EMPRESA Y EMPRESARIO

Doctrina

La aplicación privada del derecho para la protección de las personas físicas en materia de tratamiento de datos personales en el reglamento (UE) 2016/679

Marta REQUEJO ISIDRO

Senior research fellow, Max Planck Institute Luxembourg. Profesora titular DIPr., Universidad de Santiago de Compostela.

FICHA TÉCNICA

Resumen: *La regulación jurídica del tratamiento de datos personales de las personas físicas se realiza tanto desde una vertiente pública como desde la*

privada. En la práctica la protección del derecho fundamental a la autodeterminación informativa se produce ante todo a través de mecanismos de Derecho público; el recurso a la vía civil se encuentra aún infrautilizado. El Reglamento 2016/679 va a tratar de incentivarlo reforzando la posición del interesado con medidas de carácter sustantivo, apoyadas por útiles procesales y otros que garantizan la aplicación de las normas en casos transfronterizos dentro y fuera de la UE. El estudio realiza un primer análisis y evaluación del conjunto, también desde la perspectiva de la LOPD y del Proyecto de noviembre de 2017.

Palabras clave: Protección de datos personales; aplicación privada del Derecho; tutela judicial; indemnización; responsabilidad civil de responsables y encargados; acciones representativas; carga de la prueba; situaciones transfronterizas

Abstract: *The processing of personal data of natural persons is currently regulated by means public and private mechanisms. In practice, the protection of the fundamental right to informational self-determination occurs primarily through instruments of public law; the private enforcement possibility remains underused. Regulation 2016/679 tries to encourage it by reinforcing the data subject's position with substantive measures, supported by procedural tools and tools ensuring the cross- border application of the rules (within the EU as well as in cases involving third States). The study carries out a first analysis and evaluation of the whole, also from the perspective of the Spanish LOPD and the Bill of November 2017.*

Keywords: Personal data protection; private enforcement; right to an effective judicial remedy; compensation; civil liability of controllers and processors; representative actions; burden of proof; cross-border cases

I. Introducción

La preocupación por la protección de los datos personales en la UE cristalizó hace dos décadas en un instrumento común: la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 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 (1) . La evolución del contexto del tratamiento de datos desde entonces hasta hoy ha forzado al legislador europeo a reaccionar, dando lugar al Reglamento (UE) 2016/679, que derogará el régimen anterior. La entrada en vigor del Reglamento se produjo a los veinte días de la publicación en el DOUE el 4 de mayo de 2016 (2) ; se aplicará a partir del 25 de mayo de 2018.

Para asegurar el cumplimiento de las obligaciones que impone sobre responsables y encargados del tratamiento el Reglamento yuxtapone instrumentos públicos —en manos de las autoridades de control—, instrumentos privados —en manos de los interesados—, y autorregulación —elaborados por asociaciones u organismos representativos de responsables y encargados—. El recurso a mecanismos privados en términos de *private enforcement*, incluyendo pero superando el interés del individuo singular, es posible al amparo del régimen aún vigente: su utilización resulta, no obstante, inhabitual (3) . El Reglamento va a tratar de incentivarlo a través de diversas medidas: así, mediante el reconocimiento explícito de la responsabilidad del encargado del tratamiento frente al interesado, o añadiendo los daños inmateriales como indemnizables al lado de los materiales (4) . Ahora bien, para que estos mecanismos logren su objetivo es preciso acompañarlos de otros útiles: procesales, por un lado, en forma de recurso colectivo, facilidad en la prueba, financiación por terceros. Por otro, en un ámbito donde la internacionalidad del

tratamiento es la regla, de aquellos que posibiliten su proyección transfronteriza, lo que requiere criterios adaptados de competencia judicial internacional y para la determinación de la ley aplicable. En las páginas que siguen analizaremos estos aspectos: primero en el Reglamento, y luego más brevemente en la legislación española para los extremos sobre los que el Reglamento no se pronuncia, o remite expresamente la cuestión a los Estados.

II. Comparativa de derechos y obligaciones. Directiva-Reglamento

El Reglamento de protección de datos introduce nuevos derechos para los interesados y obligaciones para responsables y encargados del tratamiento, y refuerza otros ya existentes. En el apartado III nos centraremos en el régimen de la responsabilidad civil frente al interesado en su vertiente sustantiva y procesal; en este enunciaremos de forma resumida el resto de los cambios relevantes.

1 Interesados: nuevos derechos y refuerzo de los existentes

El Reglamento 2016/679 revisa y fortalece la posición que los interesados ostentan conforme a la Directiva: así, por ejemplo, en cuanto a la información mínima que los responsables del tratamiento deben proveer sobre la recogida y procesamiento de datos, recibidos del interesado o de terceros y que ahora, por mandato explícito del art. 12 Reglamento, debe ser «concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño», y en general facilitada por escrito. El derecho de acceso del interesado, en el art. 15, se precisa y amplía añadiéndose extremos tales como información sobre el plazo previsto de conservación de los datos personales, o sobre la fuente de los datos cuando no han sido obtenidos del interesado. El mismo precepto establece la gratuidad de la primera copia de los datos objeto de tratamiento solicitada por el interesado. El art. 17 precisa las circunstancias en que cabe ejercer el derecho de supresión; el art. 19 recuerda que si el responsable ha comunicado a terceros los datos que el interesado posteriormente rectifica, estos terceros deben ser notificados, y añade que el responsable deberá informar al interesado que lo solicite acerca de quiénes son los destinatarios de la notificación.

Son nuevos en relación con la Directiva varios extremos que recogen el art. 12, el art. 18 y el art. 20. El primero establece la obligación del responsable del tratamiento de facilitar al interesado el ejercicio de sus derechos —si bien en el caso de que se produzca una solicitud para el ejercicio de los derechos a que se refieren los arts. 15 a 22, el responsable podrá negarse a actuar según lo requerido si puede demostrar que no está en condiciones de identificar al interesado (art. 12.2). Se estipula un plazo máximo, pero prorrogable, de un mes para que el responsable facilite al interesado la información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22. El art. 18 recoge el derecho a limitar el tratamiento en determinadas circunstancias, mientras que el derecho a la portabilidad de los datos aparece por primera vez en el art. 20.

2 Responsable y encargado: obligaciones

Desde la perspectiva del responsable y el encargado del tratamiento el Reglamento viene a precisar las del primero y a potenciar la posición del interesado frente al segundo: ello se refleja en el régimen de responsabilidad civil que veremos más adelante además de en lo que exponemos a continuación. En relación con el responsable, a tenor del art. 5 rige ahora el principio de «responsabilidad proactiva», que engloba tanto el cumplimiento con los principios y obligaciones en materia de protección de datos como la capacidad de demostrar tal cumplimiento. La protección de datos se impone desde el diseño y por defecto: señala el art. 25 que el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, las medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos, y para garantizar que, por defecto, solo son objeto de tratamiento los datos personales necesarios para cada uno de los fines específicos del tratamiento. A tenor del art. 27 un responsable no establecido en la UE deberá — como regla— nombrar un representante que atenderá junto al responsable o al encargado, o en su lugar, a las consultas de

las autoridades de control y de los interesados sobre todos los asuntos relativos al tratamiento. La elección del encargado del tratamiento debe adoptar la forma de un acuerdo vinculante en el que se expliciten sus obligaciones, según lo establecido por el art. 28. A partir de la fecha de aplicación del Reglamento no será necesario notificar a la autoridad de protección de datos (APD) antes del tratamiento, pero el responsable deberá llegar un registro de las actividades de tratamiento bajo su responsabilidad, detallando los extremos que enumera el art. 30. Como regla, el art. 33 impone al responsable del tratamiento la obligación de notificar la violación de la seguridad de los datos personales a la autoridad de control competente sin dilación indebida y, de ser posible, en las 72 horas después de que haya tenido constancia de ella; el art. 34 estipula por su parte que si hay riesgo para los interesados deberá notificarles la violación sin dilación, salvo que pueda acogerse a alguna de las circunstancias que el propio precepto especifica.

Frente a la Directiva el Reglamento se ocupa con detalle de la figura del encargado del tratamiento de datos, tanto en la vertiente de Derecho público como de Derecho privado, imponiéndole obligaciones directas frente a la situación anterior, aún vigente, en la que en general solo tienen obligaciones contractuales- y precisando las que le vinculan al responsable del tratamiento. Además de lo relativo a su responsabilidad civil frente al interesado, que veremos a continuación, se concretan extremos como el relativo al nombramiento de un encargado por otro, lo que ahora requiere expresamente el consentimiento del responsable otorgado por escrito conforme al art. 28; o la obligación establecida en el mismo precepto de informar inmediatamente al responsable cuando una de sus instrucciones infrinja el Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros. Se añaden como novedades la obligación de llevar registros del tratamiento, art. 30, con un contenido mínimo determinado; de cooperar con las autoridades de protección de datos, art. 31; de adoptar las medidas técnicas y organizativas pertinentes para garantizar un nivel de seguridad del tratamiento, art. 32; de comunicar sin dilación indebida al responsable cualquier violación de seguridad de la que tenga conocimiento, art. 33; de nombrar un delegado de protección de datos, art. 37. Los encargados están también vinculados por el capítulo V sobre la transferencia de datos personales a terceros países.

III. Aplicación privada del Reglamento

1 Tutela judicial efectiva y derecho a compensación

A. La tutela judicial

El Reglamento 2016/679 prevé el derecho a tutela judicial efectiva del interesado contra el encargado o el responsable del tratamiento en su art. 79.1; el art. 82 contempla por su parte el derecho de toda persona que haya sufrido daños y perjuicios como consecuencia de una infracción del Reglamento a recibir una indemnización del responsable o el encargado del tratamiento. Ambos preceptos encuentran antecedente en la Directiva 95/46/CE: el primero en el art. 22, el segundo en el art. 23. La formulación allí empleada es similar a la que utiliza el Reglamento. En castellano la tutela judicial efectiva se denomina allí «recurso judicial», sin que del cambio se deriven consecuencias — la expresión no cambia en otras versiones lingüísticas, como la francesa («recours juridictionnel») o la inglesa («judicial remedy»). Más relevante, al menos en potencia, es el dato relativo al titular de la protección. La Directiva conoce ya la noción de «interesado», aunque no la define, como tampoco lo hace el Reglamento; los derechos de los arts. 22 y 23 Directiva se atribuyen a cualquier persona, mientras que el Reglamento se refiere al interesado en el art. 79 (tutela judicial efectiva), y a toda persona en el art. 82 (compensación). Es difícil saber si la distinción, apta para producir consecuencias, es o no intencionada.

