las acciones colectivas de daños derivados del tratamiento ilícito de datos personales en el marco de la derogada LOPD, *vid.* PUYOL MONTERO, J.: «Comentario del artículo 19 de la LOPD», en *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal* (A. TRONCOSO REIGADA, Dir.), Ed. Civitas, Cizur Menor, 2010, pg. 1266.

Las limitaciones subjetivas de la regulación de las acciones colectivas de daños en el Derecho español determina la inadecuación de éste a la Recomendación, a tenor de la cual la finalidad de la presente Recomendación de la Comisión Europea de 11 de junio de 2013 sobre los principios comunes aplicables a los mecanismos de recurso colectivo de cesación o de indemnización en los Estados miembros en caso de violación de los derechos reconocidos por el Derecho de la Unión (DOUE de 26 de julio de 2013; L 201/60) y cuya finalidad es facilitar el acceso a la justicia, poner fin a las prácticas ilegales y permitir a las partes perjudicadas obtener una indemnización en caso de daños masivos causados por infracciones de los derechos reconocidos por el Derecho de la Unión, estableciendo al mismo tiempo las garantías procesales necesarias para evitar los litigios abusivos. La Recomendación de la Comisión señala que los Estados miembros deberían disponer de mecanismos de recurso colectivo a nivel nacional, tanto de cesación como de indemnización, que respeten los principios básicos establecidos en la presente Recomendación. Estos principios deben ser comunes a toda la Unión y respetar al mismo tiempo las distintas tradiciones jurídicas de los Estados miembros. Los Estados miembros deben velar por que los procedimientos de recurso colectivo sean justos, equitativos, oportunos y no excesivamente onerosos.

fichiers et aux libertés llevada a cabo por la *Ordonnance* n°2018-1125 de 12 de diciembre 2018. En el Derecho español, sólo una interpretación amplia del art. 6.1.7º de la LECiv, en consonancia con la previsión del art. 7.3 de la LOPJ, ampararía el ejercicio de una acción colectiva indemnizatoria prescindiendo de la cualidad de consumidores y usuarios de los sujetos perjudicados, como acontece en todos aquellos casos en los que la acción se funde en el art. 1902 del CC[19].

En el Derecho francés, el vigente apartado 2º del art. 37 de la *Loi núm. 78-17, du 6 janvier 1978* dispone que cuando varias personas físicas situadas en una posición similar sufran un daño que tenga como causa común una infracción de la misma naturaleza de las disposiciones del RGPD o de la propia Ley francesa, imputable a un responsable de tratamiento de datos personales o un encargado del tratamiento, puede ejercitarse una acción colectiva ante la jurisdicción civil o ante la jurisdicción administrativa competente en atención a los casos individuales presentados por el actor, previo informe de la *Commission nationale de l'informatique et des libertés.* El ap. 3º del mismo precepto, precisa que esta acción puede ser ejercitada con la finalidad de hacer cesar la infracción o con la finalidad de imputar la responsabilidad civil a la persona que ha causado el daño, con el propósito de obtener una reparación de los perjuicios materiales y morales sufridos, así como las dos finalidades: cesación e indemnización. En todo caso la responsabilidad sólo puede ser imputada con el fundamento en este precepto en el caso de que el hecho generador del daño sea posterior al 24 de mayo de 2018 (fecha de entrada en vigor del RGPD). El apartado 4º del art. 37 de la Ley francesa de protección de datos enuncia los sujetos activamente legitimados para ejercitar la referida acción colectiva, presentado este elenco el carácter de *numerus clausus:* 1º) Las asociaciones válidamente constituidas, con una antigüedad superior a cinco años y que tengan como objeto estatutario la protección de la vida privada o la protección de los datos personales. 2º) Las asociaciones de defensa de los consumidores representativas a nivel nacional y sujetas a la aplicación del art. 811-1 del *Code de la consommation*, cuando el tratamiento de los datos personales afecte a los consumidores. 3º) Las organizaciones sindicales y de funcionarios representativas en el sentido de los artículos L. 2122-1, L. 2122-5 o L. 2122-9 del *Código de trabajo* o del apartado III del art. 8.*bis* de la *Loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires ou les syndicats représentatifs de magistrats de l'ordre judiciaire*, en aquellos casos en los que el tratamiento afecte a los intereses de las personas cuyos intereses los estatutos de estas organizaciones contemplen defender. Asimismo, se precisa que cuando la acción colectiva ejercitada pretenda la reparación de los perjuicios causados, se ejercitará en el marco del procedimiento individual de reparación establecido en el Capítulo 1º del Título V de la *Loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXI^e siècle* y en el Capítulo X del Título VII del Libro VII del *Code de justice administrative.*

La STJUE de 25 de enero de 2018 (asunto C-498/16; *Schrems vs. Facebook*), resuelve la cuestión prejudicial plateada por el *Oberster Gerichtshof* (Tribunal Supremo Civil y Penal de

[19] En este sentido se pronuncia, *v.gr.*, ARIZA COLMENAREJO, MªJ.: «Acciones colectivas: especial referencia a la legitimación, eficacia de la sentencia y ejecución forzosa», en *Daño, responsabilidad y seguro* (M.J. HERRADOR GUARDIA, DIR.), Ed. Lefebvre - El Derecho, Madrid, 2016, pgs. 810 y 811. Tampoco en el ámbito de la responsabilidad civil por daños al medioambiente existe una posición doctrinal favorable a la viabilidad de las acciones colectivas o de grupo en el Derecho español. Sobre esta última cuestión, *vid.* RUDA GONZÁLEZ, A.: *El daño ecológico puro. La responsabilidad civil por el deterioro del medio ambiente, con especial atención a la Ley 26/2007, de 23 de octubre, de responsabilidad medioambiental,* Ed. Aranzadi, Cizur Menor, 2008, pg. 510.

Austria) conociendo, en grado de casación, de la demanda interpuesta por *M. Schrems* frente a *Facebook Ireland Lted*., como consecuencia del espionaje masivo de cuentas abiertas en esta red social por parte de los servicios de inteligencia de USA, fundada en la infracción del normativa de la UE en materia de protección de datos personales y ejercitando pretensiones declarativas en relación con la invalidez de varias cláusulas contractuales, de cesación en el uso de sus datos, de información sobre el destino de éstos, de rendición de cuentas y de indemnización de daños y perjuicios, argumentando la competencia territorial en el fuero especial del domicilio del consumidor previsto en el art. 16.1 del Reglamento 44/2001 (vigente Reglamento 1215/2012), si bien el actor (*M. Schrems*) es un jurista especializado en Derecho informático y protección de datos, al tiempo que ejercita la acción agrupando la propia derivada de su relación contractual con *Facebook,* con otras similares que le han cedido otros usuarios austriacos, de otros Estados de la UE e incluso de terceros Estados. Respecto de la primera cuestión planteada, el TJUE considera como consumidor a un experto en la materia que ha convertido el litigio propio en fuente de ingresos como acontece con el Sr. *Schrems*; pero no admite el fuero de competencia territorial especial del consumidor, señalando que éste sólo es aplicable cuando el demandante actúa en defensa de derechos nacidos de su relación contractual con el empresario o profesional, sin que dicho fuero se extienda también a las acciones cedidas por usuarios domiciliados en distintos Estados[20], argumentando sobre el carácter excepcional del fuero tuitivo del consumidor, al tiempo que considera que esta solución es la que mejor garantiza la previsibilidad de la atribución de competencia, es uno de los objetivos perseguidos por el Reglamento Bruselas-I»: el empresario espera razonablemente que el consumidor con quien contrató le demande ante los tribunales de su domicilio, de manera que la posibilidad de que el conocimiento del asunto acabe en una jurisdicción distinta por el azar de la cesión de acciones resulta sorpresiva y generadora de incertidumbre. El TJUE da así al traste con el intento de *M. Schrems* de construir una especie de *class action»* similar al sistema del Derecho de los USA, partiendo de los escasos mimbres que, a estos efectos, le brinda la legislación procesal austríaca, utilizando las instituciones jurídicas de la cesión y acumulación de acciones, atribuyéndole el papel de representante y defensor del grupo de afectados por *Facebook*, al igual que acontece con el *representative plaintiff»* del Derecho USA[21].

4 LEGITIMACIÓN PASIVA

El art. 82.1 del RGPD identifica a los sujetos pasivamente legitimados para el ejercicio de la acción indemnizatoria: el responsable del tratamiento de los datos personales (*controller personal data»*) y, en su caso, el encargado de su tratamiento (*proccesor»*) por cuenta de aquél. La Directiva 95/46/CE atribuía a las legislaciones de los Estados determinar el régimen de responsabilidad civil del encargado del tratamiento y, en particular, si la responsabilidad civil de éste, podía, o no, concurrir con la del responsable del tratamiento, optando por una

[20] Comentando la STJUE de 25 de enero de 2018 LAFUENTE TORRALBA apunta a que la razón que subyace en este pronunciamiento radica en el temor al *fórum shopping* o admisión de un fuero de conveniencia, en línea con lo apuntado en las conclusiones del Abogado General (M. BOBEK) en el referido asunto. *Vid.* LAFUENTE TORRALBA, A.J.: «Acciones colectivas, protección de datos y redes sociales: reflexiones al hilo de un reciente pronunciamiento de la Corte de Luxemburgo», en *Acciones colectivas. Cuestiones actuales y perspectivas de futuro* (T. ARMENTA DEU Y D. PEREIRA PUIGVERT, COORDS.), Ed. M. Pons, Madrid, 2018, pg. 361 y 362.

[21] Sobre las *class action* en el Derecho de USA puede verse, *v.gr.*, LÓPEZ SÁNCHEZ, J.: *El sistema de las* class actions *en los Estados Unidos de América*, Ed. Comares, Granada, 2011.

respuesta afirmativa a esta compatibilidad el legislador español en el art. 19 de la derogada LOPD, en tanto que, a tenor de este precepto, tanto el responsable, como el encargado del tratamiento podían incurrir en responsabilidad civil frente al titular de los datos personales objeto de tratamiento, sin necesidad de acudir a otras normas sectoriales (*v.gr.,* el art. 9.3 de la LO 1/1982) o la regla general del art. 1902 del CC para fundar la responsabilidad civil del encargado de tratamiento.

En el caso del RGPD los dos sujetos respecto de los que, atendiendo a sus funciones y responsabilidades en el tratamiento de los datos personales, se les atribuye la función de garantes del tratamiento lícito y, con ello, la responsabilidad civil derivada de un tratamiento ilícito dañoso, son el responsable y el encargado del tratamiento, si bien, también se identifican otros sujetos que, en determinadas ocasiones, tienen atribuciones y responsabilidades en el tratamiento de datos personales y que, en consecuencia, pueden resultar responsables de ilícitos dañosos extracontractuales. Son los casos del subencargado de tratamiento, del delegado de protección de datos y, en su caso, del representante en la UE del responsable o del encargado a que se refiere el art. 27 del RGPD. La posible imputación de responsabilidad civil por el tratamiento ilícito de datos personales será objeto de una consideración específica seguidamente.

Fuera de los supuestos en los que el daño cuyo resarcimiento se pretenda sea imputable a alguno de los sujetos enunciados es posible que un tercero ajeno a la esfera de control del responsable y del encargado del tratamiento de datos personales aproveche una infracción, en particular en materia de seguridad o de cesión inconsentida, en cuyo caso es posible que, adicionalmente, a la responsabilidad del sujeto o sujetos que reciben un tratamiento específico en el RGPD, se acumule la responsabilidad civil del tercero ajeno, que se regirá por las normas generales que regulan la responsabilidad civil extracontractual, suscitándose, en su caso, la aplicación de la regla que, en el Derecho español, impide la indemnización del perjudicado en una suma que rebase la cuantía del daño padecido por el perjudicado.

4.1. El responsable del tratamiento

A tenor de lo dispuesto en el art. 4.7 del RGPD, el responsable del tratamiento de datos personales -*controller»*- es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento, situándolo así en una posición de garante frente al titular de los datos personales objeto de tratamiento y, con ello, situándolo en la posición de garante en el caso de tratamientos ilícitos generadores de daños y perjuicios. El hecho de que exista un encargado de tratamiento no pone al responsable al amparo del ejercicio de una acción de responsabilidad civil por el interesado que haya resultado dañado o perjudicado, lo que resulta acorde con la obligación de asegurar y garantizar un tratamiento adecuado conforme al ya enunciado principio de *accountability»* o de responsabilidad activa que acoge el RGPD (arts. 5.2 y 24.1). Este principio obliga al responsable a verificar el cumplimiento efectivo de la normativa de protección de datos personales, debiendo llevar a cabo las verificaciones necesarias y estableciendo los protocolos de actuación necesarios para evitar que el tratamiento de datos personales vulnere las previsiones del

RGPD y de las propias leyes nacionales en la materia. De aquí se desprende la existencia de una formulación abierta del deber de protección a cargo del responsable de tratamiento de los datos personales, de manera tal que parece amparar poner a cargo del responsable de tratamiento los daños y perjuicios que puedan derivarse de un tratamiento ilícito o que contravenga las previsiones normativas[22]; si bien, no puede desconocerse que un criterio de imputación objetiva como es el de protección de la norma despliega un papel menos estricto en estos supuestos de normas abiertas que remiten a estándares genéricos, frente a lo que acontece en aquellos casos en los que se las normas definen conductas o deberes de actuación de manera más detallada o precisa.

Acaso merezca una consideración específica la condición de responsable del tratamiento de datos que corresponde al empleador respecto de los datos personales de sus trabajadores. En efecto, a tenor de la opinión manifestada en el año 2010 por el G29 (Grupo de trabajo del artículo 29 de la, ahora derogada, Directiva de 24 de octubre de 1995)[23], integrado por representantes de las CNIL europeas, el empleador es considerado como responsable del tratamiento de datos personales y ello a pesar de la inexistencia de cualquier disposición normativa que lo prevea, en tanto su condición resulta de la toma en consideración de reglas jurídicas generales y, en particular, de las normas propias del Derecho del trabajo: el empleador es el responsable de los datos personales de sus trabajadores. El RGPD armoniza el concepto de responsable de tratamiento y reafirma posibilidad de concurrencia de una pluralidad de responsables de tratamiento concurrentes, lo que, en el ámbito del Derecho laboral puede acontecer en el caso de las sociedades que formen parte de un grupo empresarial o de un grupo mercantil de empresas[24]. En el marco de estos grupos de sociedades, la sociedad matriz puede ser acreedora de la condición de responsable del tratamiento en aquellos casos en los que determine las finalidades o los elementos esenciales de los medios de tratamiento utilizados por las sociedades filiales, puede realizar el tratamiento por cuenta de otras sociedades del grupo a las que presta determinados servicios (*v.gr.,* servicios de confección de nóminas y de pago, contabilidad, control y sanción de los trabajadores, etc.) o puede estandarizar los mecanismos de tratamiento utilizado en el grupo empresarial, al tiempo que puede tener la condición de coempleadora. En consecuencia, en estos supuestos, en el caso de que un trabajador haya visto vulnerados los derechos que el RGPD o la Ley nacional le reconocen en relación con sus datos personales (seguridad, derecho de acceso, derecho a la información, derecho al olvido, etc.), podrá ejercitar la acción indemnizatoria frente a la sociedad filial de la que es empleado, pero también frente a la sociedad matriz, en ambos casos por la totalidad de la indemnización[25]; sin perjuicio de la posibilidad de ejercicio de la acción de regreso en los términos contemplados en el art. 82.5 del RGPD.

4.2. El encargado del tratamiento

[22] *Vid.* Considerandos 77 y 78 del RGPD, así como el estudio del Grupo de trabajo del artículo 29 «Opinion 3/2010 on the principle of accountability», 13 de julio de 2010 (10/EN WP 173).

[23] G29, «Parecer 1/2010 sobre los conceptos de responsable y de encargado de tratamiento», 16 de febrero de 2010, pgs. 10 y 11.

[24] A estos efectos, ha de tenerse en cuenta el concepto normativo de «grupo empresarial» que ofrece el art. 4.19 del RGPD: *«grupo constituido por una empresa que ejerce el control y sus empresas controladas».*

[25] MERCELLIN, S. y SEMIK, J.: «La responsabilité des traitements de données partagées dans un groupe», *Le RGPD,* Ed. Dalloz (Grand Angle), París, 2018, pg. 231.

La doctrina suele poner de manifiesto que una de las novedades relevantes del art. 82 del RGPD radica precisamente en la posibilidad de imputar la responsabilidad por daños al encargado del tratamiento y, en su caso, al subencargado de tratamiento, creando una corresponsabilidad para el caso de daños y perjuicios derivados de vulneraciones normativas en materia de tratamiento de datos personales que resulten imputables. Conforme a lo dispuesto en el art. 4.8 del RGPD, el encargado del tratamiento –o, simplemente, el encargado- es la persona, física o jurídica, autoridad púbica, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento[26]. El art. 28.1 del RGPD exige que el responsable debe elegir a un encargado de tratamiento que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento de datos personales que realice sea conforme con las exigencias del propio RGPD y garantice la protección de los derechos del interesado. Asimismo, el apartado 2º del mismo art. 28 del RGPD prescribe que el encargado de tratamiento no puede recurrir a otro encargado sin la autorización previa, en forma escrita, específica o general, del responsable del tratamiento y, en el caso de que se recurra a otro encargado de tratamiento, el primero está obligado a informar al responsable de cualquier cambio previsto en la incorporación o sustitución, pudiendo el responsable del tratamiento oponerse a estos cambios. A su vez, el art. 28.3 del RGPD especifica que el tratamiento por el encargado se regirá por un contrato o por otro acto [negocio] jurídico –*v.gr.,* un acto unilateral del responsable que defina la posición jurídica del encargado del tratamiento, lo que puede resultar frecuente en el ámbito de las Administraciones Públicas, al existir relaciones de jerarquía y de subordinación orgánica- que sea conforme al Derecho de la UE o de los Derechos nacionales, estableciendo el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, así como las obligaciones y derechos del responsable de tratamiento, debiendo contener las previsiones que se relacionan en las ocho letras que integran el contenido del referido precepto. En relación con esta cuestión, procede recordar que el acceso a los datos personales por parte del encargado de su tratamiento no requiere una legitimación adicional a la que sustenta el tratamiento por parte del responsable, al no existir una comunicación o cesión de datos en sentido propio. En

[26] La SAN, Sala de lo Contencioso-Administrativo, de 29 de abril de 2005 [JUR 2005\124220], a propósito de la distinción entre la cesión de datos y el encargo de tratamiento, precisó, en su F.D. 4º: *«Se plantea en definitiva a la Sala el problema de la diferenciación entre la cesión y el encargado de tratamiento, "encargado de tratamiento" que no venía expresamente regulado en la LO 5/1992, pero entendía la doctrina que tenía cabida en lo establecido en el art. 27. Siguiendo lo dispuesto en tal Directiva Europea 95/46/CE, la LO 15/1999 ha regulado específicamente la figura en los aludidos Art. 3.g) y 12, y de hecho la definición de "encargado de tratamiento" contenida en el art. 3.g) no es sino trascripción del art. 2.e) de la Directiva. Y si bien la diferencia entre encargo de tratamiento y cesión, como reconoce la doctrina, en algunos casos es compleja, lo que es evidente es que no puede haber cesión cuando existe encargo de tratamiento y no resulta preciso el consentimiento del afectado. […] Lo típico del encargo de tratamiento es que un sujeto externo o ajeno al responsable del fichero va a tratar datos de carácter personal pertenecientes a los tratamientos efectuados por aquél con el objeto de prestarle un servicio en un ámbito concreto. Habría por tanto encargo de tratamiento en los supuestos de outsourcing o en los de prestación derivada de un contrato de obra o arrendamiento de servicios con un fin concreto. Siendo esencial, para no desnaturalizar la figura, que el encargado del tratamiento se limite a realizar el acto material de tratamiento encargado, y no siendo supuestos de encargo de tratamiento aquellos en los que el objeto del contrato fuese el ejercicio de una función o actividad independiente del encargado. En suma, existe encargo de tratamiento cuando la transmisión o cesión de los datos está amparada en la prestación de un servicio que el responsable del tratamiento recibe de una empresa externa o ajena a su propia organización, y que le ayuda en el cumplimiento de la finalidad del tratamiento de datos consentida por el afectado».*

relación con el ejercicio de derechos por los titulares de los datos personales objeto de tratamiento, en el contrato deberá precisarse si corresponde al encargado de tratamiento la atención a la respuesta a las solicitudes realizadas, o si éste debe proceder a comunicar al responsable el ejercicio de un determinado derecho. Asimismo, el encargado del tratamiento, conforme la previsión del art. 33.4 de la LOPDPGDD puede conservar los datos personales en estado de bloqueo en cuanto puedan derivarse responsabilidades para él por su relación con el responsable de tratamiento.

El aspecto relevante de la relación entre responsable y encargado de tratamiento radica en que es al primero a quien corresponde decidir sobre el uso de los datos y la finalidad a que se destinan, mientras que el encargado de tratamiento debe cumplir con las instrucciones dadas por el responsable, de manera que, conforme a las previsiones de los arts. 28.10 del RGPD y 33.2 de la LOPDPGDD será considerado como responsable y no como encargado quien, aun en el caso de que exista contrato con el encargo del tratamiento, utilice los datos personales para sus propias finalidades.

En el momento presente es habitual que los servicios de procesamiento o tratamiento de datos sean prestados por sociedades especializadas en la prestación de estos servicios y que, con frecuencia, los responsables de tratamiento los externalicen a través de la celebración de contratos de *outsourcing* con prestadores de servicios de *cloud computing*, *Software as a Service* (SaaS)[27], *Platform as a service* (PaaS)[28], o *Infraestructure as a Service* (IaaS)[29], cuya prestación comporta el tratamiento de datos personales por cuenta del responsable de tratamiento.

En particular, en el caso de los servicios de *cloud computing* resultarán relevantes, en orden a determinar el sujeto al que se impute la responsabilidad civil por daños derivados de un tratamiento ilícito de datos personales, las medidas técnicas y organizativas determinadas

[27] Se trata de un modelo de distribución de *software* en el que el soporte lógico y los datos que maneja se alojan en servidores de una entidad prestadora de servicios de tecnologías de información y comunicación (TIC). La empresa proveedora de servicios TIC se ocupa del servicio de mantenimiento, de la operación diaria y del soporte del software usado por el cliente. Ordinariamente el software puede ser consultado en cualquier computador, se encuentre presente en la empresa o no y la información, el procesamiento, los insumos, y los resultados de la lógica de negocio del software, están hospedados en la compañía de TIC.

