

COMPETENCIA JUDICIAL INTERNACIONAL  
Y NECESARIA COHABITACIÓN ENTRE EL REGLAMENTO  
“BRUSELAS I BIS”, EL REGLAMENTO GENERAL  
DE PROTECCIÓN DE DATOS DE LA UE Y EL NUEVO  
REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL  
(ANTE SUPUESTOS DE RESPONSABILIDAD CIVIL  
EXTRA CONTRACTUAL POR UN USO INADECUADO  
DE SISTEMAS DE INTELIGENCIA ARTIFICIAL)

*INTERNATIONAL JUDICIAL COMPETENCE  
AND NECESSARY COHABITATION BETWEEN  
THE “BRUSSELS I BIS” REGULATION, THE EU GENERAL  
DATA PROTECTION REGULATION AND THE NEW  
EUROPEAN ARTIFICIAL INTELLIGENCE REGULATION  
(IN CASES OF NON-CONTRACTUAL CIVIL LIABILITY  
FOR IMPROPER USE OF ARTIFICIAL INTELLIGENCE  
SYSTEMS)*

Alfonso Ortega Giménez\*

**Palabras clave:** Unión Europea, protección de datos, competencia judicial internacional, inteligencia artificial, responsabilidad civil extracontractual.

**Keywords:** European Union, data protection, international jurisdiction, artificial intelligence, non-contractual civil liability.

**SUMARIO:** 1. CONSIDERACIONES PREVIAS. 2. RESOLUCIÓN JUDICIAL INTERNACIONAL DE CONTROVERSIAS, TRATAMIENTO ILÍCITO INTERNACIONAL DE DATOS PERSONALES DERIVADO DE UN USO INADECUADO DE SISTEMAS DE INTELIGENCIA ARTIFICIAL, REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE LA UE Y REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL. 3. RESOLUCIÓN JUDICIAL INTERNACIONAL DE CONTROVERSIAS, TRATAMIENTO ILÍCITO INTERNACIONAL DE DATOS PERSONALES DERIVADO DE UN USO INADECUADO DE SISTEMAS DE INTELIGENCIA ARTIFICIAL Y REGLAMENTO “BRUSELAS I BIS”. 4. REFLEXIONES FINALES.

---

\* Profesor Titular de Derecho internacional privado de la Universidad Miguel Hernández de Elche (UMH) (alfonso.ortega@umh.es – <https://orcid.org/0000-0002-8313-2070>). Este trabajo se enmarca en el Proyecto “La potestad sancionadora de las autoridades de control en materia de protección de datos: delimitación, garantías y efectos” (ref. PID2022-139265OB-I00), investigadores principales: Julián Valero Torrijos y María Magnolia Pardo López.

## 1. CONSIDERACIONES PREVIAS

El flujo internacional de datos personales no sólo constituye una industria auxiliar respecto de empresas, entidades o personas que se dedican a realizar o utilizar las transferencias bancarias, las reservas de pasajes aéreos o el auxilio judicial internacional sino en un sector económico creciente, en sí mismo considerado.

Frente al tratamiento o la obtención ilícita de datos personales, resulta imprescindible garantizar a sus titulares mecanismos de defensa que sean tanto adecuados como efectivos.

La Inteligencia Artificial (en adelante, IA) plantea retos sin precedentes en el ámbito del Derecho internacional privado, dado su impacto en aspectos fundamentales como la jurisdicción, la ley aplicable y la naturaleza de las relaciones contractuales. Una de las áreas más desafiantes es la regulación de los contratos inteligentes basados en *blockchain*. Estos acuerdos automatizados y autoejecutables redefinen las dinámicas tradicionales del derecho contractual al operar sin intervención humana directa, lo que complica su encaje en los marcos normativos vigentes. En este contexto, la IA introduce desafíos complejos en el ámbito del Derecho internacional privado, especialmente en lo referente a la regulación de riesgos y la protección de los derechos fundamentales. Estos sistemas, diseñados para operar con autonomía, procesan grandes volúmenes de datos, lo que plantea preocupaciones significativas sobre la privacidad, la equidad y la seguridad de los derechos fundamentales. La UE, consciente de estas implicaciones, ha implementado normativas como el Reglamento europeo de Inteligencia Artificial, (en adelante, el Reglamento europeo de IA)<sup>1</sup>, que clasifica los sistemas según su nivel de riesgo. Esta clasificación permite identificar aplicaciones de alto riesgo que requieren controles estrictos, como auditorías, supervisión continua y evaluaciones de impacto ético y técnico antes de su implementación.

El Reglamento europeo de IA no solo busca mitigar los riesgos inherentes a la tecnología, sino también establecer un marco normativo que fomente la confianza de los usuarios y garantice que los sistemas de IA respeten valores fundamentales, como la transparencia y la explicabilidad. Esto es esencial para proteger derechos como la privacidad y la no discriminación, asegurando que las decisiones automatizadas sean comprensibles y justificadas.

Por su parte, el Derecho internacional privado desempeña un papel crucial al proporcionar directrices sobre competencia judicial internacional y ley

---

<sup>1</sup> Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). *DOUE-L-2024/1689* de 12 de julio de 2024.

aplicable en situaciones transfronterizas relacionadas con la IA. Esto incluye la resolución de disputas contractuales y extracontractuales, así como la atribución de responsabilidades en caso de daños causados por sistemas de IA. La interacción entre las normativas europeas de IA y Derecho internacional privado destaca la necesidad de armonización legal para evitar inconsistencias y garantizar una protección adecuada en todos los Estados miembros. Dichos mecanismos se articulan a través de un equilibrio entre la atribución de derechos a los titulares de los datos y la imposición de obligaciones a quienes los recaban, procesan o controlan su tratamiento. La búsqueda de soluciones equitativas que atiendan a los intereses legítimos involucrados en las transferencias internacionales de datos plantea desafíos significativos, especialmente debido a las marcadas disparidades existentes entre los niveles de protección de los derechos y libertades individuales en el contexto internacional. Ante esta realidad, los sistemas nacionales de Derecho internacional privado han emergido como el último recurso de los titulares de datos personales cuyos derechos han sido vulnerados.

Ahora bien, la intervención del Derecho internacional privado no debe ser una intervención cualquiera sino que debe buscar la tutela adecuada, equilibrada y eficaz del perjudicado por un tratamiento ilícito de sus datos de carácter personal derivado de un uso inadecuado de sistemas de IA, sobre todo en un contexto en el que las empresas dedicadas al tratamiento de datos personales pueden deslocalizar interesadamente (*fórum shopping*) su establecimiento principal en los Estados miembros que apliquen la normativa vigente en materia de protección de datos de una forma permisiva, o cuyas autoridades de control, por sus competencias, estructura y recursos, estén en peores condiciones para garantizar eficazmente el cumplimiento de la normativa (el Reglamento General de Protección de Datos de la UE — en lo sucesivo, RGPD—<sup>2</sup>).<sup>3</sup>

La IA representa un avance tecnológico que desafía las bases tradicionales del Derecho, especialmente en lo relacionado con la responsabilidad civil extracontractual. Su autonomía y capacidad de aprendizaje la convierten en una tecnología disruptiva, capaz de tomar decisiones independientes basadas en análisis complejos de grandes volúmenes de datos. Sin embargo, estas características generan incertidumbres legales significativas, particularmente en el Derecho de daños.