Por lo demás, con la salvedad relativa a la competencia judicial internacional en el art. 79.2 — en otras palabras, ante qué Estado miembro (EM) cabe hacer valer el derecho— , que expondremos más adelante, el Reglamento no introduce novedades en materia de tutela judicial, por lo que no le dedicaremos más comentario. Lo contrario ocurre con el derecho a indemnización, que se amplía y consolida en el nuevo texto. Hay varios aspectos de interés en este sentido.

B. El derecho a indemnización

a. Frente a responsable(s) y encargado(s)

El cambio más llamativo en el texto del Reglamento por comparación con el art. 23 de la Directiva radica en las posibilidades abierta al afectado para reclamar indemnización: frente al encargado, por una parte, y frente a los corresponsables (o encargados) del tratamiento, por otra. Acerca de lo primero, la Directiva solo había previsto el derecho frente al responsable: de ahí cabía inferir la ausencia de una responsabilidad directa del encargado, cuyas obligaciones y responsabilidades se hallaban gobernadas casi en exclusiva por el contrato con el responsable (art. 16). En la Opinión expresada por el Grupo de Trabajo del art. 29 núm. 1/2010, de 16 de febrero de 2010, a propósito de las nociones de responsables y encargados, se reconocía no obstante que el encargado que actúa al margen de las instrucciones del responsable puede ser recalificado como responsable y la reclamación proceder contra él (5) . En la misma Opinión el Grupo de Trabajo admitía que la limitación de la Directiva al responsable no impide una legislación nacional más favorable, que permita también una acción directa en contra del encargado (6) . Tras el Reglamento 2016/679 los responsables del tratamiento mantienen su responsabilidad directa para con los interesados, pero estos pueden ahora reclamar también contra el encargado por los daños y perjuicios causados por el tratamiento con apoyo en el instrumento de la UE — y ya no en la legislación nacional, si la había—, en dos supuestos: cuando no haya cumplido con las obligaciones del Reglamento dirigidas específicamente a los encargados; o cuando haya actuado al margen o en contra de las instrucciones legales del responsable. En estas circunstancias cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado; en otras palabras, conforme al art. 82.4 el interesado puede elegir entre reclamar contra el responsable, el encargado, o ambos.

En caso de ser varios los encargados y/o responsables, todos y cada uno son responsables de cara al interesado por la totalidad del daño, incluso aunque exista un acuerdo entre ellos (Que de hecho es obligatorio entre los corresponsables, *vid.*. art. 26 (7)), por virtud del art. 82.4 y 26.3, en cuanto a los corresponsables, sin perjuicio de que existe un derecho de regreso como indica el art. 82.5.

El régimen de exención de responsabilidad, por su parte, se mantiene como en la Directiva (a salvo la adición de «en modo alguno», sobre cuyas posibles implicaciones *vid.*. el apartado c), extendiéndose también al encargado: señala el art. 23. 2 que el responsable del tratamiento podrá ser eximido parcial o totalmente de su responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño, lo que conforme al Cdo. 55 significa «principalmente si demuestra la responsabilidad del interesado o un caso de fuerza mayor». En el Reglamento no hay un Considerando equivalente, pero parece que la comprensión del art. 82.3 debe ser la misma.

b. Daños indemnizables

Otra novedad del Reglamento es el tipo de daños indemnizables, que a tenor del art. 82.1 abarcan ahora expresamente los inmateriales, haciéndose eco de la convicción de que en la práctica muchos de los daños son de este tipo (8) . No se regula en cambio la forma de calcular estos daños, ni se aportan pistas al respecto, lo que sin duda va a generar heterogeneidad al respecto: en algunos Estados Miembros indican en la ley las cuantías, y en otros queda al arbitrio de los jueces (9) . La redacción de texto induce a concluir que es preciso que haya daño para sostener el derecho a indemnización: en otras palabras, la mera violación de normas sobre protección de datos no debe considerarse un daño; hay, no obstante, otras opiniones (10) . Procede añadir que a diferencia de la Directiva, que aludía a «reparación», el art. 82 del Reglamento solo contempla la indemnización y emplea el término «reparación» en otros lugares como algo diferente — un ejemplo, el Cdo. núm. 108 «(…) lo que incluye el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización (…)»—, por lo que cabe entender que al amparo del art. 82 solo cabe aquella en sentido estricto. Se echa en falta una indicación expresa sobre los daños no compensatorios, que aparece en otros instrumentos de la UE para excluirlos (11) : el Cdo. núm. 146, al indicar que «El concepto de daños y perjuicios debe interpretarse en sentido amplio a la luz de la jurisprudencia del Tribunal de Justicia, de tal modo que se respeten plenamente los objetivos del presente Reglamento», podría llevar a pensar que en cambio aquí tienen cabida, lo mismo que la referencia en el mismo lugar a que la indemnización

sea «total y efectiva».

c. Tipo de responsabilidad

Se ha preguntado la doctrina, en fin, si el Reglamento aporta alguna novedad en términos de tipo de responsabilidad — por culpa u objetiva— del responsable o el encargado del tratamiento. Bajo la Directiva se habla de una *strict liability,* pero matizada: si el responsable no puede eludir su responsabilidad probando la ausencia de culpa, sigue siendo necesario demostrar que el tratamiento ha sido ilícito o que el daño es consecuencia de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la Directiva (12) . La situación no varía en el Reglamento excepto por la mención que subrayamos en su art. 82.3: «El responsable o 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». Sobre las implicaciones del uso de la expresión «en modo alguno» opinan los autores que si bien no altera la naturaleza de la responsabilidad sí tiene como consecuencia la de reducir las posibilidades de escapar de ella (13) .

2. Elementos procesales

La aplicación privada del Derecho para la protección de datos personales está abocada al fracaso si las reglas sustantivas no se acompañan de normas de procedimiento que garanticen su ejercicio efectivo. El Reglamento se hace eco de esta necesidad de forma solo parcial.

A. Acciones representativas

El art. 80 del Reglamento introduce en el panorama de la protección de datos un elemento inexistente en la Directiva (14) : la posibilidad del interesado de ser representado en juicio por una entidad, organización o asociación sin ánimo de lucro, bajo ciertas condiciones. El precepto contempla dos situaciones distintas: en su primer apartado, relativo a cualquier acción civil incluida la compensatoria, es preciso que concurra en todo caso el mandato del interesado. El apartado segundo se refiere a acciones que no sean la de indemnización, y admite la posibilidad de que sean ejercitadas aun sin mandato con tal de que ello esté previsto por la legislación del EM donde se interponga la acción.

La redacción del art. 80 ha experimentado modificaciones desde la propuesta de la Comisión, refinándose hasta alcanzar la forma final. Es interesante examinar este *iter* para una mejor comprensión del texto. Así, por lo que se refiere al interesado destaca el paso desde la fórmula empleada por la Comisión, «Any body shall have the right… *on behalf*», a la introducción del requisito del mandato en el art. 80.1, y a la posibilidad de que el mandato comprenda la reclamación de compensación. En lo relativo a las entidades, organizaciones o asociaciones, la negociación da lugar a los requisitos que hoy figuran como cumulativos, pensados probablemente para evitar el abuso en el ejercicio de la acción representativa: sin ánimo de lucro; correctamente constituidas con arreglo al Derecho de un Estado miembro; cuyos objetivos estatutarios sean de interés público; y que actúen en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales. Igualmente es el resultado de la negociación entre Comisión, Parlamento y Consejo la habilitación a los EM para que las mismas entidades, organizaciones o asociaciones puedan presentar una acción con independencia del mandato del interesado, excluyendo —una vez más como medida preventiva contra el abuso— la acción de indemnización.

El art. 80 puede considerarse un avance en la protección de datos personales. Su necesidad había sido puesta de manifiesto como instrumento para el reequilibrio de fuerzas, que ayudaría a combatir la infrautilización del *private enforcement*: los interesados no reclaman porque perciben que el causante del daño es demasiado poderoso, o por temor a las consecuencias (15) . Por eso en la práctica es célebre el asunto *Schrems*, como ejemplo hasta hoy único de *private enforcement* con ecos de recurso colectivo: paralelamente al recurso administrativo en Irlanda, Max Schrems ha inciado un procedimiento colectivo en Austria en nombre de siete usuarios de Facebook — con domicilio en Austria, India y Alemania (16) — al amparo del modelo austríaco de acción colectiva, que posibilita la cesión de la acción a otra persona, quien la interpone ante un único Tribunal. A día de hoy la pregunta sobre la competencia judicial internacional está abierta, con una cuestión

prejudicial pendiente ante el TJUE (as. C-498/16).

Pero aun representando un avance es previsible que en la práctica el art. 80 se quede corto. No basta con ampliar la legitimación para asegurar la utilidad de la disposición (17) ; otros elementos son necesarios, como la dotación de recursos vía el otorgamiento de un derecho a justicia gratuita o alguna fórmula de financiación por terceros (18) — si bien el Reglamento de protección de datos no era probablemente el lugar indicado para abordar estos aspectos (19) —. Es además un tanto decepcionante, y apto para crear divergencias en la implementación en los EM, la falta de mayor definición del modelo: es claro que el apartado primero se decanta por un sistema de legitimación por representación, pero no si el apartado segundo, con el inciso «con independencia del mandato del interesado» está pensando en una legitimación independiente de las entidades, organizaciones, u asociaciones, o derivada de la defensa de un derecho que es ajeno con una legitimación por sustitución, extraordinaria; o si simplemente la cuestión se deja en manos de los EM. Sobre otros extremos, dado que la protección datos aparece como uno de los ámbitos mencionados por la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones «Hacia un marco horizontal europeo de recurso colectivo» (20) , cabría en principio suponer que se toma inspiración de la Recomendación de la misma fecha que la acompaña —Recomendación de la Comisión 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 (2013/396/UE) —. La realidad es que el art. 80 se separa de ella en aspectos tales como los requisitos que debe reunir las entidades representativas (punto 4.c), el otorgamiento de la facultad de interponer acciones de representación a las autoridades públicas (punto 7), o la exigencia de que el consentimiento (el mandato, en el Reglamento) sea expreso, en el marco del sistema de opt-in (punto 21). En definitiva, no hay motivos para sostener que el Reglamento adopta las recomendaciones, o debe ser leído a la luz de las mismas.

