COMPETENCIA Y DERECHO APLICABLE EN EL REGLAMENTO GENERAL SOBRE PROTECCIÓN DE DATOS DE LA UNIÓN EUROPEA

Pedro Alberto DE MIGUEL ASENSIO *

Publicado en:

Revista Española de Derecho Internacional (REDI)

Volumen 69 (1) – 2017
pp. 75-108

ISSN: 0034-9380

* Catedrático de Derecho internacional privado
Facultad de Derecho
Universidad Complutense de Madrid
E- 28040 MADRID
pdmigue@der.ucm.es

COMPETENCIA Y DERECHO APLICABLE EN EL REGLAMENTO GENERAL SOBRE PROTECCIÓN DE DATOS DE LA UNIÓN EUROPEA[*]

Pedro Alberto DE MIGUEL ASENSIO
Catedrático de Derecho internacional privado
Universidad Complutense de Madrid

1. PANORAMA DE LA NUEVA NORMATIVA

1. Dos elementos condicionan la trascendencia alcanzada por la dimensión internacional de la legislación europea sobre protección de datos personales, que ha tenido un claro reflejo en la jurisprudencia reciente del Tribunal de Justicia (TJUE) –como muestran sus sentencias en los asuntos *Google Spain*[1], *Weltimmo*[2], *Schrems*[3] o *Verein für Konsumenteninformation*[4]- y es de prever que lo continúe teniendo próximamente[5], al

[*] Esta contribución se ha realizado en el marco del proyecto de investigación DER 2015-64063 (MINECO/FEDER). Todas las páginas web citadas han sido visitadas el 15 de octubre de 2016.
[1] STJUE de 13 de mayo de 2014, *Google Spain y Google*, C-131/12, ECLI:EU:C:2014:317.
[2] STJUE de 1 de octubre de 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639.
[3] STJUE de 6 de octubre de 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650.
[4] STJUE de 28 de julio de 2016, *Verein für Konsumenteninformation*, C-191/15, ECLI:EU:C:2016:612.
[5] Cabe reseñar el auto del *Oberster Gerichtshof* austriaco de 20 de julio de 2016 en el asunto *Schrems c. Facebook* que solicita al TJUE una decisión prejudicial sobre las normas de competencia judicial internacional en materia de contratos de consumo respecto de una acción colectiva frente a ciertas prácticas en materia de tratamiento de datos, consultado en *http://europe-v-facebook.org/EN/en.html*; así como la petición

tiempo que ha merecido particular atención en el proceso de revisión legislativa. De una parte, destaca la disparidad a nivel comparado entre los estándares de tutela del derecho a la protección de datos, que en la UE se configura como un derecho fundamental de conformidad con el art. 8.1 de la Carta de Derechos Fundamentales de la UE y el art. 16.1 del Tratado de Funcionamiento de la UE[6], lo que se relaciona con su elevado nivel de protección en un contexto en el que no existe un marco regulatorio común a escala global.[7] De otra parte, la utilización de información sobre personas físicas como componente esencial de actividades ofertadas o prestadas a través de Internet[8] se asocia con la relevancia práctica del ámbito espacial de aplicación de la legislación así como de las cuestiones relativas a la determinación de las autoridades y tribunales competentes, que condicionan la efectividad del régimen de protección instaurado en la UE y su eventual repercusión sobre la posición competitiva[9] y las obligaciones de los operadores afectados.

2. Tras más de un lustro de gestación[10], el 27 de abril de 2016 tuvo lugar la adopción del Reglamento (UE) 2016/679, general de protección de datos (RPD)[11], que deroga la Directiva 95/46/CE[12] con efecto a partir del 25 de mayo de 2018. Debido a su amplio alcance material, el RPD se proyecta sobre el conjunto de tratamientos de datos

---

del *Bundesverwaltungsgericht* (Alemania) en el asunto C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstei/ Wirtschaftsakademie Schleswig-Holstein GmbH*, con cuestiones sobre las competencias de las autoridades de control en situaciones internacionales.

[6] GONZÁLEZ FUSTER, G., *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Heidelberg, Springer, 2014, pp. 163-248.

[7] KUNER, C., *Transborder Data Flows and Data Privacy Law*, Oxford, OUP, 2013, pp. 157-160; e id., « The European Union and the Search for an International Data Protection Framework», *Groningen Journal of International Law*, vol. 2(2), 2014, pp. 55-71; y BYGRAVE, L.A., *Data Privacy Law, an International Perspective*, OUP, Oxford, 2014, caps. 3 y 4.

[8] Como sucede con las redes sociales, véánse las contribuciones incluidas en RALLO LOMBARTE, A. Y MARTÍNEZ MARTÍNEZ, R. (COORDS.), *Derecho y redes sociales*, 2ª ed., Navarra, Civitas, 2013, así como L. EDWARDS, «Privacy, law, code and social networking sites», en I. BROWN (ED.), *Research Handbook on Governance of the Internet*, Cheltenham, Edward Elgar, 2013, pp. 309-352; y los servicios de computación en la nube, H. CHANG, «Data protection regulation and cloud computing», en CHEUNG, A.S.Y. Y WEBER, R.H. (EDS.), *Privacy and Legal Issues in Cloud Computing*, Cheltenham, Edward Elgar, 2015, pp. 26-42.

[9] VAN ALSENOY, B., Y KOEKKOEK, M., «Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted'», *International Data Privacy Law (IDPL)*, 5.2, 2015, pp. 105-120, p. 110.

[10] Las líneas básicas de la reforma aparecían ya recogidas en Comisión Europea, «Comunicación acerca del enfoque global de la protección de los datos personales en la Unión Europea», *COM (2010) 609*, de 4 de noviembre de 2010, que se encuentra en el origen de la Propuesta de Reglamento, *COM (2012) 11*, de 25 de enero de 2012.

[11] DO L núm. 119, de 4 de mayo de 2016, p. 1.

[12] DO L núm. 281, de 23 de noviembre de 1995, p. 31.

relativos a personas físicas identificadas o identificables, salvo ciertas excepciones, como los tratamientos para la prevención, investigación, detección o enjuiciamiento de infracciones penales[13], o los efectuados por una persona física en el ejercicio de actividades exclusivamente personales o domésticas conforme al art. 2.2.c) del RPD que mantiene la excepción ya existente en el régimen previo. Al margen del Reglamento quedan las obligaciones específicas de los servicios de comunicaciones electrónicas en redes públicas de comunicación[14], si bien lo deseable es que en lo relativo al ámbito territorial de aplicación los criterios del RPD sean también aplicables en este sector.[15]

Rasgo muy destacado es el cambio de instrumento normativo, pues frente al marco legislativo previo de mera armonización[16] se ha optado por la unificación mediante un Reglamento llamado a sustituir a las legislaciones nacionales[17], salvo en aspectos en los que el RPD prevé que sus normas pueden ser especificadas o restringidas por los Estados miembros, como contempla su art. 8 sobre la edad aplicable al consentimiento de los niños. En todo caso, la aplicación de determinados aspectos del RPD, como en materia de supervisión, requerirá la adaptación de las legislaciones nacionales.

[13] Materia regulada en una Directiva de la misma fecha, que queda al margen del presente análisis, la Directiva (UE) 2016/680, de 27 de abril de 2016 (DO L núm. 119, de 4 de mayo de 2016, p. 89).

[14] Obligaciones establecidas en la Directiva 2002/58/CE, pendiente de ser revisada para asegurar la coherencia con el RPD, véanse cdo. 173 y art. 95 RPD. La subsistencia en ese ámbito de la mera armonización plantea riesgos de descoordinación con el RPD, véase KOTSCHY, W., «The proposal for a new General Data Protection Regulation—problems solved?», *IDPL*, 2014, vol. 4(4), pp. 274-281, esp. pp. 276-277.

[15] European Data Protection Supervisor, «Opinion 5/2016. Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC)», 22 de julio de 2016, p. 21, <*https://secure.edps.europa.eu/*>.

[16] El TJUE puso de relieve que la armonización llevada a cabo por la Directiva 95/46/CE era completa o de máximos pero destacó que la flexibilidad de sus normas dejaba en muchos casos en manos de los Estados la regulación de los detalles y la posibilidad de elegir entre varias opciones, SSTJUE de 6 de noviembre de 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596, apdos. 83 y 95-96; y 7 de noviembre de 2013, C-473/12, *IPI*, ECLI:EU:C:2013:715, apdo. 31.

[17] Entre las deficiencias de la situación bajo la Directiva, destacaba lo fragmentado del entorno que generaba inseguridad jurídica, véase, Comisión Europea, «La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI», COM(2012) 9, pp. 4-7, de 25 de enero de 2012, presentada junto a la Propuesta de Reglamento, *COM (2012) 11*.

3. Muy significativas son las novedades que introduce el RPD[18] en lo relativo a su dimensión internacional[19]. Tras la unificación normalmente no resultará necesario en las situaciones intracomunitarias determinar la legislación de qué concreto Estado miembro es aplicable con respecto a las materias objeto del RPD, pero se mantiene la trascendencia de precisar el alcance internacional de la legislación europea (sección 2, *infra*) y cobra una renovada importancia la precisión del Estado cuya autoridad de control es competente (sección 3, *infra*). Respecto a la tutela judicial en materia civil, la coordinación de otras novedades con normas preexistentes de Derecho internacional privado reviste particular complejidad[20], en materia de competencia judicial internacional, litispendencia y ley aplicable (sección 4, *infra*).

4. Al margen del presente trabajo, centrado en las cuestiones de competencia y derecho aplicable, quedan otros aspectos vinculados relevantes desde la perspectiva internacional, como el régimen de las transferencias de datos a terceros Estados[21], que también en el nuevo marco es objeto de notables restricciones. Mediante la ya mencionada sentencia *Schrems*, C-362/14, el TJUE declaró la invalidez de la Decisión 2000/520/CE relativa a los principios de puerto seguro, pieza fundamental para facilitar las transferencias de datos desde la UE a EEUU, que han alcanzado una gran expansión al hilo, por ejemplo, de la llamada computación en nube.[22] Sus graves deficiencias han pretendido ser corregidas mediante la Decisión (UE) 2016/1250, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU.[23] En todo caso, la existencia de este régimen no

[18] Para un análisis de conjunto, DE HERT, P., Y PAPAKONSTANTINOU, V., «The new General Data Protection Regulation: Still a sound system for the protection of individuals?», *Computer Law & Security Review*, vol. 32, 2016, pp. 179–194.
[19] Para una valoración inicial, DE MIGUEL ASENSIO, P.A., «Aspectos internacionales del Reglamento general de protección de datos de la UE (I): cuestiones de competencia», 11 de mayo de 2016; e *id*., «(II): Derecho aplicable», 19 de mayo de 2016, *http://pedrodemiguelasensio.blogspot.com.es*.
[20] BRKAN, M., «Data Protection and European Private International Law», July 2015, *Robert Schuman Centre for Advanced Studies Research Paper No. RSCAS 2015/40*, <http://ssrn.com/abstract=2631116>, pp. 1-37; e *id*., «Data protection and European private international law: observing a bull in a China shop», *IDPL*, 5.4, 2015, pp. 257-278.
[21] KUNER, C., «Extraterritoriality and regulation of international data transfers in EU data protection law», *IDPL*, vol. 5.4, 2015, pp. 235-245.
[22] STAIGER, D.N., «Cross-border data flow in the cloud between the EU and the US», en CHEUNG, A.S.Y. Y WEBER, R.H. (EDS.), *op. cit.*, nota 8, pp. 96-117.
[23] DO L núm. 207, de 1 de agosto de 2016, p. 1.

impide que en la medida en que las actividades de quienes se benefician del mismo queden comprendidas dentro del ámbito territorial de la legislación de la UE sobre datos personales ésta resulte directamente aplicable[24].

2. ÁMBITO TERRITORIAL Y DETERMINACIÓN DEL RÉGIMEN JURÍDICO

2.1. Función de las normas sobre el ámbito territorial

5. A diferencia de su antecedente el art. 4 de la Directiva 95/46/CE, titulado «Derecho nacional aplicable», el art. 3 del RPD aparece referido al «Ámbito territorial», si bien los dos artículos responden a un planteamiento similar en la medida en que el art. 4 de la Directiva, pese a su título, fue formulado también de manera unilateral. Ambas normas coinciden en su función esencial, consistente en la concreción del ámbito espacial de aplicación de la legislación europea sobre protección de datos, lo que resulta determinante de en qué situaciones los responsables o encargados del tratamiento incluso de terceros Estados deben cumplir con las obligaciones impuestas y quedan sometidos a la supervisión jurídico-pública de las autoridades de control.