---

<sup>2</sup> Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. *DOUE* L 119/1, de 4 de mayo de 2016.

<sup>3</sup> *Vid.*, en sentido amplio, Carrascosa González, Javier, “Protección de la intimidad y tratamiento automatizado de datos de carácter personal en Derecho Internacional Privado”, en *Revista Española de Derecho Internacional*, vol. XLIV, núm. 2, 1992, pp. 417-418; y LÓPEZ CALVO, José, *Comentarios al Reglamento Europeo de Protección de Datos*, Sepin, Madrid, 2017.

## 2. RESOLUCIÓN JUDICIAL INTERNACIONAL DE CONTROVERSIAS, TRATAMIENTO ILÍCITO DE DATOS PERSONALES DERIVADO DE UN USO INADECUADO DE SISTEMAS DE INTELIGENCIA ARTIFICIAL, REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE LA UE Y REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL

Ante un uso inadecuado de un sistema de IA que implique un tratamiento ilícito de datos personales de una persona física que suponga un daño o un perjuicio debemos acudir al RGPD. El artículo 82 del RGPD (*ex artículo 23 de la Directiva 95/46/CE*)<sup>4</sup> regula el derecho a indemnización de las personas físicas por los daños producidos por un tratamiento ilícito de sus datos personales<sup>5</sup>. El RGPD refuerza el artículo 82 con el artículo 83 relativo a las condiciones generales para la imposición de multas y con el artículo 84 de las sanciones, que se pueden imponer al encargado del tratamiento de datos que infrinja lo dispuesto en el RGPD y demás posibles responsables.

Como podemos observar, el artículo 82, en su apartado primero, es muy claro al establecer que la indemnización comprende los “daños y perjuicios materiales o inmateriales” de la persona afectada, por lo tanto, cuando el precepto dice “daños y perjuicios”, no debemos hacer una interpretación restrictiva del mismo.

Además, para que se produzca la indemnización, uno de los elementos importantes es que el daño producido sea real y efectivo, que sea evaluable económicamente e individualizable, con relación a una persona o grupo de personal, al igual que sucede en el derecho interno (artículo 32 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público<sup>6</sup>). Por tanto, el RGPD establece una reparación integral de la persona perjudicada que cubra no sólo los daños físicos y patrimoniales, sino también los daños morales<sup>7</sup>.

El RGPD establece una base sólida para garantizar la reparación integral de los daños causados por un tratamiento ilícito de datos personales. Este

---

<sup>4</sup> A diferencia del artículo 23 de la Directiva 95/46/CE que contenía un mandato a los legisladores nacionales para que regulasen el derecho a una indemnización de aquellos perjudicados con un tratamiento ilícito de sus datos personales, el artículo 82 del RGPD, que introduce el citado derecho de las personas físicas, es de carácter uniforme y de obligatorio cumplimiento por los Estados miembros, con las necesarias adaptaciones a los sistemas de responsabilidad civil o patrimonial de cada uno de ellos. *Vid.* NIETO GARRIDO, Eva, “XX. Derecho a indemnización y responsabilidad”, en PIÑAR MATAS, José Luis, *Reglamento general de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, editorial Reus, Madrid, 2016, pp. 555-570; y BRITO IZQUIERDO, Noemí, “Recursos, responsabilidad y sanciones (arts. 77-84)”, en LÓPEZ CALVO, José (Coord.), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*, Bosch, Madrid, 2018, pp. 633-670.

<sup>5</sup> *Vid.*, en particular, GONZALO DOMÉNECH, Juan José, “Algunas cuestiones relevantes de Derecho internacional privado del Reglamento General de Protección de Datos”, en *Rev. Boliv. De Derecho*, N° 26, julio 2018, pp. 414-417.

<sup>6</sup> BOE núm. 236, de 2 de octubre de 2015.

<sup>7</sup> El concepto de “daños y perjuicios” debe interpretarse en un sentido amplio, a la luz de la jurisprudencia del TJUE, de tal modo que se respeten plenamente los objetivos del RGPD (Considerando 146 el RGPD).

marco normativo se complementa con el Reglamento europeo de IA, que refuerza las obligaciones de los responsables y encargados en el ámbito de los sistemas de inteligencia artificial, especialmente aquellos clasificados como de alto riesgo.

El Reglamento europeo de IA introduce medidas preventivas destinadas a minimizar el impacto de los daños antes de que ocurran, como auditorías técnicas, evaluaciones de impacto ético y la implementación de sistemas de supervisión continua. Estas herramientas permiten detectar y mitigar los riesgos asociados al uso de sistemas de IA en etapas tempranas, asegurando un nivel más alto de protección para los individuos afectados. Además, el Reglamento europeo de IA especifica que los desarrolladores y operadores de sistemas de IA deben garantizar la trazabilidad y la explicabilidad de sus decisiones, facilitando la identificación de la causa de posibles daños y, en consecuencia, la atribución de responsabilidades.

En cuanto a la indemnización, el Reglamento europeo de IA trabaja en conjunto, “en equipo”, con el RGPD para fortalecer el principio de responsabilidad solidaria. Esto implica que cualquier responsable o encargado puede ser considerado plenamente responsable de los daños, incluso en casos donde haya múltiples actores involucrados. Este enfoque garantiza que las víctimas tengan acceso efectivo a la reparación y evita vacíos legales que podrían dificultar la reclamación. Dicha indemnización puede derivar tanto de una responsabilidad contractual como extracontractual. Aunque el artículo no hace una referencia específica a los actos del responsable del tratamiento de datos, su apartado segundo establece que la responsabilidad puede originarse tanto por una acción como por una omisión. Esto implica que, si el responsable del tratamiento incumple una obligación mediante una inacción, dicha omisión constituye un acto generador de responsabilidad.

Al adoptar un enfoque centrado en los derechos fundamentales y la prevención de daños, el Reglamento europeo de IA no solo refuerza las disposiciones del RGPD, sino que también promueve la creación de un entorno tecnológico seguro y confiable que respete los principios éticos y legales de la UE.

Se configura como una responsabilidad por daños, de naturaleza resarcitoria, que no tiene su origen en un incumplimiento contractual, sino en la vulneración de un derecho fundamental. Su finalidad no es reparar un incumplimiento de obligaciones contractuales, sino subsanar el perjuicio ocasionado por dicha lesión.