[28] PaaS es un servicio que proporciona al cliente entorno de desarrollo e implementación completo en la nube, con recursos que permiten entregar todo, desde aplicaciones sencillas basadas en la nube hasta aplicaciones empresariales. Al igual que sucede en el caso de la IaaS, los servicios de PaaS incluyen infraestructura (servidores, almacenamiento y redes), pero también incluye middleware, herramientas de desarrollo, servicios de inteligencia empresarial (BI), sistemas de administración de bases de datos, etc. Los servicios de PaaS permiten evitar el gasto y la complejidad que suponen la compra y la administración de licencias de software, la infraestructura de aplicaciones, el middleware subyacente y las herramientas de desarrollo y otros recursos. El cliente administra las aplicaciones y los servicios que desarrolla y, generalmente, el proveedor de servicios en la nube administra todo lo demás.

[29] Se trata de un proveedor que alquila infraestructura informática y la ofrece como servicio en Internet. A estos efectos generalmente cuenta con centros de datos propios, donde se aloja el hardware necesario para ello, ocupándose de su administración y de su mantenimiento. Los proveedores de IaaS pueden garantizar a sus clientes el acceso a recursos de computación (procesador, memoria RAM, disco duro) y estructuras de red integradas (*routers*, cortafuegos y sistemas de seguridad y *backup*) en función de sus necesidades, pudiendo elegir los usuarios los recursos necesitan (servidores, *routers* y cortafuegos) así como la potencia o la capacidad que han de tener los diferentes elementos de red.

por el responsable del tratamiento de los datos personales a través del denominado documento de seguridad[30], sin perjuicio de la adicional obligación de informar a sus clientes de las medidas de seguridad que apliquen, de conformidad con las previsiones del art. 12.*bis*, apartados 2 y 5 de la LSSICE. La fuente de la obligación del prestador de servicios de *cloud computing* de incorporar medidas de seguridad es inherente a la propia naturaleza del contrato (en su condición de encargado del tratamiento de datos personales), al tiempo que se deriva de las obligaciones legales de privacidad propia de las normas reguladoras de la protección de datos[31].

El contrato de *cloud computing* debe identificar al responsable del fichero de datos personales, así como al encargado del tratamiento, incluyendo las medidas de seguridad que éste debe adoptar para cumplir con las exigencias del RGPD, de la LOPDPGDD y del Reglamento de la LOPD (que sigue vigente en cuanto no contravenga las previsiones de las dos normas anteriores), tratando de manera precisa los aspectos atinentes a las transferencias internacionales de datos de carácter personal, ya sea con destino a otros Estados de la UE, con un marco normativo de protección equiparable, ya sea a terceros Estados. Teniendo en cuenta esta última circunstancia, los proveedores de servicios de *cloud computing* deberían comunicar todas las ubicaciones físicas de sus centros de datos –incluidas las de los servidores en los que se realizan las copias de seguridad de los ficheros-, para poder determinar si existe una transferencia internacional de datos a terceros Estados no sometidos al RGPD. Las personas físicas que ceden sus datos personales deben conocer la localización física o geográfica de los centros de datos del encargado de tratamiento o prestador de servicios de esta naturaleza, con la finalidad de que puedan realizar restricciones a las transferencias de datos personales fuera del EEE; así como para garantizar la confidencialidad de los mismos[32].

Ha de tenerse en cuenta que, aplicando una regla general común a todos los supuestos en los que concurre la actuación de un profesional, en el caso del encargado de tratamiento de datos, comoquiera que tiene unos conocimientos específicos para el desempeño de sus funciones, así como de las reglas técnicas y organizativas que ha de aplicar, el estándar de diligencia que se le exige en el cumplimiento de aquellas es superior al exigido al responsable de tratamiento, como ha tenido ocasión de precisar, de manera reiterada, la jurisprudencia en materia de responsabilidad civil profesional[33], exigiendo la adecuación de la diligencia a las

[30] *Vid.,* entre otros, PUYOL MONTERO, J.: *Algunas consideraciones sobe Cloud Computing*, Ed. AEPD – BOE, Madrid, 2013, especialmente las pgs. 219 y ss.; DOMÍNGUEZ GARCÍA, Á.M.: *La contratación del Cloud Computing*, Ed. Aranzadi, Cizur Menor, 2019, especialmente las pgs. 210 a 214.

[31] ROSELLÓ RUBERT, F.Mª: *Cloud Computing. Régimen Jurídico para empresarios*, Ed. Aranzadi, Cizur Menor, 2018, pgs. 269 y 270; VALLE, L.; RUSSO, B.; BONZAGNI, D. y LOCATELLO, D.Mª: «Struttura dei contratti e trattamento dei dati personali nei servizi di *cloud computing* alla luce del nuovo reg. 2016/679 UE», *Contratto e impresa,* 1/2018, especialmente las pgs. 377 y 378 (§§.5 y 5.1)

[32] Procede recordar como en el año 2013, un número significativo de relevantes empresas tecnológicas (entre las que se encontraban, *v.gr.*, Microsoft, Apple, Facebook, Yahoo, Google, PalTalk, AOL, Skype o YouTube) reconocieron que permitieron al Gobierno de USA entrar en sus servidores, en los que almacenaban los datos personales recabados de sus clientes en todo el mundo, a través del programa de espionaje PRISM, al amparo de las previsiones de la *USA Patriot Act*, fundamentando esta medida en la investigación de actividades de terrorismo internacional.

[33] La culpa que permite imputar a un profesional la responsabilidad civil por un determinado resultado lesivo, en el marco de un sistema de responsabilidad civil subjetiva viene representada por una falta de diligencia o de previsión, habiendo sido definida adecuadamente como la infracción por parte del profesional de algún deber propio de su profesión y, más concretamente, del deber de actuar con la diligencia objetivamente exigida por la naturaleza del acto que se ejecuta, según las circunstancias de las personas, del tiempo y del lugar. La observancia

circunstancias de las personas, del tiempo y del lugar en que se desarrolla la conducta objeto de enjuiciamiento[34].

Por último, debe traerse a colación la posibilidad que contempla el art. 28.4 del RGPD, cual es la designación por parte del encargado del tratamiento de datos personales de un **subencargado** para realizar determinadas operaciones de tratamiento[35]. En los casos en los que se recurra a esta figura del subencargado, aquella norma establece que el encargado seguirá siendo responsable frente al responsable del tratamiento en relación con el cumplimiento de los deberes del subencargado, si bien no dice nada respecto de las consecuencias en la responsabilidad civil por daños frente al perjudicado y, en particular, acerca de la posibilidad del encargado del tratamiento de exonerarse de responsabilidad civil acreditando que la conducta infractora de la normativa causante de los daños y perjuicios cuyo resarcimiento se pretende es imputable exclusivamente al subencargado[36]. A mi juicio, la aplicación analógica de la regla que acoge el art. 82.4 del RGPD determina que, en estos supuestos y frente al perjudicado, el encargado de tratamiento responde junto con el subencargado, como garante que es de la licitud de las operaciones de tratamiento y de la indemnidad del titular de los datos personales objeto de tratamiento. El art. 26 del RGPD consagra la noción de corresponsabilidad de los responsables conjuntos del tratamiento de datos personales. En consecuencia, el sub-encargado, será responsable, de manera conjunta con el encargado y con el responsable de tratamiento. Por esta razón, se hace preciso prestar una especial atención a la redacción de las estipulaciones contractuales que vinculan, en las relaciones internas, a estos tres sujetos, definiendo claramente las funciones y las responsabilidades de cada uno de ellos.

de las reglas que rigen la actuación del profesional y que conforman su *«lex artis»* –integrada, en esencia, por los llamados *«protocolos»* de actuación- permite, en línea de principio, rechazar la calificación de negligente o imprudente del comportamiento del profesional. La llamada *«lex artis ad hoc»* se erige así como el criterio valorativo de la corrección del concreto acto realizado por el profesional. *Vid.*, entre otros en este sentido, YZQUIERDO TOLSADA, M.: *La responsabilidad civil del profesional liberal*, Ed. Reus, Madrid, 1989, pg. 206; DÍEZ-PICAZO, L.: *Fundamentos del Derecho civil patrimonial*, T. V (*La responsabilidad civil extracontractual*), Ed. Civitas, Cizur Menor, 2011, pg. 275; CARRASCO PERERA, Á.: *Derecho de contratos*, Ed. Aranzadi, Cizur Menor, 2017 (2ª edic.) pgs. 859-860 (§.18/29); ASÚA GONZÁLEZ, C.I.: «Comentario del art. 1104 del CC», en *Comentarios al Código Civil* (R. BERCOVITZ RODRÍGUEZ-CANO, DIR.), T. VI, Ed. Tirant lo Blanch, Valencia,2013, pg. 8092.

En efecto, el concepto de *«lex artis»* se configura como *«aquel criterio valorativo para calibrar la diligencia exigible en todo acto»* (FD 1º de la STS de 18 de diciembre de 2006 [RJ 2006\9172]). La *«lex artis ad hoc»* es la forma particular de tratar un caso concreto; sería la aplicación de las reglas y normas de actuación en un supuesto concreto y determinado (la personalización de cada acto del profesional). De esta manera, se toman en consideración las especiales características del profesional, de su posible especialización, de la complejidad y trascendencia del acto y todas las demás circunstancias objetivas y subjetivas concurrentes. El criterio es también compartido en la jurisprudencia penal, *v.gr.*, STS, Sala de lo Penal, 1187/1997, de 3 de octubre [RJ 1997\7169; Recurso de casación núm. 2326/1996]. En relación con la prestación de servicios médicos y sanitarios, puede verse, *v.gr.*, GARCÍA GARNICA, MªC.: *Aspectos básicos de la responsabilidad civil médica*, Ed. Aranzadi, Cizur Menor, 2010, pgs. 55 y ss.

[34] PEÑA LÓPEZ, F.: *La culpabilidad en la responsabilidad civil extracontractual*, Ed. Comares, Granada, 2002, pg. 458.

[35] A estos efectos, la AEPD considera adecuada tanto la autorización específica a una entidad concreta, como la realizada de manera genérica, permitiendo la subcontratación sin determinar la entidad respecto de la que se autoriza la subcontratación.

[36] VAN ALSENOY, B.: «Liability under EU Data Protection Law. From Directive 95/46 to the General Data Protection Regulation», *JIPITEC*, 2016 (3), pg. 286

4.3. Las relaciones jurídicas entre el responsable y el encargado de tratamiento y su incidencia en la imputación de la responsabilidad civil

En orden a determinar la responsabilidad civil (también la administrativa) del responsable y del encargado de tratamiento, el incumplimiento de las obligaciones que incumben al proveedor encargado del tratamiento (con frecuencia, un proveedor de servicios de esta naturaleza) puede amparar la imputación de responsabilidad al responsable del tratamiento que ha contratado sus servicios.

En efecto, el responsable del tratamiento tiene, entre otras, las obligaciones de contratar a proveedores de servicios de tratamiento de datos que ofrezcan garantías suficientes y de controlar su actividad, llegando a auditarlos en el caso de los proveedores críticos, de manera que el incumplimiento de la primera obligación permitirá la imputación de responsabilidad al responsable de tratamiento por *culpa in eligendo»*, mientras que el incumplimiento de la segunda amparará su imputación por mediar *culpa in vigilando»*[37]. De aquí se deriva también que, en el caso de que el encargado de tratamiento informe al responsable, con carácter previo, de un posible incumplimiento, éste ignore sus recomendaciones o no adopte las medidas técnicas posibles para evitarlo, la responsabilidad se imputará al responsable y no al encargado del tratamiento, en tanto aquél decida ignorar las advertencias o indicaciones del éste[38].

En la siguiente tabla se puede ver como podrían distribuirse las responsabilidades entre el responsable y el encargado del tratamiento en cada uno de los escenarios en los que puede surgir la responsabilidad civil frente al titular de los datos personales objeto de tratamiento:

Evento dañoso	Legitimación activa	Tipo de RC	Responsabilidad administrativa
	Responsable de tratamiento	RC contractual del encargado de tratamiento	Responsable y encargado de tratamiento

[37] Ha de tenerse en cuenta, a estos efectos, el contenido del Considerando 81 del RGPD, a tenor del cual, *«para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encarados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento. La adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable».*

En el sentido expresado en el texto, GIL MEMBRADO, C.: *Privacidad y turismo: perfil del turista,* big data *y plataformas colaborativas,* Ed. Reus, Madrid, 2019, pg. 88.

[38] En este sentido, para el caso del Derecho alemán, KLUG, C.: «Improving self-regulation through (law-based) Corporate Data Protection Officials», 2002, disponible en *https://www.gdd.de/international/english; y,* en el Derecho español, SANTAMARÍA RAMOS, F.J.: *El encargado independiente. Figura clave para un nuevo Derecho de protección de datos*, Ed. La Ley, Madrid, 2011, pg. 151

Brecha de seguridad: violación de confidencialidad, de integridad o de la disponibilidad	Interesados	RC extracontractual del encargado + RC contractual del responsable	
Incumplimiento del RGPD atendiendo a las instrucciones del responsable	Interesados	RC contractual o extracontractual del responsable	Responsable del tratamiento
Incumplimiento del RGPD mediando incumplimiento del responsable de tratamiento	Responsable de tratamiento	RC contractual del encargado de tratamiento	Responsable del tratamiento
	Interesados	RC extracontractual del encargado de tratamiento	

Tabla de distribución de responsabilidad civil y administrativa:
responsable de tratamiento / encargado de tratamiento

Con frecuencia, la acción indemnizatoria ejercitada por el interesado / perjudicado se dirigirá frente responsable del tratamiento en su condición de pasivamente legitimado siempre que exista entre ambos una relación contractual en el marco de la cual se haya realizado la cesión y el tratamiento de los datos personales de aquél, si bien, también en estos supuestos cabrá el ejercicio de una acción de responsabilidad civil extracontractual frente al encargado del tratamiento, excepción hecha de los supuestos en los que la infracción del RGPD se haya realizado mediando órdenes o instrucciones expresas dirigidas por el responsable al encargado de tratamiento en el marco de la relación contractual que les vincula.

En el marco de la relación contractual entre el responsable del tratamiento y el encargado del tratamiento tendrá cabida la repercusión de las indemnizaciones pagadas a los interesados por el responsable derivadas de conductas imputables al encargado de tratamiento. Es en este ámbito de la acción de regreso en el cobrarán virtualidad las limitaciones contractuales de responsabilidad que hayan podido pactar[39], así como, en su caso, las que puedan resultar de las limitaciones de cobertura del seguro de responsabilidad civil (o de ciberriesgos, que, a diferencia de los seguros de responsabilidad civil, suelen incluir la cobertura del riesgo derivado de las sanciones de la AEPD) concertado por el encargado de tratamiento[40]. Es posible que en estas situaciones el responsable del tratamiento se vea atrapado entre las reclamaciones de los interesados perjudicados por una actuación imputable al encargado del tratamiento y las limitaciones de responsabilidad contractuales eficaces en relación con el encargado de tratamiento (proveedor de servicios de tratamiento de datos) que ha incumplido el

[39] La limitación de responsabilidad civil por vía contractual puede ser de tres tipos: cuantitativa (establecida en una cantidad determinada o en el resultado de multiplicar el coste del servicio por una cifra), cualitativa (basada en la exclusión de unos supuestos determinados de responsabilidad) o indirecta (derivada del incumplimiento de otros requisitos o provocada de facto por la insolvencia del proveedor).

[40] Sobre esta cuestión, *vid.*, ELGUERO MERINO, J.Mª: «El seguro de responsabilidad civil por protección de datos personales», en *RRCyS*, núm. 28, 2008, pgs. 47 a 80; ORTEGA GIMÉNEZ, A.: «Tratamiento ilícito de los datos de carácter personal, contratos de seguro y Derecho internacional privado», *Revista Española de Seguros*, núm. 179, 2019, pgs. 225 a 254.

RGPD y que ha causado el perjuicio a los interesados; así como, en su caso, como consecuencia de la falta de solvencia patrimonial del encargado del tratamiento.

El análisis de la existencia y la dimensión de las tres barreras que pueden impedir la repercusión al encargado de tratamiento (límites convencionales o contractuales, límites en la cobertura del seguro y límites derivados de su situación de solvencia patrimonial) de las cantidades pagadas a los interesados en concepto de indemnización por daños y perjuicios, debe hacerse en la fase de selección y homologación de los prestadores de estos servicios**,** es decir, en la fase previa a la contratación. Estadísticamente se ha constatado un elevado nivel de responsabilidad de los encargados de tratamiento en las brechas de seguridad y en las infracciones del RGPD que se han producido hasta el momento, de donde resulta que los responsables del tratamiento deben revisar su metodología de selección, homologación, contratación y control continuado de los proveedores que traten datos personales, con el fin de introducir medidas que permitan una distribución adecuada de las responsabilidades (civiles y administrativas). Estas medidas deben incluir una revisión del contrato, de la cobertura del seguro y de la solvencia del proveedor, con el fin de identificar, gestionar y tener en cuenta, en el proceso de toma de decisiones a aplicar en la fase de selección, las limitaciones que puedan existir a la responsabilidad civil del proveedor de servicios de tratamiento de datos personales.

4.4. El delegado de protección de datos

El delegado de protección de datos –o DPO, *Data protection officer»*- está contemplado en los arts. 37, 38 y 39 del RGPD. En algunas ocasiones, previstas en el citado art. 37, el RGPD impone su designación por el responsable y por el encargado del tratamiento (*v.gr.*, tratamiento a gran escala, regular y sistemático e datos personales concernientes a datos sensibles[41]; y, en todo caso, cuando el tratamiento de datos es realizado por una administración

[41] El concepto de tratamiento *«habitual y sistemático»* no ha sido objeto de definición por el RGPD. En sus directrices, el Grupo del artículo 29 ha dado su interpretación de los términos *«regular»* y *«sistemático».* A tenor de estas directrices, *«regular»* remite a un acto que sea bien *«continuo o que se produzca a intervalos regulares durante un determinado periodo temporal»,* bien *«recurrente o que se repita en momento fijos»,* bien que *«tenga lugar de manera constante o periódica».* El término *«sistemático»* remite a un acto que se produce de conformidad con un sistema preestablecido, organizado o metódico; o, en su caso, que tenga lugar en el marco de un programa general de recogida de datos personales o que haya sido efectuado en el marco de una estrategia previamente definida. Asimismo, en las referidas directrices el Grupo del artículo 29 ofrece algunos ejemplos de actividades de tratamiento que implican la existencia de un tratamiento habitual y sistemático. Son los casos, *v.gr.*, de explotación de una red de telecomunicaciones, de suministro de servicios de telecomunicaciones, de prestación de servicios de correo electrónico, de actividades de marketing realizados sobre datos personales, de creación de perfiles con la finalidad de evaluar riesgos, actividades de geolocalización, de publicidad en atención a determinados comportamientos de mercado o de supervisión de datos sobre el bienestar, etc.

El art. 37 del RGPD prevé que la designación de un DPO es obligatoria cuando las actividades del responsable de tratamiento consisten en el tratamiento a gran escala de datos sensibles, relativos a condenas penales o a infracciones; si bien tampoco, en este caso, ofrece un concepto preciso de *«tratamiento a gran escala».* El Considerando 91 del RGPD nos ofrece algunas pistas que nos permiten identificar la existencia de un tratamiento a gran escala, que serían aquéllos que pretenda el tratamiento de un volumen considerable de datos de carácter personal a nivel regional, nacional o supranacional, que puedan afectar a un número considerable de personas. En sus líneas directrices, el Grupo del artículo 29 precisa cuatro factores que pueden ser tomados en consideración en orden a determinar si nos encontramos ante un tratamiento a gran escala: el número de

o autoridad pública, excepción hecha de los órganos jurisdiccionales), sin perjuicio de su recomendación general con la finalidad de facilitar que los responsables y los encargados de tratamiento puedan cumplir con las normas reguladoras[42]. En esencia, el delegado de protección de datos tiene las funciones de información, de consejo y de control interno, en orden a asegurar la seguridad jurídica del tratamiento de los datos personales, al tiempo que puede actuar como interlocutor adecuado con las autoridades nacionales administrativas supervisoras (como es el caso, en España, de la AEPD), así como con las personas cuyos datos personales hayan sido objeto de tratamiento, en orden al ejercicio de los derechos que las normas les atribuyen. Esta obligación de designar un DPO que resulta de las previsiones del art. 37 del RGPD supone una evolución del anterior sistema que preveía una declaración a la autoridad nacional de supervisión de protección de datos que debía contener informaciones similares, así como la facultad que tenían los responsables de tratamiento de designar un responsable del fichero de datos cuyas funciones eran próximas a las propias del actual DPO.

El delegado de protección de datos puede ser un miembro de la propia organización responsable de tratamiento (personal interno o dependiente en régimen laboral –con frecuencia, el elegido es una persona integrante de la dirección de los sistemas informáticos o del departamento jurídico-) o un tercero ajeno a la misma, vinculado con un contrato de prestación de servicios, permitiendo el art. 35 de la LOPDPGDD que esta designación recaiga en una persona jurídica, mientras que el RGPD alude exclusivamente a profesionales individuales (Considerando 97). El RGPD precisa que la designación de éste debe hacerse en atención a las cualidades profesionales del designado y, en particular, de sus conocimientos especializados en Derecho y prácticos en materia de protección de datos –lo que exige tanto conocimientos estrictamente jurídico, como técnicos-, así como en su capacidad para realizar sus funciones, entre las que se encuentra la cooperación con la autoridad de control, la información y el consejo al responsable del fichero y al encargado del tratamiento, así como verificar el control del cumplimiento de las previsiones del propio RGPD. El art. 37.1 de la LOPDPGDD prevé que los afectados por el tratamiento ilícito de sus datos personales puedan, de manera voluntaria, dirigirse al delegado de protección de datos con la finalidad de solucionar, de manera amistosa, la controversia surgida, antes de dirigirse a la autoridad de control.

personas afectadas –tanto en valor absoluto, como en valor relativo en relación a la población afectada-, el volumen de datos o el espectro de datos objeto de tratamiento, la duración o la permanencia de las actividades de tratamiento de datos; así como la extensión geográfica de la actividad de tratamiento.