En Europa varios EM se ha dotado ya de un mecanismo de acción colectiva específico en materia de protección de datos (21) : es el caso de Alemania, anterior a la adopción del Reglamento (Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen, de 27 de agosto de 2002, modificada por la Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts, de 17 de febrero de 2016). También de Francia con posterioridad a la entrada en vigor del Reglamento: Loi nº 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle — Article 91, que modifica la sección 2 del capítulo V de la Ley nº 78-17 du 6 janvier 1978 relative à linformati'que, aux fichiers et aux libertés, añadiendo un article 43 ter) —. En Bélgica, la Ley de 28 de marzo de 2014, Loi portant insertion dun' titre 2 « De laction' en réparation collective » au livre XVII « Procédures juridictionnelles particulières » du Code de droit économique et portant insertion des définitions propres au livre XVII dans le livre 1er du Code de droit économique, art. 3, ya incluía la reparación de violaciones de la Ley de 8 de diciembre de 1992 sobre la protección de la vida privada en relación con el tratamiento de datos personales. De estos ordenamientos es llamativo ante todo el caso de Francia: aunque la ley se adopta cuando ya se conoce el texto final del Reglamento solo se incluye la acción de cesación. Las disposiciones de los países mencionados confirman ya que existirán divergencias entre los EM: así, en cuanto a las condiciones que permitirán a las entidades o asociaciones interponer una acción (con una antigüedad de cinco años en Francia, y de uno en Alemania), o respecto a qué tratamientos de datos o categorías de datos afectados (en Alemania, exclusivamente la recogida, procesamiento y uso de datos de consumidores para propósitos comerciales; sin especificación en Francia).

B. Otros aspectos procesales

La previsión de un mecanismo de representación ante los tribunales de los interesados puede servir a incentivar el recurso a la vía civil en materia de protección de datos: pero, como ya hemos indicado, es probablemente insuficiente. A las reflexiones en el apartado anterior se suma otra relativa al acceso a las pruebas y a la carga de la misma. Las acciones por daños consecuentes a la violación de las obligaciones en el tratamiento de datos suelen requerir un análisis fáctico complejo. Como ocurría en el marco de la Directiva, bajo el Reglamento 2016/679 el demandante deberá demostrar tres elementos: la infracción del Reglamento, la existencia de daños, y la

relación causal entre ambos. Habida cuenta de que el tratamiento de datos se lleva a cabo en general «a puerta cerrada», la prueba puede resultar muy compleja para el interesado. Bajo la Directiva algún autor alude la posibilidad de recurrir a presunciones, o a otras construcciones judiciales de efecto similar previstas en la legislación nacional (22) : un ejemplo, el «principio de proximidad de la prueba», que coloca la carga de la prueba sobre la parte para la cual la misma es accesible, o más fácilmente accesible (23) . El Reglamento se hace eco hasta cierto punto en su art. 5.2, conforme al cual «El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo ("responsabilidad proactiva")». De este precepto deriva la doctrina que «(…) the DPD and the GDPR create (…) a basic fault-based regime (…) with a reversed burden of proof» (24) . La «capacidad de demostración» traslada la prueba del incumplimiento o del error en el tratamiento de datos desde el interesado al responsable a partir del momento en que exista un principio de prueba: «At the very least, the argument can be made that the provisions of the GDPR regarding accountability (which require controllers to "be able to demonstrate compliance") reinforce the notion that the controller is in fact "best placed" to proffer evidence of the measures it has taken to ensure compliance. Even if the legal burden of proof is still borne by the data subject, the evidential burden of proof should de facto shift to the controller as soon as the data subject has offered *prima facieprima facie* evidence of an unlawful processing activity» (25) . Con todo, la conclusión solo vale para responsable del tratamiento, y no para el encargado, que no se halla sujeto a lo dispuesto por el art. 5.2 Reglamento. Además solo se aplica al primer elemento de los tres que hay que probar: el daño que sigue a la violación no se presume (26) .

IV. Aseguramiento de la protección. Los casos transfronterizos

1 Ámbito de aplicación del Reglamento

La pregunta sobre el alcance del Reglamento debe ser abordada desde varias perspectivas. De entrada, cabe formularla en términos de quién se beneficia de la protección: a lo que el Reglamento responde a través del Cdo núm. 14, en el que por una parte se excluye a las personas jurídicas, y por otra se incluye a las personas físicas independientemente de su nacionalidad o de su lugar de residencia.

La protección aparece así concebida de una manera muy amplia, que marca una diferencia respecto a cualquier otra legislación: ello podría explicarse — como la extraterritorialidad que resulta— en que está en juego un derecho fundamental del individuo (27) . El art. 3 Reglamento viene no obstante a limitarla al determinar qué tratamientos de datos, y bajo qué circunstancias, están sujetos a él (28) : lo que, desmintiendo el párrafo anterior, puede requerir que el interesado tenga su residencia o se encuentre en la UE (sobre las diferentes versiones lingüísticas del art. 3.2 remitimos al apartado B).

A. Establecimiento en la UE

El Reglamento se aplica en primer lugar al tratamiento de datos que ocurre en el contexto de las actividades de un establecimiento en la UE, independientemente de que el tratamiento tenga lugar en la Unión o no. Las nociones básicas de «establecimiento» y «contexto de las actividades» no están definidas en el articulado. Se refiere a ellas el Cdo núm. 22, siguiendo de cerca el núm. 19 de la Directiva 95/46/CE: «Un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades, ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto» (29) . Hay acuerdo en la doctrina en el sentido de que el Reglamento, al utilizar el mismo lenguaje de la Directiva, retoma la jurisprudencia del TJUE recaída a propósito de esta (30) : en el as. C-230/14, *Weltimmo* (31) , por lo que se refiere al «establecimiento »; y en el as. C- 131/12, *Google Spain* (32) , en lo relativo al tratamiento en «el contexto de las actividades». La consecuencia es un ámbito de aplicación muy amplio para el Reglamento, acorde con la filosofía de procurar una protección «eficaz y completa» del derecho subjetivo (33) : desde la perspectiva del «establecimiento» el criterio, que finalmente es fáctico, comprende el ejercicio de cualquier actividad real y efectiva mediante una instalación estable, incluso aunque dicha actividad sea

mínima; la presencia de un único representante puede bastar en determinadas circunstancias para entender satisfecho el requisito, si actúa con un grado de estabilidad suficiente a través de los medios necesarios para la prestación de los servicios concretos de que se trate en el Estado miembro en cuestión (34) . Desde la perspectiva de las actividades se entiende que el tratamiento por parte del responsable se «lleva a cabo en el marco de las actividades» de un establecimiento en la UE cuando se halla indisociablemente ligado a ellas, incluso cuando el segundo establecimiento no participe en el tratamiento de los datos: la Directiva 95/46 no exige que el tratamiento de datos personales controvertido sea efectuado «por» el propio establecimiento en cuestión, sino que se realice «en el marco de las actividades» de éste (35) .

B. Ausencia de establecimiento en la UE

El caso de ausencia de establecimiento en la UE está contemplado bajo el art. 3.2, conforme al cual el Reglamento resultará aplicable en este supuesto en función de dos condiciones: que el interesado resida en la Unión, y que las actividades de tratamiento estén relacionadas bien con la oferta de bienes o servicios a dichos interesados en la Unión, bien con el control de su comportamiento, en la medida en que este tenga lugar en la Unión. Merece la pena precisar que en otras versiones lingüísticas del Reglamento el primer requisito no es la residencia: separándose de la propuesta de la Comisión la fórmula solo requiere que el interesado *esté* en la UE (36) . Los otros dos requisitos incorporan por primera vez en el ámbito de la protección de datos el criterio de *targeting*, hasta el punto de que han sido calificados de «giro copernicano» en este contexto (37) . Son conocidos, en cambio, en otros ámbitos, en particular en el Derecho procesal civil europeo. Es por eso por lo que en la interpretación de la oferta de bienes y servicios, opinan los autores (38) —en particular a la luz del Cdo. 23 del Reglamento— que se ha trasladado al mismo la jurisprudencia recaída a propósito del art. 15 (1)(c) del Reglamento 44/2001, antecedente del actual Reglamento (UE) núm. 1215/2012 del Parlamento Europeo y del Consejo de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil, Bruselas I bis, en los as. *Pammer* y *Altenhoff* (39) , apuntando al tiempo las dudas sobre su oportunidad: en primer lugar, por su componente subjetivo (la intención del vendedor, en *Pammer* y *Altenhoff*; la del responsable o encargado del tratamiento, en el caso de la protección de datos) (40) . En segundo lugar, porque los elementos objetivos que el TJUE, primero, y luego el legislador, han elaborado como indicios de la voluntad de dirigir la actividad al EM donde se haya el titular de los datos, serán con frecuencia impracticables en el contexto del tratamiento de datos: por ejemplo, en el caso de servicios *on line* solo accesibles en inglés y pagaderos en *bit coins* (41) . Finalmente, el requisito relativo al control del comportamiento del interesado, que planeará sobre la actividad de los operadores de redes sociales, buscadores de internet o proveedores de servicios como cuentas email, plantea dudas relativas a su interpretación (¿en qué consiste el comportamiento? (42)) y su aplicabilidad en la práctica (una vez más la intención del responsable pasa a primer plano (43)).

Finalmente interesa recordar que en el caso contemplado bajo el art. 3.2 el Reglamento exige en su art. 27 — siguiendo el ejemplo de la Directiva— la designación por escrito de un representante en la UE como regla general; veremos las repercusiones que ello puede tener en términos de competencia judicial internacional.

2 Competencia judicial internacional

A. Acción del interesado

a. Los foros del Reglamento

Asegurar el cumplimiento de las reglas sustantivas sobre protección de datos requiere el acompañamiento con normas sobre jurisdicción: en otras palabras, los criterios de competencia judicial internacional deben — además de responder por definición a las exigencias derivadas de la tutela judicial efectiva de demandante y demandado— reflejar el ámbito de aplicación de aquellas reglas, apoyándolas. El Reglamento se hace eco de esta preocupación cuando establece en su art. 79.2 que «Las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales acciones 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», lo que vale tanto para las acciones al amparo del art. 79.1 (tutela judicial), como para las de indemnización del art. 82.

Se abren así para los interesados (en el marco del art. 82 para «toda persona que haya sufrido daños y perjuicios materiales o inmateriales») dos foros específicos, alternativos entre sí y, a tenor del texto, excluyentes de cualquier otro («deberán»): en particular de los previstos por el Reglamento 1215/2012, cuyo art. 67 reconoce la primacía de las disposiciones contenidas en actos de la UE.

b. ¿Otros foros?