En la Directiva 95/46/CE la concreción de la legislación nacional aplicable también determinaba el Estado o Estados miembros cuyas autoridades de control eran competentes para la supervisión, habida cuenta de la estricta correlación entre ley aplicable y autoridad competente característica del ámbito administrativo, como puso de relieve el TJUE en su sentencia *Weltimmo*. En el RPD las normas sobre su ámbito territorial contenidas en el art. 3 no cumplen una función semejante, habida cuenta de que el RPD unifica la normativa para el conjunto de la Unión. No obstante, en la medida en que las legislaciones no resultan plenamente unificadas –por ejemplo, en relación con la edad para el consentimiento de los niños (art. 8 del RPD)- puede plantearse la necesidad de concretar la de qué Estado miembro es aplicable (o si lo son las de varios). Por su formulación el art. 3 RPD no parece diseñado para esa función, pero a falta de reglas específicas puede servir de referencia al respecto.

[24] Véase, v.gr., COLONNA, L., « Article 4 of the EU Data Protection Directive and the irrelevance of the EU–

6. La supervisión de la aplicación del RPD –incluida la tramitación de reclamaciones, la práctica de investigaciones y la imposición de sanciones administrativas- es responsabilidad de las autoridades de control de los Estados miembros y no de una autoridad de control de ámbito europeo. En las situaciones vinculadas con más de un Estado miembro continúa siendo de gran importancia la determinación del Estado o Estados miembros cuyas autoridades de control son competentes, si bien ya no son decisivos a este respecto sus criterios sobre el ámbito de aplicación territorial de la legislación sino normas específicas sobre competencia en el ámbito administrativo.

7. Más allá de los mecanismos jurídico-públicos de supervisión, el ámbito de aplicación territorial de la legislación sobre protección de datos es también de gran importancia en litigios entre particulares ante los tribunales del orden civil. A modo de ejemplo, cuando un interesado ejercite acciones de indemnización frente a un responsable por los daños y perjuicios sufridos como consecuencia de un tratamiento con infracción del RPD, sólo prosperará en la medida en que la situación quede comprendida dentro de su ámbito de aplicación. No obstante, los aspectos de ley aplicable a cuestiones distintas de la licitud del tratamiento de datos vendrán típicamente determinados por las reglas de conflicto en cada caso relevantes, como el art. 10.9 Cc (véase sección 4.7, *infra*).

2.2. Evolución de los criterios de aplicación

8. Esa función común que desempeñan el art. 4.1 de la Directiva 95/46/CE y el art. 3 del RPD, con respecto a la delimitación del ámbito territorial de aplicación de la legislación de la Unión, explica las semejanzas estructurales entre ambos preceptos. Los dos parten de una clasificación tripartita y prevén como primer criterio determinante del sometimiento a la legislación europea el que el tratamiento de datos tenga lugar en el contexto (marco) de las actividades de un establecimiento del responsable o del encargado en la Unión (un Estado miembro). Como criterio alternativo, contemplan su aplicación cuando el responsable esté establecido en un lugar en que el Derecho de los Estados miembros se aplica en virtud del Derecho internacional público, como en el caso de una

US Safe Harbor Program?», *International Data Privacy Law*, 2014, Vol. 4, No. 3, pp. 203-221, p. 215.

misión diplomática u oficina consular de un Estado miembro (cdo. 25 del RPD). Por último, se fijan cuáles son los otros criterios que determinan en qué medida la legislación europea es aplicable cuando el responsable o encargado del tratamiento no está establecido en la UE, cuestión en la que sí se aprecian importantes diferencias entre el RPD y la Directiva.

9. Precisamente, con respecto a los responsables y encargados no establecidos en la UE, el RPD abandona el criterio recogido en el art. 4.1.c) de la Directiva 95/46/CE, que hacía depender la aplicación de la ley de un Estado miembro de la utilización en el tratamiento de datos de medios situados en su territorio, lo que en España tiene su reflejo en el art. 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)[25]. Con el propósito de que la protección de la Directiva no desapareciera cuando el responsable tuviera su establecimiento en un Estado tercero, su art. 2 previó en tales casos la aplicación de la ley del Estado miembro en cuyo territorio se encuentren situados los medios –automatizados o no– a los que recurra para el tratamiento de datos personales, salvo que los utilice con fines de mero tránsito. El RPD abandona ese enfoque.

10. Desde sus inicios se puso de relieve que la referencia al recurso a medios en un Estado miembro resultaba fuente de incertidumbre y podía conducir a atribuir un ámbito de aplicación excesivo[26]. El propio Grupo de Trabajo sobre Protección de Datos creado en virtud del art. 29 de la Directiva 95/46/CE (GTPD) señaló cómo la interpretación amplia del término «medios» («*equipment*» en la versión inglesa) podía en la práctica llevar a aplicar la legislación europea sobre protección de datos a situaciones que no presentan una

[25] *BOE* núm. 298, de 14 de diciembre de 1999. Ese mismo criterio aparece en el art. 3.1.c) del Reglamento de desarrollo de la LOPD aprobado mediante R.D. 1720/2007, de 21 de diciembre (*BOE* núm. 17, de 19 enero 2008).

[26] Véanse SWIRE, P.P., «Of Elephants, Mice, and Privacy: International Choice of Law and the Internet», *Int. Lawyer*, vol. 32, 1998, pp. 991-1025, p. 1007; BYGRAVE, L.A., «Determining Applicable Law Pursuant to European Data Protection Legislation», *Computer Law and Security Report*, vol. 16, 2000, pp. 252-257, pp. 254- 255; KUNER, C., *European Data Protection Law*, 2ª ed., Oxford, OUP, 2007, pp. 117-119; SANCHO VILLA, D., *Negocios internacionales de tratamiento de datos personales*, Navarra, Civitas, 2010, pp. 43-49; MOEREL, L., «The long arm reach of EU data protection law: does the Data Protection Directive apply to

vinculación real con la UE, en particular cuando medios situados en la UE se utilizan por un encargado para el tratamiento de datos de personas no residentes en la UE por cuenta de un responsable establecido fuera de la UE.[27]

De acuerdo con la interpretación del GTPD, indicativa de la posición prevalente entre las autoridades nacionales de supervisión, en virtud de ese criterio la normativa de la UE sobre protección de datos no sólo era aplicable en la medida en que el prestador empleara centros de datos o servidores situados en un Estado miembro para el almacenamiento o tratamiento de datos, sino también en otras situaciones como aquellas en las que sitios web cuyos responsables no están establecidos en la UE emplean dispositivos para la recogida activa de datos procedentes de los terminales de los usuarios (considerados como un «medio» a esos efectos) situados en Estados miembros, incluyendo la colocación de cookies o archivos similares en el disco duro del usuario con el objeto de que reciba, almacene y remita información a un servidor ubicado en un tercer Estado. Algunas críticas relativas a que el ámbito de aplicación podía resultar excesivo, destacaban que la efectividad de la aplicación de la normativa de los Estados miembros a esas situaciones era limitada[28], al tiempo que se fue desarrollando la idea de que la captación de datos sólo debería considerarse comprendida en el ámbito de aplicación de la legislación europea en la medida en que el sitio web o actividad se halle dirigido a algún Estado miembro[29].

---

processing of personal data of EU citizens by websites worldwide?», *IDPL*, 2011, vol 1(1), pp. 28-46, esp. pp. 38-43; y DE MIGUEL ASENSIO, P.A., *Derecho privado de Internet*, 5ª ed., Navarra, Civitas, 2015, pp. 359-367.

[27] GTPD, «Dictamen 8/2010 sobre derecho aplicable», de 16 de diciembre de 2010, WP 179, p. 24, consultado, al igual que el resto de los documentos del GTPD, en *http://ec.europa.eu/justice/data-protection/article-29/index_en.htm*. En relación con la computación en nube, véase HON, W.K., HÖRNLE. J. Y MILLARD, C., «Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3», *Queen Mary University of London, School of Law Legal Studies Research Paper No 84/2011*, 9 de febrero de 2012, *http://ssrn.com/abstract=1924240*, pp. 25-30.

[28] SCHERZER, D.V., «EU Regulation of Processing of Personal Data by Wholly Non-Europe-Based Websites», *European Intellectual Property Review*, 2003, pp. 292-300, pp. 298-299.

[29] Véase JOTZO, F., «Gilt deutsches Datenschutzrecht auch für Google, Facebook & Co. bei grenzüberschreitendem Datenverkehr?», *Multimedia und Recht*, 2009, pp. 232-237; GTPD, «Dictamen 8/2010…", *op. cit.*, nota 27, p. 25; KUNER, C., «Data Protection Law and International Jurisdiction on the Internet (Part 2)», *Int'l J.L. & Info. Tech*., vol. 18.3, 2010, pp. 227-247, p. 240; y MOEREL, L., *op. cit*., nota 26, p. 45.

Aunque en el debate acerca del eventual alcance extraterritorial de la legislación europea sobre protección de datos se ha prestado especial atención a su compatibilidad con el Derecho internacional público[30], la flexibilidad de los estándares internacionales sobre el particular facilita la apreciación de que el legislador de la UE goza de un significativo margen de apreciación al fijar los criterios de aplicación de su legislación en la materia así como el alcance de la competencia de sus autoridades de control y tribunales.[31] Más allá del debate acerca de su fundamentación en una concreta teoría jurisdiccional[32], la tendencia de los Estados a legislar sobre el tratamiento de datos personales de los residentes o quienes se encuentran en su territorio respecto de actividades vinculadas con el extranjero se halla ampliamente extendido a nivel comparado incluso en países con estándares en la materia divergentes[33].

2.3. Establecimiento del responsable o encargado del tratamiento

11. En línea con la situación anterior, el RPD fija como primer criterio que su ámbito territorial comprende el tratamiento de datos «en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no» (art. 3.1). Las innovaciones respecto al texto del art. 4.1.a) de la Directiva son aquí menores, pues se limitan a que el RPD va referido no sólo al «responsable» sino también al «encargado» del tratamiento, así como a la circunstancia, no mencionada en la Propuesta de la Comisión, de que este criterio opera «independientemente de que el tratamiento tenga lugar en la Unión o no», junto con la sustitución del término «marco» por «contexto». Por otra parte, se elimina la referencia a las situaciones en las que un mismo responsable del tratamiento esté establecido en varios

[30] Véanse KUNER, C., «Data Protection Law and International Jurisdiction on the Internet (Part 1)», *Int'l J.L. & Info. Tech*., vol. 18.2, 2010, pp. 176-193, pp. 181-191; y SVANTESSON, D.J.B., *Extraterritoriality in Data Privacy Law*, Copenhague, Ex Tuto, 2013, pp. 127-160.
[31] MOINY, J.P. "Cloud and jurisdiction: mind the borders", en CHEUNG, A.S.Y. Y WEBER, R.H. (EDS.), *op. cit.*, nota 8, p. 121.
[32] TAYLOR, M., «Permissions and Prohibitions in Data Protection Jurisdiction», *Brussels Privacy Hub Working Papers*, núm. 6, mayo de 2016, *www.brusselsprivacyhub.org/publications.html.*
[33] KUNER, C., *op. cit.*, nota 6, pp. 126-127, con referencia al ámbito de aplicación de la US Children's Online Privacy Protection Act (COPPA).

Estados miembros como circunstancia que llevaba a tener que cumplir con sus respectivas legislaciones en el régimen anterior[34].

Más allá de estos ajustes puntuales, el RPD confirma los elementos básicos de la interpretación previa de este criterio, como las precisiones en su cdo. 22 en el sentido de que un establecimiento «implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables» sin que sea un factor determinante «la forma jurídica que revistan tales modalidades». Algunos aspectos controvertidos de su aplicación, como su proyección a entidades cuyo establecimiento responsable de la prestación del servicio que lleva a cabo el tratamiento se encuentra en un tercer Estado –en los términos de la STJUE *Google Spain*-, perderán parte de su trascendencia en el nuevo régimen con respecto al Derecho aplicable, en la medida en que con frecuencia no resultará controvertido que esas situaciones se hallan sometidas a la legislación europea, al quedar comprendidas en su ámbito territorial en virtud del nuevo criterio recogido en el art. 3.2, incluso cuando no exista establecimiento en un Estado miembro.

12. Para garantizar un alto nivel de protección, se mantiene el concepto amplio y flexible de establecimiento, que se extiende «a cualquier actividad real y efectiva, aun mínima, ejercida mediante una instalación estable» (apdo. 31 de la sentencia *Weltimmo*), como recoge el cdo. 22 del RPD. Ahora bien, es necesario que el tratamiento se produzca en el contexto de las actividades del establecimiento.