Tomando en consideración las consideraciones precedentes y el carácter genérico de las expresiones «tratamiento a gran escala» y tratamiento «habitual y sistemático», no es sencillo determinar con certeza si un responsable de tratamiento está, o no, obligado a designar un delegado de protección de datos. La ausencia de designación en el caso de que concurra la obligación se sanciona con una multa administrativa que puede ascender a la suma de diez millones de euros o al 2% de la cifra de negocio. En esta situación, como medida de prevención y con el fin de evitar una posible sanción de este importe, en el caso de que existan dudas, debe procederse a la designación del DPO.

[42] Sobre la figura del delegado de protección de datos puede verse el estudio realizado por el Grupo de Trabajo del artículo 29 sobre protección de datos, titulado «Directrices sobre los delegados de la protección de datos (DPD)» de 13 de diciembre de 2016, disponible en *https://www.aepd.es/media/criterios/wp243rev01-es.pdf.* En España, durante el primer año de vigencia de la LOPDPGDD se ha notificado a la AEPD la designación de casi 50.000 Delegados de Protección de Datos, de los cuales aproximadamente 43.000 lo fueron en el sector privado y más de 6.000 en el sector público.

Teniendo en cuenta las atribuciones y funciones que las normas atribuyen a los delegados de protección de datos, obvio resulta que pueden causar o contribuir, con su comportamiento, a causar daños vinculados a un tratamiento ilícito de datos personales, si bien el art. 82 del RGPD no los menciona, de manera expresa, como posibles legitimados pasivos en la acción indemnizatoria. La ausencia de esta previsión ampara dos interpretaciones:

1ª) La responsabilidad civil recae exclusivamente en el responsable y en el encargado del tratamiento y no en el delegado de protección de datos, que no es más que un dependiente o un auxiliar en el cumplimento de las obligaciones legales que incumben a aquéllos, quienes responderán de los hechos de los delegados de protección de datos frente a los perjudicados, de conformidad con las previsiones del art. 1903 del CC. Sin embargo, existen notas propias de la configuración normativa de las funciones del delegado de protección de datos que permiten cuestionar la concurrencia de la relación de dependencia y subordinación a las instrucciones del principal que constituye el substrato de la previsión del art. 1903.IV del CC y ello por cuanto el art. 39.3 del RGPD establece que el responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción sobre el desempeño de sus funciones; a tiempo que, a tenor de lo dispuesto en el art. 36.2 de la LOPDPGDD, el delegado de protección de datos no podrá ser destituido, ni sancionado por desempeñar sus funciones, salvo en casos de dolo o de culpa grave.

2ª) La responsabilidad civil de los delegados de protección de datos frente a terceros se rige de conformidad con las previsiones generales del art. 1902 del CC, siendo compatibles las acciones indemnizatorias que, con fundamento en las previsiones del art. 82 del RGPD se ejerciten frente a los responsables de los ficheros y frente a los encargados de tratamiento, con las ejercitadas con fundamento en las reglas generales de la responsabilidad civil extracontractual frente al delegado de protección de datos que, responderá de conformidad con un criterio subjetivo de imputación, exigiéndosele una diligencia propia de un profesional, a tenor de las condiciones que el propio RGPD exige para su designación.

4.5. El representante en la UE del responsable o del encargado de tratamiento

A tenor de la previsión del art. 27 del RGPD, los responsables o encargados de tratamiento no establecidos en un Estado de la UE que estén llevando a cabo determinados tratamientos de datos personales de personas que residan en la UE y cuyas actividades de tratamiento estén relacionadas con la oferta de bienes o servicios a estos sujetos, están obligados a designar a un representante en la UE. El art. 27.5 del RGPD establece que *la designación de un representante por el responsable o encargado del tratamiento se entenderá sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable o encargado».* A su vez, para el caso de representantes en la UE domiciliados en territorio español, el art. 30.2 de la LOPDPGDD prescribe que en caso de exigencia de responsabilidad civil al amparo de lo dispuesto en el art. 82 del RGPD, *los responsables, encargados y representantes responderán solidariamente de los daños y perjuicios causados».*

Así las cosas, el perjudicado que resida en España y que pretenda ejercitar una acción indemnizatoria o resarcitoria de daños o perjuicios causados por un tratamiento ilícito de datos personales, podrá ejercitar la acción frente al representante en España del responsable o

del encargado de tratamiento, sometiéndose la acción al Derecho español y al conocimiento de los órganos jurisdiccionales españoles.

4.6. Responsables y encargados de tratamiento que sean autoridades o Administraciones Públicas

En el caso de que el responsable o el encargado de tratamiento de los datos personales sean personas jurídicas públicas o autoridades públicas, resultan también de aplicación las previsiones del RGPD y ello a tenor de las definiciones que de *responsable de tratamiento»* y de *encargado del tratamiento»* se contienen en su art. 4, incluyendo a las personas físicas y jurídicas y, expresamente a la *autoridad pública, servicio u otro organismo»* que, en el primer caso, sólo o junto con otros determine los fines y medios del tratamiento y, en el segundo, trate datos personales por cuenta del responsable del tratamiento. Lo que sí se excluye de su ámbito objetivo de aplicación es el tratamiento de datos personales *por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas de la seguridad pública y su prevención»* (art. 2, letra *d),* del RGPD).

Consecuencia de la referida extensión subjetiva del ámbito de aplicación del RGPD a las Administraciones y autoridades púbicas es que en aquellos casos en los que el responsable o el encargado del tratamiento de datos personales tengan esta naturaleza, con independencia de la tesis que se asuma en relación con la naturaleza, subjetiva u objetiva de la responsabilidad imputable a los referidos sujetos con fundamento en el art. 82 del RGPD, se les aplicará este régimen de responsabilidad civil, en detrimento del régimen de responsabilidad civil de naturaleza objetiva que resulta de lo dispuesto en los arts. 32 a 37 de la LRJSP/2015[43], sin perjuicio de que, en estos supuestos, corresponda su conocimiento a los órganos de la jurisdicción contencioso-administrativa (*ex* arts. 9.4 de la LOPJ y 2.*e)* de la LJCA). De los referidos preceptos de la LRJSP lo que sí resulta es que, si el encargado de tratamiento es una persona al servicio de una Administración Pública, en el sentido amplio que resulta del art. 36 de la LRJSP, la acción indemnizatoria deberá dirigirse directamente frente a la Administración Pública al servicio de la cual realizan las labores propias de encargados del tratamiento.

5 SUPUESTOS DE PLURALIDAD DE RESPONSABLES

[43] En este mismo sentido se pronunció NIETO GARRIDO, E.: «Derecho a indemnización y responsabilidad», en *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (J.L. PIÑAR MAÑAS, DIR.), Ed. Reus, Madrid, 2016, pg. 561. Frente a este parecer, LÓPEZ ÁLVAREZ sostiene que el art. 106.2 de la CE impone que, en el caso de daños o perjuicios imputables a la actuación de una Administración Púbica, el régimen de responsabilidad civil es el propio de la objetiva, de manera que el ajuste de la conducta al RGPD no impedirá que surja el deber de indemnizar, bastando con demostrar que la causa del daño ha sido el funcionamiento o la actuación de la Administración Pública, que el daño es evaluable económicamente y que el interesado no tiene la obligación jurídica de sopórtalo. *Vid.* LÓPEZ ÁLVAREZ, L.F.: «XVII. La responsabilidad del responsable», en *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (J.L. PIÑAR MAÑAS, DIR.), Ed. Reus, Madrid, 2016, pg. 281.

El apartado 4 del art. 82 del RGPD da una respuesta expresa a la cuestión suscitada en los casos de concurrencia de pluralidad de responsables del hecho dañoso –sean de una misma o de distinta categoría-, estableciendo el régimen de solidaridad entre todos los ellos[44], y lo hace en los siguientes términos: *cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado de tratamiento hayan participado en la misma operación de tratamiento y sean, con arreglo a los apartados 2 y 3, responsables de cualquier daño o perjuicio causado por dicho tratamiento, cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado».*

Sin perjuicio de la previsión de esta regla general, el RGPD ampara que los Estados miembros puedan establecer que, en el caso de que resulte posible acreditar la contribución causal de cada sujeto a la producción del daño, se pueda prorratear la indemnización a cuyo pago venga obligado cada uno de ellos; si bien esta norma no existe en el Derecho español.

En consecuencia, la solidaridad se aplica tanto en los supuestos de actuaciones lesivas en las que hayan participado de manera simultánea o sucesiva un responsable y un encargado de tratamiento o hayan participado varios responsables[45] y/o varios encargados de tratamiento, siempre que tratemos de la imputación y del resarcimiento de daños derivados de una misma operación de tratamiento[46]. El hecho de que la pluralidad de sujetos intervinientes conlleve la diversificación de funciones entre ellos (*v.gr.*, uno decide sobre el tratamiento que deben recibir los datos y el otro el nivel de seguridad que ha de adoptarse) no justifica la exoneración de responsabilidad de alguno de ellos, lo que resulta acorde con el hecho de que se trate de un pacto no oponible a terceros (*ex* art. 1257 del CC) y posiblemente contrario al orden público que, como sabemos, es un límite a la autonomía privada (*ex* art. 1255 del CC)[47]. Esta conclusión no puede ser discutida si pensamos en un régimen de responsabilidad civil objetiva, si bien sería acreedora de alguna precisión en un régimen subjetivo de imputación.

En todo caso y a pesar de su origen legal, se trata de una solidaridad *impropia,* en tanto que no trae causa de una previsión contractual previa a la infracción de las normas de protección de datos personales y a la propia generación del daño resarcible. Este carácter tiene una única consecuencia jurídica relevante a tenor de la doctrina jurisprudencial: el art. 1974 del

[44] La responsabilidad de naturaleza solidaria para los supuestos de pluralidad de responsables y/o de encargados del tratamiento se ha postulado en el régimen resultante de la derogada LOPDP, de conformidad con el criterio jurisprudencial mayoritario en el ámbito de la responsabilidad extracontractual, por GARCÍA RUBIO, Mª P.: «Bases de datos y confidencialidad en Internet», en *El comercio electrónico* (J. A. ECHEBARRÍA SÁENZ, COORD.), EDISOFER, S.L., Madrid, 2001, pg. 487.

[45] El art. 26 del RGPD contempla el supuesto de corresponsables del tratamiento de datos, estableciendo, en su apartado 1º, la regla general conforme a la cual *«cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento».*

[46] Sobre el concepto de misma operación de tratamiento resulta relevante la STJUE de 5 de junio de 2018 (asunto C-210/16; Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein *vs.* Wirtschaftsakademie Schleswig-Holstein GmbH, con intervención de Facebook Ireland Ltd. y Vertreter des Bundesinteresses beim Bundesverwaltungsgericht).

[47] GRIMALT SERVERA, P.: *La responsabilidad civil en el tratamiento automatizado de datos personales*, *op. cit.*, pág. 121.

CC no se aplica en caso de solidaridad impropia cuando la prescripción de la acción se interrumpió frente a uno(s), pero no frente a otro(s) de los deudores solidarios (así, *v.gr.*, SSTS de 17 de septiembre de 2015 [RJ 2015, 4004, 4005 y 4006])[48].

Una vez que alguno de los sujetos responsables solidarios frente al perjudicado proceda a hacer frente al pago de la indemnización, en la relación interna entre los coobligados solidarios procederá el ejercicio de la acción de reembolso, de regreso o de reintegro, de conformidad con las previsiones el art. 1145 del CC[49]. Es esta la acción del Derecho nacional a cuya aplicación remite el art. 82.5 del RGPD, a tenor del cual, el corresponsable que procediera al pago de la indemnización contará con una acción de repetición frente al resto de corresponsables del daño.

6 PRESUPUESTO OBJETIVO: INFRACCIÓN DE LAS NORMAS QUE REGULAN EL TRATAMIENTO DE DATOS PERSONALES (LA CONDUCTA ANTIJURÍDICA)

Como ya he señalado, el nacimiento de una responsabilidad civil a cargo del responsable de los datos personales o del encargado de su tratamiento requiere, en los términos del art. 82.1 del RGPD que concurra una actuación que sea susceptible de ser calificada como una infracción de las previsiones del propio RGDP, si bien no será necesario, de conformidad con lo que se expone y argumenta *infra* §.11, que exista una previa declaración, calificación o condena de la conducta infractora por parte de la autoridad administrativa supervisora del cumplimiento de la normativa de protección de datos personales. Sin embargo, a pesar de la literalidad del precepto, la conducta que hace surgir la responsabilidad que nos ocupa también puede consistir en una infracción de otras normas reguladoras de la tutela de los datos personales -y de los derechos subjetivos que pueden resultar lesionados como consecuencia de aquella infracción (intimidad o privacidad, honor, imagen de solvencia patrimonial, *goodwill*, etc.)- y, en particular, de la LOPDPGDD. A estos efectos, es pertinente tomar en consideración que el Considerando 146 del RGPD explica que un tratamiento en infracción del presente Reglamento también incluye aquel tratamiento que infringe actos delegados y de ejecución, contemplados en sus arts. 92 y 93, adoptados de conformidad con el mismo y el Derecho de los Estados miembros que especifique las normas del propio RGPD[50]. Por otra parte, es sabido que, en el ámbito de la responsabilidad civil por prestación de servicios, con carácter general, la inobservancia por el prestador de las normas de seguridad aplicables a la actividad o servicios, de conformidad con las previsiones legales o reglamentarias, que tenga influencia causal en la producción del daño determina que la responsabilidad deba imputarse al prestador, por

[48] En este sentido, *vid.*, entre otros, CARRASCO PERERA, Á.: «Responsabilidad civil solidaria de los miembros de un cártel», *Revista Doctrinal Aranzadi Civil-Mercantil,* núm. 1/2018, §.IV [BIB 2017\43639].

[49] En este sentido, RUBÍ PUIG, A.: «Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD», *op. cit.*, pg. 69; quien cita la aplicación de una norma similar del BGB (el §.426) en el caso del Derecho alemán, fundando su aplicación en el parecer expresado por FRENZEL, E.M.: «DS-GVO Artikel 82. Haftung und Recht auf Schaenersatz», en *Datenschutz-Grundveordnung: DS-GVO* (PAAL, B. y PAULY, D.; Eds.), C.H. Beck, Munich, 2017.

[50] En este sentido se expresa, *v.gr.*, RUBÍ PUIG, A.: «Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD», *op. cit.*, pg. 58.

más que el perjudicado conociese la posibilidad de acaecimiento del daño como riesgo propio del servicio cuya prestación ha demandado[51].

Comoquiera que la prueba de la concurrencia de una infracción de las normas reguladoras del tratamiento de datos personales y de los derechos de sus titulares recae sobre el actor perjudicado, reviste una especial relevancia la atribución de la carga de la prueba y la forma de probar el referido incumplimiento, así como las circunstancias que puede alegar el responsable o el encargado del tratamiento frente a los que se dirija la acción indemnizatoria. En este escenario alcanza una especial relevancia la precisión que resulta del Considerado 81 el RGPD a tenor del cual la adhesión del encargado a un código de conducta aprobado, o a un mecanismo de certificación aprobado, puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable o de encargado de tratamiento.

El hecho de que los responsables y los encargados de tratamiento dispongan de protocolos de buenas prácticas certificados o se hayan adherido a un mecanismo o instrumento de certificación aprobado y su efectiva implantación en su organización limita los riesgos de vulneración de los derechos de los titulares de datos personales objeto de tratamiento, sin perjuicio de que, aun en estos supuestos, la vulneración resulta posible. En este último caso la cuestión que surge es la atinente a la forma adecuada de actuar por parte del responsable y del encargado de tratamiento en los casos de vulneración de las normas de tratamiento de datos personales. En estos casos, de existencia de vulneración, *v.gr.*, imputable a la actuación de un tercero que provoca el acceso o la divulgación no autorizada de los datos personales objeto de tratamiento, ante la alteración de los mismos, el responsable del tratamiento está obligado a notificar los hechos a la autoridad de control competente, así como a los interesados afectados. Se deben notificar las incidencias de seguridad que impliquen una violación de datos personales sin demora injustificada y, de ser posible, antes de que transcurran 72 hs. desde que se haya tenido constancia del ataque o de la vulneración de la seguridad de los sistemas informáticos de la sociedad que alberguen datos personales (de trabajadores, proveedores, clientes, etc.). En efecto, en el momento actual todos los responsables y encargados de tratamiento que hayan sufrido una brecha de seguridad, independientemente del sector al que pertenezcan, se encuentran obligadas a realizar una notificación expresa a la AEPD sin demora, en un plazo máximo de 72 horas siempre que sea posible. La notificación dirigida a la AEPD (que se realizará por el responsable o por el encargado del tratamiento de datos personales, utilizando el certificado electrónico, a través de la sede electrónica de la AEPD), deberá incluir las siguientes circunstancias: *(i)* naturaleza del incidente; *(ii)* identidad y datos de contacto del delegado de protección de datos de la sociedad; *(iii)* consecuencias del incidente; y *(iv)* medidas correctoras propuestas o adoptadas. Una vez transcurrido el plazo de las referidas 72 hs., y en caso de que no hubiera realizado la notificación, se deberá notificar asimismo a la AEPD las causas de la dilación o del retraso. El incumplimiento de la obligación de notificar las violaciones de seguridad que afecten a datos personales objeto de tratamiento, por parte del responsable del tratamiento se considera como infracción grave y puede ser sancionada con multas administrativas, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior. Adicionalmente es necesario que ante el descubrimiento de un ataque informático se proceda a la denuncia del hecho ante la

[51] En este sentido, expresamente, PASQUAU LIAÑO, M.: «Capítulo 2: El defecto de seguridad como criterio de imputación de responsabilidad al empresario de servicios», en *La responsabilidad civil por daños causados por servicios defectuosos* (A. ORTI VALLEJO y Mª C. GARCÍA GARNICA, DIRS.), Ed. Aranzadi, Cizur Menor, 2015 (2ª edic.), pg. 116

Policía Nacional, la Guardia Civil o el Juzgado de Guardia. Lo recomendable es interponer la denuncia, por el responsable de tratamiento de datos de la empresa o por un administrador o apoderado de la misma ante la Policía Nacional, para que proceda a la investigación y averiguación del origen de la actuación lesiva imputable a un tercero (con frecuencia estaremos en presencia de un ataque cibernético)[52].

En el caso de incumplimiento de estos protocolos de actuación, el responsable o, en su caso, el encargado de tratamiento no solo incurrirán en una actuación susceptible de sanción al estar tipificada como una infracción administrativa, sino que también constituirá el substrato de hecho adecuado para la imputación de responsabilidad civil en el caso de que la lesión aun imputable a un tercero, haya generado daños y perjuicios a los titulares de datos personales cuyos derechos hayan sido vulnerados.

7 LA NATURALEZA JURÍDICA DE LA RESPONSABILIDAD CIVIL: LOS SUPUESTOS DE EXENCIÓN DE RESPONSABILIDAD CIVIL DE LOS RESPONSABLES Y DE LOS ENCARGADOS DE TRATAMIENTO

La doctrina no es uniforme en orden a la calificación de la naturaleza jurídica de la responsabilidad civil imputable a los responsables y a los encargados de tratamiento de datos personales derivada de ilícitos dañosos realizados en el ejercicio de estas actividades. Las discrepancias en su calificación afectan tanto a la naturaleza contractual o extracontractual de la misma, como al criterio de imputación que se establece y, en consecuencia, a su calificación como una responsabilidad objetiva o subjetiva lo que, a su vez, como es conocido, está indisolublemente vinculado a las causas de exoneración de responsabilidad civil que los agentes del daño pueden invocar eficazmente.

7.1. La naturaleza extracontractual de la responsabilidad civil del responsable y del encargado de tratamiento

En cuanto a la primera de las cuestiones enunciadas en el párrafo que abre este epígrafe, la doctrina mayoritaria considera que se trata de un supuesto de responsabilidad civil extracontractual[53]. Frente a esta opinión, se ha preconizado por alguna autora la consideración de la responsabilidad civil *ex* art. 19.1 de la LOPDCP como contractual y ello por cuanto

[52] Actualmente tanto la Guardia Civil con el Grupo de Delitos Telemáticos y la Policía Nacional con la Brigada de Investigación Tecnológica perteneciente a la UDEF, disponen de equipos de trabajo, especialmente formados para la investigación de estos ciberdelitos (disponen de grupos de trabajo que investigan y focalizan su trabajo, únicamente a delitos informáticos cometidos en el seno de empresas). Sin perjuicio del resultado de la investigación por estas unidades especializadas de la Policía Nacional o de la Guardia Civil, resulta conveniente formalizar la denuncia para tener constancia de la reacción adecuada de la sociedad que ha recibido el ataque, también para el caso de que, en el futuro, se descubra que se han vulnerado normas o pactos de confidencialidad con terceros o se hayan revelado secretos empresariales o datos protegidos (distintos de datos personales).

[53] En este sentido, sobre el texto de la derogada LORTAD se pronunciaban expresamente, ORTÍ VALLEJO, A.: *Derecho a la intimidad e informática (Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada)*, Ed. Comares, Granada, 1994, pg. 170;

surge del incumplimiento de obligaciones legales previas que recaen sobre el responsable del tratamiento de datos personales, sin perjuicio de la aplicación preferente de las previsiones contenidas en la Ley Orgánica 1/1982, cuando haya sido infringido uno de los derechos fundamentales a cuya tutela se preordena esta Ley, respecto de la que aquélla es subsidiaria[54]. Obviamente la cuestión no resulta baladí o una mera disquisición dogmática, pues la asunción de una u otra naturaleza conlleva la aplicación de regímenes jurídicos diversos.

A mi juicio, no parece que pueda darse una respuesta universalmente válida para todos los supuestos, pues la naturaleza contractual o no de la acción ejercitada con fundamento en el precepto que nos ocupa dependerá de la existencia o no de una relación contractual entre el titular de los datos personales y el responsable del tratamiento, con fundamento o al amparo de la cual se hayan cedido los datos personales al referido responsable[55], de forma tal que al margen de estos supuestos –en los que las obligaciones del responsable del fichero o del encargado del tratamiento han de integrarse, además y *ex* art. 1258 del CC, con las obligaciones legales y reglamentarias previstas- la acción de responsabilidad civil, en tanto que la obligación incumplida se mueve al margen de la órbita de lo pactado, derivándose de una previsión legal, habrá de ser calificada como extracontractual y por lo tanto sometida al conocido plazo prescriptivo anual (*ex* art. 1968.2º del CC), excepción hecha de aquellos casos en los que la acción se ejercite en orden a la protección del derecho al honor, a la intimidad personal o familiar o la propia imagen, en cuyo caso se aplicará el plazo de caducidad de cuatro años establecido en el art. 9.5 de la Ley Orgánica 1/1982.