Pese a la claridad de los términos «deberán ejercitarse» (44) la doctrina sostiene de forma general que son aplicables, al lado del art. 79, las reglas de competencia del citado Reglamento 1215/2012 (45) . Tal opinión se apoya por una parte en la filosofía del Reglamento 2016/679, favorable a una protección amplia del interesado; y por otra en su Cdo. 147, del que efectivamente se desprende que tales normas se mantienen, siempre «sin perjuicio de la aplicación de [las] normas específicas» (46) . Conforme a esta interpretación, en la acción contra el encargado o el responsable del tratamiento se suman a los foros de su establecimiento y de la residencia habitual del interesado los siguientes: el foro del domicilio demandado, conforme al art. 4 Reglamento Bruselas I bis, concretado según lo indicado en los arts. 62 y 63 del mismo Reglamento; los foros del lugar de ejecución de la obligación que da base a la demanda (art. 7.1); y el foro del lugar del hecho dañoso (art. 7.2), todos ellos en las interpretaciones del TJUE. Igualmente será posible emplear el art. 8, en particular el art. 8.1, lo que permitirá atraer a un responsable y un encargado del tratamiento de datos, o a varios, ante los tribunales del EM de domicilio de uno de ellos. El recurso a los criterios de competencia de la sección 4ª del Capítulo II, contratos celebrados por los consumidores, está abierto cuando se reúnan las condiciones allí previstas. La sumisión tácita del art. 26 debe admitirse, si bien quizá proceda una extensión analógica de lo previsto en su párrafo 2º — el órgano jurisdiccional se asegurará, antes de asumir la competencia en virtud del apartado 1, de que se ha informado al demandado de su derecho a impugnar la competencia del órgano jurisdiccional y de las consecuencias de comparecer o no— en todo caso (47) . La elección de foro prevista en el art. 25 cabe en la medida en que no sea limitativa de los foros disponibles para el interesado (48) .

c. Consecuencias y valoración

La suma de los foros del Reglamento 1215/2012 a los del Reglamento sobre protección de datos cuando el interesado es el demandante — no está resuelto si los mismos foros son accesibles cuando sea una entidad, asociación u organización la que actúe por representación (49) — desemboca en un régimen flexible a su favor. Es cierto, no obstante, que la utilidad de los criterios puede ser más teórica que práctica: por ejemplo, el del lugar de la obligación que sirve de base a la demanda (art. 7.1.a) no es fácil de concretar para el tratamiento de datos que se produce en línea — aunque puede pactarse o recurrirse a una ficción—. Hay que recordar además que los foros aludidos entrarán en juego solo cuando concurran las condiciones de aplicabilidad del Reglamento Bruselas I bis: el Reglamento de protección de datos no define su ámbito de aplicación en atención al domicilio del demandado en un EM; sí lo hace (con carácter general) el Reglamento 1215/2012; y el «domicilio», a determinar conforme indica el propio Reglamento — art. 62 y art. 63— no es equivalente al «establecimiento» en el sentido del Reglamento 2016/679.

Al mismo tiempo los criterios son susceptibles de multiplicarse aún a través de la interpretación: de entrada, la del TJ, que implica por ejemplo en el caso del art. 7.2 Bruselas I bis la incorporación del «Mosaïc Prinzip», y la posibilidad de reclamar, en el caso de daños plurilocalizados, en cada uno de los EM donde haya habido daños de forma limitada a estos (50) . En la misma línea, en el marco del art. 79 Reglamento 2016/679 ha sugerido la doctrina que para el responsable o encargado sin establecimiento en la UE se atienda a los efectos de la competencia judicial internacional a la figura de su representante aquí (art. 27) (51) .

Se añade a lo anterior que para recurrir al foro de la residencia habitual del interesado

demandante no es precisa ninguna condición adicional, pese a que la doctrina había aconsejado cierta prudencia y añadir la condición de que el responsable o el encargado dirijan su actividad al EM de residencia, o a varios incluido ese (52) — cabe recordar, no obstante, que para el caso de que el demandado no tenga él mismo establecimiento en Europa el correctivo vendrá dado por las condiciones que el art. 3.2 Reglamento exige para la sujeción global al mismo—. A propósito del establecimiento, dos elementos concurren a que la competencia sobre la base de la noción pueda resultar extraordinariamente amplia: por una parte, la propia definición de establecimiento del Reglamento a luz de la jurisprudencia *Weltimmo*, como vimos bajo IV.1A). Por otra, no se requiere en el marco del art. 79 (a diferencia de lo que ocurre en el art. 3) que el tratamiento de datos que da base a la demanda ocurra en el marco de las actividades de ese concreto establecimiento en la UE; en otras palabras, *a priori a priori* cualquier establecimiento del encargado o responsable sujeto al Reglamento por virtud del art. 3.1 puede servir para atribuir competencia (53) . Es de esperar que la solución no prospere en la práctica: la intervención de principios característicos del ámbito de la competencia judicial internacional — ligados al derecho de tutela judicial efectiva: previsibilidad, igualdad de armas— vendrán a matizarla (54) . Cabe incluso preguntarse si en caso de presencia de varios establecimientos sería aceptable la reducción del criterio previsto en el art. 79.2 al «establecimiento principal» de responsable y encargado, tal como viene definido en el propio Reglamento (Cdo. núm. 36), esto es, en atención a la naturaleza e importancia de la actividad allí desempeñada (55) .

En nuestra opinión es cuestionable la lectura del Reglamento 2016/679 que acoge también los foros del Reglamento 1215/2012. Más allá del argumento formal —la literalidad del texto, que no puede considerarse concluyente, ya que el art. 79 no retoma la flexibilidad del Cdo. 147—, debe tenerse presente el teleológico, que es doble. La vertiente relativa a la protección del interesado, siendo vocacionalmente muy amplia («efectiva» y «completa»), no puede considerarse como un valor absoluto. Por el contrario, no solo debe mantenerse el equilibrio con otros derechos fundamentales (lo que recuerda el Cdo. 4 del Reglamento), sino también con otro objetivo esencial de la reglamentación europea, cual es la libre circulación de datos personales como una necesidad del buen funcionamiento del mercado interior (Cdo. 6, 13). En el ámbito de la ley aplicable, que veremos luego, esto se traduce en la idea de que «An operation concerning the processing of personal data can only be subject to the legislation of a single member State» (56) . En el de la competencia judicial internacional requiere que el sistema no resulte tan gravoso para los responsables o encargados como para disuadirles de entrar o permanecer en el mercado: lo que puede ocurrir si el abanico de criterios de competencia entre los cuales puede elegir el demandante es muy abierto. De este modo la previsibilidad en cuanto a los tribunales ante los cuales cabe ser demandado añade un nuevo significado al que posee en términos de tutela judicial efectiva, y en definitiva, de legitimidad de las opciones legislativas en materia de competencia judicial internacional.

B. Acción contra el interesado

Las reglas comunes — esto es, las del Reglamento Bruselas I bis— se mantienen para el caso de demanda de un encargado o responsable contra el interesado: el Reglamento sobre protección de datos no ha previsto criterios específicos para este supuesto. La lectura de tales reglas deberá hacerse de forma que sean compatibles con el Reglamento 2016/679: así, como ya hemos dicho, una cláusula de elección de foro pactada en un contrato no podrá operar en detrimento de las posibilidades abiertas al interesado en términos de competencia judicial internacional.

C. Reglas comunes

Del Reglamento Bruselas I bis podrán tomarse en todo caso la sección sobre comprobación de la propia competencia y de la admisibilidad (arts. 27 y 28). Con mayores dudas, también la relativa a litispendencia y conexidad (arts. 29 a 34), probablemente limitada a los casos de litispendencia entre EM —con exclusión por lo tanto del art. 33—. El recurso a estas reglas dependerá de cómo se interprete el art. 81 Reglamento 2016/679, sobre suspensión de los procedimientos: a tenor del Cdo. núm. 144 el texto solo se aplica a las acciones judiciales contra decisiones de las autoridades de control; pero lo cierto es que tal interpretación no parece tener sentido, al menos en cuanto a su apartado 3, y ello porque tales autoridades solo podrán ser demandadas ante la jurisdicción de

los Estados a los que pertenecen. Procede recordar también que en la Propuesta de la Comisión la regla (entonces el art. 76) sí comprendía los procedimientos civiles (57) ; su desaparición apunta a que han quedado absorbidos por lo dispuesto en el art. 81. En todo caso, la proyección de los arts. 29 y 30 Reglamento 1215/2012 deberá hacerse siempre en una interpretación que no menoscabe la finalidad del otro Reglamento: señala la doctrina, por ejemplo, que no debería aplicarse la consecuencia de tales disposiciones si ello conlleva privar al interesado de un foro específico de competencia previsto en el art. 79 (58) .

3. Ley aplicable: carácter no disponible de la protección

La normativa de protección de datos del Reglamento 2016/679 posee carácter imperativo: no sólo sus disposiciones de Derecho público, sino también aquellas relativas a las relaciones *inter privatosinter privatos.* Varios motivos confluyen a reforzar esta afirmación: por un lado el carácter directamente vinculante del instrumento, que si bien no prejuzga *a priori a priori* la naturaleza de sus disposiciones singulares , sí crea una presunción en este sentido ligada a su vez al objetivo de unificación normativa para la UE. Por otro lado se encuentra el tipo de interés (público o general) que informa las reglas sobre protección de datos. Se trata por tanto de previsiones no disponibles a través de un ejercicio de la autonomía de la voluntad material: las partes en un contrato están constreñidas a observar reglas tales como el art. 7 u 8 del Reglamento, relativas a las condiciones para el consentimiento al tratamiento, y al consentimiento de los niños en relación con servicios de la sociedad de la información, respectivamente (59) . Tampoco es posible la autonomía conflictual o elección de ley. Más aún: ni la aplicabilidad del Reglamento en casos transfronterizos depende de la designación del ordenamiento de un EM a través de normas de conflicto, ni dejarán de aplicarse sus reglas cuando la ley aplicable a la relación entre los particulares (contractual, extracontractual) resulte ser la de un tercer Estado. En otras palabras, se trata de normas materiales imperativas o leyes de policía: disposiciones cuya observancia un país considera esencial para la salvaguardia de sus intereses públicos, tales como su organización política, social o económica, hasta el punto de exigir su aplicación a toda situación comprendida dentro de su ámbito de aplicación, cualquiera que fuese la ley aplicable a la relación considerada (60) .

Hay, con todo, dos situaciones en las cuales seguirá siendo necesario el recurso a normas de conflicto una vez sea aplicable el Reglamento. En primer término, para los aspectos de las relaciones *inter privatosinter privatos* que no son de interés del Reglamento y no están contemplados en él: por ejemplo reglas de aplicación general, como la relativa a la capacidad para contratar del interesado (61) . Por otro, para extremos que sí encuentran regulación, pero para los que el Reglamento opera una remisión a los EM autorizándoles a introducir «disposiciones más específicas» (por ejemplo, el art. 6.2), o «condiciones adicionales» (el art. 9.4) (62) . La variedad que la remisión aludida puede generar entre los ordenamientos de los EM suscita un problema de determinación de la ley aplicable que el Reglamento no resuelve. En la medida en que se trate de cuestiones de Derecho privado —típicamente relativas a una relación contractual o a una responsabilidad extracontractual— (63) , esas reglas serán completadas por otras especiales, de aplicación directa, si las hubiera (64) ; o identificadas a través de la norma de conflicto correspondiente. En materia contractual esta será la que indique el Reglamento (CE) núm. 593/2008 del Parlamento Europeo y del Consejo de 17 de junio de 2008 sobre la ley aplicable a las obligaciones contractuales, Roma I (65) . En materia extracontractual hay acuerdo casi unánime en la exclusión de la protección de datos del ámbito de aplicación del Reglamento (CE) núm. 864/2007 Parlamento Europeo y del Consejo de 11 de julio de 2007 relativo a la ley aplicable a las obligaciones extracontractuales, Roma II (66) . Es cierto que lo contrario podría sostenerse: ni el argumento literal ni el histórico obligan a concluir que la protección de datos está comprendida en la referencia a «las obligaciones extracontractuales que se deriven de la violación de la intimidad o de los derechos relacionados con la personalidad; en particular, la difamación» (art. 1.2.g del Reglamento). Por otra parte, desde el punto de vista conceptual los derechos de la personalidad y a la protección de datos son independientes, como prueba que sean objeto de proclamación por separado en los arts. 7 y 8 Carta de Derechos Fundamentales respectivamente. Con todo, la opinión mayoritaria es favorable a la no aplicación del Reglamento Roma II (67) , atendiendo a las dificultades prácticas de delimitación a la hora de establecer la ley aplicable a una reclamación por violación de un derecho de la personalidad ligada a la de la protección de datos.