Conforme al criterio desarrollado en la sentencia *Google Spain* (apdos. 55 y 56), el tratamiento se produce «en el marco de las actividades» de un establecimiento cuando las actividades del responsable (como la prestación del servicio de motor de búsqueda, red social…) situado en un tercer Estado «están indisociablemente ligadas» a las de su establecimiento en un Estado miembro. Ese vínculo puede existir aunque el establecimiento en la UE no participe en el tratamiento de datos, por ejemplo, cuando sirve para obtener fondos aunque los mismos no financien directamente la prestación del servicio, de modo

[34] Véase DAMMANN, U. Y SIMITIS, S., *EG-Datenschutzrichtlinie*, Baden Baden, Nomos, 1997, pp. 124-129.

que tal vínculo puede estar presente aunque la relación económica entre ambas actividades no sea particularmente directa.[35]

13. La amplitud con la que se define el que el tratamiento se produzca «en el marco de las actividades» de un establecimiento del responsable en la Unión, junto con la ausencia en la sentencia *Google Spain* de precisiones acerca del alcance internacional del llamado "derecho al olvido", ha llevado a criticar que puede servir para pretender su aplicación incluso a situaciones en las que el reclamante carece de vínculos significativos con la Unión y se dirige a un responsable de un tercer Estado pero que cuenta con un establecimiento en la UE.[36] El documento sobre la aplicación de esa sentencia adoptado por el GTPD vincula los beneficiarios del llamado derecho al olvido con el art. 8 de la Carta de Derechos Fundamentales de la UE, referido «a toda persona», si bien precisa que las autoridades de control se centrarán en reclamaciones en las que exista una conexión clara entre el interesado y la Unión, por ejemplo al ser nacional o residente de un Estado miembro[37]. En dicho documento se considera que para garantizar satisfactoriamente los derechos de los interesados no basta con suprimir los enlaces del buscador en las versiones del mismo que se ofrecen bajo dominios europeos, pero la posición del GTPD no excluye cierta flexibilidad, pues hace referencia a que la supresión debería ser efectiva también en todos

[35] El GTPD ha ofrecido pautas para precisar la existencia de ese vínculo. Una de ellas es que la mera pertenencia a un mismo grupo de empresas no resulta suficiente para apreciarlo, en particular cuando las actividades de la sociedad que lleva a cabo el tratamiento (por ejemplo, una red social establecida en un tercer Estado) y las de la sociedad del mismo grupo establecida en la UE carecen de toda conexión (por ejemplo, una sociedad dedicada al comercio al por mayor de productos alimenticios sin vinculación con la red social), véase GTPD, «Update of Opinion 8/2010 on applicable law in light of the CJEU judgment in Google Spain», 16 de diciembre de 2015, Annex II.

[36] Véase KUNER, C., «The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges», en HESS, B. Y MARIOTTINI, M. (EDS.), *Protecting Privacy in International and Procedural Law and by Data Protection (European and American Developments)*, Baden-Baden, Ashgate-Nomos, 2015, pp. 19-44, pp. 28-31.

[37] GTPD, «Guidelines on the Implementation of the CJEU Judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12», 26 de noviembre de 2014, pp. 8-9.

los dominios «relevantes» incluido «.com», de modo que, en función de la estructura del buscador, podrían quedar al margen de la prohibición búsquedas desde fuera de la UE.[38]

2.4 Responsables o encargados no establecidos en la Unión

14. Aunque en su codo. 14 el RPD parte de que la protección que establece «debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia», cuando el tratamiento no se produce en el contexto de las actividades de un establecimiento en la Unión, la protección se limita a los interesados que se encuentren en la UE y se requiere una conexión adicional con la Unión, lo que resulta de gran relevancia de cara a evitar una injustificada aplicación extraterritorial, así como para asegurar la tutela de los interesados en el contexto global de Internet.

Frente al criterio de la Directiva basado en el recurso a medios situados en un Estado miembro, el art. 3.2 del RPD prevé que el Reglamento es aplicable al tratamiento de datos personales de interesados que residan en la Unión cuando las actividades de tratamiento estén relacionadas con cualquiera de estos dos elementos: « a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión». En la versión española del Reglamento, el texto del art. 3.2 (al igual que el del cdo. 24) establece que se aplica al tratamiento de datos de interesados «que residan en la Unión»[39], mientras que en otras versiones –como la inglesa, la francesa, la alemana o la italiana -esa expresión que figuraba en la Propuesta de la Comisión ha sido sustituida por la referencia a que sean interesados que se encuentren en la Unión. El hecho de que el texto

[38] Yendo más allá del texto del documento del GTPD, la nota de prensa de la AEPD sobre el mismo, titulada «Las Autoridades europeas de protección de datos aprueban los criterios comunes para aplicar la sentencia sobre el 'derecho al olvido», de 28 de noviembre de 2014, <*https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2014/notas_prensa/common/nov_14/141128_NP_AEPD_Aplicacion_Sentencia_TJUE.pdf*> afirma: «…la exclusión debe también ser eficaz en todos los dominios relevantes, incluidos los .com lo cual abarca, en todo caso, aquellos que sean accesibles desde el territorio europeo». Para el usuario puede resultar muy sencillo recurrir a una versión del buscador bajo un dominio de un tercer Estado si sospecha que en las versiones bajo dominios de un Estado miembro se han suprimido ciertos enlaces. En tales circunstancias, lo más apropiado sería que el alcance de la prohibición no viniera determinado en función de la versión del buscador empleada sino principalmente por la ubicación –en el territorio de la Unión- del aparato desde el que se lleva a cabo la búsqueda, VAN ALSENOY, B., Y KOEKKOEK, M., *op. cit*, nota 9, pp. 113-115.

final sea resultado de la modificación de la propuesta de la Comisión sobre este punto favorece la idea de que la referencia debe entenderse hecha a que se trate de personas que se encuentren en la Unión, de acuerdo con el planteamiento de que su protección «debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia».[40]

15. Esta nueva disposición, de la que resulta también cuándo el responsable o encargado establecido en el extranjero debe designar un representante –que debe ser una persona física o jurídica establecida en la Unión- en lo que respecta a sus obligaciones derivadas del RPD (cdo. 80 y art. 27)[41], refleja una evolución que se corresponde con el propósito de hacer depender la aplicación de la legislación de que el responsable dirija a la Unión la actividad en el marco de la cual tiene lugar el tratamiento.

En principio, el lugar de situación del afectado por el tratamiento de datos personales constituye un criterio legítimo para fundar tanto la competencia internacional como la ley aplicable[42], en especial cuando va acompañado de elementos indicativos de una vinculación adicional. Pese a que la concreta redacción del art. 3.2 RPD puede plantear dificultades interpretativas, en general responde a un enfoque que facilita el sometimiento a la legislación europea (y a la competencia de las autoridades de control de sus Estados miembros) de quienes no se encuentran establecidos en la Unión pero tratan datos de personas que se encuentran en la Unión en circunstancias en las que esa consecuencia resulta en principio apropiada.

---

[39] Lo mismo sucede en la versión portuguesa.

[40] En todo caso, el que en la versión final del RPD el control del comportamiento de los afectados sólo opera como criterio de aplicación en la medida en que tenga lugar en la Unión (al igual la oferta de bienes o servicios) parece eliminar el riesgo de que pudiera llegar a considerarse la mera residencia del interesado en la Unión como determinante de la aplicación del RPD incluso en situaciones en las que personas residentes en la Unión se desplazan al extranjero, riesgo en el que insiste SVANTESSON, D., *op. cit.*, nota 30, pp. 107-108.

[41] Véase, *v.gr.*, HÄRTING, N., *Datenschutz-Grund-verordnung*, Colonia, Otto Schmidt, 2016, pp. 59-60. De acuerdo con el cdo. 80 del RPD, el representante debe estar sujeto a medidas coercitivas en caso de incumplimiento por el responsable o el encargado.

[42] Conferencia de La Haya de Derecho internacional privado, «Les échanges de données informatisées, Internet et le commerce électronique», Doc. prel., nº 7, abril 2000, p. 25, *https://assets.hcch.net/upload/wop/gen_pd7f.pdf*.

16. Al interpretar el inciso a) del art. 3.2 del RPD, punto de partida ha de ser su cdo. 23, según el cual resulta preciso determinar «si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros». Además de aclarar que la mera accesibilidad en la Unión «o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento» no basta para determinar dicha intención, se limita a mencionar como factores que, entre otros, pueden revelar esa intención del responsable el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa lengua, o la mención de clientes o usuarios que residen en la Unión.

Aunque el estándar no sea plenamente coincidente, puede ser de utilidad como referencia la jurisprudencia del TJUE relativa al criterio de que la actividad comercial vaya dirigida al Estado de la residencia habitual del consumidor, del art. 17.1.c) del Reglamento (UE) 1215/2012 o Reglamento Bruselas I bis (RBIbis) -o art. 15.1.c) de su antecedente el Reglamento Bruselas I)- y del art. 6.1.c) del Reglamento (CE) 593/2008 (Roma I). Salvando las distancias, como el que estas disposiciones relativas a la protección de los consumidores presuponen la celebración de un contrato, lo que no es el caso en el marco del art. 3 del RPD, los criterios de vinculación establecidos con carácter indicativo –no exhaustivo- por el TJUE en los asuntos acumulados *Pammer y Hotel Alpenhof* [43] pueden ser relevantes.

Entre los indicios relevantes según el Tribunal se encuentran «todas las expresiones manifiestas de la voluntad de atraer a los consumidores de dicho Estado miembro» (ap. 80), como la mención de que ofrece sus servicios o sus bienes en ese Estado miembro o la publicidad en medios que facilitan el conocimiento de su sitio por consumidores domiciliados en ese Estado. Ahora bien, la conclusión de que un sitio va dirigido al Estado miembro del domicilio del consumidor también puede alcanzarse en situaciones en las que no cabe apreciar expresiones manifiestas de la voluntad de atraer a los consumidores de ese país. Como otros indicios que pueden ser relevantes, los apdos. 83 y 84 y el fallo de la Sentencia enumeran sin ánimo exhaustivo: el carácter internacional de la actividad; la

mención de números de teléfono con indicación del prefijo internacional; la utilización de un nombre de dominio de primer nivel geográfico distinto al del Estado en que está establecido el vendedor, incluidos los genéricos (como «.com»); la descripción de itinerarios desde un Estado miembro al lugar de la prestación del servicio; la mención de una clientela internacional formada por clientes domiciliados en Estados miembros; el empleo de lenguas o divisas que no se corresponden con las habituales en el Estado a partir del cual ejerce su actividad el empresario.[44]

17. Aunque al aplicar el criterio de que las actividades vayan dirigidas a un territorio se plantea una cuestión de gradación[45], la formulación del art. 3.2.a) del RPD facilita apreciar que típicamente concurre esta circunstancia cuando se ofrecen bienes o servicios sin restricciones geográficas respecto de la UE y son adquiridos o utilizados por un número significativo de personas en la Unión, incluso a falta de expresiones manifiestas de la voluntad de atraer en concreto a clientes de la UE. Los prestadores no establecidos en la Unión que quieran excluir posibles riesgos legales en este sentido pueden recurrir al uso de mecanismos de geolocalización de empleo ampliamente extendido.

18. Con carácter alternativo, el art. 3.2.b) del RPD se refiere a su aplicación cuando el tratamiento de datos de interesados que residan (se encuentren) en la Unión esté relacionado «con el control de su comportamiento, en la medida en que este tenga lugar en la Unión». Este supuesto parece ideado básicamente para aquellas situaciones en las que ese control, en particular al hilo del empleo de archivos o programas informáticos que almacenan y permiten el acceso a información en el equipo de usuario -como cookies-, no tiene lugar en el marco del ofrecimiento al interesado de productos o servicios.[46] Ese tipo de control puede resultar de gran importancia para la llamada publicidad «comportamental»

---

[43] Sentencia de 7 de diciembre de 2010, *Pammer y Hotel Alpenhof*, C-585/08, ECLI:EU:C:2010:740.
[44] La sentencia *Pammer y Hotel Alpenhof* precisa también que ciertos elementos no son relevantes a esos efectos, como la utilización de una lengua cuando es la del empresario (apdos. 77, 78 y 91).
[45] HON, W.K., HÖRNLE. J. Y MILLARD, C., *op.cit*, nota 27, p. 36.
[46] ALBRECHT, J.P. Y JOTZO, J., *Das neue Datenschutzrecht der EU*, Baden-Baden, Nomos, 2017, p. 68; y ERNST, S., "Art. 3" en PAAL, B.P. Y PAULY, D.A. (Hrsg.), *Datenschutz-Grundverordnung*, Munich, C.H. Beck, 2017, pp. 25-26.

y plantea especiales riesgos en relación con el tratamiento de datos de los usuarios de Internet.[47]

El cdo. 24 del RPD se limita a señalar que el criterio de este inciso b) resulta operativo si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, indicando que tal puede ser el caso cuando las personas son objeto de un seguimiento en Internet para elaborar un perfil con el fin de analizar sus preferencias, comportamientos y actitudes.

3. DELIMITACIÓN DE LA COMPETENCIA DE LAS AUTORIDADES DE CONTROL

3.1. Tratamientos transfronterizos

19. Los interesados pueden hacer valer sus derechos en materia de protección de datos a través de dos vías; mediante una reclamación ante una autoridad de control, y ejercitando las acciones correspondientes en vía judicial contra el responsable o el encargado del tratamiento. Con respecto al desempeño de las funciones asignadas a las autoridades de control nacionales –que incluye conocer de las reclamaciones de los interesados (art. 57 del RPD)- así como el ejercicio de sus poderes de investigación, corrección y autorización conforme al art. 58, el criterio de base es el alcance territorial de la competencia. En línea con lo que es propio del ámbito administrativo, de conformidad con el art. 55 del RPD, cada autoridad es competente en el territorio de su Estado (y con respecto a los tratamientos efectuados por autoridades públicas de su propio país).