7.2. Naturaleza subjetiva de la responsabilidad civil del responsable y del encargado de tratamiento

7.2.1. La naturaleza de la responsabilidad civil en la LOPDCP

La cuestión atinente a la naturaleza objetiva o subjetiva de la responsabilidad civil del responsable o del encargado del tratamiento de datos personales ha recibido tres respuestas diversas en la doctrina que se ocupó del estudio del art. 19 de la derogada LOPDCP. La redacción del art. 19.1 de la LOPDCP permitía considerar que, en cuanto concurriese el incumplimiento de las previsiones normativas, el comportamiento del responsable del fichero o del tratamiento de datos habría de de ser calificado como *negligente* y, en consecuencia, nos encontraríamos ante un régimen de responsabilidad civil subjetivo, de manera que el responsable no respondería de los daños imputables a supuestos de caso fortuito o de fuerza mayor y el interesado que hubiese resultado perjudicado habría de probar el dolo o la culpa en que haya

HEREDERO HIGUERAS, M.: *La Ley Orgánica 5/1992, de regulación de tratamiento automatizado de datos personales*, Ed. Tecnos, Madrid, 1996, pg. 140. Este parecer fue compartido bajo la vigencia de la LOPDCP, entre otros, por APARICIO SALOM, J.: *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal,* Ed. Aranzadi, Cizur Menor, 2002 (2ª edic.), pg. 167.

[54] En este sentido se pronunció GARCÍA RUBIO, Mª P.: «Bases de datos y confidencialidad en Internet», *op. cit.*, pg. 487.

[55] En este sentido, BUTTARELLI, G.: *Banche dati e tutela della riservatezza (La* privacy *nella Società dell'Informazione)*, Giuffrè Editore, Milán, 1997, pgs. 351 y 352.

incurrido el responsable del fichero o el encargado del tratamiento[56]. En todo caso, el incumplimiento habría de ser probado por el perjudicado demandante de conformidad con las reglas generales que rigen la distribución de la carga de la prueba en el proceso civil (*ex* art. 217.2 de la LECiv). En este contexto normativo militaba también a favor de la calificación de la responsabilidad civil por infracción de la normas de protección de datos personales como un supuesto de responsabilidad civil subjetiva la toma en consideración de la norma que constituye, en este ámbito, el Derecho común, cual es la contenida en el art. 1902 del CC[57], de forma tal que, en defecto de previsión expresa de un título de imputación distinto de la culpa –o de que la actividad se realice un ámbito en el que pueda inducirse del sistema de responsabilidad civil que nos encontramos ante la posibilidad de imputación por riesgo[58]-, ha de considerarse la aplicación de éste. Algunos autores, interpretando el precepto que nos ocupa, escindieron la naturaleza de la responsabilidad civil aplicable en estos supuestos en dos hipótesis distintas[59]: **1ª)** Supuestos en los que el daño cuyo resarcimiento se pretende trae causa del incumplimiento por el responsable o por el encargado del tratamiento de datos personales de su obligación de seguridad –*v.gr.*, casos de pérdida, de tratamiento y de cesión no autorizada de datos personales-. En estos casos, el responsable o el encargado del tratamiento respondería en virtud de un régimen subjetivo de responsabilidad con inversión de la carga de la prueba de la culpa, pudiendo exonerarse de responsabilidad civil mediante la prueba de su actuación diligente. **2ª)** En el resto de los supuestos, la responsabilidad civil aplicable sería de naturaleza objetiva: casos de recogida irregular de datos personales, de tratamiento sin el consentimiento del interesado, de aplicación del fichero o del tratamiento a una finalidad distinta de aquélla par la que ha obtenido el consentimiento, de no cancelación una vez alcanzada la finalidad prevista, de alta de actualización o de puesta al día de los datos –con infracción del derecho a la calidad de los datos de que es titular el interesado- y casos de cesión de datos no autorizada.

Frente a ambos pareceres, en la doctrina se ha sostenido, con apoyo en las discusiones habidas durante su tramitación y con el relevante argumento derivado de la interpretación de

[56] En este sentido se pronunció de manera expresa, VEGA VEGA, J.A.: *Contratos electrónicos y protección de los consumidores*, Ed. Reus, S.A., Madrid, 2005, pg. 380.

[57] *Vid.* REGLERO CAMPOS, L. F.: «Los sistemas de responsabilidad civil», Capítulo II del *Tratado de responsabilidad civil* (L.F. REGLERO CAMPOS y J.M. BUSTO LAGO COORDS.), *op. cit.* (4ª edic.), pgs. 296 a 301; PEÑA LÓPEZ, F.: *La culpabilidad en la responsabilidad civil extracontractual*, *op. cit.*, pgs. 191 a 196.

[58] El criterio de imputación por riesgo –empresarial, en particular- no puede calificarse como un criterio excepcional de imputación de la responsabilidad civil en el Derecho español –y, en particular, contrapuesto al criterio común de la culpa- (y aquí se pone de manifiesto de manera nítida los problemas que genera la ausencia de una cláusula general en el ámbito de la responsabilidad civil por actividades empresariales que suponen un incremento del riesgo). En efecto, coexiste en el interior del sistema del Derecho de daños la dicotomía: culpa y riesgo; resultando imperiosa, desde la perspectiva práctica, la necesidad de adoptar determinadas decisiones empresariales y de naturaleza tanto económica, como jurídica, de reducir a la unidad las hipótesis en la que no opera el criterio de la culpa, sino el del riesgo y, en este último caso, cuáles son las circunstancias cuya prueba permite al empresario o profesional exonerarse de la atribución de los daños y perjuicios que pretenden ponerse a su cargo. Se trata, en definitiva, de acotar la naturaleza y el ámbito objetivo de lo que algunos autores -JAMES, KESSLER y PROSSER- han llamado la responsabilidad de la empresa, para referirse a estos supuestos de imputación de la responsabilidad en atención al riesgo empresarial, cuyo antecedente comparado ha de situarse en la adopción de la Sección 402ª del *Restatement of Torts* (Segundo) por el *American Law Institute*. Sobre estas cuestiones, *vid.* ÁLVAREZ LATA, N.: *Riesgo empresarial y responsabilidad civil* (Prólogo de J.M. BUSTO LAGO), Ed. Reus, Madrid, 2014.

[59] En este sentido se ha pronunciado ORTÍ VALLEJO, A.: *Derecho a la intimidad e informática, op. cit.*, págs. 170 y 171.

la LOPDCP conforme a la Directiva 95/46/CE que traspone, que estamos ante un supuesto de responsabilidad objetiva, aunque limitada por el hecho del incumplimiento objetivo de las disposiciones contenidas en ésta[60] -de manera que, acaso, fuese más correcto hablar de un sistema típico de responsabilidad civil-: si ha existido incumplimiento, sea de quién sea el mismo, y de éste se ha derivado un daño para la persona cuyos datos personales han sido objeto de tratamiento, el responsable o el encargado del tratamiento deberán indemnizar los perjuicios con independencia de la concurrencia de la culpa. El análisis de la redacción del art. 23 de la Directiva 95/46/CE, fruto de cuya transposición fue la LOPDCP avalaba la consideración de que en éste también se instituye un régimen de responsabilidad civil objetiva limitada a la existencia de un incumplimiento de sus preceptos. El precitado art. 23 de la Directiva 95/46/CE establecía: *1. Los Estados miembros dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido. [...] 2. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño»*[61]. El segundo apartado del art. 23 de esta Directiva 95/46/CE precisaba explícitamente los casos en los que se puede exonerar de responsabilidad al responsable del fichero de datos personales y se presume que lo es salvo que pruebe que el hecho lesivo no le es imputable, porque lo es a un tercero o el daño ha sido causado mediando fuerza mayor, de manera que no puede exonerarse probando la actuación diligente. El argumento derivado de la interpretación de la Directiva, si el razonamiento que se ha realizado es correcto, es importante a efectos de interpretar el correspondiente precepto de la LOPDCP, en cuanto que es jurisprudencia consolidada del TJUE (a partir de la Sentencia *Marleasing SA c./ Sociedad Internacional de Alimentación, SA»* de 13 de noviembre de 1990 [TJCE 1991\78]) que las leyes nacionales han de interpretarse del modo que mejor encajen con las previsiones contenidas en las Directivas de la UE, también en el caso de que éstas hayan sido objeto de trasposición a los Derechos nacionales.

La naturaleza objetiva del régimen de responsabilidad civil previsto para los responsables y encargados de tratamiento de datos personales de titularidad privada fue asumido, de manera acorde con el parecer mayoritario de la doctrina de los autores, por la jurisprudencia.

[60] En relación con el texto de la LORTAD, GRIMALT SERVERA, P.: *La responsabilidad civil en el tratamiento automatizado de datos personales*, Ed. Comares, Granada, 1999, págs. 150 y ss.; quien mantiene su parecer ya en relación con el texto contenido en el art. 19.1 de la LOPDCP, en «Deberes y responsabilidades en materia de protección de datos», en *Deberes y responsabilidades de los servidores de acceso y alojamiento (Un análisis multidisciplinar)* (S. CAVANILLAS MÚGICA, Coord.), Ed. Comares, Granada, 2005, pg. 200; ABERASTURI GORRIÑO, U.: «El derecho a la indemnización en el artículo 19 de la Ley Orgánica de Protección de Datos de Carácter Personal», *Revista Aragonesa de Administración Pública*, núm. 41-42, 2013, pg. 190. En sentido concordante ya bajo el imperio de la LOPDCP, GARCÍA RUBIO, Mª P.: «Bases de datos y confidencialidad en Internet», en *El comercio electrónico* (J. A. ECHEBARRÍA SÁENZ, Coord.), *op. cit.*, pg. 488; HERRÁN ORTIZ, A. I.: *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, Ed. Dykinson, Madrid, 2002, pg. 259. También considera que se trata de una responsabilidad civil subjetiva, sin ofrecer más argumentos que la mera remisión al art. 1902 del CC, APARICIO SALOM, J.: *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal,* Ed. Aranzadi, Cizur Menor, 2002 (2ª edic.), pg. 167.

[61] El precepto es reproducido de forma prácticamente literal en algunas leyes nacionales de transposición, *v.gr.*, en el art. 21 de la Ley belga de 8 de diciembre de 1992, *relativa a la protección de la vida privada en relación con los tratamientos de datos de carácter personal*, modificada por la Ley de 11 de diciembre de 1998.

Así, *v.gr.*, la SAP de Segovia 121/2002, de 25 de abril [JUR 2002\185043], confirmando la sentencia dictada en la primera instancia, declaró que: *[…] la responsabilidad civil prevista en la Ley* [se refiere a la LOPDCP]*, entiende de forma casi unánime la doctrina, que se trata de naturaleza objetiva, dados los términos de redacción del art. 23 de la Directiva 95/46, a cuya transposición obedece la LO 15/1999»* (*cfr.* FD 1º, *in fine*).

7.2.2. La naturaleza de la responsabilidad civil en el artículo 82 del RGPD

A tenor de la regulación del art. 82 del RGPD tampoco puede darse una respuesta que no ofrezca dudas acerca de la naturaleza de la responsabilidad civil que establece a cargo de los responsables y de los encargados de tratamiento de datos personales. Tan es así que, en los primeros estudios publicados sobre esta cuestión se ha sostenido la naturaleza subjetiva[62] y la naturaleza objetiva de la misma[63]. En esencia, el debate se centra en el significado que haya de atribuirse al apartado 3º del referido art. 82 del RGPD, a tenor del cual *el responsable o el encargado del tratamiento estará exento de responsabilidad en virtud del apartado 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios».*

A tenor de las previsiones normativas que acaban de ser invocadas, parece poder afirmarse que el RGPD establece un sistema de responsabilidad civil subjetiva con inversión de la carga de a prueba de la culpa[64], en tanto que, en los casos de causación de un daño o perjuicio

[62] Es la tesis propugnada por NIETO GARRIDO, E.: «Derecho a indemnización y responsabilidad», *op. cit.*, pg. 561, argumentando esencialmente sobre el significado del art. 82.3 del RGPD.

[63] RUBÍ PUIG, A.: «Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD», *op. cit.*, pgs. 62 y 63. Este autor, después de afirmar que el RGPD no sujeta al responsable de tratamiento a un régimen de responsabilidad por riesgo, afirma que rige una regla de responsabilidad objetiva para la compensación de los daños causados, de manera que, una vez que se haya acreditado la infracción de una de las obligaciones relativas al tratamiento de datos personales prevista en el RGPD, el responsable deberá compensar al actor sin que pueda probar que su comportamiento fu diligente o que desconocía y no podía saber que él o el encargado del tratamiento estaban infringiendo el RGPD.

[64] El parecer es compartido en la doctrina italiana, *v.gr.*, por DI LEO, D.: «La responsabilità civile alla luce del GDPR e del decreto 101/2018», en *www.agendadigitale.eu,* 29 de abril de 2019. La referida autora explica como el art. 82 del RGPD establece un sistema de responsabilidad civil fundado en la inversión de la carga de la prueba de la culpa, de igual manera que el previsto en el *Codice Privacy.* En su redacción originaria del año 2003, el primer párrafo del art. 15 del *Codice Privacy* preveía un régimen de responsabilidad civil en el sentido del art. 2050 del *Codice civile*, a cargo de quien hubiese ocasionado un daño a otro como consecuencia del tratamiento de datos personales. El precepto era claro en el sentido de que establecía un sistema de responsabilidad civil por el ejercicio de una actividad peligrosa, de conformidad con el cual, cualquiera que causase un daño a otro en el desarrollo de una actividad peligrosa, por su naturaleza o por la naturaleza de los medios utilizados, viene obligado al resarcimiento del daño causado, siempre que no pruebe que ha adoptado todas las medidas idóneas para evitar el daño, encuadrándose así, de manera expresa, la actividad de tratamiento de datos personales dentro de las actividades peligrosas. La referida norma preveía un sistema de inversión de la carga de la prueba a cargo del agente del daño y el segundo apartado del referido art. 15 del Decreto Legislativo 196/2003 establecía el carácter resarcible del daño extrapatrimonial también en el caso de vulneración del art. 11, regulador de la modalidad de tratamiento y requisitos de los datos personales. El referido art. 15 del Decreto Legislativo 196/2003 no contenía previsión alguna respecto del carácter solidario, o no, de la responsabilidad civil que, en el Derecho italiano, resultaba de aplicación por virtud de la aplicación de la remisión a la regla general del art. 2055 del *Codice civile* (fruto de la remisión a éste por parte del propio art. 2050 del *Codice civile*).

al titular de datos personales objeto de tratamiento, cuando haya mediado un incumplimiento de alguna de las previsiones específicas contenidas en el propio RGPD y que, debe hacerse extensivo a las contempladas en las normas nacionales de protección de datos personales; de tal manera que la acreditación por el responsable o, en su caso, por el encargado de tratamiento del cumplimiento de las previsiones legales que rigen su actividad, lo pondrá al amparo de la posibilidad de exigirle responsabilidad civil por los daños y perjuicios que haya padecido el titular de los datos personales[65]. De esta forma, las normas que contemplan y disciplinan la actuación de los responsables y de los encargados de tratamiento de datos personales se erigen en determinaciones normativas de estándares de diligencia de observancia preceptiva, cuyo incumplimiento permite la calificación de la actuación de los referidos sujetos como negligente y, en consecuencia, suficiente para considerar que concurre el título de imputación subjetiva de su responsabilidad civil.

El art. 15, así como el resto del Título III de la Parte I del Decreto Legislativo núm. 196/2003, fueron derogados por el ya citado Decreto Legislativo núm. 101/2018. En consecuencia, en materia de responsabilidad civil, en el Derecho italiano vigente no existe ninguna norma que se remita expresamente a la aplicación del art. 2050 del *Codice civile*, al tiempo que no existe ninguna previsión específica en esta materia en el DLeg. 101/2018, de manera que la norma de aplicación es el art. 82 del RGPD. Es precepto, como se expone de manera detallada en el texto contempla el derecho de cualquier perjudicado a obtener el resarcimiento del daño sufrido siempre que haya existido una vulneración de las previsiones del RGPD por parte del responsable o del encargado del tratamiento. La doctrina italiana ha puesto de manifiesto que una primera diferencia entre el régimen jurídico que resulta del art. 82 del RGPD, respecto de su precedente, el art. 15 del DLeg. 196/2003, radica en el primer los responsables frente al perjudicado son el responsable de tratamiento y el encargado de tratamiento, en tanto que en el precepto derogado lo era cualquiera que hubiese ocasionado el daño; al tiempo que conforme al RGPD puede ser requerida la indemnización tanto de daños patrimoniales, como de daños extrapatrimoniales, pudiendo ejercitarse a acción ante los órganos jurisdiccionales competentes.

En el Derecho brasileño también se debate acerca de la naturaleza de la responsabilidad civil de los agentes de tratamiento de datos personales, considerando que la LGPD de 2018 establece un sistema de responsabilidad civil subjetiva, entre otros, BODIN DE MORAES, MªC.; DE QUEIROZ, J.Q.: «Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD», en *Cadernos Adenauer*, Vol. 3*, op. cit.*, pg. 130; y, siguiendo a los anteriores, DA SILVA LIMA, H.: «Responsabilidade civil objetiva, subjetiva ou proativa? Pela Lei Geral de Proteção de Dados e suas implicações: contexto brasileiro», *Revista Jurídica de Daños, op. cit.*, expresamente la pg. 8.

En sentido contrario, en la doctrina española sostienen que tanto la responsabilidad civil del responsable del tratamiento, como la del encargado de tratamiento, es objetiva, en tanto que, a su juicio, no se hace depender de la concurrencia de culpa, al no existir ninguna referencia a la misma en las normas examinadas del RGPD, RUBÍ PUIG, A.: «Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD», *op. cit.*, pgs. 62-63; y GRIMALT SERVERA, P.: «Intromisiones ilegítimas en los derechos al honor, a la intimidad y a la propia imagen: tutela civil versus tutela administrativa», en *Protección de datos personales* (APDC), Ed. Tirant lo Blanch, Valencia, 2020, pgs. 364-366.

[65] La previsión de un sistema de responsabilidad subjetiva es el sistema por el que el legislador alemán ha optado expresamente en el §.83 de la F*ederal Data Protection Act* of 30 June 2017 (*Federal Law Gazette* I, pg. 2097), rubricado «*Compensation*» y del siguiente tenor: *«(1) If a controller has caused a data subject to suffer damage by processing personal data in violation of this Act or other law applicable to this processing, the controller or its legal entity shall be obligated to provide compensation to the data subject. This obligation to provide compensation shall not apply if, in the case of non-automated processing, the damage was not the result of fault by the controller.*

(2) The data subject may request appropriate financial compensation for non-material damage.

(3) If, in the case of automated processing of personal data, it is not possible to determine which of several controllers caused the damage, each controller or its legal entity shall be liable.

(4) Section 254 of the Civil Code shall apply to contributory negligence on the part of the data subject».

(5) The limitation provisions stipulated for tortious acts in the Civil Code shall apply accordingly with regard to statutory limitation».

A estos efectos ha de tenerse en cuenta que el art. 82 del RGPD pone a cargo del responsable y del encargado del tratamiento, a efectos de que puedan exonerarse de responsabilidad civil derivada de un evento dañoso cuya imputación se pretenda, bien que este evento dañoso resulta imputable a un hecho extraño a su esfera de control y de responsabilidad (hecho de un tercero o supuesto de fuerza mayor), bien que han adoptado todas las medidas normativamente exigidas y técnicamente posibles para evitar que se verificase el daño. Suele afirmarse que la razón o argumento que subyace en la inversión de la carga de la prueba de la culpa radica en el hecho de que el tratamiento de datos personales se califica como una actividad peligrosa, en tanto que expone a los titulares de los datos personales objeto de tratamiento a un riesgo[66], siendo esta actividad aceptada por la utilidad económica y social que conlleva, debiendo ser compensado aquel riesgo en el caso de que resulten vulnerados los derechos de los titulares de los datos personales que son tratado, ordinariamente en beneficio del responsable. En consecuencia, el titular de los datos personales, el interesado que ejercita la acción de responsabilidad civil habrá de acreditar: la existencia del daño o del perjuicio, así como su cuantía; la violación de una norma de tutela de los datos personales –representativa de la conducta antijurídica-, así como la relación de causalidad entre esta conducta y el daño cuyo resarcimiento pretende.

Conforme a las afirmaciones que preceden, el responsable o el encargado del tratamiento, según sea el caso, quedarán exentos de responsabilidad cuando demuestren que no les resultan subjetivamente imputables los daños y perjuicios. En este sentido, el Considerando 146 del RGPD explica que el responsable o el encargado tratamiento deben quedar exentos de responsabilidad si se demuestra que en modo alguno son responsables de los daños y perjuicios, lo que debe entenderse no como una tautología, sino como la posibilidad de exoneración en los supuestos de daños imputables a un tercero, a un evento externo al ámbito de riesgo (fuerza mayor), así como en aquellos casos en los que acrediten haber actuado de manera diligente.

Sin perjuicio de lo anterior, el derecho a indemnización tampoco será exigible si no se ha producido una infracción del RGPD o, en los términos ya expuestos, de la LOPDPGDD, en el sentido de que dicha infracción produzca un daño económico o moral al interesado cuyos datos personales son objeto del tratamiento; esto es, en aquellos casos en los que el daño

[66] Cuando se alude al riesgo derivado del tratamiento de datos personales ha de tenerse en cuenta que estos riesgos son múltiples, de conformidad con las previsiones del Considerando 75 del RGPD, a tenor del cual *«los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados».*

cuyo resarcimiento se pretenda no pueda calificarse como antijurídico; lo que sucederá también en aquellos casos en los que no haya un tratamiento ilícito de datos personales (*v.gr.,* en aquellos casos en los que se tratan son datos anonimizados, sin que sea posible reidentificar a la persona a la que se tratan, de manera que no concurre una conducta ilícita).