Otro dato que denota la amplia protección del RGPD es la responsabilidad solidaria que establece el apartado cuarto señala que “cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado”. Apuntar que la responsabilidad solidaria no es absoluta, sino que, si se demuestra que algu-

no de los encargados del tratamiento de los datos, no ha sido responsable del daño producido podrá repetir la cantidad a la que hizo frente en concepto de indemnización a los responsables, e incluso si, aun teniendo responsabilidad satisface la indemnización completa, también podrá exigir el abono de la parte que correspondería a cada uno de los responsables (apartado quinto del artículo 82 del RGPD).

Finalmente, el apartado 6 del artículo 82 del RGPD establece el foro competente para que el perjudicado presente su reclamación de responsabilidad patrimonial, remitiéndose a lo dispuesto en el artículo 79.2 del RGPD. Este precepto permite al afectado interponer su reclamación no solo ante los tribunales del Estado miembro donde el responsable o encargado tenga su establecimiento, sino también ante los tribunales competentes del Estado miembro donde el perjudicado tenga su domicilio. Esta disposición representa un avance significativo en la protección del derecho fundamental a la tutela efectiva en materia de protección de datos personales, al eliminar las barreras que anteriormente dificultaban el ejercicio del derecho a una indemnización, como la necesidad de litigar en un Estado miembro distinto del domicilio del afectado debido a la localización del establecimiento del responsable o encargado.

El artículo 82 del RGPD (que nos remite al artículo 79.2 del RGPD) nos indica que las acciones dirigidas contra encargados o responsables deberán dirigirse ante los tribunales competentes del Estado miembro donde estos tengan un establecimiento (en concordancia con el Considerando 22 del RGPD, el establecimiento implicará el ejercicio de manera efectiva y real de una actividad a través de modalidades estables, con independencia de la forma jurídica que revistan las mismas, pudiendo tratarse de una sucursal sin personalidad jurídica, o de una filial con personalidad jurídica). Alternativamente, podrán ejercitarse tales acciones ante los tribunales competentes del Estado miembro donde el reclamante tenga su domicilio, en concordancia con lo estipulado en el Considerando 145<sup>8</sup>. A menos que el responsable o el encargado sea una autoridad pública de un estado miembro, que actúe en ejercicio de sus poderes públicos; en cuyo caso, sólo podrá ejercitarse ante los tribunales donde esté establecida la autoridad pública correspondiente.

Aunque se dé por hecha la adecuación de esta acción a los supuestos de responsabilidad extracontractual cuando exista un perjuicio relacionado con un tratamiento de datos ilícito (según el artículo 82.6 del RGPD) es posible que ese tratamiento de datos se produzca en el contexto de un contrato, y según la jurisprudencia del TJUE, una acción de responsabilidad civil de natu-

---

<sup>8</sup> Por lo que respecta a las acciones contra los responsables o encargados del tratamiento, el reclamante debe tener la opción de ejercitarlas ante los tribunales de los Estados miembros en los que el responsable o el encargado tenga un establecimiento o resida el afectado, a menos que el responsable sea una autoridad pública de un Estado miembro que actúe en el ejercicio de poderes públicos.

raleza contractual deberá entenderse incluida en la materia contractual a los efectos del artículo 7 del Reglamento “Bruselas I Bis” si el comportamiento recriminado comporta un incumplimiento de las obligaciones contractuales cuando se estudie caso por caso el objeto del contrato<sup>9</sup>. Puesto que en un contrato se puede pactar el compromiso del cuidado de los datos personales en virtud de la legislación vigente (aunque, eso sí, la mayoría de los supuestos que nos encontraremos en la práctica serán de naturaleza extracontractual).

El Reglamento europeo de IA complementa al RGPD al incorporar disposiciones que fortalecen la protección de los derechos de las personas afectadas por el uso inadecuado de sistemas de IA. Una de las medidas clave es el derecho a recibir explicaciones claras y comprensibles sobre las decisiones automatizadas que les afectan, reforzando así el principio de transparencia y explicabilidad. Este derecho no solo facilita la comprensión por parte del afectado, sino que también permite una mayor supervisión y rendición de cuentas de los responsables del tratamiento.

Además, el Reglamento europeo de IA introduce medidas que amplían el alcance de la responsabilidad y las garantías para las víctimas en casos transfronterizos. Estas incluyen la posibilidad de ejercer acciones legales no solo en el Estado miembro donde el responsable o encargado tiene un establecimiento, sino también en el Estado miembro donde reside la persona afectada. Este enfoque, inspirado en las disposiciones del artículo 79.2 del RGPD, elimina barreras jurisdiccionales y asegura que las víctimas tengan acceso efectivo a los mecanismos de reparación en su lugar de residencia habitual.

El Reglamento europeo de IA también aborda desafíos relacionados con la jurisdicción en casos donde el impacto de los sistemas de IA se extiende más allá de las fronteras de la Unión Europea. Las disposiciones extraterritoriales del Reglamento europeo de IA garantizan que los proveedores y usuarios de sistemas de IA ubicados fuera de la UE estén sujetos a las normativas europeas si sus actividades tienen consecuencias dentro de la Unión. Esto refuerza la capacidad de las víctimas para litigar contra entidades extranjeras que utilizan IA en detrimento de los derechos fundamentales.

El artículo 79.2 permite demandar en el Estado miembro en el que el responsable o el encargado tengan un establecimiento. Debemos abogar por un concepto flexible de “establecimiento”, tal y como se indica en la STJUE *Weltimmo*; de forma que “establecimiento” debe extenderse a “cualquier actividad real y efectiva, ejercida mediante una instalación estable”<sup>10</sup>. Para ello debe valorarse tanto el “grado de estabilidad de la instalación como la efectividad del desarrollo de las actividades la naturaleza específica de las actividades económicas y de las prestaciones de servicios en cuestión”.

<sup>9</sup> Vid. SSTJUE de 13 de marzo de 2014, *Brogstetter*, C-548/12; 14 de julio de 2016, *Granarolo*, C-196/15.

<sup>10</sup> Vid. Apartados 31 de la STJUE *Weltimmo* y 75 de la STJUE *Amazon EU Sàrl*.



En la STJUE *Amazon EU Sàrl* se entiende posible considerar la existencia de un establecimiento en un Estado miembro cuando no exista ni una filial o sucursal, siendo necesario valorar el grado de estabilidad de la instalación y la efectividad del desarrollo de las actividades en ese Estado<sup>11</sup>, siendo posible considerar como “establecimiento” a un representante de la sociedad si actúa con un grado de estabilidad suficiente<sup>12</sup>. De esta consideración se desprende que cualquier establecimiento del encargado o del responsable permite atribuir la competencia a los tribunales del Estado miembro en el que esté sito. Tampoco será necesario que la acción esté dirigida a las actividades de ese concreto establecimiento, sino que la existencia de cualquier establecimiento extienda el daño causado.

El foro alternativo que prevé el RGPD permite a los afectados demandar ante los tribunales del Estado donde tengan su residencia habitual. Para su consideración, será necesario que el afectado tenga un grado de permanencia que revele una situación de estabilidad<sup>13</sup>.