En el régimen previo de la Directiva, el TJUE puso de relieve la imposibilidad para las autoridades de control de imponer sanciones fuera del territorio de su propio Estado, lo que además debía coordinarse con la estricta correlación en ese ámbito entre ley aplicable y autoridad competente[48]. En el Reglamento esta correlación se presenta en términos

[47] Véase GTPD, «Dictamen 2/2010 sobre publicidad comportamental en línea», de 22 de junio de 2010; y NAVAS NAVARRO, S., *La personalidad virtual del usuario de Internet,* Valencia, Tirant lo Blanch, 2015, pp. 149-193.
[48] Véase el apdo. 57 de la mencionada sentencia *Weltimmo*.

diferentes, pues se da entre el RPD y las autoridades de control de todos los Estados miembros.

20. El alcance territorial de la competencia de estas autoridades implica que abarque normalmente los tratamientos en el contexto de las actividades de un establecimiento en su Estado miembro, los realizados por autoridades públicas de ese Estado, los que afecten a interesados en su territorio, así como los realizados por quienes no están establecidos en la Unión cuando sus destinatarios son interesados residentes en su territorio (cdo. 122 del RPD). Este enfoque conduce en principio a la posibilidad de que un responsable quede sometido incluso en relación con una misma actividad a la competencia de diversas autoridades de control[49], especialmente en la medida en que tenga establecimientos –en el sentido amplio antes reseñado- en más de un Estado miembro o el tratamiento afecte a interesados que se encuentran en varios territorios, como es frecuente en el marco de Internet.[50] En este contexto el RPD introduce un modelo de ventanilla única como un régimen específico para la determinación de las autoridades de control competentes en ciertas situaciones vinculadas con dos o más Estados miembros, que evite el sometimiento cumulativo a varias autoridades de control, lo que facilita la actividad de los responsables o encargados.

21. Elemento básico para delimitar el alcance del modelo de ventanilla única es la categoría de «tratamiento transfronterizo», que engloba con carácter alternativo dos tipos de situaciones: a) el tratamiento realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, y b) el realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado en la Unión, pero que afecta o puede afectar sustancialmente a interesados en más de un Estado miembro (art. 4.23 del RPD).

[49] SVANTESSON, D.J.B., «Article 4(1)(A) 'Establishment of the Controller' in EU Data Privacy Law – Time to Rein in this Expanding Concept?, *IDPL*, 6(3), 2016, *http://ssrn.com/abstract=2820205*.
[50] La estructura societaria del responsable puede plantear dificultades interpretativas, como ilustran las cuestiones sobre la Directiva 95/46/CE planteadas al TJUE en el asunto pendiente C-210/16, ya reseñado.

3.2. El modelo de ventanilla única y sus límites

22. Punto de partida es la identificación de una "autoridad de control principal", que es la del establecimiento principal o del único establecimiento del responsable o del encargado. Reciben la consideración de autoridades de control "interesadas" el resto de las autoridades a las que afecta el tratamiento, por estar establecido el responsable o encargado en el territorio de su Estado miembro (sin tener allí su establecimiento principal), por ser probable que se vean sustancialmente afectados los interesados que residen en su Estado, o por haberse presentado ante ella una reclamación (art. 4.22). En relación con los tratamientos transfronterizos opera el régimen especial de competencia previsto a favor de la autoridad de control principal (art. 56), si bien debe actuar conforme al procedimiento de cooperación con las autoridades de control interesadas (art. 60).

El RPD no introduce reglas específicas sobre la competencia de las autoridades de control respecto de los responsable y encargados al no tener al menos un establecimiento en la Unión quedan al margen del mecanismo de ventanilla única[51], lo que repercutirá especialmente en situaciones en las que se aplique el Reglamento en virtud de su art. 3.2, en particular cuando el tratamiento afecte a interesados de varios Estados miembros.[52]

23. En consecuencia, cuando el responsable o encargado tiene establecimientos en más de un Estado miembro resulta de gran importancia la definición de establecimiento principal, contenida en el art. 4.16, al permitir concretar cuál es la autoridad de control principal. Esa definición se diferencia del concepto general de establecimiento en la Unión del art. 3.1 como elemento determinante del ámbito territorial del RPD.

Con respecto al responsable del tratamiento, se considera que el establecimiento principal se halla «en el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se

[51] PADOVA, Y., «What the European Draft Regulation on Personal Data is going to change for companies», *IDPL*, vol 4(1), 2014, pp. 39-52, p. 44.

considerará establecimiento principal». El cdo. 36 precisa que tal establecimiento «debe determinarse en función de criterios objetivos y debe implicar el ejercicio efectivo y real de actividades de gestión que determinen las principales decisiones en cuanto a los fines y medios del tratamiento a través de modalidades estables», así como que no resulta determinante si el tratamiento se realiza en dicho lugar. Señala además que «(l)a presencia y utilización de medios técnicos y tecnologías para el tratamiento de datos personales o las actividades de tratamiento no constituyen, en sí mismas, establecimiento principal y no son, por lo tanto, criterios determinantes de un establecimiento principal». En lo relativo a los encargados, el establecimiento principal es el lugar de su administración central en la Unión y, a falta del mismo, el lugar en el que se llevan a cabo las principales actividades de tratamiento en la Unión.

24. Entre los riesgos para los interesados que podrían resultar de la implantación de un modelo de ventanilla única, destaca su potencial para menoscabar la posibilidad de tramitar una reclamación ante la autoridad de control del país de su residencia habitual, en las situaciones en las que el establecimiento principal del responsable se localice en otro Estados miembro. Asimismo, un modelo de ese tipo también podría ir asociado a riesgos de deslocalización de los responsables y encargados del tratamiento[53], en caso de existir diferencias significativas en el desempeño de sus funciones entre las autoridades de control. Para hacer frente a esos riesgos, en la tramitación del RPD se matizó de manera significativa el criterio de ventanilla única, habiendo sido éste uno de los aspectos objeto de mayor transformación entre la Propuesta y el texto final del Reglamento.[54] Además, como destaca su cdo. 129, el RPD pretende asegurar que las autoridades de todos los Estados miembros tengan los mismos poderes y dispongan de medios apropiados.

---

[52] HÄRTING, N., *op. cit*, nota 41, p.184.
[53] BARNARD-WILLS, D., PAUNER CHULVI, C., Y DE HERT, P., «Data protection authority perspectives on the impact of data protection reform on cooperation in the EU», *Computer Law & Security Review*, vol. 32, 2016, pp. 587–598, p. 590.
[54] DE HERT, P., Y PAPAKONSTANTINOU, V., *op. cit.*, nota 18, p. 191; ALBRECHT, J.P. Y JOTZO, J., *op. cit*, nota 46, pp. 116-117; y B. KÖRFFER, "Art. 55", en PAAL, B.P. Y PAULY, D.A. (Hrsg.), *op. cit.*, nota 46, pp. 615-616.

Como excepción a la aplicación del procedimiento de coordinación del art. 60 liderado por la autoridad de control principal o mecanismo de ventanilla única, se contempla que cada autoridad de control es competente para tratar una reclamación que le sea presentada o una posible infracción del RPD, cuando se refiera únicamente a un establecimiento situado en su Estado o sólo afecte de manera sustancial a interesados en su Estado (art. 56.2), incluso cuando sean procedimientos relativos a responsables o encargados con establecimiento principal en otro Estado miembro. Ahora bien, en estos casos la autoridad de control principal, que debe ser informada por aquella ante la que se ha presentado la reclamación, decidirá si se trata el caso conforme al procedimiento del art. 60, pudiendo la autoridad de control que haya informado presentar un proyecto de decisión. También excepcionalmente una autoridad de control interesada puede adoptar medidas provisionales relativas a su propio territorio.

25. El procedimiento típico en relación con los tratamientos transfronterizos es el de cooperación del art. 60, que fija el marco en el que la autoridad de control principal debe cooperar con las demás autoridades de control interesadas para esforzarse en llegar a un consenso de cara a adoptar una decisión vinculante. La autoridad de control principal puede solicitar asistencia mutua (art. 61) y la realización de operaciones conjuntas (art. 62) y es a ella a quien corresponde preparar un proyecto de decisión. Si cualquiera de las autoridades de control interesadas formula una objeción pertinente y motivada en un plazo de cuatro semanas, la autoridad de control principal puede optar por seguir la objeción y adoptar la decisión en la que estén de acuerdo todas las autoridades implicadas, que además notificará al establecimiento principal del responsable o encargado, mientras que la autoridad de control ante la que se haya presentado una reclamación informará de la decisión al reclamante. En el supuesto de que la decisión sea desestimar o rechazar una reclamación, será la autoridad de control ante la que se haya presentado la que adopte la decisión, la notifique al reclamante e informe al responsable del tratamiento, lo que condiciona la competencia en relación con el derecho a la tutela judicial efectiva contra una autoridad de control.

Si alguna de las autoridades de control interesadas ha presentado objeciones al proyecto de decisión con las que no esté de acuerdo la autoridad de control principal, ésta habrá de someter el asunto al mecanismo de coherencia del art. 63. Dicho mecanismo contempla que el Comité Europeo de Protección de Datos ("Comité", que sustituirá al GTPD) adopte decisiones vinculantes, entre otros casos, en aquellas situaciones en las que haya divergencias sobre cuál de las autoridades de control «es competente para el establecimiento principal»; así como cuando una autoridad de control interesada haya manifestado una objeción pertinente y motivada a un proyecto de decisión de la autoridad principal. En estos supuestos la autoridad de control principal o, en su caso, la autoridad de control ante la que se presentó la reclamación adoptará su decisión definitiva sobre la base de esa decisión (art. 65). Según el considerando 143 del RPD, en caso de impugnación un tribunal nacional no es competente para declarar inválida la decisión del Comité, debiendo remitirlo al Tribunal de Justicia conforme al art. 267 TFUE.

Habida cuenta de la complejidad inherente a la aplicación del RPD por una pluralidad de autoridades de control, así como de la configuración del procedimiento de cooperación y del mecanismo de coherencia, cabe esperar que la actividad del Comité resulte de gran importancia, lo que también se proyectará sobre otros aspectos del RPD, respecto de los que entre las funciones del Comité se encuentra emitir directrices, recomendaciones y buenas prácticas (art. 70).

3.3. Reclamaciones ante las autoridades de control y tutela jurisdiccional

26. El art. 77.1 establece el derecho de todo interesado a presentar una reclamación ante una autoridad de control si considera que el tratamiento de datos que le conciernen infringe el RPD, previendo que puede presentarse, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción. Esta vía de reclamación, sometida a menores costes y esfuerzos para el reclamante que el ejercicio de acciones judiciales, constituye un mecanismo esencial para que los afectados puedan solicitar la protección de sus derechos.

El art. 77 adopta un criterio flexible acerca de la autoridad ante la que el interesado puede presentar su reclamación, con el objetivo de facilitar la protección de sus derechos, que se ve reforzada por el significado atribuido a esa autoridad, en la medida en que será considerada «autoridad de control interesada» a los efectos de los procedimientos antes reseñados.

27. Desde la perspectiva de la protección de los interesados, el RPD no sólo garantiza la posibilidad de que presenten la reclamación ante la autoridad de control de su entorno más próximo o más vinculada con la actividad de que se trate. La determinación de la autoridad nacional que posteriormente adopta la decisión tiene singular trascendencia en relación con el derecho a la tutela judicial frente a esa decisión (art. 78 del RPD). De ahí la importancia de que cuando la decisión desestime o rechace una reclamación, sea la autoridad de control ante la que se haya presentado –y no la principal- la que formalmente adopte la decisión, lo que resultará determinante de la competencia de los tribunales de dicho Estado –en la práctica el elegido por el interesado para presentar su reclamación- para conocer de las acciones que puedan ejercitarse en vía judicial, típicamente por el afectado, frente a la desestimación de la reclamación. En estos casos podrán plantearse dificultades específicas, por ejemplo, al haberse aplicado en el procedimiento a los aspectos no regulados en el RPD las normas de otro ordenamiento, en concreto, el del Estado del establecimiento principal y no el del Estado cuyos tribunales son competentes para conocer de los recursos judiciales frente a la decisión de la autoridad de control.

El art. 78.3 del RPD, como es propio del ejercicio de acciones frente a actos administrativos, establece que las acciones contra una autoridad de control deberán ejercitarse ante los tribunales del Estado de dicha autoridad. Se trata de un criterio que está en línea con lo previsto en la legislación española por el art. 24 de la LOPJ relativo a la extensión de la jurisdicción de los tribunales españoles del orden contencioso-administrativo. Ahora bien, cuando la autoridad ante la que se presenta la reclamación no da curso a la misma, sólo se reconoce al interesado el derecho a ejercitar acciones contra la autoridad de control si ésta es competente en virtud de los arts. 55 y 56 del RPD, es decir,

se trata de la autoridad de control principal o la del Estado al que pertenece la autoridad pública que efectúa el tratamiento.