4. Reconocimiento y ejecución de decisiones

En su Propuesta de 2012 la Comisión hacía dos referencias al reconocimiento de decisiones judiciales en materia de tratamiento de datos en Europa (68) . El art. 74.5, bajo el epígrafe «Derecho a un recurso judicial contra una autoridad de control», recogía la obligación de los Estados miembros de ejecutar las resoluciones definitivas de los órganos jurisdiccionales en las acciones entabladas contra decisiones de autoridades de control. La disposición era apta para suscitar controversia, por razón de la naturaleza de las decisiones contestadas y del propio demandado (la autoridad de control); por eso no sorprende que no haya pasado al texto final. El art. 75.4, por su parte, ubicado bajo el título «Derecho a un recurso judicial contra un responsable o encargado», recogía el mismo mandato para las decisiones judiciales en procesos *inter privatosinter privatos*; no obstante tampoco ha quedado plasmado en el Reglamento. Actualmente solo una previsión, la del art. 48 en el Capítulo V («Transferencias de datos personales a terceros países u organizaciones internacionales»), alude al reconocimiento para decisiones muy concretas: las de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales, que únicamente serán reconocida o ejecutable si se basan en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro. La norma funciona como refuerzo o garantía defensiva, siguiendo la tónica del Capítulo al que pertenece (69) .

V. Reflexiones sobre el *private enforcement* en España

1. Estado de la cuestión

La trasposición en España de la Directiva 95/46/UE se produjo a través de Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos (70) . La doctrina ha criticado la insuficiencia de la misma en relación con los aspectos que aquí interesan: «la formulación de la ley es excesivamente genérica y resulta insuficiente al no concretar con cierto rigor los requisitos que han de cumplirse para reclamar la indemnización (…) sin regular nada sobre los perjuicios que deben ser indemnizados, sobre los criterios a tener en cuenta para valorar los daños, así como los casos de exclusión de responsabilidad» (71) . O, comparando con la LO 1/1982 sobre protección civil del derecho al honor, intimidad personal y familiar, y propia imagen (72) : «También la Ley Orgánica 1/1982 (…) regula la acción civil indemnizatoria aunque, lejos de limitarse a mencionarla, como apenas hace el artículo 19 de la LOPD, contiene un régimen específico más detallado sobre tipo de procedimiento, plazo de ejercicio, intervención del Ministerio Fiscal, legitimación activa, presunción *iuris tantumiuris tantum* de producción de daño tan pronto se cometa una de las intromisiones ilegitimas del artículo 7, extensión de la reparación al daño moral, así como unos criterios básicos para cuantificación» (73) . Este carácter más desarrollado en la LO 1/1982 explica probablemente su peso sobre la doctrina que estudia la LO 15/1999, que típicamente la emplea como referente, y más aún sobre la jurisprudencia a propósito de ella: las decisiones no suelen analizar las características del derecho a indemnización del art. 19 LOPD porque van juntos la violación de un derecho de la LO 1/1982 y la protección de datos, y la indemnización no se apoya en el art. 19, o no solo en él (74) .

Desde la perspectiva de la responsabilidad la LOPD se adelantó al Reglamento al extenderla ya al encargado del tratamiento; señala el art. 19.1 que «Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados». Otros aspectos sustantivos, en cambio, no están regulados y son controvertidos: así, a quién imputar un incumplimiento a pesar de haber el encargado actuado al margen de las instrucciones recibidas, en razón del deber de tutela que corresponde al responsable del fichero sobre el encargado del tratamiento (75) . Tampoco hay normativa sobre la pluralidad de responsables o encargados, aunque la idea de que la responsabilidad debe ser solidaria aparece en la doctrina (76) . Igualmente discutido es el tipo de responsabilidad, que para una jurisprudencia minoritaria es objetiva, lo que sostiene también algún autor (77) .

Hay diferencia de opiniones sobre el término «reparación» en el art. 23 de la Directiva, y si autoriza algo diferente a la indemnización, que es la traducción que ha recibido en el art. 19 LOPD (78) . En cuanto a los daños, está aceptado que los morales también son indemnizables pero no hay unanimidad ni entre la doctrina ni en la jurisprudencia sobre la manera de repararlos ni la cuantía de la indemnización, en su caso. Acerca de lo primero se encuentran decisiones que optan —o parecen optar, en una lectura *sensu contrario*— por excluir la indemnización económica (79) . Sobre lo segundo, algunos autores y decisiones han seguido las pautas establecidas en el art. 9.3 LO 1/1982: circunstancias del caso, gravedad de la lesión efectivamente producida, y beneficio obtenido por el causante de la lesión (80) . Otra doctrina, en cambio, ha propuesto la aplicación analógica de las cuantías previstas para las sanciones administrativas (81) . En todo caso se señala que en el uso de su discreción para la cuantificación del daño moral los tribunales no han sido particularmente generosos (82) , lo que ayudaría a explicar que los particulares no recurran a la vía judicial.

En relación ahora con los aspectos procesales hay dudas sobre el foro para el ejercicio de la acción: mientras que la del art. 19 está clara en virtud de sus párrafos dos y tres, no sucede lo mismo en relación con la tutela de los derechos que contempla el art. 18, correspondiente al art. 22 de la Directiva; del texto de la ley se desprende que el recurso es solo ante las autoridades de control, lo que no parece acorde con la norma comunitaria (83) . Otro punto controvertido es de los plazos para interponer la acción civil, donde más allá de las dudas sobre si la responsabilidad es contractual o extracontractual — lo que en realidad depende de que en el caso medie o no una relación contractual entre el perjudicado y el responsable del fichero—, surge la de si debe aplicarse la regla prevista en la LO 1/1982 de cuatro años de caducidad. La doctrina está dividida (84) ; cabe encontrar algún ejemplo en la jurisprudencia (85) . La influencia de aquella ley se deja sentir igualmente en materia de presunciones: la LOPD no prevé la presunción de daño por el hecho de la violación (86) como ocurre en el caso de los derechos protegidos por la LO 1/1982, art. 9.3; alguna jurisprudencia simplemente invoca esta (87) .

No hay en España, en fin, ninguna previsión específica de acción colectiva en materia de protección de datos. Indica la doctrina a propósito de la LOPD que «tampoco se contempla la posibilidad del ejercicio de acciones colectivas, salvo en el caso de que se trate de consumidores y usuarios afectados, en cuyo caso sería de aplicación la legitimación que atribuye a las asociaciones de éstos y a las entidades legalmente constituidas que tengan por objeto su protección o defensa, de conformidad con las previsiones del art. 11 de la LECiv» (88) .

Finalmente, por lo que se refiere a los casos transfronterizos no plantea problemas particulares la cuestión de la competencia judicial internacional en la medida en que los criterios vienen dados por un Reglamento de la UE — el Bruselas I bis, con anterioridad al Reglamento de protección de datos—, y no precisan (ni autorizan) implementación a nivel nacional. En materia de ley aplicable a la responsabilidad extracontractual la situación es diferente si se concluye, como vimos más atrás, en la inaplicabilidad del Reglamento Roma II: es necesario recurrir a los regímenes residuales vigentes en cada EM, lo que en España significa el vetusto art. 10.9 Cc.

2. El Proyecto de Ley Orgánica de Protección de Datos

En julio de 2017 se publicaba el Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal; el Proyecto ha sido aprobado el 11 de noviembre en Consejo de Ministros, y remitido a las CortesEl texto debe ser criticado tanto por lo que dice como por lo que no. En relación con lo primero, a través de normas tales como el art. 11, sobre transparencia e información al afectado, el Proyecto parece desconocer la naturaleza de reglamento de la norma de la UE, sin que quepa considerar que el legislador español está amparado por la autorización a que se refiere el Cdo. 8: «En los casos en que el presente Reglamento establece que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros, estos, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, pueden incorporar a su Derecho nacional elementos del presente Reglamento». Otro ejemplo, este de interés directo para este estudio, es el art. 30.2 del Proyecto, en virtud del cual se extiende la responsabilidad prevista en el art. 82 Reglamento al representante que responsable o/y encargado del tratamiento sin establecimiento en Europa deben

nombrar a tenor del art. 27, y que no figura en el art. 82 como deudor frente al interesado.