La residencia habitual no es un concepto sinónimo al de “centro de intereses de la víctima” que promulga la STJUE *eDate Advertising*<sup>14</sup>, que aunque en principio suele coincidir con la “residencia habitual”, podemos encontrarlo en otro Estado cuando exista un vínculo particularmente estrecho con ese otro Estado que resulte de otros indicios, como el ejercicio de una actividad profesional. La consideración de este foro de competencia no parece ser la más adecuada para determinar el tribunal que debe conocer de la pretensión, puesto que no exige que exista una vinculación entre el centro de intereses y el lugar donde efectivamente se produce el daño.

Por su parte, el Título I del Reglamento europeo de IA delimita el ámbito de aplicación de las nuevas normas, abarcando aspectos como la introducción en el mercado, la comercialización, la puesta en servicio y la utilización de sistemas de inteligencia artificial. Este marco normativo se caracteriza por su alcance extraterritorial, lo que implica que: “las organizaciones de fuera de la UE tendrán que cumplir la ley en determinadas circunstancias específicas al igual que las de dentro de la UE. Más concretamente, el Reglamento europeo de IA establece disposiciones para frenar esta tendencia al determinar que las normas de la UE pueden aplicarse “automáticamente” con un efecto extraterritorial limitado al aplicarse también a los proveedores de terceros países que comercializan sistemas de IA en la UE y, lo que es aún más importante, a los proveedores y usuarios de sistemas de IA ubicados en un tercer país cuando el resultado del sistema de IA se utiliza en la UE. Sin embargo,

---

<sup>11</sup> Vid. Apartados 76 y 77.

<sup>12</sup> Vid. Apartado 30 de la STJUE *Weltimmo*.

<sup>13</sup> Vid. STJUE 22 de diciembre de 2010, C-497/10, Mercredi ECLI:EU:C:2010:829.

<sup>14</sup> Vid. STJUE C-509/09 y C-161/10 *eDate Advertising* ECLI:EU:C: 2011:685.



en ciertos casos, las autoridades públicas de los países asociados pueden quedar exentas de estas responsabilidades”<sup>15</sup>.

El artículo 2.1 del Reglamento europeo de IA puede ser considerada, desde el punto de vista del Derecho internacional privado, como una norma de derecho aplicable<sup>16</sup> y, concretamente, como una norma de conflicto unilateral cuyo objetivo es determinar a qué situaciones de la UE es aplicable el Reglamento europeo de IA.

El Reglamento europeo de IA también aborda desafíos relacionados con la jurisdicción y su aplicación extraterritorial. En este sentido, la UE enfrenta el reto de garantizar que sus disposiciones sean respetadas más allá de sus fronteras, especialmente en un entorno digital altamente globalizado. Para ello, será necesario promover acuerdos bilaterales y multilaterales, así como mantener un diálogo continuo con otras jurisdicciones. Este enfoque busca asegurar una cooperación efectiva en la supervisión y el cumplimiento de las normativas, consolidando la gobernanza internacional en materia de inteligencia artificial.

---

<sup>15</sup> Vid. en sentido amplio, SCOTT, J., “Extraterritoriality and territorial extension in EU law”, *Am. J. Comp. L.*, vol. 62, n° 1, 2024, pp. 87–126; y, en particular, FERNÁNDEZ ROZAS, José Carlos, “La Ley de Inteligencia Artificial de la Unión Europea: un modelo para innovaciones radicales, responsables y transparentes basadas en el riesgo”, en Revista *LA LEY Unión Europea*, año XI, Número 124, abril de 2024, p. 20.

<sup>16</sup> Sin embargo, aunque sí lo hace la UE en relación con la protección de datos de carácter personal (Vid., en particular, ORTEGA GIMÉNEZ, Alfonso, *El intercambio de datos de carácter personal como paradigma de desarrollo de una economía global. Desde la óptica del Derecho internacional privado*, Editorial Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2022, pp. 165-224), el Reglamento europeo de IA presta escasa atención a los posibles problemas que podrían surgir en el ámbito del Derecho internacional privado, “aunque esta carencia no afecta por igual a todos los sectores regulados por este ordenamiento, ya que el Reglamento “Roma II” puede aplicarse eficazmente en relación con los sistemas de IA, especialmente en casos de daños causados por ellos. Esto se debe en gran medida a que este instrumento se basa en factores de conexión que no dependen únicamente de la ubicación de la víctima, sino también de la localización de la propia IA. Sin embargo, las características particulares de la IA, como su complejidad, opacidad y comportamiento semiautónomo, plantean desafíos en cuanto a la determinación del Derecho aplicable. La naturaleza virtual de la IA y los daños que puede causar pueden generar problemas de localización, estos no son exclusivos de la IA y pueden resolverse mediante la creación de ficciones jurídicas y la búsqueda de conexiones con elementos del mundo real”. No obstante, la situación es distinta en lo que respecta a las cuestiones de competencia judicial internacional, ya que el Reglamento europeo de IA no recoge criterio alguno de determinación de la competencia judicial internacional, “lo que significa que no garantizan una adecuada aplicación en casos contra proveedores, operadores y usuarios de sistemas de IA de terceros Estados. Dado que las acciones contra demandados de terceros Estados no están cubiertas por el ámbito de aplicación del Reglamento “Bruselas Ibis”, esto podría dejar a los demandantes sin recurso ante un tribunal de un Estado miembro”; Vid., en general, CAPIELLO, Benedetta, *AI-systems and non-contractual liability: a European private international law analysis*, Turín, Giappichelli, 2022; y HENCKEL, Kristen, “Issues of conflicting laws – a closer look at the EU’s approach to artificial intelligence”, en *Nederlands internationaal privaatrecht*, vol. 41, no 2, 2023, pp. 199-226; y, en particular, FERNÁNDEZ ROZAS, José Carlos, “La Ley de Inteligencia Artificial de la Unión Europea: un modelo para innovaciones radicales, responsables y transparentes basadas en el riesgo”, Revista *LA LEY Unión Europea*, año XI, Número 124, abril de 2024, p. 21.

Es crucial que las regulaciones de la UE tengan en cuenta el impacto en los países en desarrollo, que con frecuencia carecen de la infraestructura necesaria para cumplir con estándares estrictos. En este contexto, la cooperación internacional y la asistencia técnica se convierten en elementos esenciales para garantizar que la IA sea una herramienta de progreso y no un factor de desigualdad o exclusión.

El Reglamento europeo de IA tiene el potencial no solo de transformar el panorama regulatorio europeo, sino también de influir significativamente en la gobernanza global de la IA. No obstante, para que su implementación sea efectiva y equitativa, es necesario integrarlo dentro del marco del Derecho internacional, respetando los tratados vigentes y fomentando el desarrollo de nuevos estándares y principios. Esto exige un esfuerzo coordinado que combine cooperación internacional, diplomacia tecnológica y un enfoque inclusivo y holístico, capaz de abarcar todas las regiones y sectores de la sociedad.