La indemnización requiere que el interesado pruebe que ha producido un daño, bien sea económico o patrimonial (material) o moral (inmaterial). En relación con el concepto de daño, el Considerando 146 del RGPD explica que el concepto de daños y perjuicios debe interpretarse en sentido amplio a la luz de la jurisprudencia del Tribunal de Justicia de la UE, de tal modo que se respeten plenamente los objetivos del mismo. En el caso de que no se produzca daño o perjuicio alguno, pero sí concurra una vulneración de otras normas del Derecho de la Unión Europea o de los Estados miembros en materia de tutela de los titulares de los derechos personales objeto de tratamiento, aunque no fuera aplicable el derecho a indemnización acogido en el art. 82 del RGP, sí cabe la posibilidad de que el interesado presente una reclamación ante la autoridad nacional de protección de datos, si se trata de una conducta tipificada como ilícita, siendo susceptible de una sanción administrativa.

8 LA NO APLICACIÓN DEL RGPD A LOS PRESTADORES DE SERVICIOS DE INTERMEDIACIÓN EN INTERNET (ISPs)

Determinando el ámbito de aplicación material del RGPD, el art. 2.4 del propio RGPD establece que *el presente Reglamento se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE, en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15»*. A mi juicio esta previsión debe interpretarse en el sentido de que los prestadores de servicios de intermediación en Internet responden en el caso de daños ocasionados como consecuencia de la vulneración de la privacidad y, en particular, de la protección de datos personales, conforme a su régimen de responsabilidad civil propio que, como es conocido, en un régimen de responsabilidad civil de naturaleza subjetiva.

La Ley 34/2002, de 11 de julio, *de Servicios de la Sociedad de la Información y de Comercio Electrónico,* en virtud de la que se transpone la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, *relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico),* entre otros aspectos del comercio electrónico, regula, en sus arts. 13 a 17, la responsabilidad civil de los prestadores de servicios que actúan como intermediarios en la sociedad de la información –*service providers», on-line service providers»* (OSPs)» o *Internet service providers»* (ISPs)–. El ámbito subjetivo de aplicación de la LSSI viene determinado por la presencia de un *prestador de servicios de la sociedad de la información»,* con independencia de la condición subjetiva del destinatario o usuario de los mismos que, por lo tanto, podrá ser cualquier persona física o jurídica que utilice, por motivos personales o profesionales, un servicio de la sociedad de la información, si bien el hecho de que tenga la condición subjetiva de consumidor o usuario, de acuerdo con la legislación de consumo, implicará el sometimiento de la prestación del servicio a las previsiones del régimen estatutario diseñado por este sector del Ordenamiento jurídico. El concepto de servicio de la

sociedad de la información se contiene en la Directiva 98/34/CE, así como en el art. 1.*b)* de la Directiva 2015/1535/CE, a tenor del cual, es todo servicios prestado ordinariamente contra una remuneración, a distancia, por vía electrónica, a petición individual de un destinario de los servicios. La prestación de servicios en el ámbito que se ha dado en llamar de economía colaborativa ha suscitado la cuestión atinente a la calificación como prestadores de servicios de la sociedad de la información de las sociedades que ponen a disposición de terceros plataformas virtuales que permiten la contratación entre los destinatarios de las mismas, como es el caso, entre otros muchos, de *Airbnb*, respecto del que la STJUE de 19 de diciembre de 2019 (asunto C-390/18, *Airbnb*) ha calificado como un servicio de intermediación propio de los servicios de la sociedad de la información y, en consecuencia, sometido al régimen de la Directiva 200/31/CEE, no resultando de aplicación las exigencias normativas (nacionales) previstas para la prestación de servicios propios de las agencias inmobiliarias.

La LSSI viene a dar respuesta a una cuestión de capital importancia, dada la trascendencia económica que implica, cual es la relativa a si puede serles –y, en su caso, en qué circunstancias– imputada responsabilidad civil por daños derivados de contenidos ajenos transmitidos o alojados por ellos o a los que faciliten o permitan de cualquier manera el acceso o su localización en la red Internet. El principio general en que se asienta la respuesta resulta de la afirmación expresa del sometimiento de los prestadores de servicios de la sociedad de la información a las normas generales reguladoras de la responsabilidad civil, penal y administrativa del Ordenamiento jurídico español (art. 13.1 de la LSSI). Respecto de la responsabilidad civil, la regla general que acaba de enunciarse supone la remisión, con las precisiones en orden a la determinación del canon de diligencia exigible que se concretan en los arts. 14 a 17 de la LSSI para los distintos ISPs», a las previsiones de los arts. 1902, 1903 y concordantes del CC, al tiempo que la precisión contenida en el núm. 2 del art. 13 de la LSSI parece ampliar el ámbito de exención derivado del respeto a aquellas exigencias de diligencia a los ámbitos propios de la responsabilidad penal y administrativa. En cuanto a esta última, la propia LSSI contiene, en su Título VII (arts. 37 a 45) y bajo la rúbrica genérica de *Infracciones y sanciones»,* la disciplina de la responsabilidad de naturaleza administrativa en la que pueden incurrir estos prestadores de servicios.

La LSSI contempla un régimen más estricto o más laxo en función de la concreta actividad desarrollada por el ISP. El ejemplo más claro del prestador sometido al régimen menos estricto es el constituido por el que realiza la actividad de simple conducción de la información (el operador de red y el proveedor de acceso o prestador de servicios de *routing»*), al que prácticamente se le exonera de responsabilidad civil por contenidos ajenos (art. 14 de la LSSI), frente al ejemplo representado por el ISP que aloja y almacena datos ajenos (prestador de servicios de *hosting»*), que constituiría el ejemplo del prestador sometido a un régimen más estricto de responsabilidad civil (art. 16 de la LSSI). En todo caso su responsabilidad civil requiere la existencia de un conocimiento efectivo de la ilicitud de los contenidos ajenos alojados, salvo en el caso en el que tenga un papel activo que pueda darle conocimiento o control sobre los datos o sobre las informaciones alojadas, habiendo optado la Sala de lo Civil del TS por una interpretación material y estricta del concepto de conocimiento efectivo», debiendo estar al alcance de cualquiera la posibilidad de considerar los referidos contenidos o informaciones como ilícitos de manera notoria, sin que resulte suficiente una mera comunicación del afectado o potencial perjudicado. En efecto, la STS 144/2013, de 4 de marzo (RJ 2013, 3380), reiterando la doctrina asumida en su pretérita Sentencia (caso *putasgae*») 773/2009, de 9 de diciembre (RJ 2010, 131), considera que la integración del requisito del conocimiento efectivo

por el prestador de servicios de alojamiento requiere una comunicación previa de la resolución de la autoridad competente acerca de la ilicitud de los contenidos. El TS se hace eco también de la doctrina emanada de la STJUE de 16 de febrero de 2012 (asunto C-360/10) a tenor de la cual se considera contrario al derecho fundamental a la libertad de expresión ordenar un sistema de filtrado de contenidos con carácter previo. A su vez, la STJUE de 23 de marzo de 2010 (asuntos acumulados C-236/08 y C-238/08 *Google France vs. Louis Vuitton*) declaró que, para considerar responsable al prestador de servicios de intermediación, es necesario que éste *desempeñe un papel activo que pueda darle conocimiento o control de los datos almacenados»,* en tanto que, en caso contrario, es necesario que tenga un conocimiento efectivo de la ilicitud de los mismos. Precisamente el hecho de considerar la existencia un conocimiento efectivo de los datos de contenido ilícito alojados (insultos y comentarios vejatorios a un personaje público), unido al hecho de mantener un registro con un domicilio inexacto que impidió al perjudicado comunicar al prestador de los servicios de almacenamiento de datos la solicitud de interrupción del acceso a las referidas informaciones y contenidos manifiestamente ilícitos, permitió a la STS 72/2011, de 10 de febrero (RJ 2011, 313) el pronunciamiento de condena al prestador de servicios de alojamiento del sitio web *alasbarricadas.org».*

En una posición intermedia se encuentra el proveedor o prestador de servicios de copia temporal de los datos solicitados por los usuarios (servicios de *hosting»*) al que se exonera de responsabilidad civil si no modifica la información copiada, permite el acceso a ella sólo a los destinatarios que cumplan las condiciones impuestas por el destinatario cuya información se solicita, respeta las normas generalmente aceptadas y aplicadas por el sector para la utilización de la información, no interfiere en la utilización lícita de tecnología empleada en el sector con la finalidad de obtener datos sobre la utilización de la información y, en el caso de que tenga conocimiento efectivo de que la información ha sido retirada del lugar de la red en el que se encontraba inicialmente, se ha imposibilitado el acceso a ella o un tribunal o un órgano administrativo competente han ordenado retirarla o impedir el acceso a ella, retire la información que haya almacenado o haga imposible el acceso a la misma (art. 15 de la LSSI).

El art. 17 de la LSSI disciplina la responsabilidad civil de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda *(linking»).* Los intermediarios que prestan los servicios consistentes en facilitar enlaces a contenidos situados en otro lugar de la red y los que incluyen en los suyos directorios o instrumentos de búsqueda de aquellos contenidos, no responden de los daños que se puedan causar por los contenidos encontrados merced a la utilización de los instrumentos que ponen a disposición de los usuarios –y de los internautas o usuarios de la red– siempre que se cumpla alguna de las dos circunstancias enunciadas a propósito de los intermediarios que presten servicios de *hosting»* (art. 16 de la LSSI); a saber: no tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de ser indemnizados (también en este caso la existencia de una resolución de la autoridad competente declarando la ilicitud de los contenidos u ordenando su retirada, la inutilización del acceso o declarando la existencia de la lesión y aquélla fuese conocida por el prestador del servicio, impide la apreciación de esta circunstancia); o, si lo tienen, actúen con la diligencia necesaria para suprimir o inutilizar el enlace correspondiente.

En todo caso, la exención de responsabilidad derivada de la concurrencia de alguna de las dos circunstancias enunciadas en el párrafo anterior no puede apreciarse, de acuerdo con el tenor literal del art. 17.2 de la LSSI, *si el destinatario del servicio»* opera bajo la dirección,

autoridad o control del prestador que facilita la localización de aquellos contenidos, entendiendo por destinatario» no el internauta que utiliza o se vale de los instrumentos de búsqueda o de enlace con los contenidos o informaciones que le interesan, sino el titular o responsable de estos contenidos o informaciones cuya localización en la red se facilita, aun cuando usuario», en sentido estricto, sería la persona que efectivamente usa el buscador y, en su caso, activa el enlace que le permite el acceso a los contenidos deseados. Por esta razón, la norma no resulta adecuada cuando se trata simplemente de la actividad de proveer enlaces –el proveedor es quien los crea– y ello porque el destinatario o usuario, en este caso, sólo puede identificarse con quien usa y activa efectivamente el enlace creado.

Las expresiones utilizadas en la Directiva 2000/31/CE, *no se puede considerar al prestador de servicios de este tipo* [mera transmisión] *responsable de los datos transmitidos, a condición de que [...]»* (art. 12.1), *el prestador del servicio no pueda ser considerado responsable del almacenamiento automático, provisional y temporal de esta información [...] a condición de que [...]»* (art. 13.1), *el prestador de servicios* [de alojamiento de datos] *no pueda ser considerado responsable de los datos almacenados a petición del interesado, a condición de que [...]»* (art. 14.1), traducidas por el legislador español por *no serán responsables por la información transmitida salvo que [...]»* (art. 14.1), *no serán responsables por el contenido de esos datos ni por la reproducción temporal de los mismos si [...]»* (art. 15), *no serán responsables por la información almacenada a petición del destinatario, siempre que [...]»* (art. 16.1), inducen a pensar que la Directiva no exige y que el legislador estatal no ha instaurado un régimen de responsabilidad civil especial o distinto del que constituye el Derecho común en este sector del Ordenamiento jurídico. En efecto, el legislador de la UE parece limitarse a describir unas conductas en las que poder fundar la imputación de responsabilidad civil al ISP y ello en orden a soslayar los problemas que podrían suscitar otro tipo de previsiones y su adecuación a los distintos sistemas de responsabilidad civil imperantes en los distintos Estados de la UE, de acuerdo con las advertencias que se contienen en el Considerando núm. 40 de la Directiva 2000/31/CE[67]. Por su parte, el legislador español, respetando estos mínimos, los contempla como reglas que describen o perfilan los deberes de prudencia y de diligencia de los

[67] *Vid.,* entre otros, BUSTO LAGO, J. M.: «La responsabilidad civil de los prestadores de servicios de la sociedad de la información (ISPs)», en *Tratado de responsabilidad civil* (F. REGLERO CAMPOS y J.M. BUSTO LAGO COORDS.), T. II, Ed. Aranzadi, Cizur Menor, 2014 (5ª ed.) (págs. 597 a 747); *ibidem,* «La responsabilidad civil de los "Internet Service Providers" (ISPs) por la infracción en la red de los derechos de propiedad intelectual», *RdNT*, núm. 5, 2004, pgs. 39 a 73; *ibidem,* «La responsabilidad de los prestadores de servicios de intermediación en la sociedad de la información», *AJA,* núm. 542, 25 julio 2002, pgs. 1 a 6; CLEMENTE MEORO, M. E.: «La responsabilidad civil de los prestadores de servicios de la sociedad de la información», en *Responsabilidad civil y contratos en Internet (Su regulación en la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico)* (CLEMENTE MEORO; CAVANILLAS MÚGICA), Ed. Comares, Granada, 2003, pgs. 1 a 116; GARROTE FERNÁNDEZ-DÍEZ, I.: *El derecho de autor en Internet (Los Tratados de la OMPI de 1996 y la incorporación al Derecho español de la Directiva 2001/29/CE),* Ed. Comares, Granada, 2003 (2ª ed.); *ibidem,* «La responsabilidad civil extracontractual de los prestadores de servicios en línea por infracciones de los derechos de autor y conexos», en *pe.i. Revista de Propiedad Intelectual,* núm. 1, 1999, pgs. 9 a 64; JULIA BARCELÓ, R.; MONTERO, É. y SALAÜN, A.: «La proposition de Directive européenne sur le commerce électronique: Questions choisies», en *Commerce électronique (Les temps des certitudes), Cahiers du Centre de Recherches Informatique et Droit* (núm. 17), Ed. Bruylant, Bruxelles, 2000; MENDOZA LOSANA, A. I.: «Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información. Modificaciones relevantes para los operadores del sector de telecomunicaciones», *AC,* núm. 4, junio 2008, pgs. 15 a 34; DE MIGUEL ASENSIO, P.: *Derecho privado de Internet,* Ed. Civitas, Madrid, 2015 (5ª ed.); PLAZA PENADÉS, J.: «La responsabilidad civil de los intermediarios en Internet y otras redes (su regulación en el Derecho comunitario y en la LSSI)», en *Contratación y comercio electrónico* (F. J. ORDUÑA MORENO, Dir.), Ed. Tirant lo Blanch,

ISPs, constituyendo una especie de *lex artis,* de manera que sólo si incumplen alguno de los deberes positivos o negativos que imponen, entonces pueda considerarse que concurren los presupuestos necesarios para la imputación subjetiva de responsabilidad. Al margen de los presupuestos que habilitan la imputación a un ISP *ex* LSSI, no puede considerarse que éste haya incurrido en responsabilidad civil, en virtud, pongo por caso, de la aplicación de normas de protección de determinados derechos que prevean criterios de imputación más laxos (como tampoco podría exonerarse el ISP alegando que para aquellos daños una determina norma contempla un criterio más estricto de imputación). El principio general de no responsabilidad civil de los ISPs determina que la carga de la prueba de la concurrencia de los requisitos en orden a imputar aquella responsabilidad a estos prestadores de servicios recaiga sobre el perjudicado (*ex* art. 217.2 de la LECiv).

En relación con las obligaciones que pueden imponerse a una prestador de servicios de alojamiento de datos, sin que ello suponga imponer una obligación general de supervisión prohibida por el art. 15.1 de la Directiva 2000/31/CEE, a tenor de las Conclusiones del Abogado General del TJUE en el asunto C-18/18 *Eva Glawischnig-Piesczek contra Facebook Ireland Limited* (petición de decisión prejudicial planteada por el *Oberster Gerichtshof*), publicadas en fecha 4 de junio 2019, el Abogado General concluye que el art. 15, apartado 1, de la Directiva 2000/31/CE, de 8 de junio (Directiva sobre el comercio electrónico), debe interpretarse en el sentido de que no se opone a que, mediante un requerimiento judicial, se obligue a un prestador de servicios de alojamiento de datos que explota una plataforma de red social a buscar e identificar, entre todos los datos difundidos por los usuarios de esa plataforma, datos idénticos a los declarados ilícitos por el órgano jurisdiccional que haya dictado dicho requerimiento. Mediante ese requerimiento judicial puede obligarse a un prestador de servicios de alojamiento de datos a buscar e identificar datos similares a los declarados ilícitos únicamente de entre los datos difundidos por el usuario que publicó tales datos. Un órgano jurisdiccional que se pronuncie sobre la retirada de esos datos similares debe garantizar que los efectos de su requerimiento son claros, precisos y previsibles. A ese propósito, debe poner en equilibro los derechos fundamentales en juego y tener en cuenta el principio de proporcionalidad.

La Ley 25/2007, de 18 de octubre, *relativa a la conservación de datos en las comunicaciones electrónicas y a las redes públicas de comunicaciones*, en virtud de la que transpuso la Directiva 2006/24/CE, de 15 de marzo y reformada por la D.F. 4ª de la LGTel/2014, establece la obligación de los operadores que prestan servicios de comunicaciones electrónicas disponibles al público o que explotan redes públicas de comunicaciones, en los términos establecidos en la LGTel (el art. 42 de la LGTel remite a la aplicación de la Ley 25/2007, en relación con la conservación y cesión de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones), de conservar determinados datos relativos a aquéllas durante un período mínimo de doce meses, al tiempo que se establece la regulación atinente a la cesión de los mismos, siempre previa autorización judicial.

Valencia, 2003, pgs. 195 a 237; PEGUERA POCH, M.: *La exclusión de responsabilidad de los intermediarios en Internet,* Ed. Comares, Granada, 2007; GONZÁLEZ DE ALAIZA CARDONA, J.J.: «Capítulo 21: La responsabilidad civil de los prestadores de servicios intermediarios de la sociedad de la información», en *La responsabilidad civil por daños causados por servicios defectuosos* (A. ORTI VALLEJO y Mª C. GARCÍA GARNICA, DIRS.), *op. cit.* (2ª edic.), en particular afirmando la culpa como criterio de imputación de la responsabilidad civil, pg. 1156.

9 TIPOLOGÍA DE DAÑOS RESARCIBLES: SUPUESTOS PARTICULARES DE TRATAMIENTOS DE DATOS PERSONALES ILÍCITOS QUE GENERAN DAÑOS Y PERJUICIOS RESARCIBLES AL TITULAR DE LOS DATOS

9.1. Consideración general

El propio RGPD, en su Considerando 75, pone de manifiesto que los daños y perjuicios que pueden vincularse causalmente al tratamiento de datos personales mediando el incumplimiento de las normas reguladoras de esta actividad son muy variados, tanto en su etiología, como en su naturaleza y gravedad[68]. Por su parte, el art. 82 del RGPD alude expresamente al derecho del perjudicado al resarcimiento tanto de los daños y perjuicio materiales, como de los *inmateriales»;* esto es, tanto de los daños y perjuicios patrimoniales, como de los extrapatrimoniales o morales, como ya se ha adelantado.

9.2. Daños materiales o patrimoniales

La cuantificación o valoración del daño patrimonial es una cuestión de prueba, debiendo acreditarse su realidad y su cuantía por el actor e incluyéndose tanto el daño emergente como el lucro cesante (*ex* art. 1106 del CC). En esta partida indemnizatoria han de incluirse todos los gastos derivados de los esfuerzos y actividades realizadas por el interesado para hacer cesar la irregularidad en el tratamiento de sus datos personales, así como los daños que se puedan derivar, *v.gr.*, de la frustración de operaciones financieras o de crédito (en el caso de inclusión indebida en un fichero de solvencia patrimonial negativa)[69]. También pueden considerarse como daños patrimoniales los derivados del uso masivo de datos personales (*big*

[68] El Considerando 75 del RGPD es del siguiente tenor: *«Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados».*

[69] Ha de precisarse, en relación con esta última afirmación, que no puede tomarse en consideración la suma de la operación frustrada como consecuencia de la indebida inclusión en un fichero de solvencia patrimonial cuando aquélla consista en la concesión de un préstamo o de un crédito en tanto que la no realización de un gasto no puede considerarse pérdida económica. Así se ha pronunciado la SAP de Valencia, Secc. 7ª, de 19 de noviembre de 2003 [EDJ 2003\224188], en su F.D. 4º; si bien la afirmación contenida en esta Sentencia ha de ser objeto de alguna precisión de forma inmediata, en tanto que la frustración de la operación haya podido suponer algún

data»), sin el consentimiento de los titulares de los datos objeto de tratamiento con la finalidad de elaborar perfiles que permitan a las empresas suministradoras de productos o servicios segmentar por grupos de consumidores en un mercado, generando sobrecostes en el acceso a los referidos bienes y servicios[70].

9.3. Daños morales o extrapatrimoniales: lesiones del derecho al honor

La indemnización de la que es acreedor el titular de los datos personales objeto del tratamiento ilícito generador del daño o del perjuicio habrá de ser comprensiva tanto del daño patrimonial experimentado por el perjudicado por el tratamiento de sus datos personales, como del daño moral que éste haya sufrido (*v.gr.*, SAP de Badajoz, Secc. 3ª, de 18 de julio de 2001 [JUR 2001\261932])[71]. Así, por ejemplo, ha de incluirse la valoración del descrédito personal o empresarial que pueda derivarse del indebido o inadecuado tratamiento de que hayan sido objeto los datos personales de una determinada persona[72], como puede acontecer en el caso de la infracción del derecho al olvido en Internet (*vid., infra,* §.9.4), divulgación no consentida de datos sobre un despido laboral[73], inclusión indebida de datos personales en ficheros policiales[74] o el acceso a historias clínicas informatizadas[75].