En relación con lo segundo se pierde la ocasión para el desarrollo de normas procesales y de conflicto que apoyarían el *private enforcement* del Reglamento. No es necesario reiterar en la ley nacional el derecho a tutela judicial efectiva o a compensación, y tampoco que no se ejercitan ante las autoridades de control sino ante los tribunales ordinarios (89) . El Reglamento mismo aborda también algún punto antes oscuro, como los referidos anteriormente, en el aptdo. III, sobre contra quién interponer la reclamación, o la responsabilidad solidaria, de manera que tampoco es relevante que no aparezcan en el Proyecto. En cambio sí sería oportuna la intervención del legislador español para aclarar el régimen de la responsabilidad y dotarlo de los rasgos de especialidad que se estimen pertinentes por comparación con el régimen común, y para solventar las dudas sobre la proyección en la materia de lo previsto en la LO 1/82: al fin y al cabo no solo los derechos que contemplan esta LO y la LOPD son independientes entre sí (claramente, arts. 7 y 8 de la CDFE; y en la jurisprudencia española (90)), sino que además los objetivos o *policies* no son los mismos en un ámbito y en otro, como no lo son tampoco los valores que actúan como contrapartida de los derechos fundamentales en cada caso; piénsese en particular en la preocupación europea por la libre circulación de datos. Ello se proyecta también sobre el ámbito procesal, donde además otros puntos merecen atención. De entrada, a fin de evitar malas *praxis* (aun cuando no sean comunes) hay que dejar claro que la acción civil no precisa de la previa reclamación administrativa (91) . Por otra parte, ya que en ausencia de legislación de la Unión las acciones de los particulares para la protección de datos se rigen por las normas y procedimientos nacionales de los Estados miembros en el marco de la autonomía procesal y su contrapartida — los principios de efectividad y equivalencia—, habrá que realizar una reflexión sobre la correspondencia y la compatibilidad del sistema español en conjunto con el objetivo del art. 80 del Reglamento. Baste aquí una observación desde la perspectiva de los sujetos protegidos: aunque es cierto que por tratarse de personas naturales en la mayoría de los casos aparecerán como consumidores, es de esperar que surjan dudas para supuestos en que el interesado actúe en parte en el marco de su actividad profesional (92) ; y sin embargo el Reglamento 2016/679 no limita la protección al interesado-persona física en función de que actúe en calidad de una cosa u otra. No es este el lugar para realizar un estudio a fondo, pero sí cabe indicar ya algunas interrogantes sobre el modelo común (el de la LEC): en relación con la legitimación otorgada a los grupos de afectados (art. 11.2 LEC) y al Ministerio Fiscal (art. 11.5 LEC); en tanto en cuanto permite a las asociaciones interponer la acción de indemnización previamente a recibir cualquier mandato, o incluso sin él (93) ; y en atención a la extensión de la cosa juzgada, a tenor del art. 221 y 222 LEC (94) . Finalmente, sería conveniente reflexionar sobre una norma de conflicto específica en materia de responsabilidad extracontractual, con preferencia sobre el genérico art. 10.9 Cc (95) .

VI. Conclusión

La protección del derecho fundamental a la autodeterminación informativa (protección de datos) se produce mayoritariamente a través de mecanismos de Derecho público: la afirmación está empíricamente constatada (96) . La aplicación forzosa de normas tales como la LOPD, que implementa en España la aún vigente Directiva 95/46/CE, y las correspondientes en el resto de los EM, tiene lugar sobre todo a través del recurso a las autoridades de protección de datos. El tratamiento de datos, sin embargo, posee además de la dimensión pública otra privada, bajo forma contractual o extracontractual. La defensa del derecho fundamental puede producirse por tanto también por la vía judicial civil; una posibilidad que completa la vía administrativa, y está libre de los defectos que — presuntamente- afectan a esta: falta de recursos de las autoridades de protección, competencias limitadas, dudas sobre su independencia. Dotada de los útiles adecuados el *private enforcement* se convierte en una forma de litigación estratégica, que tiene en el punto de mira no solo a responsables y encargados del tratamiento, sino también el legislador, bien sea para la revisión de las normas, bien de sus condiciones de aplicación. Sin embargo, en Europa la vía civil no se emplea con esta orientación, lo que parece deberse a la falta del instrumental— especialmente procesal- pertinente (97) .

El Reglamento 2016/679, ya en vigor y aplicable a partir del año próximo, incluye entre sus

previsiones mecanismos para incentivar el recurso al *private enforcement* siguiendo una pauta practicada en otros ámbitos (típicamente, el Derecho de la competencia), y que en el de la protección de datos se amplifica a través de instrumentos ya adoptados —como la Directiva Directiva (UE) 2016/680 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— o en trámite — véase la Propuesta Reglamento sobre la privacidad y las comunicaciones electrónicas—. Son relevantes en este contexto el reconocimiento expreso de la responsabilidad del encargado del tratamiento frente al interesado, solidaria con la del responsable, así como la de los corresponsables y los diversos encargados del tratamiento si fueran varios; la inclusión de los daños morales entre los indemnizables; el endurecimiento de las condiciones para la exención de responsabilidad; la ampliación de la legitimación activa a asociaciones o entidades representativas del interesado; y la mayor facilidad para la prueba por el interesado del incumplimiento o del error en el tratamiento de datos, que resulta de la exigencia al responsable de su capacidad de demostrar que cumple con el Reglamento. Las reglas que definen el ámbito de aplicación (muy amplio) del Reglamento, así como las que invisten a los tribunales de los EM de competencia judicial para aplicarlo en casos transfronterizos, y el carácter de normas materiales imperativas de las normas, que las hace ineludibles en los mismos casos, refuerzan igualmente el *private enforcement*. Con todo, son muchos aspectos los que el Reglamento no ha tratado o deja abiertos, creando espacio para el fracaso de sus buenas intenciones y para la duda; y tampoco los aborda el Proyecto español de julio de 2017. En estas condiciones no es posible compartir —no plenamente— el entusiasmo de la doctrina según la cual «Private enforcement is a significant part of the *Copernican revolution* worked by the GDPR» (98) .

Notas

(1) *DO* L, núm. 281, de 23 de noviembre de 1995.

Ver Texto

(2) *DO* L, núm. 119 .

Ver Texto

(3) Sobre la tendencia a recurrir a las autoridades de protección de datos (APD) en lugar de a la vía judicial y los motivos *vid*. el Informe de la European Union Agency for Fundamental Rights (FRA), *Access to data protection remedies in EU Member States*, 2013, Luxemburgo, Publications Office of the European Union, 2013, pp. 32-35, así como el conjunto de informes nacionales recopilados en la obra colectiva de Brkan, M., Psychogiopoulos, E., *Courts, Privacy and Data Protection in the Digital Environment*, Edward Elgar Pub., 2017.

Ver Texto

(4) En la misma línea *vid.* arts. 54 y 56 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. Véase también los arts. 21 y 22 de 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) 10 final.

Ver Texto

(5) Accesible en línea: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf (última visita 31.10.2017), p. 25. *Vid.* el actual art. 28.10 Reglamento.

Ver Texto

(6) *Loc. ult. cit.,* p. 28. Un ejemplo es el art. 19 Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos (LOPD), *BOE* núm. 298, de 14 de diciembre.

Ver Texto

(7) Sobre el caso de varios encargados del tratamiento y su régimen *vid.* art. 28.

Ver Texto

(8) European Union Agency for Fundamental Rights (FRA), p. 28 ss. España, así como otros países de la UE (por ejemplo UK a partir del asunto *Google Inc. V. Vidal Hall*, [2016] QB 1003, [2015] EWCA Civ 311) ya incluía los daños morales en la indemnización : *vid*. *infra* bajo V. A).

Ver Texto

(9) *Vid.* European Union Agency for Fundamental Rights (FRA), p. 21.

Ver Texto

(10) Informe del Center on Regulation in Europe (CERRE), *Consumer privacy in network industries - a CERRE policy report,* 25 de enero de 2016, en línea, http://www.cerre.eu/sites/cerre/files/160125_CERRE_Privacy_Final.pdf (última visita 31.10.2017), p. 58, con apoyo en art. 9 del Cc francés.

Ver Texto

(11) Así, en materia de Derecho de la competencia, *vid.* la Directiva 2014/104/UE del Parlamento Europeo y del Consejo, de 26 de noviembre de 2014, relativa a determinadas normas por las que se rigen las acciones por daños en virtud del Derecho nacional, por infracciones del Derecho de la competencia de los Estados miembros y de la Unión Europea, *DO* L, núm. 349, de 5 de diciembre de 2012, Cdo. 13 y art. 3.

Ver Texto

(12) VAN ALSENOY, B., «Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation», 7 (2016) JIPITEC 271, para. 6 (pero *vid.* para. 8, sobre una responsabilidad objetiva del responsable en relación con las acciones del encargado , incluso aun demostrando la ausencia de negligencia en la elección o supervisión del encargado; hay no obstante opiniones distintas, como reconoce el propio autor).

Ver Texto

(13) VAN ALSENOY, B., para. 39. En parecido sentido ya el Informe del Center on Regulation in Europe, CERRE, p. 58.

Ver Texto

(14) *Vid*. no obstante los arts. 27.3, 27.3 y 28.4 de la Directiva sobre la posibilidad de que una asociación representativa interponga acciones, si bien ante autoridades de control.

Ver Texto

(15) European Union Agency for Fundamental Rights (FRA), pp. 30-31.

Ver Texto

(16) Gracias a una web *ad hoc* website, 25.000 usuarios más han cedido su acción a Max Schrems; 50.000 más están registrados en una lista de espera.

Ver Texto

(17) Una legitimación que como hemos visto depende además o del mandato del interesado, o de una previsión legal específica - y que no comprende acciones de indemnización. Crítico, ERDOS, D., «European Data Protection Regulation and Online New Media: Mind the Enforcement Gap», *Journal of Law and Society,* 2016, pp. 534-564, *esp.* p. 160.

Ver Texto

(18) En el caso *Schrems* el litigio está financiado por un tercero, ROLAND ProzessFinanz AG, con sede en Alemania. La empresa cubre las costas del juicio y del abogado; en caso de éxito recibirá el 20% de la indemnización.

Ver Texto

(19) Que ni siquiera está claro que puedan ser abordados desde la UE. Otros elementos potencialmente disuasorios de la acción judicial son el tiempo y los costes del proceso, como recoge el European Union Agency for Fundamental Rights (FRA), pp. 30, 31.

Ver Texto

(20) COM/2013/0401 final.

Ver Texto

(21) En Austria el mecanismo para la «colectivización» de las reclamaciones, basado en la cesión, no presenta un límite por razón de la materia, de manera que podría ser empleado igualmente en este contexto, si bien sólo es posible la cesión en el caso de reclamaciones de dinero, y no de pretensiones mero-declarativas. Sobre el caso español *vid.* bajo V.

Ver Texto

(22) Otra posibilidad: si la acción civil se configura como *follow-on* a una sanción por parte de la autoridad de protección de datos podrá beneficiarse de lo haya quedado probado a efectos de la imposición de esta. La praxis de demandas civiles subsiguientes a la intervención administrativa no es común.

Ver Texto

(23) VAN ALSENOY, B., para. 12, 13, refiriéndose a la decisión del (entonces aun existente) Tribunal de la Función pública en el as. F-30/08, *Fotios Nanopoulos,* ECLI:EU:F:2010:43, para. 161. El asunto versaba sobre la divulgación no autorizada de datos personales. *Vid*. también el asT-259/03, *Kalliopi Nikolaou*, ECLI:EU:T:2007:254, para. 141-142.

Ver Texto

(24) Center on Regulation in Europe (CERRE), p. 58. También de HERT, P., PAPAKONSTANTINOU, V., WRIGHT, D., GUTWIRTH S., «The proposed Regulation and the construction of a principled-driven system for individual data protection», *Innovation: The European Journal of Social Science Research*, 2013, pp. 133-144, *esp.* p. 141.

Ver Texto

(25) VAN ALSENOY, B., para. 43, en lo que se refiere al responsable del tratamiento.

Ver Texto

(26) En el Reglamento. Otra cosa es que la presunción exista en el Derecho nacional: *vid. infra* bajo V. A), notas al pie núm. 94, 95, sobre el caso español.