Además, el Reglamento europeo de IA plantea importantes desafíos en términos de competencia judicial internacional y de determinación de la ley aplicable. La naturaleza intrínsecamente global de la IA y de su industria asociada requiere un análisis detallado sobre cómo las normativas europeas pueden influir —o ser implementadas— por entidades que operan a nivel internacional. En este sentido, la aplicación del artículo 2.1 del Reglamento europeo de IA subraya la necesidad de adoptar un enfoque regulatorio global y armonizado, que priorice la cooperación internacional y garantice una regulación coherente y efectiva.

La preocupación primordial en cuanto a la jurisdicción es el alcance extra-territorial del Reglamento europeo de IA. Es decir, la UE debe definir cómo sus normas afectarán a las empresas y entidades fuera de su territorio que producen o proveen sistemas de IA utilizados dentro de la UE.

La aplicación del artículo 2.1 del Reglamento europeo de IA por las autoridades nacionales competentes enfatiza la necesidad de un diálogo global y la colaboración para desarrollar un enfoque armonizado y equitativo hacia la regulación de la IA. En última instancia, el éxito de la UE en la regulación de la IA no se medirá sólo por la eficacia de su legislación interna, sino también por su capacidad para influir y formar parte de un marco normativo global cohesivo.

Las autoridades nacionales competentes no se limitan a ser simples ejecutoras de la legislación de la UE en materia de IA, sino que desempeñan un rol activo en el ámbito regulatorio global. A través de la aplicación del artículo 2.1 del Reglamento europeo de IA, estas entidades contribuyen a configurar un marco internacional más cohesivo, justo y equilibrado. Su función trasciende la mera implementación de políticas, al influir directamente en la gobernanza global de la IA, aspecto crucial para afrontar los desafíos que esta tecnología plantea en una sociedad cada vez más interconectada.

El artículo 2.1 del Reglamento europeo de IA también establece que su aplicación puede surgir en el contexto de acciones civiles presentadas ante órganos judiciales. Esto incluye, por ejemplo, casos de responsabilidad civil extracontractual derivados del funcionamiento defectuoso de un sistema de IA, el incumplimiento de un contrato entre un proveedor y un usuario de estos sistemas, o disputas contractuales entre cualquiera de las partes involucradas y un particular que forma parte de un contrato de prestación de servicios donde se utilicen sistemas de IA. En este tipo de litigios, el incumplimiento de los requisitos u obligaciones establecidas por el Reglamento, en función de la categoría del sistema de IA implicado, puede ser invocado como base para sustentar la demanda.

En la Sección 4 (“Vías de recurso”) del Capítulo IX (“Vigilancia poscomercialización, intercambio de información, vigilancia del mercado”) del Reglamento europeo de IA, que abarca los artículos 85 a 87 se recogen las vías de recurso con las que cuentan los particulares contra el incumplimiento del Reglamento por parte de proveedores, responsables del despliegue o cualquier otro operador involucrado en la cadena de valor de la IA<sup>17</sup>. En el artículo 85 del Reglamento europeo de IA se regula el derecho a presentar una reclamación ante una autoridad de vigilancia del mercado; y al artículo 86, relativo al derecho a explicación de decisiones tomadas individualmente (de forma que se refuerza la exigencia de explicabilidad que deben tener todos los sistemas de IA desarrollados y comercializados en la UE). Por su parte, el artículo 87 contiene una remisión a la Directiva 2019/1937 sobre la protección de los denunciantes (Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión).

La reclamación presentada con base en el artículo 85 del Reglamento europeo de IA no será por una infracción del RGPD, de forma que no conocerán las autoridades nacionales europeas en materia de protección de datos de carácter personal, sino las autoridades de vigilancia del mercado (que tienen jurisdicción para conocer de las reclamaciones relativas a infracciones ocurridas en el territorio de su Estado miembro).

Es más, en la medida en que el artículo 85.1 del Reglamento europeo de IA no ofrece un mecanismo efectivo para que los particulares puedan reclamar un incumplimiento del propio Reglamento, las opciones pasarán por: a) la presentación de una demanda ante tribunales civiles frente al operador de sistemas de IA presuntamente incumplidor en la que se solicite el cese de una actividad que no es conforme con el Reglamento europeo de IA y una

---

<sup>17</sup> Vid. en sentido amplio, el análisis exhaustivo de LÓPEZ-TARRUELLA MARTÍNEZ, Aurelio, sobre las vías de recurso para los particulares en el Reglamento europeo de IA (“derecho a presentar una reclamación” y “derecho a una explicación”) en COTINO HUESO, Lorenzo y SIMÓ CASTELLANOS, Pere (Coords.), *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, Aranzadi La Ley, Cizur Menor, 2024.

indemnización por los perjuicios que esa actividad haya podido ocasionar. El derecho a una explicación, previsto en el artículo 86 del Reglamento europeo de IA, se trata de un derecho inspirado en el artículo 22 del RGPD en relación con las decisiones automatizadas, de utilidad práctica limitada, por cuanto sólo podrían ser beneficiarias las personas jurídicas. Y, como ya se ha señalado, el artículo 87 del Reglamento europeo de IA contiene una remisión a la Directiva 2019/1937 sobre la protección de los denunciantes, que otorga una protección a las personas que denuncien infracciones de la normativa europea. Estas denuncias permiten detectar, investigar y enjuiciar de manera efectiva esas infracciones, mejorando así la transparencia y la rendición de cuentas. En particular, la Directiva obliga a los Estados miembros a adoptar las medidas necesarias para garantizar que no se desvele la identidad del denunciante sin su consentimiento expreso (artículo 16), y para prohibir todas las formas de represalias contra estas personas (artículos 19 y 21). Asimismo, se deben habilitar medidas de apoyo para el denunciante, como ofrecimiento de información y asesoramiento completo e independiente, asistencia efectiva de las autoridades frente a represalias y asistencia jurídica (artículo 20). También se deben establecer medidas de apoyo para otras personas afectadas por su relación con el denunciante (artículo 22).

Así las cosas, al margen del derecho a presentar una reclamación ante una autoridad de vigilancia del mercado, previsto en el artículo 85 del RIA (“Sin perjuicio de otras vías administrativas o judiciales de recurso, toda persona física o jurídica que tenga motivos para considerar que se ha infringido lo dispuesto en el presente Reglamento podrá presentar reclamaciones ante la autoridad de vigilancia del mercado pertinente”), tratándose de litigios en materia civil o mercantil, la competencia judicial internacional del tribunal del Estado miembro ante el que se presente la demanda vendrá determinada por el Reglamento “Bruselas I bis” —siendo competentes los Tribunales del estado donde el presunto perjudicado tenga su residencia habitual, los del lugar de trabajo o donde se produjo la infracción del Reglamento europeo de IA—; y la ley aplicable por el Reglamento “Roma II” —si se trata de un litigio por responsabilidad civil extracontractual— o el Reglamento “Roma I” —si el litigio es sobre el incumplimiento de un contrato internacional—. Eso sí, el derecho sustantivo aplicable (la *lex causae*) será el propio Reglamento europeo de IA, y no podrán aplicar derecho extranjero de un tercer Estado.