También suelen incluirse en el ámbito de los daños extrapatrimoniales derivados del inadecuado tratamiento de datos personales, la inclusión de datos de esta naturaleza en ficheros de solvencia patrimonial negativos, si bien, esta actuación ilícita puede conllevar también la causación de daños patrimoniales en forma de no concesión de la financiación solicitada, concesión en unas condiciones económicas más gravosas o en la no contratación de la prestación de un determinado servicio. En particular, las SSTS de 18 de febrero de 2015 [RJ 2015/574], de 12 de mayo de 2015 [RJ 2015/2027], 26 de abril de 2017 [RJ 2017/1737] y

coste para el titular de los datos personales objeto del tratamiento ilícito (*v.gr.*, comisiones ya pagadas, gastos derivados de las gestiones realizadas, etc.) o cuando la frustración de la operación suponga una pérdida de oportunidades debidamente acreditada (*v.gr.*, imposibilidad de concertar el préstamo en determinadas condiciones de mercado, imposibilidad de participar en una operación económica de carácter lucrativo, etc.); PARRA MEMBRILLA, L.: «Precios a medida para los consumidores: la consecuencia del Big Data», en *http://centrodeestudiosdeconsumo.com*, 12 de febrero de 2020.

[70] En este sentido, *vid.*, ZHU, B.: «A traditional tort for a modern threat: applying intrusion upon seclusion to dataveillance observations», 89 *N.Y.U.L. Rev.* 2381, diciembre de 2014; RUBÍ PUIG, A.: «Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD», *op. cit.*, pgs. 76 y 77.

[71] El carácter resarcible del daño moral o extrapatrimonial en este ámbito resulta ser un parecer doctrinal común, también en la doctrina comparada. Así, *v.gr.,* el art. 29 de la Ley italiana 675/1996, de 31 de diciembre, relativa a la tutela administrativa y jurisdiccional en relación con el tratamiento de datos personales, precisa expresamente en su apartado 9 que el daño patrimonial es resarcible también en los casos de violación de las previsiones del art. 9, en el que se regula la recogida de los datos personales objeto de tratamiento, así como los principios de calidad y relativos a la duración del tratamiento. *Vid.* ARIETA, G.: «Art. 29, commi VI, VII, VIII», en *La tutela dei dati personali. Commentario alla L. 675/1996* (E. GIANNANTONIO / M. G. LOSANO / V. ZENO-ZENCOVICH), CEDAM, Padua, 1999 (2ª edic.), pgs. 384 y 385.

[72] En este sentido, expresamente, la SAP Barcelona, Secc. 1ª, de 13 de mayo de 2005 [AC 2005\990].

[73] STS 609/2015, de 12 de noviembre [RJ 2015\5063], revocando la SAP Barcelona, Secc. 14ª, 404/2013, de 18 julio [JUR 2013\337466].

[74] STSJ País Vasco, C-Adm, Secc. 3ª, 617/2008, de 19 de septiembre [RJCA 2008\660].

[75] SJCA núm. 2 de Tarragona 55/2014, de 4 de marzo [JUR 2014\132891].

512/2017, de 21 de septiembre [RJ 2017\4056], distinguen los siguientes tipos o clases de daños, que se pueden/suelen derivar de una lesión del honor por inclusión indebida en un registro de morosos[76]:

a) Daños patrimoniales, dentro de los que el TS distingue los que denomina daños patrimoniales concretos», "*fácilmente verificables y cuantificables (por ejemplo, el derivado de que el afectado hubiera tenido que pagar un mayor interés por conseguir financiación)*"; y los que el TS identifica como daños más difusos pero también reales e indemnizables» "*como son los derivados de la imposibilidad o dificultad para obtener crédito o contratar servicios*" y "*los daños derivados del desprestigio y deterioro de la imagen de solvencia personal y profesional*" causados por la inclusión ilícita en un fichero de solvencia patrimonial negativo.

b) Daños morales que el TS clasifica, a su vez, en tres subtipos o clases: los "*consistentes en la afectación de la dignidad en su aspecto interno o subjetivo*", los que consisten en esta misma afectación, pero en el aspecto "*externo u objetivo relativo a la consideración de las demás personas*"; y, por último, los daños consistentes en el "*quebranto y la angustia producida por las gestiones más o menos complicadas que haya tenido que realizar el afectado para lograr la rectificación o cancelación de los datos incorrectamente tratados*".

Los denominados ficheros de solvencia patrimonial y crédito son ficheros privados (*v.gr.,* el RAI –contiene información relativa a impagos exclusivamente de personas jurídicas, cuya cuantía sea igual o superior a 300,00 €-, ASNEF-EQUIFAX, EXPERIAN-BADEXCUG e ICIRED –plataforma *on-line»* que permite el intercambio de información sobre impagos comerciales, tanto de personas jurídicas, como de personas físicas-) –salvo la CIRBE, que es un servicio público que gestiona una base de datos en la que constan prácticamente todos los préstamos, créditos, avales y riesgos en general que las entidades financieras tienen con sus clientes-. Los sistemas de información crediticia o ficheros de solvencia patrimonial se nutren de la información que suministran las empresas adheridas a ellos –ordinariamente entidades financieras y de crédito y grandes empresas de servicios- y a la que sólo éstas tienen acceso, de conformidad con las previsiones de la letra *e)* del art. 20.1 de la LOPDPGDD. Las condiciones para la inclusión de los datos personales de un deudor en un fichero de este tipo, ya contemplados en la derogada LOPD y en su Reglamento (RD 1720/2007, de 21 de diciembre) no contemplan la exigencia del consentimiento del deudor incumplidor[77], existiendo amparo legal de esta

[76] *Vid*. PEÑA LÓPEZ, F.: «Daños al honor. Intromisión ilegítima por inclusión indebida de datos en un fichero de morosos. Criterios de determinación del daño resarcible. Indemnizaciones simbólicas: comentario a la STS de 21 septiembre 2017 (RJ 2017\4056)», *CCJC*, núm. 106, 2018, pgs. 225 a 238.

[77] En el Derecho español, a diferencia de lo que acontece con los ficheros de solvencia negativos que, como hemos visto, conforme a las previsiones de la LOPDPGDD no requieren del consentimiento del deudor incumplidor para que sus datos sean incorporados a los mismos, la jurisprudencia ha considerado que para que los prestamistas compartan información positiva sí es necesario el consentimiento del afectado (*v.gr.*, STS, C-Adm, de 15 de julio de 2010 [ROJ:STS 4050/2010 - ECLI:ES:TS:2010:4050] dictada resolviendo el recurso contencioso-administrativo deducido por la entidad mercantil «Experian Bureau de Crédito, S.A.» contra el RD

conducta, con carácter previo a la entrada en vigor de la LOPDPGDD, en la previsión del art. 60.*Quinto* de la Ley 44/2002, de 22 de noviembre, *de reforma del sistema financiero*- y sin que exista una previsión específica en el RGPD que determine una necesaria modificación de éstos. Estos requisitos que se regulan, ahora, en el art. 20 de la LO 3/2018, de PDPGDD, son los que siguen[78]:

1) Que los datos que se incorporan hayan sido facilitados por el acreedor o por quien actúe por su cuenta o interés.

1720/2007, de 21 diciembre). Este criterio se mantiene en la vigente LOPDPGDD, mientras que en el Reglamento UE de Protección de Datos 2016/679, de 27 de abril (en vigor desde el día 25 de mayo de 2018) no se contiene una regulación específica en materia de tratamiento de datos de solvencia patrimonial. Esta ausencia de una regulación específica en el RGPD resulta cónsone con su carencia de previsiones sectoriales, sin perjuicio de que las normas nacionales hayan de adecuarse a los principios genéricos que establece en relación con el tratamiento de los datos personales. En particular, conforme al art. 6 del RGDP, los legisladores nacionales podrán concretar que el tratamiento de la información económico-financiera de un determinado sujeto por diferentes agentes –entidad suministradora de la información, entidad que la consulta y entidad gestora de los ficheros o bases de datos- es conforme a Derecho, bien exigiendo el consentimiento del interesado, bien remitiéndose a la exigencia de la necesidad del tratamiento *«para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales»;* pudiendo conjugarse estas exigencias con otras, como la necesidad del tratamiento *«para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales»,* o para *«el cumplimiento de una obligación legal aplicable al responsable del tratamiento»* -que resultarían predicables de las entidades prestamistas-*;* o, por último, *«para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento»* -que concurrirá en el caso de la creación de registros públicos-.

En el sentido indicado, en el *Dictamen del Consejo de Estado al Anteproyecto de Ley Orgánica de Protección de Datos* se advierte que la voluntad del legislador de la UE es que la determinación de las circunstancias en que un determinado sistema de información crediticia sea legítimo debe ser valorado, caso a caso, por el propio responsable del tratamiento y, en último término, por las autoridades de protección de datos y por los tribunales. A juicio de Consejo de Estado, esta decisión implica la necesaria desaparición de la regulación sobre estos tratamientos que se contenía en el art. 29 de la derogada LOPDP/1999 y la consiguiente supresión de la regulación contenida en el referido *Anteproyecto de Ley Orgánica de Protección de Datos*, añadiendo que *«la única área de intervención del legislador nacional en estos casos sería la relativa a aquellos sistemas de información crediticia que respondan a un determinado interés público, al amparo de lo dispuesto en el artículo 6.2 y 3 del Reglamento».* Concluye el Consejo de Estado en el referido Dictamen que, *«todo lo anterior ha de entenderse sin perjuicio de la ya apuntada posibilidad de redactar estas previsiones en forma de presunción* iuris tantum*, tal y como se indicó en las observaciones al artículo 9.3 del Anteproyecto».* Pues bien, precisamente en forma de presunción *«iuris tantum»* de licitud se ha redactado el art. 20.1 de la LOPDPGDD*,* en tanto que reputa lícito, salvo prueba en contrario, el tratamiento de datos personales relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito por sistemas comunes de información crediticia cuando se cumplan una serie de requisitos, entre los que la letra *e),* contempla –como ya se ha señalado- que los datos referidos a un deudor determinado solamente puedan ser consultados cuando quien consulte el sistema mantuviese una relación contractual con el afectado que implique el abono de una cuantía pecuniaria o este le hubiera solicitado la celebración de un contrato que suponga financiación, pago aplazado o facturación periódica, como sucede, entre otros supuestos, en los previstos en la legislación de contratos de crédito al consumo y de contratos de crédito inmobiliario. Además, el apartado 3º del mismo art. 20 de la LOPDPGDD precisa que la referida presunción no se extiende a los supuestos en que la información crediticia fuese asociada por la entidad que mantuviera el sistema a informaciones adicionales a las contempladas en dicho apartado, relacionadas con el deudor y obtenidas de otras fuentes, a fin de llevar a cabo un perfilado del mismo, en particular mediante la aplicación de técnicas de calificación crediticia.

[78]. Sobre estos requisitos aplicando la derogada LOPD, *vid.* SAN MARTÍN ARIAS, I.: *Protección de datos en el crédito al consumo,* Ed. Aranzadi, Cizur Menor, 2015., pgs. 55 y ss.

2) Que los datos incorporados al fichero o sistema de información crediticia se refieran a una deuda existente, cierta, vencida, exigible, que haya resultado impagada; siendo necesario, además, que su existencia y/o cuantía no haya resultado controvertida por el deudor en virtud de una reclamación administrativa, un procedimiento judicial o acudiendo a un sistema alternativo de resolución de conflictos entre las partes (un sistema de ADR) cuya resolución sea vinculante para las partes. Si la deuda es controvertida, la falta de pago no es indicativa de la insolvencia del deudor, de manera que su inclusión en un fichero de solvencia negativo no será conforme a Derecho y, en particular, no respetará la exigencia dimanante del principio de calidad de los datos. En esta circunstancia la inclusión de los datos del pretendido deudor en un fichero de la naturaleza que nos ocupa vulnerará el honor del titular de los mismo, como ha reconocido, *v.gr.* la SJPI Badajoz núm. 3 de 16 de julio de 2018 *[La Ley* 83953/2018].

3) Debe practicarse un requerimiento de pago previo a la inclusión en el fichero o sistema de información crediticia a la persona obligada al pago de la deuda.

4) No deben haber transcurrido más de cinco años –en la regulación previa a la LOPDPGDD este plazo era de seis años- desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto, de manera que, con independencia del cumplimiento, o no, de la obligación, los datos no pueden mantenerse en el fichero de solvencia más de seis años. Este límite de permanencia se deriva de la exigencia de veracidad y actualidad de los datos incorporados y el plazo de cinco años que contempla la letra *d)* del art. 20.1 de la LOPDPGDD concuerda con el plazo general de prescripción de las obligaciones de naturaleza personal que establece el art. 1964.2 del CC.

La inclusión de una persona en un fichero de esta naturaleza (fichero de solvencia negativo), sin que se cumplan estos presupuestos determina el nacimiento de una responsabilidad civil extracontractual de la persona, física o jurídica –ordinariamente una sociedad mercantil-, que los haya facilitado (*v.gr.,* STS 174/2018, de 23 de marzo [ROJ:STS 962/2018 - ECLI:ES:TS:2018:962], declarando la vulneración del derecho al honor y a la protección de datos personales por la inclusión en un registro de morosos de una deudor que había discutido de manera justificada la existencia de la deuda que motivó aquella inclusión; STS 512/2017, de 21 de septiembre [ROJ:STS 3322/2017 - ECLI:ES:TS:2017:3322], en relación con la vulneración del derecho al honor del usuario de servicios de telecomunicaciones al que se incluye en un registro de morosos por presunto impago de facturas[79]; con anterioridad, la STS 176/2013,

[79]. Sobre esta STS, *vid.* PEÑA LÓPEZ, F.: «Daños al honor. Intromisión ilegítima por inclusión indebida de datos en un fichero de morosos. Criterios de determinación del daño resarcible. Indemnizaciones simbólicas: Comentario a la STS de 21 septiembre 2017», en *CCJC,* núm. 106, 2018, pp. 225 a 238. *Vid.,* también, entre otros, RUBIO TORRANO, E.: «Inclusión indebida en fichero de morosos: intromisión ilegítima en el derecho al honor», *Revista Doctrinal Aranzadi Civil-Mercantil,* núm. 7/2012 (BIB 2012\3143); GARCÍA PÉREZ, C.L.: «Intromisión ilegítima en el derecho al honor y protección de datos. Especial referencia a su afectación por ingreso en registros de moroso», en *Daño, responsabilidad y seguro* (M.J. HERRADOR GUARDIA, DIR.), *op. cit.*, especialmente las pgs. 406 y ss.; CUENA CASAS, M.: «Préstamo responsable y datos de solvencia patrimonial en la Ley Reguladora de los Contratos de Crédito Inmobiliario», *Actualidad Civil,* núm. 9, 2019; BUSTO LAGO, J.M.: «El deber de evaluar la

de 6 de marzo [ROJ:STS 1715/2013 - ECLI:ES:TS:2013:1715] consideró concurrente la lesión del derecho al honor de una persona física cuyos datos habían sido incorporados a un fichero negativo de solvencia patrimonial, siendo dudosa la existencia de la deuda que motivó la comunicación de los referidos datos por la entidad financiera pretendidamente acreedora; la STS 226/2012, de 9 de abril [ROJ:STS 2638/2012 - ECLI:ES:TS:2012:2638], estimó la vulneración del derecho al honor de una persona jurídica en estos supuestos de inclusión errónea en un registro de morosos y la STS 899/2011, de 30 de noviembre [ROJ:STS 8213/2011 - ECLI:ES:TS:2011:8213], apreció la concurrencia de daños continuados en el caso de inclusión indebida en estos registros, entre el momento de la indebida inclusión y hasta el momento en el que se da de baja).

Los datos que sobre el deudor se suministran al fichero o sistema de información crediticia son lo que la LOPDPGDD llama pertinentes, exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si cumplen con estos requisitos, la incorporación en el fichero no afecta al honor de la persona en cuanto se derive que no es moroso, como precisó la STS 586/2017, de 2 de noviembre [ROJ:STS 3799/2017 - ECLI:ES:TS:2017:3799], en el caso de incorporación de los datos de una persona referidos al riesgo indirecto por su condición de avalista de la sociedad de la que fue socio). El acreedor no puede incorporar a estos ficheros más información que la necesaria en orden a satisfacer la finalidad de estos, consistente, en esencia, en la identificación del deudor y el origen e importe de la deuda no satisfecha tempestivamente.

En todo caso, ha de tenerse en cuenta que el daño moral puede presentar relevancia *per se»*, sin necesidad de aparecer vinculado a una daño de naturaleza patrimonial (así se contempla expresamente, *v.gr.*, en el art. 140 del TRLPI y así sucede también en muchas ocasiones en el ámbito de aplicación de la LO 1/1982[80]).

9.4. El llamado derecho al olvido y las consecuencias jurídicas de su infracción

Otro supuesto paradigmático en el que la jurisprudencia ha reconocido al perjudicado el derecho a obtener una indemnización es el caso de la infracción del denominado derecho al olvido digital. El reconocimiento expreso del llamado derecho al olvido, especialmente en Internet (art. 93 de la LOPDPGDD y art. 151-6.5 de la *Propuesta de CC* elaborada por la APDC), se ha producido a partir de la STJUE de 13 de mayo de 2014 (asunto C-131/12, *Mario Costeja*) y de la STS 210/2016, de 5 de abril [RJ 2016\1006][81]. Se reconoce el derecho al olvido, tanto de la información que el propio interesado haya consentido en desvelar en su día como de

solvencia del consumidor de crédito como mecanismo de prevención del sobreendeudamiento y su regulación en España», en *Sobreendeudamiento de consumidores. Estrategias para garantizar una segunda oportunidad* (M. CARBALLO FIDALGO, COORD.), Ed. J.Mª Bosch, Barcelona, 2019, especialmente las pgs. 36 a 42.

[80] Así se contempla, también de manera expresa, en el inciso segundo del art. 18.2 de la Ley 51/2003, de 2 de diciembre, *de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad* [BOE núm. 289, de 3 de diciembre de 2003].

[81] Entre otros muchos estudios sobre esta STJUE, puede verse, GARCÍA GARNICA, Mª C.: «La protección de los datos personales frente a su tratamiento on-line tras la Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014», en *Estudios sobre Jurisprudencia Europea (Materiales del I y II Encuentro anual del Centro español del European Law Institue)* (A. RUDA GONZÁLEZ y C. JEREZ DELGADO, DIRS.), Ed. Sepin, Madrid, 2017, pgs. 543 a 561.

aquellos datos que, afectando a sus derechos de la personalidad, se hayan publicado lícitamente, y se conserven en sistemas de búsqueda y almacenamiento de datos. Transcurridos cinco años el interesado debe contar con algún cauce para poder eliminar el acceso a dicha información. Se trata de un plazo razonable, coincidente con el que el Código Penal establece para la cancelación de los antecedentes penales en las penas menos graves, iguales o superiores a tres años (art. 136 del CP), así como con el propio de la prescripción general de las acciones personales (art. 1964.2 del CC).

Son numerosas las Sentencias de la Sala de lo Contencioso-Administrativo de la AN que ha reconocido el derecho al olvido en Internet en relación con motores de búsqueda y la exigencia de eliminación de datos personales con fundamento el ejercicio de los derechos de oposición y de cancelación del titular del mismo, en todos aquellos casos en los que se ha determinado que no prevalece un interés público que justifique el mantenimiento de datos, por diversos motivos en los que subyace el perjuicio del titular de los referidos datos, en el ámbito laboral (*v.gr.* SAN, C-Adm, de 28 de enero de 2015 [JUR 2015\57452]) así como en aquellos casos en los que se vincula al interesado con conductas penalmente relevantes (*v.gr.* SSAN, C-Adm, de 29 de diciembre de 2014 [JUR 2015\26504] y de 20 de febrero de 2015 [JUR 2015\104978]); incluyendo los supuestos de publicación en páginas *web* de sentencias sin anonimizar (SAN, C-Adm, 155/2015, de 31 de marzo [RJCA 2015\600]). El derecho al olvido puede ejercitarse solicitando la adopción de medidas que impidan la indexación de los datos publicados en diarios oficiales (SAN, C-Adm, 121/2015, de 13 de marzo [JUR 2015\104161]), siempre que concurran los presupuestos enunciados por la STJUE de 13 de mayo de 2014 (asunto C-131/12), así como en medios de comunicación, en aquellos casos de noticias antiguas[82], con errores en la información facilitada y relativas a personas sin relevancia pública (SAN, C-Adm, 341/2015, de 2 de octubre [RJCA 2015\869]). Por el contrario, no procede en relación con la publicación de información sobre hechos de extraordinaria gravedad e impacto social como es el caso de la atinente a una persona juzgada por un delito grave y absuelta por falta de prueba de cargo, no cabiendo el silenciamiento del nombre y apellidos del afectado, habida cuenta, además, del escaso tiempo transcurrido desde el juicio (STS 426/2017, de 6 de julio [RJ 2017\3194]).

La STS 210/2016, de 5 de abril [RJ 2016\1006] confirmó la SAP Barcelona, Secc. 16ª, 364/2014, de 17 de julio [AC 2014\1661], en virtud de la que se condenó a *Google Spain, S.L.* a indemnizar al actor en la suma de 8.000,00 € por considerar que se había vulnerado por la entidad demandada su derecho a la protección de datos personales: determinados buscadores de Internet, entre los que se encontraba *Google»,* permitían enlazar el nombre del actor con el contenido del BOE que publicaba un indulto que le había sido concedido en el año 1999. El actor ejercitó el derecho al olvido, ejercitando simultáneamente las acciones fundadas en la LO 1/1982 y la acción indemnizatoria *ex* art. 19 de la LOPD. El TS consideró que el núcleo de la controversia lo constituye, en el supuesto sometido a su consideración, la responsabilidad de las entidades demandadas por el daño causado al actor por la infracción de su derecho a la protección de los datos personales, sin perjuicio de considerar que, en cuanto al derecho al honor, que la información de que una persona fue condenada por cometer un delito contra la

[82] La STS 545/2015, de 15 de octubre [RJ 2015\4417] consideró que el derecho al olvido ha de ser reconocido en relación con informaciones y hechos ocurridos mucho tiempo atarás. Sobre esta STS, *vid.* RUDA GONZÁLEZ, A.: «Indemnización por daños al derecho al olvido. La responsabilidad por la no exclusión de la indexación de una hemeroteca digital por los buscadores generales (Caso El País). Comentario a la Sentencia de 15 de octubre de 2015 (RJ 2015, 4417)», en *CCJC*, núm. 101, 2016 [BIB 2016\4040].

salud pública, obtenida a partir de la información sobre el indulto de la pena impuesta por la comisión del referido delito, puede afectar a la buena reputación de la persona y, en consecuencia, hacerle desmerecer en la consideración ajena, generando descrédito social.