4. TUTELA JUDICIAL CIVIL CONTRA UN RESPONSABLE O ENCARGADO

4.1. Acciones civiles

28. El art. 79 del RPD está dedicado a regular la tutela judicial contra un responsable o encargado del tratamiento, que resulta de especial importancia respecto al derecho de toda persona que sufra daños y perjuicios como consecuencia de una infracción del RPD a recibir una indemnización (art. 82). La interposición de una reclamación ante la autoridad de control no es una vía que permita obtener la reparación del daño, por lo que el ejercicio de acciones judiciales resulta necesario para hacer efectivo el derecho a indemnización.[55] El RPD no introduce mecanismos de coordinación entre la tutela civil y la supervisión administrativa, pues en el art. 79 no se ha incluido la previsión recogida en la norma equivalente de la Propuesta de la Directiva, que contemplaba la posibilidad de que un tribunal que conociera de una demanda contra un responsable o encargado, suspendiera el procedimiento cuando estuviere pendiente ante el mecanismo de coherencia un procedimiento referido a la misma medida, decisión o práctica (art. 75.3 de la Propuesta).

A diferencia de las reclamaciones ante las autoridades de control, cuyas decisiones son objeto de recursos administrativos y eventualmente ante tribunales del orden contencioso-administrativo, el ejercicio de acciones judiciales por los interesados frente a los responsables o encargados que han vulnerado sus derechos como consecuencia de un tratamiento de datos personales da lugar típicamente a litigios ante los tribunales del orden civil (salvo que el responsable o encargado sea una administración pública).

29. Al margen del derecho de indemnización, ante los tribunales del orden civil también pueden ejercitarse otro tipo de acciones fundadas en la infracción de normas del RPD, respecto de las cuales la vía civil puede representar una alternativa a la reclamación

[55] Vénase GRIMALT SERVERA, P., *La responsabilidad civil en el tratamiento automatizado de datos personales*, Granada, Comares, 1999; y, en relación con el derecho al olvido, SIMÓN CASTELLANO, P. *El régimen constitucional del derecho al olvido digital*, Valencia, Tirant lo Blanch, 2012, pp. 190-194.

ante una autoridad de control, por ejemplo, para obtener la imposición al responsable de una limitación o prohibición al tratamiento. Así lo ilustra la STS (Sala de lo Civil) de 15 de octubre de 2015[56], con respecto a las obligaciones del periódico editor de una noticia como responsable del tratamiento de los datos personales que aparecen en su sitio web, tanto en relación con la indemnización de los daños como con la adopción de medidas para que la información relevante no pueda ser indexada por los motores de búsqueda.

Ejemplo de la doble vía de tutela –pública o privada- en materia de datos personales es la jurisprudencia del TS relativa al ejercicio del llamado derecho al olvido, como resulta en particular del contraste entre la STS (Sala de lo Civil) de 5 de abril de 2016[57] y las sentencias de la Sala de lo Contencioso del TS sobre recursos de casación contra sentencias de la Audiencia Nacional, relativas a resoluciones sancionatorias de la AEPD frente al buscador Google.[58] A diferencia de las resoluciones pronunciadas en el orden contencioso, la adoptada en el orden civil contempla la eventual indemnización de los daños.

30. En relación con estos litigios la jurisprudencia tanto de la Sala de lo Civil como de la Sala de lo Contencioso del TS ha insistido en la existencia de «distintos criterios rectores» entre ambas jurisdicciones, «por la diversidad de las normativas que con carácter principal se aplican», destacando que, a diferencia de lo que sucede en el orden civil, en el ámbito contencioso fundamentalmente se trata de conocer de impugnaciones frente a resoluciones de la AEPD tras una reclamación administrativa interpuesta por el afectado. El concepto de responsable del tratamiento ha sido objeto de interpretaciones expresamente contradictorias por parte de la Sala de lo Civil y de la Sala de lo Contencioso al determinar la responsabilidad –civil o administrativa- derivada de la ilicitud en el tratamiento de datos

[56] ECLI:ES:TS:2015:4162.
[57] ECLI:ES:TS:2016:1280.
[58] En particular las SSTS (Sala de lo Contencioso) de 11 de marzo de 2016 (ECLI:ES:TS:2016:1057), de 14 de marzo de 2016 (ECLI:ES:TS:2016:1056 y ECLI:ES:TS:2016:964), de 15 de marzo de 2016 (ECLI:ES:TS:2016:1103), así como las ocho sentencias pronunciadas por dicha Sala el 13 de junio de 2016 (ECLI:ES:TS:2016:2696; ECLI:ES:TS:2016:2699; ECLI:ES:TS:2016:2702; ECLI:ES:TS:2016:2707; ECLI:ES:TS:2016:2722; ECLI:ES:TS:2016:2723; ECLI:ES:TS:2016:2724; ECLI:ES:TS:2016:2725). En estas últimas sentencias la Sala de lo Contencioso dedica un Fdto. Jdco. específicamente a abordar las implicaciones sobre este particular de la sentencia de la Sala de lo Civil de 5 de abril de 2016, a modo de ejemplo puede verse el Fdto. Jdc.o Undécimo de la STS (Contencioso) de 13 de junio, ECLI:ES:TS:2016:2696.

por la prestación de un mismo servicio. La Sala de lo Contencioso –en línea con la sentencia *Google Spain* del TJUE- ha entendido que sólo Google Inc., sociedad con domicilio en EEUU y gestora del motor de búsqueda, es responsable del tratamiento de datos personales, mientras que la Sala de lo Civil ha considerado también a Google Spain SL, la filial en España, corresponsable del tratamiento por parte del buscador.[59]

31. Para justificar la divergencia, la STS (Civil) de 5 de abril de 2016 destaca que recae en un proceso civil que tiene por objeto la protección de derechos fundamentales del demandante (apdo. 13 del Fdto. de Dcho Tercero). Ahora bien, lo cierto es que tanto en uno como en otro caso de lo que se trataba sobre este particular es de determinar si Google Spain SL es "responsable del tratamiento" en el sentido del art. 2.d) de la Directiva 95/46/CE -art. 3.d) de la LOPD-, lo que en el proceso civil resulta presupuesto del derecho a indemnización, de modo que la interpretación de ese concepto no debería variar en función del orden jurisdiccional. El RPD reafirma esta idea, pues el concepto de responsable del tratamiento es exactamente el mismo en el art. 82 del RPD -relativo al derecho a indemnización- que en su art. 17 que regula el derecho de supresión («el derecho al olvido»), con independencia de que se ejerciten acciones civiles o se plantee una reclamación administrativa. Entre otros escenarios, no será extraño que tras la sanción administrativa, el afectado pretenda obtener una indemnización por la vía civil.

32. Desde la perspectiva de la competencia internacional resulta de interés que la sentencia de la Sala de lo Civil de 5 de abril de 2016 fundamenta su criterio en la circunstancia de que tener que demandar en España a una empresa extranjera (y no a su filial española) supondría en este caso frustrar el objetivo de asegurar una protección eficaz del derecho fundamental a la protección de datos. El Tribunal destaca las dificultades asociadas a tener que litigar contra un demandado domiciliado en el extranjero, como el coste de la traducción de la demanda, la dilación que implicaría el emplazamiento (con lo que se prolongaría la vulneración de los derechos fundamentales), o la eventual necesidad

[59] DE MIGUEL ASENSIO, P.A., «La contradictoria doctrina del Tribunal Supremo acerca del responsable del tratamiento de datos por el buscador Google», *Diario La Ley*, Nº 8773, 31 de mayo de 2016, pp. 1-6.

de solicitar la ejecución de la sentencia en EEUU. [60] Esta posición explica que las posteriores sentencias de 8 de abril de 2016 de la Sala de lo Contencioso incluyan una explicación del funcionamiento de la vía contencioso administrativa, para destacar que la circunstancia de que el responsable se halle establecido en el extranjero no implica en este orden jurisdiccional que la tutela para el afectado resulte más gravosa.

33. El peso atribuido a esos elementos de dificultad práctica por la Sala de lo Civil del TS contrasta con la circunstancia de que el mecanismo de protección establecido en materia civil por la legislación de la UE para proteger a una parte débil, como un consumidor, en las transacciones internacionales se basa precisamente en facilitar que pueda demandar ante los tribunales de su propio domicilio a una empresa establecida en el extranjero, incluido un tercer Estado, unido a la aplicación de la normativa de protección del foro. Además, la idea de que la víctima pueda demandar ante los tribunales de su residencia habitual (o su centro de vida) a quienes (teniendo su domicilio en el extranjero) infringen sus derechos de la personalidad, incluido el derecho a la protección de datos personales, ha constituido también un elemento clave de la evolución del DIPr de la UE con el objetivo de favorecer a los afectados, como refleja la sentencia del TJUE en los asuntos *eDate Advertising y Martinez*[61], así como la regla específica de competencia judicial internacional incluida ahora en el RPD (art. 79.2).

4.2. Regla especial de competencia: alcance

34. Destaca como innovación del RPD la previsión de una norma especial de competencia judicial internacional en materia civil. Su art. 79.2 atribuye a los interesados que consideren que sus derechos en virtud del RPD han sido vulnerados la posibilidad de demandar al responsable o al encargado del tratamiento ante los tribunales de cualquier Estado en el que tengan un establecimiento, y alternativamente prevé que puedan demandar ante los tribunales de su propia residencia habitual. Las situaciones a las que es aplicable este fuero vienen delimitadas por el apdo. 1 del art. 79 del RPD, que va referido a la tutela

[60] Véanse especialmente apdos. 9 a 12 del Fdto. Dcho. Tercero.
[61] STJUE de 25 de octubre de 2011, *eDate Advertising y Martinez*, C-509/09 y C-161/10, ECLI:EU:C:2011:685, apdo. 49.

judicial de los interesados contra un encargado o responsable del tratamiento cuando consideren que sus derechos en virtud del RPD han sido vulnerados como consecuencia de un tratamiento de sus datos. Se trata típicamente de acciones civiles –salvo que el responsable o encargado sea una administración pública- comprendidas en el ámbito de aplicación del RBIbis[62], ya que no se refieren a ninguna de las materias excluidas conforme a su art. 1.2. Por ello, la interacción entre el art. 79.2 del RPD y el RBIbis reviste particular interés.

35. Esta regla de competencia se proyecta sobre litigios comprendidos en el RBIbis, al ser «materia civil y mercantil» en el sentido de su art. 1. El inciso final del art. 79.2 del RPD excluye que opere el fuero alternativo a favor de la residencia habitual del interesado (incluso a partir del cdo. 145 cabría sostener que la exclusión va referida a la norma en su conjunto) en aquellos casos en los que «el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos». De acuerdo con la jurisprudencia del TJUE, la caracterización como «materia civil y mercantil» resulta de un análisis funcional[63], conforme al cual si bien determinados litigios entre una autoridad pública y una persona de Derecho privado pueden estar comprendidos dentro del ámbito del RBIbis, la aplicación de éste queda excluida cuando la tutela que se pretende tenga su fundamento en actividades de esa autoridad en el ejercicio del poder público[64]. Ejemplo de situaciones excluidas son también las que derivan de la tutela judicial contra una decisión de una autoridad de control[65], como prevé el art. 78 del RPD, ya que el ejercicio de los poderes atribuidos a las autoridades de control implica típicamente el desarrollo de actividades en el ejercicio del poder público. También puede ser el caso en situaciones en las que el perjuicio tiene su origen en tratamientos de titularidad pública, objeto de reclamación en vía contencioso administrativa.

[62] MOINY, J.P, *op. cit*., nota 31, p. 123.
[63] Véase, v.gr., MANKOWSKI, P., «Art 1 Brüssel Ia-VO», en RAUSCHER, T., *EuZPR/EuIPR*, vol. I, 4ªed., 2016, Colonia, Otto Schmidt, p. 107.
[64] Veánse, con ulteriores referencias, SSTJUE de 11 de abril de 2013, *Sapir*, C-645/11, ECLI:EU:C:2013:228, apdo. 33; y de 12 de septiembre de 2013, *Sunico*, C-49/12, ECLI:EU:C:2013:545, apdo. 34.
[65] BRKAN, M., *op. cit*., nota 20 pp. 8-9.

36. Habida cuenta de que el fundamento de la tutela que el interesado solicita en el marco del art. 79 es la vulneración de sus derechos en virtud del RPD, podría tratarse en principio a los efectos del RBIbis de acciones en materia de responsabilidad extracontractual, para hacer valer el derecho a recibir una indemnización por los daños y perjuicios sufridos como consecuencia de la infracción del RPD (art. 82.6). Ahora bien, no es extraño que entre el responsable del tratamiento (por ejemplo, un prestador de servicios de la sociedad de la información) y el interesado medie un contrato. Conforme a la jurisprudencia del TJUE cuando una parte ejercita una acción de responsabilidad civil frente a otra (de naturaleza extracontractual en la legislación nacional) debe considerarse comprendida en la «materia contractual» a los efectos del art. 7 RBIbis si el comportamiento recriminado es un incumplimiento de las obligaciones contractuales, tal como pueden determinarse teniendo en cuenta el objeto del contrato, lo que será normalmente el caso cuando la interpretación del contrato resulta indispensable para determinar la licitud del comportamiento controvertido.[66] El art. 79 RPD no incorpora ninguna restricción al respecto, por lo que, habida cuenta de su finalidad protectora de los interesados, no cabe excluir que la regla especial de competencia del art. 79.2 RPD pueda operar en relación con el ejercicio de acciones por el interesado frente al responsable (o el encargado) relativas a un contrato entre ambos en la medida en que tengan por objeto la vulneración de las normas del RPD.