### **3. RESOLUCIÓN JUDICIAL INTERNACIONAL DE CONTROVERSIAS, TRATAMIENTO ILÍCITO DE DATOS PERSONALES DERIVADO DE UN USO INADECUADO DE SISTEMAS DE INTELIGENCIA ARTIFICIAL Y REGLAMENTO “BRUSELAS I BIS”**

La compatibilidad entre los foros de competencia judicial internacional del artículo 79.2 y los del Reglamento “Bruselas I Bis” deriva del artículo 67

de este último Reglamento al estipular que no prejuzgará la aplicación de las disposiciones contenidas en instrumentos particulares. Por su parte, el Considerando 147 del RGPD afirma que las normas generales de competencia judicial del Reglamento “Bruselas I Bis” “deben entenderse sin perjuicio de la aplicación de las normas específicas del RGPD”. El Considerando 145 estipula que el demandante “deberá tener la opción” de ejercitar las acciones en los tribunales de los Estados miembros.

El RGPD pone a disposición de los afectados la posibilidad de que puedan utilizar los foros de competencia del artículo 79.2 en contra del inciso imperativo que recoge ese mismo párrafo. Por tanto, cabe afirmar que los foros recogidos en el RGPD son complementarios a los recogidos por el Reglamento “Bruselas I Bis”<sup>18</sup>. Estos foros de competencia judicial internacional serían<sup>19</sup>: a) el Principio de autonomía de la voluntad; y, b) los foros concurrentes.

El artículo 82 del RGPD remite al artículo 79.2, en el que nos indica el lugar donde debe dirigirse el afectado derivado de un supuesto de responsabilidad, el cual dispone que las acciones dirigidas contra encargados o responsables deberán dirigirse ante los tribunales competentes del Estado miembro donde estos tengan un establecimiento.

Alternativamente, podrán ejercitarse tales acciones en los tribunales competentes del Estado miembro donde el reclamante tenga su domicilio, en concordancia con lo estipulado en el Considerando 145<sup>20</sup>.

Como hemos visto, las acciones objeto del artículo 82 tienen un carácter “civil-mercantil”, que, a su vez, se encuadran dentro del ámbito de aplicación del artículo 1.1 del Reglamento “Bruselas I Bis”, y cuya materia no está en los supuestos de exclusión del artículo 1.2.

Aunque se dé por hecha la adecuación de esta acción a los supuestos de responsabilidad extracontractual cuando exista un perjuicio relacionado con

---

<sup>18</sup> Vid. ALBRECHT, Jan Phillipp y JOTZO, Florian, *op. cit.*, pp. 127-128. Aunque se ha entendido que los fueros del RGPD plantean conflictos con las competencias exclusivas del Reglamento Bruselas I bis. Cfr. BRKAN, Maja, “Data Protection and European Private International Law”, Julio 2015, *Robert Schuman Centre for Advanced Studies*, Research Paper No. RSCAS 2015/40, p. 23.

<sup>19</sup> Vid., en sentido amplio, DE MIGUEL ASENSIO, Pedro Alberto, “Competencia y Derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea”, en *Revista Española de Derecho Internacional*, vol. 69/1, enero-junio 2017, Madrid; GARCÍA ROMERO, Susana, “Nuevo marco jurídico europeo en protección de datos: novedades conocidas y otras no tan conocidas”, en *Diario La Ley*, N° 8691, Wolters Kluwer, Madrid, 2016; OREJUDO PRIETO DE LOS MOZOS, Patricia, “La vulneración de los derechos de la personalidad en la jurisprudencia del tribunal de justicia”, en *La Ley Unión Europea*, N° 4, 2013. y SANCHO VILLA, Diana, *Negocios internacionales de tratamiento de datos personales*, Navarra, Civitas, 2010; y, en particular, GONZALO DOMÉNECH, Juan José, “Algunas cuestiones relevantes de Derecho internacional privado del Reglamento General de Protección de Datos”, *op. cit.*, pp. 417-426.

<sup>20</sup> Por lo que respecta a las acciones contra los responsables o encargados del tratamiento, el reclamante debe tener la opción de ejercitarlas ante los tribunales de los Estados miembros en los que el responsable o el encargado tenga un establecimiento o resida el afectado, a menos que el responsable sea una autoridad pública de un Estado miembro que actúe en el ejercicio de poderes públicos.

un tratamiento de datos ilícito según el artículo 82.6 del RGPD; pero es posible que ese tratamiento de datos se produzca en el contexto de un contrato, y según la jurisprudencia del TJUE, una acción de responsabilidad civil de naturaleza extracontractual deberá entenderse incluida en la materia contractual a los efectos del artículo 7 del Reglamento “Bruselas I Bis” si el comportamiento recriminado comporta un incumplimiento de las obligaciones contractuales cuando se estudie caso por caso el objeto del contrato<sup>21</sup>. Puesto que en un contrato se puede pactar el compromiso del cuidado de los datos personales en virtud de la legislación vigente; aunque la mayoría de los supuestos que nos encontraremos en la práctica serán de naturaleza extracontractual.

Concretando más en el fuero del establecimiento del responsable, el artículo 79.2 permite demandar en el Estado miembro en el que el responsable o el encargado tengan un establecimiento. Debe tenerse un concepto flexible de “establecimiento”, tal y como se indica en la STJUE *Weltimmo* debe extenderse “a cualquier actividad real y efectiva, ejercida mediante una instalación estable”<sup>22</sup>. Para ello, debe valorarse también el “grado de estabilidad de la instalación como la efectividad del desarrollo de las actividades la naturaleza específica de las actividades económicas y de las prestaciones de servicios en cuestión”.

En la STJUE *Amazon EU Sari*, considera posible considerar la existencia de un establecimiento en un Estado miembro cuando no exista ni una filial o sucursal, siendo necesario valorar el grado de estabilidad de la instalación y la efectividad del desarrollo de las actividades en ese Estado<sup>23</sup>, siendo posible considerar como “establecimiento” un representante de la sociedad si actúa con un grado de estabilidad suficiente<sup>24</sup>.

De esta consideración se desprende que cualquier establecimiento del encargado o del responsable permite atribuir la competencia a los tribunales del Estado miembro en el que esté sito. Tampoco será necesario que la acción esté dirigida a las actividades de ese concreto establecimiento, sino que la existencia de cualquier establecimiento extiende el daño causado.

El foro alternativo que prevé el RGPD permite a los afectados demandar en los tribunales del Estado donde tengan su residencia habitual. Para su consideración, será necesario que el afectado tenga un grado de permanencia que revele una situación de estabilidad<sup>25</sup>.

La residencia habitual no es un concepto sinónimo al de “centro de intereses de la víctima” que promulga la STJUE *eDate Advertising*<sup>26</sup>, que aunque en

<sup>21</sup> Vid. SSTJUE de 13 de marzo de 2014, *Brogsitter*, C-548/12; 14 de julio de 2016, *Granarolo*, C-196/15.