La STJUE de 24 de septiembre de 2019 (asunto C-507/17, *Google vs. CNIL*) vino a determinar la extensión de la obligación del gestor de un motor de búsqueda cuando recibe una solicitud de retirada de enlaces, señalando que no estará obligado a proceder a dicha retirada en todas las versiones de su motor, sino en las versiones de éste que correspondan al conjunto del Estados miembros, combinándolas, en caso necesario, con medidas que impidan de manera efectiva o, al menos, dificulten seriamente a los internatutas que obtengan resultados de sus búsquedas que los redirijan a los enlaces objeto de la solicitud de retirada[83].

10 LA INDEMNIZACIÓN DEL TITULAR DE LOS DATOS PERSONALES QUE HA RESULTADO DAÑADO O PERJUDICADO

10.1. Precisiones generales sobre la acción ejercitando el derecho a la indemnización por el interesado perjudicado

El derecho a indemnización del interesado que reconoce el art. 82 del RGPD, en los términos ya expuestos, ampara el ejercicio de la acción indemnizatoria o resarcitoria del daño o perjuicio patrimonial o extrapatrimonial, que se ejercitará ante los tribunales competentes, que en nuestro caso sería la vía jurisdiccional civil, para que pueda obtener una indemnización de aquellos daños o perjuicios. El art. 82.6 del RGPD establece que las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes de conformidad con el Derecho del Estado miembro que se indica en el art. 79.2 del propio RGPD, lo que determina la competencia, objetiva y funcional, de los juzgados de primera instancia, determinándose la competencia territorial de conformidad con las previsiones de los arts. 51 y 52 de la LECiv[84]. En efecto, la competencia de los órganos jurisdiccionales civiles se extiende al conocimiento de todas las materias que no estén expresamente atribuidas a otros órdenes jurisdiccionales, de conformidad con la *vis attractiva»* de que la dota el art. 9.2 de la LOPJ, si bien ha de tenerse en cuenta que algunos autores provenientes del ámbito social o laboral del

[83] *Vid.* DE DIEGO ARIAS, J. L.: «Derecho de supresión o derecho al olvido: sobre la extensión de la obligación del gestor de un motor de búsqueda cuando recibe una solicitud de retirada de enlaces», *Diario La Ley*, 29 de octubre de 2019 («Comentarios»).

[84] El cauce procesal será el juicio ordinario de conformidad con lo dispuesto en el art. 249.1.2º de la LECiv/2000, a tenor del cual, se decidirán en el juicio ordinario, cualquiera que sea su cuantía, las demandas que pretendan la tutela del derecho al honor, a la intimidad y a la propia imagen, así como las que pidan la tutela civil de cualquier otro derecho fundamental (excepción hecha de las que se refieran al derecho de rectificación), al tiempo que precisa que será siempre parte el Ministerio Fiscal y que su tramitación será preferente, dando así satisfacción a las exigencias constitucionales de un procedimiento basado en los principios de preferencia y sumariedad para la tutela de los derechos fundamentales *ex* art. 53.2 de la CE[84]. Frente a este parecer, el Auto de la AP de Cádiz, Secc. 7ª, de 30 de enero de 2004 [AC 2004\635], revocando el Auto dictado por el JPI núm. 4 de Algeciras, consideró que las acciones ejercitando acciones indemnizatorias con fundamento en los dispuesto en el art. 19 de la LOPDCP han de tramitarse por el procedimiento que corresponda –verbal u ordinario- según la cuantía que sea objeto de reclamación y ello en virtud de la remisión que realizar el propio art. 19 de la LOPDCP a la jurisdicción ordinaria, frente a lo que sucede en aquellos supuestos en los que se ejercita una acción con fundamento en la previsiones de la LO 1/1982.

Derecho han considerado que se ampara el reconocimiento de la competencia de la jurisdicción social para conocer de aquellos supuestos en los que la acción de responsabilidad civil sea ejercitada por un trabajador frente al empresario o empleador en el marco de la relación laboral que les vincula (*ex* arts. 25 de la LOPJ y 2.*b)* de la LJS/2011). En efecto, estos autores afirman con rotundidad la competencia de la jurisdicción social para conocer de las reclamaciones ejercitadas por un trabajador que considere vulnerado su derecho a la autodeterminación informática[85].

La indemnización puede reclamarse ante cualquier responsable o encargado del tratamiento que, como consecuencia de una infracción del RGPD en el tratamiento de los datos personales, cause un daño o perjuicio material o extrapatrimonial al interesado, resultando de aplicación la regla de la solidaridad entre los múltiples responsables que hayan podido concurrir a la causación del daño, de conformidad con la previsión del Considerando 146 del RGPD, a tenor del cual si los responsables o encargados participan en el mismo tratamiento, cada responsable o encargado debe ser considerado responsable de la totalidad de los daños y perjuicios. Con la finalidad de garantizar que el interesado que haya sufrido un daño sea indemnizado, el art. 82.4 del RGPD prescribe que cuando haya varios responsables o encargados del tratamiento o también cuando un responsable y un encargado hayan participado en la misma operación de tratamiento sean responsables de cualquier daño o perjuicio causado por dicho tratamiento, cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado. Sin perjuicio de esta responsabilidad solidaria, como es propio de este tipo de responsabilidad, en el ámbito de la relación interna, el responsable o el encargado que pague una indemnización total tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados (*ex* art. 82.5 del RGPD).

10.2. Criterios jurisprudenciales sobre el derecho a la indemnización

El art. 82.1 del RGPD ampara la aplicación, también en este ámbito de la responsabilidad civil, del principio general constituido por la reparación integral del daño causado, si se quiere que cumpla su prístina función reparadora[86], siendo indemnizables tanto los daños pa-

[85] Entre otros, FERNÁNDEZ VILLAZÓN, L.A.: «Tratamiento automatizado da datos personales en los procesos de selección de trabajadores», *Relaciones laborales*, T. I, 1994, pg. 534; THIBAULT ARANDA, J.: «El Derecho español», en *Tecnología informática y privacidad de los trabajadores* (M. JEFFERY / J. THIBAULT / Á. JURADO, COORDS.), Ed. Aranzadi, Cizur Menor, 2003, pgs. 91 y 92. Con carácter general, *vid.* GÓMEZ LIGÜERRE, C.: *Derecho aplicable y jurisdicción competente en pleitos de responsabilidad civil extracontractual*, Ed. M. Pons, Madrid, 2019, pgs. 237 y ss.

[86] Se trata, en efecto, de un principio vigente en la generalidad de los Ordenamientos jurídicos europeos, aunque no indiscutible desde una perspectiva estrictamente teórica. Entre otras muchas resoluciones del orden

trimoniales, como los daños morales o extrapatrimoniales que haya podido sufrir el perjudicado[87]. En este sentido, el Considerando 146 del RGPD afirma que *el responsable o el encargado del tratamiento debe indemnizar cualesquiera daños y perjuicios que pueda sufrir una persona como consecuencia de un tratamiento en infracción del presente Reglamento»*. Este precisión no resulta especialmente relevante en un sistema de daños como el español en el que resulten resarcibles todos los daños, de acuerdo con la premisas propias de un sistema atípico de derechos e intereses legítimos indemnizables, alcanzando su virtualidad en sistemas u ordenamientos caracterizados por la tipicidad de los derechos e intereses jurídicamente protegidos resarcibles a través del instrumento de la responsabilidad civil extracontractual, así como en sistemas también atípicos, como es el caso del Derecho italiano, en el que se restringe o limita el daño extrapatrimonial susceptible de resarcimiento.

El referido Considerando 146 del RGPD indica que, en orden a la determinación de la indemnización del perjudicado por una actuación lesiva con ocasión del tratamiento de datos personales imputable habrá que atender a la jurisprudencia del TJUE. La STS de 210/2016, de 5 de abril [RJ 2016\1006] recuerda que no son admisibles las indemnizaciones de carácter meramente simbólico[88] y, por otra parte, son numerosas las Sentencias de la misma Sala de lo Civil en las que, a propósito de la lesión del derecho al honor derivada de la indebida inclusión en un registro de morosos, señalan que la escasa cuantía de la deuda no disminuye la importancia del daño moral que le causó al perjudicado la inclusión en los registros de morosos (*v.gr.* STS 261/2017, de 26 de abril [RJ 2017\1737]).

Por otra parte, conforme a los criterios generales de articulación de la indemnización en el ámbito de la responsabilidad civil extracontractual, han de tenerse en cuenta, por un lado, los daños patrimoniales concretos, fácilmente verificables y cuantificables; pero también, en su caso, los extrapatrimoniales o morales derivados del desprestigio y deterioro de la imagen de solvencia personal y profesional, de cuantificación estimativa. Así, de conformidad con lo que resulta de los apartados 4 y 5 del F.D. 5º de la STS 81/2015, de 18 de febrero [RJ 2015\574], el perjuicio indemnizable ha de incluir el daño patrimonial, y en él, tanto los daños patrimoniales concretos, fácilmente verificables y cuantificables (por ejemplo, el derivado de que el afectado hubiera tenido que pagar un mayor interés por conseguir financiación al estar incluidos sus datos personales en uno de estos registros), como los daños patrimoniales más difusos pero también reales e indemnizables, como son los derivados de la imposibilidad o dificultad para obtener crédito o contratar servicios (puesto que este tipo de registros está

jurisdiccional contencioso-administrativo que afirman la vigencia de este principio, *vid.*, SSTS (Sala 3ª) de 5 de abril de 1989 [RJ 21989\816], de 18 de julio de 1989 [RJ 1989\5836], de 15 de octubre de 1990 [RJ 1990\8127), de 4 de mayo de 1995 [RJ 1995\4210], de 30 de junio de 1999 [RJ 1999\6336] y 84/2020, de 27 de marzo [RJ 2020\35126] y ATS (Sala 3ª) de 3 de febrero de 1984 [RJ 1984\1021]; y, en la jurisdicción civil, *v.gr.*, SSTS, Sala 1ª, 50/2020, de 22 de enero [RJ 2020\61] y ATS de 20 de febrero de 2019 [JUR 2019\72037]

[87] En este sentido, por todos, GRIMALT SERVERA, P.: «Intromisiones ilegítimas en los derechos al honor, a la intimidad y a la propia imagen: tutela civil versus tutela administrativa», en *Protección de datos personales* (APDC), *op. cit.*, pg 360.

[88] El motivo por el cual el TS declara la inadmisibilidad de estas indemnizaciones simbólicas radica en que con este tipo de indemnizaciones *«se convierte la garantía jurisdiccional en un acto meramente ritual o simbólico incompatible con el contenido de los artículos 9.1, 1.1 y 53.2 CE y la correlativa exigencia de una reparación acorde con el relieve de los valores e intereses en juego»* (*cfr.* SSTS de 12 de diciembre de 2011 [RJ 2012\35] y de 4 de diciembre de 2014 [RJ 2014\6360]. En esencia, la interdicción de las indemnizaciones simbólicas tiene que ver esencialmente con el especial valor que tienen los derechos fundamentales que son objeto de tutela en estos casos. La trascendencia de estos derechos es el factor que que impide que su lesión se pueda indemnizar con una suma meramente simbólica o de carácter irrisorio.

destinado justamente a advertir a los operadores económicos de los incumplimientos de obligaciones dinerarias de las personas cuyos datos han sido incluidos en ellos) y también los daños derivados del desprestigio y del deterioro de la imagen de solvencia personal y profesional causados por dicha inclusión en el registro, cuya cuantificación ha de ser necesariamente estimativa. En efecto, la indemnización también ha de resarcir el daño moral, entendido como aquel que no afecta a los bienes materiales que integran el patrimonio de una persona, sino que supone un menoscabo de la persona en sí misma, de los bienes ligados a la personalidad, por cuanto que afectan a alguna de las características que integran el núcleo de la personalidad, como es en este caso la dignidad. La determinación de la cuantía de la indemnización por estos daños morales ha de ser también estimativa.

Las dificultades inherentes a la valoración del daño moral o extrapatrimonial resultan evidentes[89]. Por esta razón y por la identidad de naturaleza de los derechos lesionados, se ha postulado la aplicación analógica a este supuesto de los criterios de valoración del daño moral contemplados en el inciso final del art. 9.3 de la LO 1/1982 y en el párrafo segundo del mismo precepto –similares a los criterios contemplados en el párrafo 2º del art. 140 del TRLPI para la valoración del daño moral derivado de la infracción de los derechos protegidos por esta norma- y que habrán de ser tenidos en cuenta por el Juzgador a estos efectos: las circunstancias del caso y la gravedad de la lesión efectivamente producida -a cuyos efectos resulta relevante la difusión o audiencia del medio a través del que se haya producido-, así como el beneficio que, en su caso, haya obtenido el causante de la lesión. En este orden de consideraciones, sin mayores precisiones, *v.gr.*, la SAP de Barcelona, Secc. 1ª, de 13 de mayo de 2005 [AC 2005\990], en un supuesto en el que se ventilaba una acción de responsabilidad civil por vulneración del derecho al honor de la actora como consecuencia de su inclusión indebida en un fichero de solvencia patrimonial, le concedió una indemnización que cifra en 3.000,00 € (la actora había solicitado 18.000,00 €, si bien, fundamentalmente a efectos de imposición de las costas procesales del procedimiento –*ex* art. 394.1 de la LECiv-, se consideró estimada íntegramente la demanda[90]) y ello únicamente sobre la consideración de la poca difusión acreditada de los hechos y de que la exacta valoración de la indemnización es una cuestión sometida al criterio discrecional del órgano jurisdiccional. La aplicación de los criterios de cuantificación del daño moral que contempla el art. 9.3 de la LO 1/1982 se justifica en algunas resoluciones jurisprudenciales sobre el fundamento de la infracción del derecho al honor que es objeto de tutela por aquella Ley, cuando ésta traiga causa de la infracción de la normativa de datos personales. Así sucede, *v.gr*., en la SAP de Madrid, Secc. 19ª, de 20 de diciembre de 2004 [EDJ 2004\246333], en cuyo F.D. 2º se precisa que la inclusión indebida de los datos personales de la actora en un fichero de solvencia patrimonial es una infracción del derecho al honor de aquélla en una de sus manifestaciones o aspectos más delicados y prestigiosos del tráfico, cual

[89] Pueden verse, entre otros, GÓMEZ POMAR, F. y PENALVA ZUASTI, J.: «Capítulo II. Problemas de concepto, valoración y cuantificación del daño moral (Análisis económico del Derecho)», en *El daño moral y su cuantificación* (F. GÓMEZ POMAR e I. MARÍN GARCÍA, DIRS.), Ed. Bosch, Barcelona, 2017 (2ª edic.), pgs.73 y ss.; HERRÁN ORTIZ, A. I.: *El derecho a la intimidad en la nueva Ley Orgánica de protección de datos personales*, Ed. Dykinson, Madrid, 2004, pg. 258.

[90] Con todo, el plausible criterio sostenido por la SAP de Barcelona, Secc. 1ª, de 13 de mayo de 2005 [AC 2005\990] a efectos de imposición de las costas procesales derivadas de la tramitación del procedimiento, no puede considerarse generalizado, sirviendo como ejemplo de doctrina contradictoria, la SAP de Toledo, Secc. 2ª, de 12 de julio de 2004 [EDJ 2004\81704], en la que no se imponen las costas procesales a ninguna de las partes procesales, en tanto que se estimaba la demanda pero se condena a la entidad demandada a pagar al actor la suma 3.005,60 €, cuando se habían solicitado 18.030,36 €.

es el crédito comercial, con menoscabo de su fama y que no se produce al amparo de la LOPDCP, sino de la LO 1/1982, de 5 de mayo. En todo caso, ha de tenerse en cuenta que los daños morales o extrapatrimoniales incluyen los daños "*consistentes en la afectación de la dignidad en su aspecto interno o subjetivo*" reconducibles a lo que doctrinalmente se denominan daños morales objetivos o daños funcionales; los daños derivados de la lesión del honor en su aspecto "*externo u objetivo relativo a la consideración de las demás personas*" y los consistentes en el "*quebranto y la angustia*", derivados de la inclusión en el registro negativo de solvencia patrimonial, que no son otra cosa que los habitualmente denominados o conocidos como daños morales puros o *pecunia doloris»*. Estos último son daños especialmente difíciles de probar y de cuantificar y, en esta labor el respeto al principio de igualdad debe jugar un papel importante (daños de este tipo se intentaron probar sin éxito en el caso resuelto, *v.gr.*, por la STS de 12 de mayo de 2015 [RJ 2015\2027]).

A efectos de calcular o cuantificar la indemnización derivada de daño moral se ha propuesto también la utilización analógica de las cuantías previstas para las sanciones administrativas que pueden imponerse al responsable del tratamiento de los datos en función de cuál haya sido el comportamiento del que se ha derivado el daño para el interesado y cuyo resarcimiento se pretende (*ex* art. 83 del RGPD, en relación con el art. 76 de la LOPDPGDD)[91]. La aceptación de este último criterio choca, sin embargo, con las distintas funciones y principios que inspiran el instituto de la responsabilidad civil y el instituto de la infracción y la sanción administrativa careciendo el primero, con carácter general, en el marco del Ordenamiento jurídico español de una función punitiva, que es propia del segundo y correspondiéndole una función prístinamente reparadora, sin perjuicio de que de ella puedan derivarse, como corolarios, funciones de prevención.

Por otra parte, procede recordar que, sin perjuicio de la adopción de medidas tendentes a evitar la reiteración del daño en el futuro –la cesación de las conductas lesivas-, la doctrina ha considerado la posibilidad de que el fallo de la Sentencia que estime la acción de responsabilidad civil ejercitada por el perjudicado establezca otras medidas de reparación distintas a la indemnización o compensación pecuniaria –formas de reparación no pecuniarias que se reputan como especialmente idóneas para la reparación del daño no patrimonial[92]- como pueden ser la rectificación de la información, la cesación en la utilización del fichero de datos personales objeto de tratamiento –que puede adoptarse cautelarmente con fundamento en el art. 727.11 de la LECiv y cumpliéndose los requisitos contemplados en los arts. 728 y concordantes de la Ley procesal civil (se trata de una media prevista expresamente en el art. 59 de la LOPDPGDD, para el caso de tratamientos contrarios a las previsiones del RGPD, que puede ser adoptada en el seno del procedimiento sancionador, por la propia AEPD[93])- o la publicación de la sentencia (aplicando analógicamente lo dispuesto en el art. 9.2 de la LO

[91] En este sentido, RUIZ CARRILLO, A.: *Los datos de carácter personal (Concepto, requisitos de circulación, procedimientos y formularios)*, Ed. Bosch, Barcelona, 1999, pgs. 36 y 37; *ibidem*, *La protección de los datos de carácter personal*, Ed. Bosch, Barcelona, 2001, pg. 109.

[92] *Vid.*, entre otros, SALVI, C.: *La responsabilità civile*, Giufrrè Editore, Milán, 1998, pgs. 233 a 237.

[93] Además de la imposición de sanciones pecuniarias (multas) al autor / responsable de la infracción administrativa, de acuerdo con el art. 76.3 de la LOPDGDD, a tenor de la previsión del art. 58.2 del RGPD, la AEPD puede adoptar otras medidas complementarias, como la consistente en imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición (apartado *f*), *«ordenar la rectificación o supresión de datos personales o la limitación del tratamiento»* (aparatado *g*) u *«ordenar la suspensión de flujos hacia un destinatario situado en un tercer país o hacia una organización internacional»* (apartado *j*).

1/1982)[94]. Sin embargo, esta interpretación plausible choca con el tenor literal del 92 del RGPD –en este sentido similar a los derogados arts. 19.1 de la LOPDCP y 17.3 de la LORTAD- rubricado precisamente *derecho a la indemnización y responsabilidad»* y en el que se otorga a los interesados que hayan experimentado un perjuicio, un derecho *a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos»*, a diferencia, *v.gr.*, del término *reparación»* del daño que se utiliza en el art. 1902 del CC y en el que se comprende tanto la reparación *in natura»*, como la reparación mediante equivalente pecuniario; todo ello sin perjuicio del ejercicio del derecho de rectificación en Internet que establece el art. 85 de la LOPDPGDD.

11 PROCEDIMIENTO ADMINISTRATIVO SANCIONADOR Y ACCIÓN INDEMNIZATORIA

Conocido es que tanto el Derecho previo a la entrada en vigor del RGPD, como el resultante de éste, contemplan la concurrencia de la tutela pública y privada de los derechos fundamentales y subjetivos que se pretenden proteger con la normativa reguladora del tratamiento de datos personales: los derechos fundamentales a la intimidad y a la privada, así como el derecho específico a la protección de los datos personales reconocido, de manera expresa, por los arts. 18.4 de la CE, 16.1 del TFUE y 8 de la Carta de los Derechos Fundamentales de la UE[95]. Esta doble tutela parece desprenderse del art. 79.1 del RGPD, en tanto que dispone que *sin perjuicio de los recursos administrativos o extrajudiciales disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control en virtud del artículo 77, todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales».* Sin perjuicio de que, en hipótesis, el precepto pueda dejar abierta la posibilidad de que las normas nacionales atribuyan a las autoridades administrativas de control el conocimiento de las reclamaciones indemnizatorias[96], lo que sí es claro es que contempla la

[94] En este sentido se pronuncia GRIMALT SERVERA, P.: *La responsabilidad civil en el tratamiento automatizado de datos personales*, *op. cit,* pg. 338.

[95] La protección reforzada del derecho a la protección de los datos personales ha sido objeto de reiterado reconocimiento por la jurisprudencia del TJUE, *v.gr.*, Sentencias de 20 de mayo de 2003 (asuntos acumulados C-465/00, C-138/01 y C-139/01), de 29 de enero de 2008 (asunto C-275/06) y de 21 de diciembre de 2016 (asuntos acumulados C-203/15 y C-698/15).