37. En los tratamientos de datos que afectan a un gran número de interesados reviste mucha importancia la posibilidad de ejercitar acciones colectivas, de lo que a escala europea proporciona un ejemplo destacado la controversia Schrems c. Facebook, que es también ilustrativa de la dualidad entre la tutela pública y la privada[67]. El RPD se limita en su art. 80 a facilitar que una entidad, organización o asociación sin ánimo de lucro pueda representar a los interesados. El art. 80 del RPD no incorpora normas de competencia

[66] Véase SSTJUE de 13 de marzo de 2014, *Brogsitter*, C-548/12, ECLI:EU:C:2014:148, apdos. 23 a 25; y de 14 de julio de 2016, *Granarolo*, C-196/15, ECLI:EU:C:2016:559, ap. 21. Resulta también de interés la sentencia de 1 de octubre de 2002, *Henkel*, C-167/00, ECLI:EU:C:2002:555, esp. apdos. 37 a 41.

[67] Así el litigio principal en el mencionado asunto C-362/14, *Schrems*, tenía su origen en una reclamación presentada ante el *Data Protection Commissioner* irlandés, como detalla el auto del *Oberster Gerichtshof*

judicial. Ante las carencias en materia de acciones colectivas del RBIbis[68], puede presentar singular interés la interpretación respecto de esas situaciones de las normas de competencia del art. 79.2 del RPD.

4.3. Fuero del establecimiento

38. Como primer criterio, el art. 79.2 atribuye competencia a los tribunales del Estado miembro en el que el responsable o encargado contra el que se ejercita la acción «tenga un establecimiento». Como ha quedado reseñado, frente a la Directiva 95/46/CE, en el RPD el concepto de establecimiento pierde su importancia previa para determinar la competencia de las autoridades nacionales de supervisión. Ahora bien, ese concepto sí resulta relevante en el nuevo marco como fuero de competencia, en la medida en que el art. 79 considera competentes a los tribunales del Estado miembro en que el responsable o encargado tenga un establecimiento, como categoría flexible que puede estar presente al igual que en el sistema de la Directiva en más de un Estado miembro[69], a diferencia del concepto de «establecimiento principal» relevante en relación con el mecanismo de ventanilla única.

39. Aunque en muchas situaciones el establecimiento coincidirá con el Estado en el que se localiza el domicilio del demandado en el sentido del fuero general del art. 4.1 del RBIbis, se trata de dos categorías diferentes, susceptibles de conducir a resultados diversos. El domicilio, a los efectos del art. 4.1 del RBIbis, viene determinado para las personas jurídicas de manera autónoma por su art. 63, que prevé que se encuentra con carácter alternativo en su sede estatutaria, administración central o centro de actividad principal; mientras que respecto de las personas físicas el art. 62 conduce a la aplicación de la legislación interna del foro para determinar si el demandado está ahí domiciliado.

---

austriaco de 20 de julio de 2016 que plantea una cuestión prejudicial en esta ocasión acerca de la interpretación de los arts. 15 y 16 RBIbis en el marco de una acción colectiva contra Facebook.

[68] Ámbito en el que puede resultar una significativa aportación la eventual sentencia del TJUE en el asunto mencionado en la nota anterior.

[69] MOEREL, L., «Back to basics: when does EU data protection law apply?», *IDPL*, vol. 1(2), 2011, Vol. 1, pp. 92-110, esp. pp. 94-103.

Por su parte, el art. 79.2 del RPD no utiliza ese concepto de domicilio al atribuir competencia a los tribunales de cualquier Estado miembro en el que tenga un «establecimiento». Como ha quedado ya reseñado, el RPD mantiene el concepto amplio y flexible de establecimiento, que se extiende «a cualquier actividad real y efectiva, aun mínima, ejercida mediante una instalación estable».[70]

40. Conforme a la sentencia *Weltimmo* a esos efectos debe valorarse «el grado de estabilidad de la instalación como la efectividad del desarrollo de las actividades… tomando en consideración la naturaleza específica de las actividades económicas y de las prestaciones de servicios en cuestión», lo que facilita la posibilidad de determinar que existe una instalación estable en un Estado distinto al del domicilio social, especialmente para las empresas que se dedican a ofrecer servicios por Internet (apdo. 29). La actividad puede llevarse a cabo a través de Internet, por ejemplo, cuando tiene lugar mediante un sitio web dirigido a ese territorio, aunque resulta preciso además que disponga ahí de una instalación estable (apdo. 32). En su sentencia *Verein für Konsumenteninformation* el TJUE puso de relieve que puede existir un establecimiento a estos efectos aunque la entidad no posea una filial ni una sucursal en el Estado miembro en cuestión, si bien no es suficiente que en su territorio se pueda acceder al sitio de Internet de la entidad, siendo preciso valorar el grado de estabilidad de la instalación y la efectividad del desarrollo de las actividades en ese Estado (apdos. 76 y 77). Puede bastar a tal fin la presencia en ese país de un único representante de la sociedad domiciliada en otro Estado si actúa con un grado de estabilidad suficiente (apdo. 30 de la sentencia *Weltimmo*).[71]

41. El objetivo de garantizar los derechos de los afectados que justifica el empleo del concepto amplio y flexible de establecimiento del RPD como fuero de competencia se corresponde con la circunstancia de que puede servir para atribuir competencia a tribunales de Estados miembros que no la tendrían con base en el art. 4 del RBIbis o incluso otras

[70] Apdo. 31 de la sentencia *Weltimmo* y apdo. 75 de la sentencia *Verein für Konsumenteninformation*, ya citadas.
[71] El Abogado General en el asunto *Verein für Konsumenteninformation* consideró que no es descartable que la existencia de un servicio posventa destinado a los clientes residentes en un Estado miembro pueda constituir un establecimiento a estos efectos (ECLI:EU:C:2016:388, apdo. 121).

normas de competencia de ese instrumento, lo que podría ser de particular utilidad en relación con el ejercicio de acciones colectivas por parte de interesados procedentes de diversos Estados[72]. De hecho, a tenor del art. 79.2 del RPD cabe entender que cualquier establecimiento del responsable o del encargado en un Estado miembro puede ser relevante para atribuir competencia, pues no se exige, frente al texto del art. 3.1 del RPD, que la acción vaya referida a un tratamiento que tiene lugar en el contexto de ese concreto establecimiento (aunque puede plantearse la conveniencia de apreciar que resulta compatible con la exigencia de previsibilidad para el demandado). Cabe además entender que la competencia fundada en la existencia de un establecimiento del demandado se extiende al conjunto del daño que el tratamiento haya causado al interesado.

4.4. Residencia habitual del interesado

42. Como criterio alternativo de competencia el art. 79 del RPD prevé que las acciones frente al responsable o encargado podrán ser ejercitadas por el interesado ante los tribunales del Estado miembro en que tenga su propia residencia habitual. En relación con el empleo del concepto de "residencia habitual" en las normas de competencia de otros Reglamentos que no contienen una remisión expresa al Derecho de los Estados miembros, el TJUE ha considerado que debe realizarse atendiendo al contexto en el que se insertan las disposiciones y al objetivo pretendido.[73] Ante la ausencia de un concepto específico, cabe partir de que la "residencia habitual" no viene determinada por la mera presencia, resultando preciso que sea en principio de cierta duración para que revele una estabilidad suficiente.[74]

Aunque con frecuencia coincidirán, la "residencia habitual" del interesado no es un concepto idéntico al de "centro de intereses de la víctima", como criterio atributivo de competencia desarrollado por el TJUE para concretar el lugar donde se ha producido el daño a los efectos del art. 7.2 del RBIbis en los supuestos de lesión de un derecho de la

[72] Son ilustrativas las dudas surgidas acerca del alcance de las normas sobre protección de los consumidores del RBIbis en el asunto *Schrems c. Facebook*, pendiente ante el TJUE, nota 5, *supra*.
[73] STJUE 22 de diciembre de 2010, C-497/10, *Mercredi*, ECLI:EU:C:2010:829, apdo. 46.
[74] Ibíd., apdo. 51.

personalidad a través de Internet. En su sentencia *eDate Advertising* el TJUE puso de relieve que aunque normalmente ambos elementos se localizan en el mismo lugar, una persona puede tener su centro de intereses en un Estado miembro en el que no resida habitualmente, cuando un vínculo particularmente estrecho con ese Estado resulte de otros indicios, como el ejercicio de una actividad profesional.

43. Ante la falta de restricciones en el texto de la norma y teniendo en cuenta el objetivo que la inspira, cabe entender que el alcance de la competencia fundada en la residencia habitual del interesado se extiende también al conjunto del daño que el tratamiento por el demandado le haya causado, de modo que no se limita al producido en el Estado de su residencia habitual. Del texto del art. 79 RPD tampoco resulta que la operatividad de esta regla de competencia se subordina al cumplimiento de requisitos específicos, como la circunstancia de que las actividades del responsable estén dirigidas al Estado miembro de la residencia habitual[75], pero tal resultado podría alcanzarse en la medida en que se considere que la regla de competencia del art. 79 se halla también limitada por los criterios sobre el ámbito territorial de las normas del RPD de su art. 3.

4.5. Interacción con las reglas de competencia del Reglamento Bruselas I bis

44. El marco de relaciones entre los fueros del art. 79 del RPD y el RBIbis deriva fundamentalmente de lo dispuesto en el art. 67 de este último y en los cdos. 145 y 147 del RPD. Conforme a su art. 67, el RBIbis no prejuzga la aplicación de las disposiciones particulares que en materias especiales regulan la competencia judicial en los actos de la Unión, como es el caso del art. 79 RPD. En esta misma línea, el cdo. 147 del RPD afirma que las normas generales de competencia judicial del RBIbis «deben entenderse sin perjuicio de la aplicación» de las normas específicas del RPD». Además, acerca del significado de su art. 79.2, el cdo. 145 del RPD manifiesta que en lo relativo a las acciones contra los responsables o encargados, «el reclamante debe tener la opción de ejercitarlas ante los tribunales de los Estados miembros» designados por el art. 79.2 RPD.

[75] Planteando la cuestión, BRKAN, M., *op. cit*., nota 20, pp. 22-23.

Lo anterior revela que el objetivo de protección de los interesados se traduce en que la función de las reglas de competencia del RPD es poner a disposición de los interesados la posibilidad de ejercitar sus acciones ante los tribunales de los Estados miembros en los que el responsable o encargado tenga un establecimiento o de la propia residencia habitual del perjudicado, resultando desmentida la formulación imperativa del primer inciso del art. 79.2 («las acciones… deberán ejercitarse») por el contexto, contenido y función de la norma, así como por su redacción en otras lenguas. Cabe sostener que se trata de fueros adicionales que tiene a su disposición el interesado y que complementan en el seno de la Unión el régimen establecido en el RBIbis.[76] El mismo criterio de solución se impone en aquellos casos en los que no resulte de aplicación el RBIbis sino las legislaciones internas de los Estados miembros –como en España, la LOPJ- en virtud de la remisión contenida en el art. 6.1 RBIbis, pues en esas situaciones la legislación nacional debe entenderse sin perjuicio de la aplicación de las reglas especiales de competencia del RPD, cuyo alcance no se limita a los demandados domiciliados en un Estado miembro.

45. Desde la perspectiva del ejercicio de acciones por parte de los interesados, el art. 79.2 del RPD complementa los fueros disponibles en virtud del RBIbis y requiere que éstos se interpreten de modo que no priven de efecto útil al art. 79.2. En consecuencia, junto a los fueros previstos en el RPD, los interesados tendrán a su disposición los establecidos en el RBIbis que resulten operativos en cada caso[77], como la prórroga de jurisdicción (arts. 25 y 26, si bien en la práctica resultará poco frecuente que el interesado pretenda hacer valer esta posibilidad en detrimento de la competencia de los Estados miembros designados por el art. 79.2 del RPD que tiene carácter preferente), el fuero general del domicilio del demandado (art. 4 RBIbis, que normalmente coincidirá con un Estado miembro en el que el demandado tenga «un establecimiento» a los efectos del art. 79.2), los fueros basados en una relación de

[76] ALBRECHT, J.P. Y JOTZO, J., *op. cit.*, nota 46, pp. 127-128, se limitan a afirmar que los fueros del RPD desplazan a las normas generales de competencia del RBIbis. Aunque se ha llegado a plantear el eventual conflicto de los fueros del RPD con las competencias exclusivas del RBIbis -BRKAN, M., *op. cit.*, nota 20, p. 23-, lo cierto es que en la medida en que las reglas del art. 79 RPD van referidas a acciones relativas a la vulneración de los derechos del interesado como consecuencia del tratamiento de sus datos personales con infracción del RPD cabe entender que típicamente versas sobre materias distintas de las que son objeto de competencias exclusivas en el art. 24 RBIbis.

conexidad (art. 8 RBIbis que incluye el de la pluralidad de demandados), o el fuero especial en materia extracontractual del art. 7.2 RBIbis.