<sup>22</sup> Vid. Apartados 31 de la STJUE *Weltimmo* y 75 de la STJUE *Amazon EU Sari*.

<sup>23</sup> Vid. Apartados 76 y 77.

<sup>24</sup> Vid. Apartado 30 de la STJUE *Weltimmo*.

<sup>25</sup> Vid. STJUE 22 de diciembre de 2010, C-497/10, Mercredi ECLI: EU: C: 2010:829.

<sup>26</sup> Vid. STJUE C-509/09 y C-161/10 *eDate Advertising* ECLI: EU: C: 2011:685.



principio suele coincidir con la “residencia habitual”, podemos encontrarlo en otro Estado cuando exista un vínculo particularmente estrecho con ese otro Estado que resulte de otros indicios, como el ejercicio de una actividad profesional. La consideración de este foro de competencia no parece ser la más adecuada para determinar el tribunal que debe conocer de la pretensión, puesto que no exige que exista una vinculación entre el centro de intereses y el lugar donde efectivamente se produce el daño<sup>27</sup>.

Por lo que se puede dar el caso, por ejemplo, de que una persona conocida en Islandia que resida en España sin que sea conocido, sufra una difamación en España utilizando para ello la lengua islandesa. En este supuesto, el nacional islandés podrá demandar ante los tribunales españoles, aunque no se haya producido efectivamente el daño<sup>28</sup>. En el caso de que el centro de intereses del afectado no se encuentre en el Estado de residencia, sino en el Estado con vínculos profesionales; volviendo al ejemplo anterior, supongamos que este nacional trabaja como tertuliano en una televisión española, y sufre una difamación que atenta contra sus derechos a la personalidad; pero tal publicación está escrita en islandés, por lo que no tiene efecto “real” en España. En este sentido, creemos que hubiera sido mejor el criterio del Abogado General del asunto estudiado, el cual proponía como criterio para determinar la competencia —el cual rechazó seguir el TJUE— el “centro de gravedad del conflicto”<sup>29</sup>. Este criterio bebe del asimilado por el TJUE, que lo consagra como

<sup>27</sup> Vid. OREJUDO PRIETO DE LOS MOZOS, Patricia, “La vulneración de los derechos de la personalidad en la jurisprudencia del tribunal de justicia”, en *La Ley Unión Europea*, N° 4, 2013, p. 23.

<sup>28</sup> Sentencia del Tribunal Federal Supremo alemán (*Bundesgerichtshof*) BGH NJW 2011, 2059: El demandante y el acusado eran de Rusia y habían asistido a la escuela secundaria juntos en Moscú. Habiendo terminado la escuela, el demandante llegó a residir habitualmente en Alemania, el demandado en los Estados Unidos. Se reunieron de nuevo en septiembre de 2006 para una reunión de clases en Moscú. Después de este acontecimiento, el demandado fijó una entrada en la página: [www.womanineurope.com](http://www.womanineurope.com), que fue funcionado por una compañía alemana. En este post, el demandado describió las condiciones de vida y el aspecto del demandante en términos bastante desfavorables. El post fue escrito en lengua rusa y en letras cirílicas. El BGH denegó la jurisdicción porque la publicación carecía de una conexión suficiente con Alemania.

<sup>29</sup> El criterio del “centro de gravedad del conflicto” no es un descubrimiento reciente. Los tribunales estadounidenses, por ejemplo, aplican un análisis de intereses al determinar la ley aplicable que también se denomina enfoque de “contactos más significativos”, o “centro de gravedad” (p. ej. *Tooker v Lopez*, 24 N.Y.2d 569, 301 N.Y.S.2d 519, 249 N.E.2d 394 (1969), o *Neumeier v Kuehner*, 31 N.Y.2d 121, 335 (1972)). Esto incluye, junto con consideraciones tradicionales como el lugar de contratación, lugar de ejecución o lugar del hecho dañoso, la consideración de qué jurisdicción mantiene la relación más significativa o los contactos con el objeto de la controversia. Estos principios están recogidos en la Section 145 of the Restatement (Second), Conflict of Laws, aprobado por el American Law Institute en 1971. El artículo 145 (1) establece que “los derechos y responsabilidades de las partes con respecto a una cuestión extracontractual son determinados por la ley del Estado que, con respecto a esa cuestión, tenga la relación más significativa con el hecho y las partes [...]”. El párrafo 2 identifica entonces los contactos que deben tenerse en cuenta en un caso de responsabilidad civil para determinar la ley aplicable a una cuestión como a) el lugar donde ocurrió la lesión, b) el lugar donde ocurrió la conducta que causó la lesión; c) el domicilio, residencia, etc., de las partes en la acción, y d) El lugar donde se centra la relación, si la hay, entre las partes, estos contactos deben evaluarse en función de su importancia relativa con respecto al asunto en cuestión. Vid. OSTER, Jan, “Rethinking Shevill. Conceptualising the EU private international law of Internet torts against personality rights”, en *International Review of Law, Computers & Technology*, vol. 26, N.º 2-3, Routledge, 2012, pp. 120.



el lugar donde el afectado “desarrolla esencialmente su proyecto vital” (59 de las Conclusiones), pero que tiene en cuenta dos criterios más: 1) El contenido de la información: esto es, si la información tiene interés en el territorio, y; 2) La conexión que pueda tener con el territorio, a la luz de indicios que derivan de la propia web, tales como el nombre de dominio de primer nivel, el idioma empleado, la publicidad que ésta contenga o las palabras clave que se han suministrado a motores de búsqueda para identificar la página, o incluso de indicios exteriores, tales como los registros de la página.

La compatibilidad entre los foros del artículo 79.2 y los del Reglamento “Bruselas I bis” deriva del artículo 67 de este último Reglamento, al estipular que no prejuzgará la aplicación de las disposiciones contenidas en instrumentos particulares, como es el caso del artículo 79.2 del RGPD. En cuanto a los argumentos presentados por el RGPD, encontramos el Considerando 147 que afirma que las normas generales de competencia judicial del Reglamento “Bruselas I bis” “deben entenderse sin perjuicio de la aplicación de las normas específicas del RGPD”. El Considerando 145 estipula que el demandante “deberá tener la opción” de ejercitar las acciones en los tribunales de los Estados miembros.

Visto esta disposición de foros otorgados por diferentes instrumentos normativos, algún autor ha sostenido que sería más apropiado regular las reglas de competencia judicial internacional en el Reglamento “Bruselas I bis” en vez del propio RGPD para evitar así esta complicada compatibilidad de foros disponibles establecida tanto por el Reglamento Bruselas I bis como por el RGPD, y los problemas de litispendencia y conexidad del artículo 81 del RGPD para, a su vez, mantener coherencia entre ambos Reglamentos<sup>30</sup>.