[96] Acaso proceda recordar que la atribución de facultades de reconocimiento de indemnizaciones de daños y perjuicios a cargo de un sujeto privado y a favor de otro a una autoridad administrativa no es algo ajeno a nuestro Derecho. Sirva a estos efectos como significativo ejemplo el art. 48 del TRLGDCU, rubricado *«Reposición de la situación alterada por la infracción e indemnización de daños y perjuicios».* Este precepto trae causa de la idea suscitado por algunos autores y por el Consejo Económico y Social de España en su Informe sobre «los derechos del consumidor y la transparencia de mercado», aprobado en su sesión plenaria de 17 de febrero de 1999, de la bondad de atribuir a los órganos administrativos de consumo competencias para liquidar daños y perjuicios ocasionados a los consumidores y usuarios por empresarios o profesionales como consecuencia de infracciones de normas propias del Derecho de consumo. En este sentido se han pronunciado, CARRASCO PERERA, Á: *El Derecho de consumo en España: Presente y futuro*, Ed. INC, Madrid, 2002, pgs. 293 a 295; CORDERO LOBATO, E.: «Resolución y liquidación de la responsabilidad civil jurídico privada en los procedimientos administrativos», *Centro de Estudios de Consumo,* Universidad de Castilla – La Mancha, enero de 2003. Sobre el art. 48 del TRLGDCU, *vid.,* entre otros, VELASCO CABALLERO, F.; DÍEZ SASTRE, S. y RODRÍGUEZ-CHAVES MIMBRERO, B.: «Comentario del artículo 48 del TRLGDC», en *Comentario del Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras Leyes Complementarias* (R. BERCOVITZ RODRÍGUEZ-CANO, COORD.), Ed.

existencia de una protección jurídico-pública del derecho a la protección de los datos personales, junto con una protección jurídico-privada vinculada a la lesión de este derecho.

La cuestión fundamental que suscita esta doble tutela de los derechos vinculados a los datos personales de la persona física radica en determinar si el ejercicio de una acción de responsabilidad civil por parte del interesado perjudicado –el titular de los datos personales- requiere un previo pronunciamiento de la autoridad administrativa de protección de datos personales, en tanto que, como se ha señalado *supra* §.6, el presupuesto objetivo de la responsabilidad civil en que pueden incurrir el responsable y/o el encargado de tratamiento está constituido por la concurrencia de una conducta infractora de la normativa de protección de datos personales. El art. 42 de la LECiv permite argumentar una respuesta negativa, en tanto que prevé que los solos efectos prejudiciales, los tribunales civiles pueden conocer de asuntos que están atribuidos a los tribunales del orden jurisdiccional contencioso-administrativo[97]. En relación con esta cuestión, la derogada LOPDCP resolvió, de modo definitivo y adecuado, la duda que suscitaba el art. 17 de la LORTAD al regular en un mismo precepto y de manera conjunta la tutela de los derechos de los interesados que se atribuía a la AEPD y el derecho a la indemnización que se otorgaba a los interesados[98]. La previsión formalmente separada de la tutela de los derechos de los interesados frente a actuaciones contrarias a lo dispuesto en la LOPDCP que se atribuye a la Agencia –sin perjuicio de la virtualidad de las reclamaciones que se ejerciten ante ella en orden a obtener determinadas medidas e incluso pronunciamientos que puedan esgrimirse a modo de prueba en la jurisdicción civil- y el derecho a la indemnización, en los arts. 18 y 19 de la LOPDCP, respectivamente, parece haber resuelto definitivamente aquella cuestión de un modo acorde con los principios generales del Ordenamiento jurídico español.

En el mismo sentido y manteniendo la respuesta argumentada en el régimen jurídico previo a la entrada en vigor del RGPD y de la LOPDPGDD, la ya citada STS de 210/2016, de 5 de abril [RJ 2016\1006] –confirmando la SAP Barcelona, Secc. 16ª, 364/2014, de 17 julio [AC 2014\1661]- recuerda que el perjudicado por un tratamiento ilícito de sus datos personales puede dirigirse frente a la AEPD, denunciado la infracción administrativa –y exigir, acumuladamente, que se le reponga en el ejercicio de los derechos que respecto de sus datos personales le reconoce el Derecho, de conformidad con las previsiones de los arts. 19 y 77 del RGPD-

Aranzdi, Cizur Menor, 2015 (2ª edic.), pgs. 604 y ss. Sin embargo, este no es el sistema acogido en el ámbito de los daños ocasionados por el ilícito tratamiento de datos personales, como han precisado, *v.gr.*, las Resoluciones de la AEPD R/03002/2017, de 15 de noviembre y R/00606/2016, de 9 de septiembre; así como las SSAN, Sala de lo Contencioso-Administrativo, de 1 de octubre de 2008 [RJCA 2009\310] y 248/2015, de 24 de marzo [JUR 2015\179600].

[97] En este sentido puede verse, *v.gr.*, la SAP A Coruña, Secc. 4ª, 164/2003, de 12 de junio [AC 2003\1756].

[98] En este sentido, expresamente, VIZCAÍNO CALDERÓN, M.: «Comentario al artículo 19 de la LOPDCP», *op. cit.*, pg. 225. Sobre el texto de la derogada LORTAD, GRIMALT SERVERA, P.: *La responsabilidad civil en el tratamiento automatizado de datos personales*, *op. cit.*, pgs. 306 y 307. En este mismo contexto normativo (vigencia del art. 17 de la LORTAD) afirmaba categóricamente que, como presupuesto previo, toda acción de reparación de daños y perjuicios debería ser sustanciada ante la Agencia de Protección de Datos, incluso cuando se trate de daños derivados de ficheros de titularidad privada, ÁLVAREZ-CIENFUEGOS SUÁREZ, J. Mª: *La defensa de la intimidad de los ciudadanos y la tecnología informática*, Ed. Aranzadi, Pamplona, 1999, pgs. 51 y 52.

La tesis que se sostiene es compartida en otros Ordenamientos jurídicos comparados, como es el caso, *v.gr.*, del italiano en el que el organismo equivalente a la Agencia de Protección de Datos, denominado *«Garante»*, con fecha 26 de octubre de 1999, ha rechazado un recurso ejercitado por un particular que pretendía el resarcimiento del daño que había sufrido como consecuencia del tratamiento ilícito de sus datos personales, declarando expresamente su incompetencia para conocer de esta cuestión, recordando que las pretensiones de esta naturaleza deben ser ejercitadas ante los órganos de la jurisdicción ordinaria.

, así como ejercitar una acción indemnizatoria frente al responsable o frente al encargado del tratamiento autores del tratamiento ilícito, no exigiendo la acción civil, como requisito o presupuesto de la misma la formulación de la denuncia administrativa, sino: (1) la concurrencia de un incumplimiento de la normativa reguladora de la protección de datos personales imputable al responsable o al encargado de tratamiento, sin que resulte preciso que este incumplimiento o la infracción de la normativa reguladora del tratamiento de datos personales haya sido declarada por la autoridad administrativa y, en particular, por la AEPD, de manera que los Tribunales civiles, a estos efectos, son plenamente competentes para valorar y calificar la existencia de una conculcación de la normativa relativa a la protección de datos personales[99]; y, (2) que al referido incumplimiento pueda vincularse causalmente el daño o perjuicio cuyo resarcimiento se pretende.

■ CONCLUSIONES

De lo expuesto en los apartados que anteceden, pueden derivarse las conclusiones que siguen en relación con el régimen de responsabilidad civil aplicable a los daños y perjuicios ocasionado como consecuencia del tratamiento de datos personales:

I) Cuando los datos personales se han tratado infringiendo el RGPD o la normativa de Derecho nacional, el interesado –titular de los datos personales objeto de tratamiento ilícito- podrá dirigirse a los tribunales del orden jurisdiccional civil para solicitar una indemnización por los daños y perjuicios patrimoniales (económicos) y morales o extrapatrimoniales que, en su caso, haya sufrido.

II) La acción indemnizatoria ejercitada ante los órganos jurisdiccionales civiles (o, en su caso, del orden social -si media una relación laboral entre el agente infractor y el titular de los datos personales perjudicado-) es independiente de la tutela administrativa que se impetre ante las autoridades administrativas competentes en materia de protección de datos, sin que

[99] La posibilidad de seguir un procedimiento administrativo sancionador y, de manera coetánea, un procedimiento de naturaleza civil con finalidad indemnizatoria o resarcitoria, ha sido admitida expresamente, *v.gr.*, por las SSTS 307/2014, de 4 de junio [RJ 2014\3020] y 671/2014, de 19 de noviembre [RJ 2014\5956]. En sentido contrario a lo afirmado en el texto puede constatarse algún pronunciamiento jurisdiccional aislado, como es el caso, *v.gr.*, de la SAP Madrid, Secc. 13ª, 37/2007, de 6 de febrero [AC 2007\1017], confirmada por la STS 592/2011, de 12 de septiembre [RJ 2011\7380]. En la doctrina sostienen el mismo parecer que se defiende en el texto, *v.gr.*, BUSTO LAGO, J.M.: «La responsabilidad civil de los responsables de ficheros de datos personales y de los encargados de su tratamiento», *Aranzadi Civil*, núm. 5, junio de 2006, pgs. 45 y 46; PUYOL MONTERO. J.: «Comentario al artículo 19 de la LOPDP», en *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal* (A. TRONCOSO REIGADA, Ed.), Ed. Civitas, Cizur Menor, 2010, pg. 1269; VÁZQUEZ DE CASTRO, E.: «Daños causados por el incumplimiento de la ley en el tratamiento de datos personales. Concordancias, discordancias y concurso de normas», *Práctica de Derecho de Daños: Revista de Responsabilidad Civil y Seguros*, núm. 112, enero-febrero de 2013, pgs. 4 y 5; y, RUBÍ PUIG, A.: «Problemas de coordinación y compatibilidad entre la acción indemnizatoria del artículo 82 del Reglamento General de Protección da Datos y otras acciones en el Derecho español», *DPyC*, núm. 34, 2019, especialmente las pgs. 215 y ss.

exista prejudicialidad contencioso-administrativa, pudiendo, a efectos de la acción civil de naturaleza indemnizatoria, calificar la infracción de la normativa reguladora de la protección de datos personales, que se erige en presupuesto objetivo necesario para la estimación de aquélla.

III) La concurrencia de una conducta infractora de la normativa reguladora del tratamiento de datos personales es la conducta antijurídica que se erige en presupuesto de la estimación de la pretensión indemnizatoria, de manera que el consentimiento del titular de los datos personales se erige como la más relevante causa de justificación determinante de la exoneración de la responsabilidad civil del responsable o del encargado del tratamiento.

IV) En cuanto a la legitimación activa, al margen de los supuestos de acciones colectivas, de naturaleza indemnizatoria, ejercitadas en el caso de que los perjudicados tengan la condición de consumidores o usuarios, esta legitimación es individual.

V) El responsable y el encargado del tratamiento tendrán que indemnizar al interesado, salvo que demuestren que no son responsables de los daños y perjuicios, en cuyo caso quedarán exentos de la misma. El sistema de responsabilidad civil en materia de protección de datos personales es un sistema de responsabilidad subjetiva con inversión de la carga de la prueba de la culpa (esta conclusión es aplicable también a la regulación brasileña fruto de la LGPD de 2018). La responsabilidad civil en el caso de concurrencia de una pluralidad se sujetos responsables es solidaria.

VI) Los daños indemnizables son tanto los patrimoniales (sean éstos concretos o difusos, como los derivados del tratamiento de *big data* y la segmentación del mercado de determinados bienes y productos de consumo), como los de naturaleza extrapatrimonial, vinculados a lesiones de los derechos fundamentales a la protección de datos personales, al derecho al honor y a la intimidad personal.

REFERÊNCIAS

ABERASTURI GORRIÑO, U. El derecho a la indemnización en el artículo 19 de la Ley Orgánica de Protección de Datos de Carácter Personal», en *Revista Aragonesa de Administración Pública*, núm. 41-42, 2013 (págs. 173 a 206).

ÁLVAREZ HERNANDO, J. Análisis jurídico de la acción de reclamación de una indemnización por haber sufrido daños y perjuicios derivados de una infracción en materia de protección de datos. Estudio de art. 82 del RGPD», en *https://www.ac-abogados.es*, 28 de enero de 2019.

BIURRUM, F.J. *"Accountability"* o responsabilidad activa en el Reglamento General de Protección de Datos», *AJA*, núm. 927, 25 de febrero de 2017.

BODIN DE MORAES, MªC.; DE QUEIROZ, J.Q. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD», en *Cadernos Adenauer*, Vol. 3 (*Proteção de dados pessoais: privacidade versus avanço tecnológico*), Ed. Fundação Konrad Adenauer, Rio de Janeiro, 2019 (pgs. 113 a 135).

BUSTO LAGO, J.M. La responsabilidad civil de los responsables de ficheros de datos personales y de los encargados de su tratamiento», *Aranzadi Civil*, núm. 5, junio de 2006 (pgs. 15 a 53).

BUSTO LAGO, J.M. El deber de evaluar la solvencia del consumidor de crédito como mecanismo de prevención del sobreendeudamiento y su regulación en España», en *Sobreendeudamiento de consumidores. Estrategias para garantizar una segunda oportunidad* (M. CARBALLO FIDALGO, COORD.), Ed. J.Mª Bosch, Barcelona, 2019 (pgs. 21 a 63).

BUSTO LAGO, J.M. Protección de datos personales y responsabilidad civil», en *Derecho de Daños 2020,* Ed. Lefebvre, Madrid, 2020 (pgs. 443 a 512).

BUTTARELLI, G. *Banche dati e tutela della riservatezza (La* privacy *nella Società dell'Informazione)*, Giuffrè Editore, Milán, 1997.

CUENA CASAS, M. Préstamo responsable y datos de solvencia patrimonial en la Ley Reguladora de los Contratos de Crédito Inmobiliario», *Actualidad Civil,* núm. 9, 2019.

DA SILVA LIMA, H. Responsabilidade civil objetiva, subjetiva ou proativa? Pela Lei Geral de Proteção de Dados e suas implicações: contexto brasileiro», *Revista Jurídica de Daños,* núm. 24, diciembre de 2021.

DÍAZ ALABART, S. *La protección de los datos y contenidos digitales de las personas fallecidas*, Ed. Reus, Madrid, 2020.

DOMÍNGUEZ GARCÍA, Á.M. *La contratación del Cloud Computing*, Ed. Aranzadi, Cizur Menor, 2019.

ELGUERO MERINO, J.Mª: El seguro de responsabilidad civil por protección de datos personales», en *RRCyS*, núm. 28, 2008 (pgs. 47 a 80).

GARCÍA GARNICA, Mª C. La protección de los datos personales frente a su tratamiento on-line tras la Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014», en *Estudios sobre Jurisprudencia Europea (Materiales del I y II Encuentro anual del Centro español del European Law Institue)* (A. RUDA GONZÁLEZ y C. JEREZ DELGADO, Dirs.), Ed. Sepin, Madrid, 2017 (pgs. 543 a 561).

GARCÍA PÉREZ, C.L. Intromisión ilegítima en el derecho al honor y protección de datos. Especial referencia a su afectación por ingreso en registros de moroso», en *Daño, responsabilidad y seguro* (M.J. HERRADOR GUARDIA, DIR.), Ed. Lefebvre – El Derecho, Madrid, 2016 (pgs. 621 a 725).

GARCÍA RUBIO, Mª P. Bases de datos y confidencialidad en Internet», en *El comercio electrónico* (J. A. ECHEBARRÍA SÁENZ, COORD.), EDISOFER, S.L., Madrid, 2001.

GIL MEMBRADO, C. *Privacidad y turismo: perfil del turista,* big data *y plataformas colaborativas,* Ed. Reus, Madrid, 2019.

GRIMALT SERVERA, P. *La responsabilidad civil en el tratamiento automatizado de datos personales*, Ed. Comares, Granada, 1999.

GRIMALT SERVERA, P. Intromisiones ilegítimas en los derechos al honor, a la intimidad y a la propia imagen: tutela civil versus tutela administrativa», en *Protección de datos personales* (APDC), Ed. Tirant lo Blanch, Valencia, 2020 (pgs. 309 a 371).

LAFUENTE TORRALBA, A.J. Acciones colectivas, protección de datos y redes sociales: reflexiones al hilo de un reciente pronunciamiento de la Corte de Luxemburgo», en *Acciones colectivas. Cuestiones actuales y perspectivas de futuro* (T. ARMENTA DEU y D. PEREIRA PUIGVERT, COORDS.), Ed. M. Pons, Madrid, 2018 (pgs. 355 a 369).

LIM YEE FEN, H. The data protection paradigm for the tort of privacy in the age of big data» (2015) 27 *SAcLJ* (pgs. 789 a 821).

MARTÍNEZ MARTÍNEZ, N. Reflexiones en torno a la protección *post mortem* de los datos personales y la gestión de la transmisión *mortis causa* del patrimonio digital tras la aprobación de la LOPDGDD», *DPyC*, núm. 35, 2019 (pgs. 169 a 212).

MARTÍNEZ MARTÍNEZ, N. El conflicto entre el derecho al olvido y la libertad de información de la prensa contenida en hemerotecas», *DPyC*, núm. 34, 2019 (pgs. 51 a 95).

MERCELLIN, S. y SEMIK, J. La responsabilité des traitements de données partagées dans un groupe», en *Le RGPD*, Ed. Dalloz - Grand Angle, París, 2018.

NÚÑEZ GARCÍA, J.L. Responsabilidad y obligaciones del responsable y del encargado del tratamiento», en *Tratado de protección de datos* (A. RALLO LOMBARTE, DIR.), Ed. Tirant lo Blanch, Valencia, 2019 (pgs. 351 a 386).

OTERO CRESPO, M. La sucesión en los "bienes digitales". La respuesta plurilegislativa española», *Revista de Derecho Civil*, Vol. VI, núm. 4, octubre-diciembre de 2019 (pgs. 89 a 133).

PARRA MEMBRILLA, L. Precios a medida para los consumidores: la consecuencia del Big Data», en *http://centrodeestudiosdeconsumo.com*, 12 de febrero de 2020.

PEÑA LÓPEZ, F. Daños al honor. Intromisión ilegítima por inclusión indebida de datos en un fichero de morosos. Criterios de determinación del daño resarcible. Indemnizaciones simbólicas: comentario a la STS de 21 septiembre 2017 (RJ 2017\4056)», *CCJC*, núm. 106, 2018 (pgs. 225 a 238).

PIÑAR MAÑAS, J.L. (Dir.): *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*, Ed. Reus, Madrid, 2016.

PUYOL MONTERO. J. Comentario al artículo 19 de la LOPDP», en *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal* (A. TRONCOSO REIGADA, ED.), Ed. Civitas, Cizur Menor, 2010 (pgs. 1263 a 1285).

RABIN, R. L. *Perspectives on Privacy, Data Security, and Tort Law»*, 66 *De Paul Law Review,* 2017; disponible en *https://via.library.depaul.edu/law-review/vol66/iss2/2.*

RODRÍGUEZ AYUSO, J.F. *Figuras y responsabilidades en el tratamiento de datos personales*, JMª Bosch Editor, Barcelona, 2019.

ROSELLÓ RUBERT, F.Mª: *Cloud Computing. Régimen jurídico para empresarios*, Ed. Aranzadi, Cizur Menor, 2018.

RUBÍ PUIG, A. Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD», *Revista de Derecho Civil*, Vol. V, núm. 4, octubre-diciembre de 2018 (pgs. 53 a 87).

RUBÍ PUIG, A. Problemas de coordinación y compatibilidad entre la acción indemnizatoria del artículo 82 del Reglamento General de Protección da Datos y otras acciones en el Derecho español», *DPyC*, núm. 34, 2019 (pgs. 197 a 232).

RUDA GONZÁLEZ, A. Indemnización por daños al derecho al olvido. La responsabilidad por la no exclusión de la indexación de una hemeroteca digital por los buscadores generales (Caso El País). Comentario a la Sentencia de 15 de octubre de 2015 (RJ 2015, 4417)», en *CCJC*, núm. 101, 2016 [BIB 2016\4040].

RUIZ CARRILLO, A. *Los datos de carácter personal (Concepto, requisitos de circulación, procedimientos y formularios)*, Ed. Bosch, Barcelona, 1999.

RUIZ CARRILLO, A. *La protección de los datos de carácter personal*, Ed. Bosch, Barcelona, 2001.

SAN MARTÍN ARIAS, I. *Protección de datos en el crédito al consumo,* Ed. Aranzadi, Cizur Menor, 2015.

SANTAMARÍA RAMOS, F.J. *El encargado independiente. Figura clave para un nuevo Derecho de protección de datos*, Ed. La Ley, Madrid, 2011.

TEPEDINO, G.; TERRA, A. de M.; GUEDES, G.S. da C. *Fundamentos de direito civil: teoría geral do direito*, Ed. Forense, Rio de Janeiro, 2020.

VALLE, L.; RUSSO, B.; BONZAGNI, D. y LOCATELLO, D.Mª: Struttura dei contratti e trattamento dei dati personali nei servizi di *cloud computing* alla luce del nuovo reg. 2016/679 UE», *Contratto e impresa,* 1/2018 (pgs. 343 a 406).

VAN ALSENOY, B. Liability under EU Data Protection Law. From Directive 95/46 to the General Data Protection Regulation», *JIPITEC*, 2016 (3) (pgs. 271 a 288).

VÁZQUEZ DE CASTRO, E. Daños causados por el incumplimiento de la ley en el tratamiento de datos personales. Concordancias, discordancias y concurso de normas», *Práctica de Derecho de Daños: Revista de Responsabilidad Civil y Seguros*, núm. 112, enero-febrero de 2013 (págs. 18 a 34).

VELA TORRES, P. J. (Coord.): ¿Qué tipo de responsabilidad puede derivarse de la filtración a terceros no autorizados de datos confidenciales que figuran en la historia clínica de un paciente?», *Encuesta jurídica Sepin*, octubre de 2019 [SP/DOCT/82956].

VIZCAÍNO CALDERÓN, M. Comentario al artículo 19 de la LOPDCP», *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, Ed. Cívitas, Madrid, 2001.

ZHU, B. A traditional tort for a modern threat: applying intrusion upon seclusion to dataveillance observations», 89 *N.Y.U.L. Rev.* 2381, diciembre de 2014.

ZUNÓN VILLALOBOS, M. La garantía civil de la privacidad», *Revista Aranzadi Doctrinal*, núm. 9, 2013 (págs. 153 a 181).