Ver Texto

(27) RYNGAERT, C., «Editorial», *International Data Privacy Law*, 2015, vol. 5, núm. 4, pp. 221-225, *esp.* p. 223. A la hora de determinar el alcance de la reglamentación europea, que pasa por ser una de las que otorga mayor protección en el mundo, el Reglamento abandona en gran medida el criterio de territorialidad y lo sustituye por el de jurisdicción. Sobre este paso *vid*. también de HERT, P., CERNIAWSKI, M., «Expanding the European data protection scope beyond territory: Art. 3 of the General Data Protection Regulation in its wider context», *International Data Privacy Law*, 2016, vol. 6 núm. 3, pp . 230-243, *esp.*

pp. 231-233.

Ver Texto

(28) Al mismo tiempo, una interpretación flexible de las nociones que se emplean en el texto es apta para reforzar la extensión del ámbito de aplicación: *vid*. las Conclusiones del Abogado General Bot en el as. C-210/16, de 24 de octubre de 2017, ECLI:EU:C:2017:796, sobre quién es «responsable» a los efectos de la Directiva 95/46/CE. La definición de esta es retomada en el Reglamento en el art. 4.7.

Ver Texto

(29) El Cdo. 19 se refería a «instalaciones» («installation», en francés), y no a «modalidades» («dispositif»), menos específico y por tanto más flexible. En la versión inglesa se emplea en ambos casos el término «arrangements».

Ver Texto

(30) *Vid.* por todos GÖMMAN, M., «The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement», *Common Market Law Review*, 2017, pp. 567-590, *esp.* pp. 570-574.

Ver Texto

(31) De 1 de octubre de 2015, ECLI:EU:C:2015:639. *Vid.* de Miguel Asensio, P., «Aspectos internacionales de la protección de datos: las sentencias Shrems y Weltimmo del Tribunal de Justicia», *La Ley Unión Europea*, núm. 31- Noviembre 2015; también «Competencia y Derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea», *Revista española de Derecho internacional*, vol. 69 (1), pp. 75-108, para. 12. A nuestro juicio podría discutirse esta extrapolación teniendo en cuenta que en *Weltimmo* la cuestión tenía una dimensión intra-europea, y en particular que la sociedad objeto de discusión estaba registrada en un EM, por lo que su sujeción a la normativa europea se produciría en todo caso.

Ver Texto

(32) De 13 de mayo de 2014, ECLI:EU:C:2014:317.

Ver Texto

(33) C- 131/12, *Google Spain*, para. 53, 58, entre otros.

Ver Texto

(34) C- 230/14, *Weltimmo*, para. 30, 31.

Ver Texto

(35) As. C- 131/12, *Google Spain*, para. 50 y ss. Que el establecimiento en Europa no determine los fines y medios del tratamiento pasa a ser irrelevante, en contra de lo decidido por ejemplo por el Tribunal de Primera Instancia de Bruselas, 9 de noviembre de 2015 (*vid*. Bu-Pasa, S., «Cross-border issues under EU data protection laws with regards to personal data protection», *Information and Communications Technology Law*, 2017, vol. 26, pp. 213-228, p. 215).

Ver Texto

(36) COM(2012) 11. *Vid.* el texto en inglés del Reglamento: «data subjects who are in the Union». En la doctrina recalca la no exigencia de residencia BRKAN, M., «Data Protection and Conflict-of-Laws: A Challenging Relationship», *European Data Protection Law Review,* 2016, vol. 3, pp. 324-341, p. 339.

Ver Texto

(37) de HERT, P., Cerniawski, M., p. 238, retomando una expresión de C. Kuner.

Ver Texto

(38) GÖMMAN, M., p. 585. Más matizado, de MIGUEL ASENSIO, P., en *REDI,* para. 16, recuerda que el estándar no es plenamente coincidente, y se limita a señalar que «puede ser de utilidad como referencia». En parecido sentido, Kuner C., «Extraterritoriality and Regulation of International Data Transfers in EU Data

Protection Law», *International Data Privacy Law*, 2015, vol. 5, núm. 4, pp. 235-245, *esp.* p. 236.

Ver Texto

(39) De 7 de diciembre de 2010, en los asuntos acumulados C- 585/07 y C- 144/09, ECLI:EU:C:2010:740. Compárese el Cdo núm. 23 Reglamento con los para. 92 y 93 de la sentencia.

Ver Texto

(40) Svantesson, D., «Extraterritoriality and targeting in EU data privacy law: The weak spot undermining the regulation», *International Data Privacy Law*, 2015, vol . 5, pp. 226-234, *esp.* 232.

Ver Texto

(41) Id., p. 228, seguido por Gömman, M., p. 586.

Ver Texto

(42) El Cdo. 24 aporta indicios sobre la actividad de control del comportamiento, pero no sobre este.

Ver Texto

(43) Gömman, M., pp. 587-587.

Ver Texto

(44) Otros idiomas apuntan en el mismo sentido: inglés —«shall»—; francés —«est intentée»; italiano—, «sono promosse»; portugués— «são propostos».

Ver Texto

(45) El análisis crítico de los criterios de competencia del Reglamento Bruselas I bis fue llevado a cabo antes de la adopción del Reglamento 2016/679 por Brkan, M., «Data protection and European private international law: observing a bull in a China shop», *International Data Privacy Law*, 2015, vol. 5, núm. 4, pp. 257-278, *esp.* pp. 264-271, pp. 275-276 , e *id.,* «Data Protection and European Private International Law», EUI Working Paper RSCAS 2015/40, a sumar a los autores que se citan en las notas al pie que siguen.

Ver Texto

(46) de MIGUEL ASENSIO, P., en *REDI,* para . 35 y ss; KOHLER, C., «Conflict of law issues in the 2016 data protection regulation of the European Union», *Rivista di Diritto Internazionale Privato e Processuale,* 2016, vol. 3, pp. 653-675, bajo V, *esp.* pp. 668-670, 672-673.

Ver Texto

(47) Debe recordarse que el Reglamento 2016/679 solo contempla la protección de datos de las personas naturales, y por tanto —en principio— de actores no sofisticados. En muchas ocasiones se tratará de consumidores: parece conveniente que el órgano juzgador advierta de que la comparecencia implica la renuncia a los foros de aquel Reglamento, y no solo a los del art. 17 y ss del Reglamento 1215/2012.

Ver Texto

(48) de MIGUEL ASENSIO, P., *REDI,* para. 47; Kohler, C., p. 669.

Ver Texto

(49) En el marco del Convenio de Bruselas de 1968 que precede al Reglamento 1215/2012 las decisiones del TJ en los as. C-89/91, *Shearson Lehman Hutton*, ECLI:EU:C:1993:15, y as. C-167/00, *Henckel,* ECLI:EU:C:2002:555, conduce a pensar que no tienen abierto el foro de la residencia habitual del representado, en la medida en que se inspira en la misma filosofía de protección de una parte estructuralmente débil, y en todo caso persona física. El resultado de la cuestión prejudicial pendiente en este momento en el as. C-498/16 será relevante, pero quizá no totalmente decisivo dadas las características del representante (Mr. Schrems es una persona física y - aunque está por decidir- posiblemente un consumidor en el sentido del Reglamento 1215/2012).

Ver Texto

(50) *Vid.* la sentencia de 7 de marzo de 1995, as. C-68/93, *Shevill*, ECLI:EU:C:1995:61. La posibilidad está limitada, no obstante, a los casos en que resulte apropiada, entendiéndose que no lo son aquellos cuyo marco es internet. En estos casos entra en juego la jurisprudencia sobre el centro de gravedad de los intereses de la víctima, desarrollados a propósito de la violación a derechos de la personalidad por internet: *vid.* as. C-194/16, *Bolagsupplysningen OÜ*, de 17 de octubre de 2017, ECLI:EU:C:2017:766, y los que cita .

Ver Texto

(51) KOHLER, C., p. 668. Es cierto que en tal caso lo más probable es que el demandado carezca también de domicilio en la UE, lo que significa que la mayoría de los foros del Reglamento 1215/2012 no entran en juego - *supra* nota al pie núm . 59.

Ver Texto

(52) BRKAN, M., EUI WP, 2015, p. 24.

Ver Texto

(53) de MIGUEL ASENSIO P., en *REDI,* para. 41.

Ver Texto

(54) de MIGUEL ASENSIO P., *loc. ult. cit.*, refiriéndose a la previsibilidad.

Ver Texto

(55) En el Reglamento la ubicación del establecimiento principal sirve expresamente a atribuir el rol de «principal» a una autoridad de control: *vid.* Cdo 124. No se abordan otras consecuencias posibles, como la expresada en el texto.

Ver Texto

(56) Opinión del AG Saugmandsgaard Oe en el as. C-191/15, *Verein für Konsumenteninformation*, ECLI:EU:C:2016:388. Debe recordarse que el TJUE no reproduce la fórmula en la sentencia, ECLI:EU:C:2016:612, lo que puede entenderse como voluntad de no pronunciarse al respecto, pero también como - en la medida en que tampoco la rechazó- aceptación implícita. En este últimos sentido Svantesson, D., «Art. 4(1)(a) *establishement of the controller* in EU data privacy law - time to rein in this expanding concept?», *International Data Privacy Law*, 2016, vol. 6, núm. 3, pp. 210-221, *esp.* pp. 220-221.

Ver Texto

(57) COM(2012) 11 final.

Ver Texto

(58) de MIGUEL ASENSIO P., *REDI,* para. 51.

Ver Texto

(59) También la interpretación de la noción será la incluida en el propio Reglamento, art. 4.11. La ausencia de definiciones no significa que la misma pueda ser tomada del ordenamiento de los EM: habrá que indagar en cada caso si procede una interpretación autónoma.

Ver Texto

(60) *Vid.* art. 9.1 Reglamento Roma I. Sobre este carácter imperativo en la doctrina Kohler, C. bajo IV; de MIGUEL ASENSIO P., *REDI,* para. 52. La cuestión se había discutido bajo la Directiva: por todos, Brkan, M., 2016, pp. 333-336; y vid. la decisión *Facebook v. Independent Data Protection Authority of Schleswig-Holstein,* caso 8 B 60/12, con referencia expresa al art. 9 Reglamento Roma I.

Ver Texto

(61) Como expresa KOHLER, C., p. 671: «The rights conferred by the Regulation do not exist in a vacuum».

Ver Texto

(62) *Vid.* WAGNER, J., BENECKE, A., «National Legislation within the Framework of the GDPR», *European Data Protection Law Review,* 2016, vol. 2, pp. 353-361, examinando las «cláusulas de apertura» más relevantes.