En relación con la eventual utilidad de este último, cabe reseñar que los criterios del art. 79.2 del RPD parecen no contemplar ciertas posibilidades que el interesado que ejercita una acción extracontractual podría tener en el marco del art. 7.2 RBIbis, en la medida en que se considere que éste no sólo permite demandar por el conjunto del daño ante los tribunales del Estado miembro del centro de intereses de la víctima -al menos en relación con ciertas actividades desarrolladas en Internet, con base en la sentencia *eDate Advertising*- sino también, aunque con un alcance limitado, ante los tribunales de otros lugares de manifestación del daño[78], como aquellos en los que se hayan divulgado los datos. Aunque se trata de un criterio afirmado reiteradamente por el TJUE con respecto a la infracción de derechos de propiedad intelectual[79], en relación con los derechos de la personalidad la cuestión ha sido expresamente planteada con respecto a acciones de supresión y rectificación de información en el asunto C-194/16, pendiente.[80]

46. Ha quedado ya señalado que, aunque el fundamento de las acciones ejercitadas por el interesado en el marco del art. 79 es la vulneración de sus derechos establecidos en el RPD, sus reglas de competencia pueden también ser operativas cuando se trate del ejercicio de acciones por parte del interesado frente al responsable o el encargado con quien esté vinculado por un contrato, en la medida en que tengan por objeto el incumplimiento de las normas del RPD. En todo caso, en materia contractual, cuando el interesado –que ha de ser una persona física- sea un consumidor[81] y se den las demás condiciones para su aplicación,

---

[77] Véase DE MIGUEL ASENSIO, P.A., *op.cit.*, nota 26, pp. 195-206.
[78] STJUE *eDate Advertising y Martinez*, ya citada, apdos. 41 a 44. Véase ROTH, W.H., «Persönlichkeit im Internet: Internationale Zuständigkeit und anwendbares Recht», *IPRax*, 2013, pp. 215-227, esp. pp. 221-224.
[79] SSTJUE de 3 de octubre de 2013, *Pinckney*, C-170/12, EU:C:2013:635, apdo. 42 y 46; y de 22 de enero de 2015, *Hejduk*, C-441/13, ECLI:EU:C:2015:28, apdos. 32 y 37
[80] Petición de decisión prejudicial planteada por el Riigikohus (Estonia) el 7 de abril de 2016 — *Bolagsupplysningen OÜ, Ingrid Ilsjan/Svensk Handel AB* (DO C núm. 211, de 13 de junio de 2016 p. 35).
[81] Sólo a los contratos celebrados fuera e independientemente de cualquier actividad o finalidad profesional, así como en las situaciones en las que el vínculo del contrato con la actividad profesional del interesado es tan tenue que resulta marginal, resulta de aplicación el régimen específico de protección del consumidor; además es necesario que quien contrata con una finalidad personal no tenga un comportamiento que dé la impresión de que actuaba con fines profesionales (STJCE 20 de enero de 2005, *Gruber*, C-464/01, ECLI:EU:C:2005:32).

las normas de protección de los consumidores -arts. 6.1 y 17 a 19 RBI bis y, en su caso, 22 quinquies d) LOPJ- también conducen en las situaciones típicas a rechazar la eficacia de los acuerdos de prórroga de jurisdicción y a atribuir competencia a los tribunales del domicilio del consumidor o interesado con respecto a las acciones contractuales.[82]

Por otra parte, de cara al desarrollo de la tutela privada de la protección de datos personales, la facilitación en la UE de mecanismos de acción colectiva por interesados de diversos Estados miembros perjudicados por un mismo tratamiento reviste gran importancia. El RPD, y en concreto su art. 81, no introduce reglas de competencia específicas con respecto al ejercicio de acciones colectivas[83], si bien ya ha quedado señalado como el potencial alcance de la regla de competencia del art. 79.2 basada en la existencia de "un establecimiento" del demandado puede facilitar en la práctica la concentración ante los tribunales de un Estado miembro, como también puede suceder en función de la estructura empresarial del demandado mediante el recurso al fuero relativo a una pluralidad de demandados del art. 8.1 RBIbis.

47. El art. 79 del RPD aparece redactado de tal manera que contempla la competencia para conocer de las acciones contra un responsable o encargado del tratamiento, pero no las que éstos puedan ejercitar frente a interesados. En relación con la posición como actores de los responsables o encargados el RPD no prevé fueros adicionales, habida cuenta del objetivo de protección de los interesados que inspira sus reglas de competencia. Además, en la práctica las acciones que el responsable ejercite frente a los interesados se basarán típicamente en la relación contractual existente entre ambos y no en el incumplimiento de las normas del RPD.

El que las reglas del RBIbis no pueden producir el resultado de privar de su efecto útil al art. 79.2 RPD puede ser determinante para limitar la eficacia de los acuerdos atributivos de jurisdicción que pudieran existir entre el responsable y el interesado (que

[82] En relación con los acuerdos de computación en nube, véase, v.gr., SUJECKI, B., «Internationales Privatrecht und Cloud Computing aus europäischer Perspektive», *Kommunikation und Recht*, 2012(5), pp. 312-317, p. 315.
[83] Para un análisis crítico, BRKAN, M., *op. cit*., nota 20, pp. 21-22.

pueden abarcar controversias extracontractuales), en particular en situaciones en las que tales acuerdos se pretendan invocar para oponerse a la demanda interpuesta por un interesado ante un tribunal competente en virtud del art. 79.2 del RPD.

48. No cabe descartar el ejercicio por un responsable frente a un interesado de acciones de carácter extracontractual, por ejemplo de acciones declarativas de no infracción, que en el sistema del RBIbis pueden ejercitar ante los tribunales del lugar de origen del daño, que típicamente coincidirá con su propio domicilio, lo que en el marco del RBIbis llevaría normalmente a apreciar litispendencia con respecto a una posterior acción de indemnización fundada en la infracción.[84] En tales circunstancias, la eventual repercusión del RPD en materia de litispendencia presenta particular relevancia.

4.6. Litispendencia y conexidad

49. El art. 81 del RPD, bajo la rúbrica «suspensión de los procedimientos», contempla que cuando procedimientos relativos a un mismo asunto en relación con el tratamiento por el mismo responsable o encargado estén pendientes ante tribunales de más de un Estado miembro, cualquier tribunal distinto de aquel ante el que se ejercitó la acción en primer lugar podrá suspender su procedimiento. Además, cuando se trate de un procedimiento pendiente en primera instancia será posible también, a instancia de una de las partes, la inhibición en caso de que el primer tribunal sea competente para conocer del asunto y su acumulación sea conforme a Derecho.

Aunque por su ubicación, inmediatamente antes de la regulación del derecho a indemnización y algunos aspectos de su redacción plantea dudas, y se ha afirmado que esa disposición básicamente desplaza a los artículos 29 y 30 del Reglamento Bruselas I bis[85], cabe entender que el artículo 81 RPD no está ideado para ser de aplicación en aquellos casos en los que la litispendencia o conexidad se plantea entre tribunales que conocen de acciones contra un encargado o responsable del tratamiento en materia civil. En principio,

[84] Véase HESS, B., «The Protection of Privacy in the Case of Law of the CJEU», en HESS, B. Y MARIOTTINI, M. (EDS.), *op. cit.* nota 36, pp. 81-113, p. 93, con referencia a la STJUE de 19 de diciembre de 2013 en el asunto *Nipponkoa*, C-452/12, EU:C:2013:858, apdo. 42.
[85] ALBRECHT, J.P. Y JOTZO, J., *op. cit.*, nota 46, p. 129.

en materia civil carece de justificación que el modelo más elaborado de litispendencia y conexidad del RBIbis sea sustituido por el art. 81 del RPD.

50. Entre los elementos que avalan esta posición, se encuentra que el cdo. 144 del RPD al introducir este mecanismo hace referencia a su aplicación «(s)i un tribunal ante el cual se ejercitaron acciones contra una decisión de una autoridad de control tiene motivos para creer que se ejercitaron acciones ante un tribunal competente de otro Estado miembro relativas al mismo tratamiento…», de modo que parece acotar su aplicación a situaciones en las que las acciones se ejercitan contra una autoridad de control. Cabe entender que este mecanismo va dirigido a facilitar la coordinación fundamentalmente entre procedimientos judiciales en diversos Estados miembros relativos a resoluciones de autoridades de control, en circunstancias en las que esa coordinación puede resultar apropiada, en especial por referirse al mismo tratamiento por un responsable o encargado, complementando la coordinación que en el ámbito administrativo resulta de otras disposiciones del RPD, como los arts. 56, 571.e) y 60.[86] Este limitado alcance del régimen de conexidad previsto, que puede llevar a la inhibición de los tribunales ante los que no se ejercitó la acción en primer lugar, se corresponde con que los requisitos de aplicación sean diferentes y menos estrictos (por ejemplo, al no exigir identidad de partes) a los previstos en el art. 29 RBIbis para la litispendencia. Aunque la posibilidad de suspensión e inhibición deriva directamente del art. 81 RPD, que se superpone a la normativa procesal de los Estados miembros, queda subordinada a la valoración por parte del tribunal correspondiente

Además, el cdo. 147 al contemplar que ciertas normas del RPD priman sobre el RBIbis se refiere tan sólo a que el RPD contiene «normas específicas sobre competencia judicial». Las normas sobre litispendencia y conexidad entre tribunales de Estados miembros del RBIbis se vinculan con su sistema de reconocimiento y ejecución, por lo que resulta apropiado que esas disposiciones del RBIbis sigan siendo aplicables al ejercicio de acciones de responsabilidad civil por la infracción de la normativa sobre protección de datos, habida cuenta de que las resoluciones que se adopten en materia civil serán

[86] M. FRENZEL, "Art. 81", en PAAL, B.P. Y PAULY, D.A. (Hrsg.), *op. cit.*, nota 46, pp. 728-733.

susceptibles de reconocimiento y ejecución en los demás Estados miembros con base en el RBIbis. Si bien la Propuesta de Reglamento incluía en su disposición relativa al ejercicio de acciones contra un responsable o encargado un último apartado (art. 75.4) según el cual los Estados miembros deberían ejecutar las resoluciones definitivas de los órganos jurisdiccionales en cuestión[87], esa previsión, de compleja coordinación con el sistema del RBIbis, no figura en la versión final del RPD, de modo que éste no incorpora normas de reconocimiento y ejecución que desplacen a las del RBIbis.

51. Ahora bien, la aplicación sin más del régimen de litispendencia previsto en el RBIbis tratándose de acciones en las materias comprendidas en el art. 79 del RPD puede plantear dificultades. En primer lugar, cabe entender que la regla del art. 31.2 RBIbis a favor del tribunal designado en un acuerdo de prórroga de jurisdicción no debe operar en detrimento de la competencia de un tribunal fundada en el art. 79.2 del RPD. Además, cuando un responsable haya ejercitado frente a algún interesado acciones declarativas de no infracción, por ejemplo ante los tribunales del lugar de su propio domicilio como lugar de origen del daño con base en el art. 7.2 RBIbis, la apreciación de litispendencia con base en el art. 29 del RBIbis a favor de los tribunales del domicilio del responsable en perjuicio, por ejemplo, de la eventual competencia de los tribunales del Estado miembro de la residencia habitual del interesado previsto en el art. 79.2 RPD podría menoscabar la protección que el RPD pretende otorgar a los interesados.

4.7. Ley aplicable

52. Han sido ya objeto de análisis aspectos de Derecho aplicable al hilo del art. 3 del RPD, cuyos criterios sobre el ámbito de aplicación territorial tienen carácter imperativo y son también determinantes cuando en un litigio entre particulares, por ejemplo en materia contractual o extracontractual, resulta relevante valorar la eventual ilicitud de ciertas conductas –o cláusulas contractuales- por su falta de conformidad con la legislación de protección de datos, incluso aunque la ley aplicable al contrato o a la responsabilidad civil

[87] COM(2012) 11 final, p. 79.

sea la de un tercer Estado.[88] El carácter internacionalmente imperativo de la legislación sobre protección de datos personales y su sometimiento a una conexión autónoma conforme al art. 3 del RPD son plenamente coherentes con el significado en la UE como derecho fundamental de la protección de datos personales.