Ver Texto

(63) El problema no se limita a los aspectos de Derecho privado del Reglamento. CHEN, J., «How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation», *International Data Privacy Law,* 2016, vol. 6, núm. 4, pp. 310-323, señala hasta 37 aspectos en los que los EM gozan de margen de discreción.

Ver Texto

(64) *Vid.* los instrumentos aludidos *supra*, nota al pie núm. 2

Ver Texto

(65) Tratándose de contratos de consumo entrarán en juego también las directivas al efecto -en particular la Directiva 93/13/CEE- y la legislación de implementación.

Ver Texto

(66) KOHLER, C., pp. 673-674, retomando a A. Dickinson; de MIGUEL ASENSIO, P., *REDI,* para. 54, también con más referencias.

Ver Texto

(67) Vid. nota precedente; también CHEN, J., pp. 318-319 o BRKAN, M., 2016, p. 331 (en relación con la Directiva) y p. 339 (el Reglamento). Otra opinón Rott, P., «Data protection law as consumer law- How consumer organizations can contribute to the enforcement of data protection law», *EuCML*, 2017, vol. 3, pp. 113-119, *esp.* p. 118, sin mayor explicación.

Ver Texto

(68) *Supra*, nota al pie núm. 67.

Ver Texto

(69) KOHLER, C., p. 657.

Ver Texto

(70) *Supra*, nota al pie núm. 7.

Ver Texto

(71) 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* , 2013, pp. 173-206, *esp.* p. 176.

Ver Texto

(72) *BOE* núm. 115, de 14 de mayo de 1982.

Ver Texto

(73) ZUNÓN VILLALOBOS M., «La garantía civil de la privacidad», *Revista Aranzadi Doctrinal* núm. 9/2013, Estudio.

Ver Texto

(74) ABERASTURI GORRIÑO U., p. 177. En este estudio no pretendemos profundizar en la jurisprudencia española en la materia; nos limitamos a algunas decisiones representativas remitiendo por lo demás a las que refieren los autores.

Ver Texto

(75) ABERASTURI GORRIÑO, U., p. 193. Cita el autor la SAN de 18 de mayo de 2010, FJ 4 (erróneamente, por cuanto la cita ha de ser a la SAN 2488/2010, de 28 de mayo de 2010, ECLI: ES:AN:2010:2488, F.J. 5).

Ver Texto

(76) BUSTO LAGO, J.M., «La Responsabilidad Civil de los responsables de ficheros de datos personales y de los encargados de su tratamiento», *Revista Doctrinal Aranzadi Civil-Mercantil,* núm. 5/2006, Doctrina, pp. 10-11, con más referencias.

Ver Texto

(77) Un resumen de posturas doctrinales se encuentra en Busto Lago, J.M., pp. 24-26. Véase también ABERASTURI GORRIÑO, U., p. 190, con más referencias, se decanta por la objetiva; cita entre otras SAP Segovia 25 de abril de 2002, FJ 1, en la que efectivamente cabe leer «Tanto más cuando la responsabilidad prevista en la Ley, entiende de forma casi unánime la doctrina, que se trata de naturaleza objetiva». No obstante recuerda el autor también que «en la mayoría de ocasiones, los tribunales no entran a analizar si en los incumplimientos se ha producido una actuación más o menos diligente», y añade que «en el caso de la responsabilidad civil extracontractual se ha admitido como norma general la responsabilidad subjetiva». ZUNÓN VILLALOBOS, M., p. 17 se inclina por una responsabilidad subjetiva al entender que el régimen español general requiere negligencia, siquiera en un mínimo grado y que la LOPD no se separa de él, al menos no expresamente.

Ver Texto

(78) Para lo primero ABERASTURI GORRIÑO, U., p. 201; BUSTO LAGO, J.M., p. 40, sostiene en cambio que sólo cabe indemnización.

Ver Texto

(79) Sería el caso de la SAP Badajoz de 29 de abril de 2004, F.J. 8, que menciona el daño moral y el patrimonial y alude a este, pero no a aquel, como «económicamente evaluable». Más clara la SAN 4849/2011 de 3 de noviembre de 2011- ECLI: ES:AN:2011:4849, F.J. 4.

Ver Texto

(80) BUSTO LAGO, J.M., pp. 42-43. No obstante, en la jurisprudencia que cita aparecen vinculadas las violaciones de la protección de datos y el derecho al honor, trayendo causa la segunda de la primera. *Vid.* también ABERASTURI GORRIÑO, U ., p. 201.

Ver Texto

(81) RUIZ CARRILLO, A., *Los datos de carácter personal (Concepto, requisitos de circulación, procedimientos y formularios)*, Bosch, Barcelona, 1999, pp. 36-37; id., *La protección de los datos de carácter personal*, Bosch, Barcelona , 2001, p. 109.

Ver Texto

(82) ZUNÓN VILLALOBOS M., p. 14, en un examen de jurisprudencia hasta 2012, indica el límite de 3000 euros, lo que se reitera en otras posteriores, como la STS (Sala de lo Civil, Sección 1ª) núm. 68/2016 de 16 de febrero. Otras posteriores, como la SAP de Asturias (Sección 1ª) núm. 94/2017 de 4 abril, o la SAP de Barcelona (Sección 16ª) núm. 364/2014 de 17 julio, F.J 28, han otorgado cuantías más elevadas.

Ver Texto

(83) ZUNÓN VILLALOBOS M., pp. 28-29.

Ver Texto

(84) Lo propone por ejemplo ESTANCONA PÉREZ, A.A., «Solvencia patrimonial y tratamiento automatizado de datos personales. Protección desde el derecho privado», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 32/2013, bajo 2.2.2, mientras que BUSTO LAGO, J.M., p. 23, limita la solución a los casos en que la acción se ejercite para la protección del derecho al honor, la intimidad o la propia imagen. En contra PUYOL MONTERO J., «Derechos de las personas: derecho a indemnización (1ª parte)», en

Estudios y Comentarios Legislativos (Civitas). *Comentario a la ley Orgánica de Protección de Datos de Carácter Personal*,, p. 9.

Ver Texto

(85) En la praxis de los tribunales *vid.* a partir de la STS (Sala de lo Civil, Sección 1ª) núm. 28/2014 de 29 enero, la de la SAP de Barcelona (Sección 16ª) núm. 364/2014 de 17 julio, F.J. 4.

Ver Texto

(86) A favor de leer en el art. 19 LOPD una presunción *iuris tantum* del daño, tanto moral como patrimonial, no obstante, Puyol Montero J., pp. 12-13.

Ver Texto

(87) ZUNÓN VILLALOBOS M., p. 14; y p. 15, su opinión en el sentido de que en el ámbito de la protección de datos se admita la presunción, pero solo *iuris tantum*. Excluyendo que se aplique la presunción del art. 9.3 la LO 1/82, pero considerando acreditada la causación del daño moral en atención a la naturaleza de los datos divulgados; y recurriendo a modo de orientación a los criterios de aquella ley, SAP de Barcelona (Sección 16ª) núm. 364/2014 de 17 julio, F.J 28. Recuerda BUSTO LAGO, J.M., pp. 27-28, en el mismo sentido la SAP Badajoz, de 29 de abril de 2004, F.J. 4, que invoca expresamente la LO 1/1982 para aplicar la presunción en un caso de vulneración de la normativa de protección de datos.

Ver Texto

(88) BUSTO LAGO J.M., p. 37. En el mismo sentido ZUNÓN VILLALOBOS, p. 27, nota al pie núm. 75; J. Puyol Montero, p. 4.

Ver Texto

(89) Discrepamos en este sentido de E. O'DELL, «Compensation for Breach of the General Data Protection Regulation», 2017, accessible en https://ssrn.com/abstract=2992351 (última visita 31.10.2017), pp. 36-38; no en cambio, del planteamiento general en el sentido de que la reglamentación nacional, siempre sea precisa porque lo requiera el Reglamento, debe ser lo más completa posible. Cabe añadir que dado que estos extremos sí serán objeto de trasposición en el marco de la Directiva (UE) 2016/680 (*supra* nota al pie núm. 4), al realizarla pueda hacerse un recordatorio, que probablemente será útil también de cara al futuro Reglamento sobre la protección en el sector de las comunicaciones electrónicas.

Ver Texto

(90) *Vid.* la STC 292/2000, de 30 de noviembre de 2000.

Ver Texto

(91) SAP de Madrid núm. 37/2007, de 6 de febrero de 2007.

Ver Texto

(92) En el contexto de la litigación internacional y de la aplicación del art. 13 del Convenio de Bruselas (hoy Reglamento Bruselas I bis), recuérdese el as. C- 464/01, *Gruber v. Bay*, de 20 de enero de 2005, ECLI:EU:C:2005:32, sobre la noción de contrato celebrado por un consumidor , donde el TJUE concluyó que «Una persona que ha celebrado un contrato relativo a un bien destinado a un uso parcialmente profesional y parcialmente ajeno a su actividad profesional no puede invocar las reglas de competencia específicas establecidas en los artículos 13 a 15 de dicho Convenio, salvo que el uso profesional sea marginal hasta el punto de tener un papel insignificante en el contexto global de la operación de que se trate, siendo irrelevante a este respecto el hecho de que predomine el aspecto no profesional».

Ver Texto

(93) La legitimación de entidad, asociación u organización deriva de su propio fin estatutario; es propia, no por representación. No obstante, en el caso de la forma asociativa se puede aceptar que en la medida en que los intereses defendidos son los de los asociados, la entidad actúa en representación de estos. Por otra parte no cabe entender que ha habido mandato en el caso de los afectados de difícil determinación que simplemente se beneficiarán de la eventual condena.

Ver Texto

(94) La cuestión, obviamente, no es solo de legitimación (art. 11 LEC), sino que afecta a toda la configuración del régimen.

Ver Texto

(95) Sobre cuál podría ser esta, KOHLER, C., nota al pie núm. 14, indica que «the way to determine the applicable law has to be assessed in each case according to the specific context», aunque añade que «the scope rules of Directive 95/46 may provide some guidance». CHEN, J., pp. 321-323, propone extraer los criterios del propio Reglamento 2016/679, en concreto de las nociones de establecimiento principal, que está ligada a la de la determinación de la autoridad de control principal (arts. 56, 60). La propuesta está concebida para la identificación de la ley aplicable para aspectos de Derecho público.

Ver Texto

(96) *Supra*, nota al pie núm. 3.

Ver Texto

(97) *Supra* nota al pie núm. 1.

Ver Texto

(98) O'DELL, E., p. 3. Optimistas, especialmente a la luz de los cambios en el Derecho material, son también el Informe del Center on Regulation in Europe (CERRE), p. 7, p. 56.; o LYSKEY, O., «Courts, privacy and data protection in the UK: Why two wrongs don't make a right», en Brkan, M., Psychogiopoulos, E., *loc. ult. cit.,* pp. 215-236, *esp.* p. 235.

Ver Texto