La legislación sobre protección de datos incorpora disposiciones cuya observancia es esencial para la salvaguarda de importantes intereses, lo que justifica su carácter internacionalmente imperativo. Así, el hecho de que un contrato internacional pueda estar regido por la ley de un tercer Estado –conforme al Reglamento Roma I- no impedirá que los tribunales de los Estados miembros, incluso en el marco de litigios contractuales deban aplicar imperativamente las normas del RPD, en la medida en que el supuesto esté comprendido dentro de su ámbito territorial. La cuestión relativa a la protección de datos ha de considerarse sometida a conexión autónoma y las disposiciones del RPD pueden ser consideradas normas internacionalmente imperativas del foro en el marco del art. 9.2 del Reglamento Roma I. La mencionada sentencia *Verein für Konsumenteninformation* resulta indicativa de cómo la eventual ilicitud de ciertas cláusulas contractuales por su falta de conformidad con la legislación de protección de datos es objeto de una conexión específica y diferenciada con respecto a la ley del contrato, pues viene determinada por la ley aplicable en materia de protección de datos, ámbito en el que, de cara al futuro, debe estarse al art. 3 del RPD.

53. Si bien las normas del RPD, en tanto que legislación sobre protección de datos, son dentro de su ámbito territorial aplicables en todo caso por los tribunales de los Estados miembros para determinar si los derechos de los interesados con base en el RPD han sido vulnerados por un tratamiento de datos, ello no excluye que sea preciso determinar conforme a las reglas de conflicto correspondientes, por ejemplo, la ley aplicable a los aspectos de la responsabilidad civil derivada de tal infracción no regulados por el RPD.

[88] En el ámbito contractual cuando sea aplicable el art. 6 del Reglamento Roma I, el consumidor podrá beneficiarse de la normativa de protección de los consumidores de su residencia habitual, véase la mencionada sentencia en el asunto C-191/15, *Verein für Konsumenteninformation*.

En concreto, en materia de acciones de indemnización el RPD establece la obligación del responsable o encargado de indemnizar los daños y perjuicios que pueda sufrir una persona como consecuencia de un tratamiento en infracción de sus normas, proporcionando pautas sobre la necesidad de una interpretación amplia del concepto de daños y perjuicios. Además, prevé que el responsable o encargado debe quedar exento «si demuestra que no es en modo alguno responsable de los daños y perjuicios»; así como la eventual responsabilidad solidaria de quienes participan en la misma operación de tratamiento (art. 82 y cdo. 146). Ahora bien, al margen de estas disposiciones y de la unificación de las normas cuya infracción resulta presupuesto del derecho a indemnización, entre las legislaciones nacionales subsisten importantes diferencias en este ámbito. Por lo tanto, en relación con el ejercicio de este tipo de acciones en situaciones transfronterizas pueden plantearse complejas cuestiones de Derecho aplicable, tanto de delimitación –entre cuestiones de protección de datos sometidas a conexión autónoma a partir del art. 3 del RPD y cuestiones regidas por la ley aplicable a las obligaciones extracontractuales- como de determinación de la ley aplicable, para las que lamentablemente el Derecho de la UE no siempre proporciona una respuesta. En concreto, la ley aplicable a las obligaciones extracontractuales derivadas de la infracción de normas sobre protección de datos es una materia en principio excluida del Reglamento (CE) 864/2007 o Reglamento Roma II.

54. Conforme a su art. 1.2.g) el Reglamento Roma II no es aplicable 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», categoría que cabe entender que incluye las acciones extracontractuales relativas a los daños y perjuicios sufridos por un interesado como consecuencia del tratamiento de sus datos personales por un responsable o encargado con infracción de las normas del RPD[89].

[89] Así parece desprenderse del propio Reglamento Roma II, en la medida en que el art. 30.2 sobre su revisión menciona que el estudio relativo a la ley aplicable a las obligaciones extracontractuales derivadas de la violación de la intimidad y de los derechos relacionados con la personalidad, deberá tener en cuenta las «las cuestiones sobre conflicto de ley relacionadas con la Directiva 95/46/CE». Pese a la diferenciación entre ambos derechos en la Carta de Derechos Fundamentales de la UE, es una idea reiterada en la jurisprudencia tanto del TJUE como del TEDH que la tutela de la intimidad constituye una dimensión esencial de la protección de datos personales, véase KOKOTT, J., Y SOBOTTA, C., «The distinction between privacy and data

Dicha exclusión tiene como consecuencia que la ley aplicable en esta materia continúe sometida a las normas de conflicto nacionales a falta de convenios internacionales, en el caso de España, el art. 10.9 Cc. Se trata de un ámbito en el que es de lamentar la falta de avances y en el que se mantienen significativas diferencias entre los Estados miembros.[90] Tanto la interpretación del art. 10.9 Cc en estos supuestos, como las alternativas disponibles para la superación de este vacío en el DIPr de la Unión quedan al margen del objeto de este trabajo. No obstante, cabe apuntar que los intereses presentes en este concreto sector tienden a favorecer la aplicación de la ley del lugar donde sufren el daño o lesión los bienes o derechos del perjudicado, típicamente, en la residencia habitual (o centro de intereses) del interesado[91], lo que se corresponde al menos parcialmente con la evolución que en materia de competencia judicial internacional favorece el art. 79.2 del RPD.

55. Conforme a su art. 2.4, el RPD debe entenderse sin perjuicio de la aplicación de la Directiva 2000/31/CE sobre el comercio electrónico[92], en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios. El «ámbito coordinado» de la Directiva 2000/31/CE, que según su cdo. 14 debe respetar plenamente los principios relativos a la protección de datos personales, incluye aspectos de Derecho privado, lo que plantea la cuestión de en qué medida las diferencias entre las legislaciones de los Estados miembros en materia de responsabilidad civil derivada de la vulneración de las normas sobre datos personales pueden constituir restricciones a los efectos del principio de origen en esa Directiva, cuestión no resuelta por el TJUE en la sentencia *Papasavvas*.[93] De dicho principio resulta la exigencia de que los prestadores de servicios de la sociedad de la información establecidos en un Estado miembro –en los términos de la Directiva 2000/31-

protection in the jurisprudence of the CJEUand the ECtHR», *IDPL*, vol. 3(4), 2013, pp. 222-228, p. 223. Sobre la exclusión del Reglamento Roma II, DICKINSON, A., The Rome II Regulation (The Law Applicable to Non-Contractual Obligations), Oxford, OUP, 2008, p. 240; SANCHO VILLA, D., *op. cit*., nota 26, pp. 94-99; y BRKAN, M., *op. cit*., nota 20, pp. 27-28.

[90] Véase VOGEL, J.B., *Das Medienpersönlichkeitsrecht im Internationalen Privaterecht (Eine Untersuchung zur Harmonisierung in Europa)*, Baden-Baden, Nomos, 2014, pp. 215-256.

[91] SANCHO VILLA, D., *op. cit*., nota 26, pp. 99-107; y DE MIGUEL ASENSIO, P.A., *op. cit*., nota 26, pp. 214-218.

[92] DO L núm. 178, de 17 de julio de 2000, p. 1.

[93] STJUE de 11 de septiembre de 2014, *Papasavvas*, C-291/13, ECLI:EU:C:2014:2209.

no estén sometidos a requisitos más estrictos que los previstos en el Derecho material del Estado miembro de establecimiento.[94]

5. CONCLUSIONES

56. Al regular su ámbito territorial de aplicación el nuevo Reglamento mantiene un planteamiento unilateral y la existencia de un establecimiento en la UE como primer criterio de aplicación, pero introduce importantes avances, en particular al sustituir el criterio relativo al empleo de medios en la UE por otro tendente a asegurar la aplicación de la normativa europea a los tratamientos de datos de personas que se encuentren en la UE cuando se producen en actividades dirigidas a la UE. Frente al modelo anterior, las normas sobre el ámbito territorial no resultan ahora determinantes del reparto de competencias entre las autoridades nacionales de control. En el sistema atenuado de ventanilla única que introduce el Reglamento para facilitar las actividades transfronterizas de los responsables y encargados establecidos en un Estado miembro, adquiere especial relevancia la noción de establecimiento principal y la coordinación entre las autoridades nacionales, que puede plantear especiales dificultades, incluso en relación con la normativa aplicable a aspectos no previstos en el RPD, en situaciones en las que la resolución ha de ser formalmente adoptada por una autoridad distinta de la que lideró su tramitación, como vía introducida en el Reglamento para facilitar la tutela judicial de los interesados contra las decisiones de las autoridades de control.

57. El Reglamento pretende facilitar la tutela civil del derecho a la protección de datos, como alternativa a las reclamaciones ante las autoridades de control, que adquiere singular importancia con respecto al derecho a indemnización. Para ello introduce reglas especiales de competencia judicial internacional en las acciones contra un responsable o encargado, que prevalecen sobre las del Reglamento Bruselas I bis y las de la legislación de fuente interna. Se prevén dos fueros adicionales con carácter alternativo, que permiten a los interesados demandar ante los tribunales de cualquier Estado miembro en el que el responsable o encargado tenga un establecimiento, en el sentido amplio y flexible en el que

[94] Véase en particular la STJUE *eDate Advertising y Martínez*, ya citada, apdo 67.

el término se utiliza por las normas sobre ámbito territorial de aplicación (a diferencia de la noción de establecimiento principal determinante en relación con la competencia de las autoridades de supervisión), o ante los tribunales del Estado de la residencia habitual del interesado. Las normas especiales sobre conexidad entre procedimientos judiciales que introduce el Reglamento parecen presentar un alcance limitado, que se reduce a los casos de ejercicio de acciones contra decisiones de autoridades de control. En relación con la tutela civil del derecho a la protección de datos, si bien el ámbito territorial del RPD resulta determinante de la aplicación de sus normas por los tribunales de los Estados miembros para decidir sobre la vulneración por un tratamiento de datos de los derechos de los interesados con base en el RPD, ello no excluye que sea preciso determinar conforme a las reglas de conflicto correspondientes la ley aplicable, por ejemplo, a aspectos de la responsabilidad civil derivada de tal infracción distintos de los regulados por el RPD u otros aspectos del contrato en el marco del cual se produce el tratamiento.

***

RESUMEN

COMPETENCIA Y DERECHO APLICABLE EN EL REGLAMENTO GENERAL SOBRE PROTECCIÓN DE DATOS DE LA UNIÓN EUROPEA

El nuevo Reglamento general de protección de datos de la UE representa una profunda transformación de la situación previa basada en la mera armonización. En lo relativo a su dimensión internacional, introduce en primer lugar importantes novedades en los criterios que determinan el ámbito territorial de la legislación europea, en particular con el objetivo de asegurar su aplicación a los tratamientos de datos de personas que se encuentren en la Unión relacionados con actividades dirigidas a su territorio. El presente estudio valora el fundamento de los cambios y pretende aportar las claves para su interpretación. Frente al modelo anterior, las normas sobre el ámbito territorial no resultan ahora determinantes del reparto de competencias entre las autoridades nacionales de control de los Estados miembros. El Reglamento incluye disposiciones específicas acerca de la competencia de las autoridades de control de los Estados miembros en las situaciones

transfronterizas, relevantes típicamente para las reclamaciones ante autoridades administrativas y los posteriores recursos judiciales frente a sus resoluciones. Además, incorpora un régimen especial de competencia judicial internacional en relación con el derecho a la tutela de los interesados contra un responsable o encargado del tratamiento, por ejemplo para el ejercicio de acciones de indemnización. La coordinación de esas reglas con otras normas de nuestro sistema, como el Reglamento Bruselas I bis es objeto de análisis en el presente estudio, al igual que el significado de las nuevas normas en materia de conexidad entre procedimientos judiciales, así como las carencias de los instrumentos de la Unión sobre ley aplicable en relación con la tutela civil del derecho a la protección de datos.

Palabras clave: *datos personales, Reglamento UE, autoridades de control, tribunales, competencia, ley aplicable*

ABSTRACT

JURISDICTION AND APPLICABLE LAW IN THE NEW EU GENERAL DATA PROTECTION REGULATION

The new EU General Data Protection Regulation brings about a deep transformation of the previous legal framework based on the mere approximation of laws. As regards the cross-border dimension, it amends the territorial scope of application of EU data protection law to clarify that it covers the processing of data of subjects who are in the Union by a controller or a processor not established in the Union where the processing activities are related to offering goods or services to such data subjects. This article discusses the rationale that supports the new approach and the relevant criteria for its interpretation. Unlike the previous regime, the provisions of the Regulation on its territorial scope do not determine the competent national supervisory authority. The Regulation includes specific provisions on the distribution of competences between the supervisory authorities of the Member States with regard to cross-border situations. Such rules play also an important role concerning the right to a judicial remedy against a supervisory authority. Additionally, new special jurisdiction rules are established concerning private claims by data subjects against a controller or processor as a result of the infringement of the rights granted to them by the Regulation. Such rules are of special significance with respect to the right to compensation where a damage results from an infringement of the Data Protection Regulation. One of the main objectives of this article is to clarify the issues raised by the relationship of the new special rules on jurisdiction and related proceedings with other provisions, such as those of the

Brussels I (Recast) Regulation. The shortcomings of EU conflict rules in the area of private enforcement of data protection law and the interplay between the new Regulation and the general EU framework on conflict of laws are also discussed.

Keywords: *personal data, EU Regulation, supervisory authorities, competence, jurisdiction, applicable law*