Mientras que la jurisdicción general es “neutral”, la jurisdicción específica al menos indica que ya hay algún tipo de conexión significativa entre el foro y la cuestión jurídica a decidir<sup>31</sup>. Podemos observarlo en los foros especiales del artículo 79.2 del RGPD en los que se permite demandar.

La coexistencia de los foros previstos en el Reglamento “Bruselas I Bis” y el RGPD pone de manifiesto la complejidad de regular los desafíos que plantea la IA en un entorno cada vez más globalizado. Ambos marcos normativos, aunque complementarios, presentan diferencias que requieren una interpretación armonizada para evitar conflictos jurisdiccionales, especialmente en litigios transfronterizos relacionados con el uso de IA.

Y, siendo, así las cosas, debemos introducir en la ecuación al Reglamento europeo de IA, que, por su parte, añade una capa de regulación específica para los sistemas clasificados como de alto riesgo, que demandan un enfoque

<sup>30</sup> Vid. BRKAN, Maja, “Data protection and European private international law: observing a bull in a China shop”, en *International Data Privacy Law*, Vol. 5, N°. 4, 2015, pp. 275.

<sup>31</sup> Vid. VON HEIN, Jan, “Social Media and the Protection of Privacy”, en *European Data Science Conference*, Luxemburgo, 2016, pp. 24.

especial tanto en su desarrollo como en su comercialización. La regulación establece que la jurisdicción debe considerar no solo el lugar donde se encuentra el establecimiento del responsable o encargado, sino también el impacto ético y legal que la tecnología puede tener en los ciudadanos de la Unión Europea<sup>32</sup>. Esta perspectiva garantiza que las normativas de la UE no se limiten al territorio europeo, sino que también incluyan actividades realizadas por empresas fuera de la UE cuyos productos o servicios afecten a sus ciudadanos.

El Reglamento europeo de IA, en conjunto con el RGPD, y el Reglamento “Bruselas I Bis”, busca proporcionar un marco coherente para que las víctimas puedan litigar eficazmente en casos de responsabilidad civil derivados de la IA. Este marco no solo asegura el acceso a la justicia en el Estado miembro donde reside el afectado, sino que también fomenta la cooperación internacional al establecer estándares éticos y legales comunes.

En última instancia, el éxito de este enfoque radica en la capacidad de los Estados miembros y las instituciones internacionales para trabajar conjuntamente. Solo mediante la armonización normativa y acuerdos globales será posible abordar los desafíos jurisdiccionales que plantea la IA, garantizando así una protección integral de los derechos fundamentales en un entorno altamente digitalizado.

Visto esta disposición de foros otorgados por diferentes instrumentos normativos, quizás, sería más apropiado regular las reglas de competencia judicial internacional en el Reglamento “Bruselas I bis” en vez de en el propio RGPD para evitar así esta complicada compatibilidad de foros disponibles establecida tanto por el Reglamento “Bruselas I bis” como por el RGPD, y los problemas de litispendencia y conexidad del artículo 81 del RGPD para, a su vez, mantener coherencia entre ambos Reglamentos<sup>33</sup>. A todo ello, debemos sumarle el Reglamento europeo de IA, que contempla al menos un mecanismo de reclamación para particulares ante la autoridad de supervisión del mercado correspondiente en caso de incumplimiento de las disposiciones del Reglamento. Además, cuando se implementan sistemas automatizados o herramientas de apoyo a la toma de decisiones clasificadas como de alto riesgo, los usuarios finales tienen derecho a recibir información y explicaciones sobre el rol del sistema de IA en el proceso de decisión. Sin embargo, este Reglamento no establece una base jurídica que permita a los demandantes acudir directamente a los tribunales. Asimismo, estas disposiciones internacionales pueden requerir el respaldo del Derecho internacional privado para clarificar su aplicación en los distintos Estados miembros de la UE.

---

<sup>32</sup> Vid. CHURNIN, Stephen, *Inteligencia artificial: retos éticos y jurídicos, y la influencia de los derechos humanos*, Servicio de Publicaciones de la Facultad de Derecho, Universidad Complutense de Madrid, Madrid, 2011, p. 21.

<sup>33</sup> Vid. BRKAN, Maja, “Data protection and European private international law: observing a bull in a China shop”, en *International Data Privacy Law*, Vol. 5, N°. 4, 2015, p. 275; y VON HEIN, Jan, “Social Media and the Protection of Privacy”, en *European Data Science Conference*, Luxemburgo, 2016, p. 24.

#### 4. REFLEXIONES FINALES

*Primera.*— *Gran dispersión competencial para la protección del titular del derecho fundamental a la protección de datos ante un uso inadecuado de sistemas de inteligencia artificial.* La compatibilidad entre los foros de competencia judicial internacional establecidos en el artículo 79.2 del RGPD y los previstos en el Reglamento “Bruselas I Bis” se fundamenta en el artículo 67 de este último, que estipula que su aplicación no prejuzgará las disposiciones contenidas en instrumentos normativos específicos. En este contexto, el Considerando 147 del RGPD refuerza esta relación al señalar que las normas generales de competencia judicial del Reglamento “Bruselas I Bis” deben entenderse “sin perjuicio de la aplicación de las normas específicas del RGPD”. Por su parte, el Considerando 145 del RGPD establece que el demandante “deberá tener la opción” de ejercitar sus acciones ante los tribunales de los Estados miembros. Por lo tanto, resulta ineludible la necesidad de que ambos instrumentos jurídicos cohabiten y operen de manera complementaria en el ámbito de la competencia judicial internacional.

Si bien es cierto que el Reglamento europeo de IA “pretende reconocer las oportunidades transfronterizas de la inteligencia artificial, evitar la elusión normativa y garantizar la protección efectiva de las personas físicas situadas en la UE. En este sentido, el Reglamento quiere asegurar que las personas físicas y jurídicas de todos los niveles de la cadena de valor de la IA estén sujetas a los requisitos del Reglamento, a menudo con independencia de su jurisdicción. Sin embargo, la aplicación del artículo 2.1.c) del Reglamento europeo de IA es, en el mejor de los casos, incierta y, en el peor, altamente expansiva. En particular, aún no se sabe con certeza cómo se interpretará el término “utilización”. A falta de futuras aclaraciones por parte de la Comisión Europea, parece poco probable que se resuelva esta incertidumbre hasta que los reguladores y tribunales pertinentes de la UE proporcionen nuevas orientaciones sobre esta cuestión. Mientras tanto, las organizaciones no establecidas en la UE que utilicen sistemas de IA deben adoptar una actitud prudente y estar atentas a la evolución en este ámbito”<sup>34</sup>.

Los artículos 85 a 87 del Reglamento europeo de IA no regulan (en perjuicio de los intereses de los particulares, y de los objetivos enunciados en el artículo 1 del propio Reglamento) un derecho a presentar una reclamación en el mismo sentido que el RGPD. Más bien, lo que configuran es un derecho a presentar una petición ante la autoridad de vigilancia del mercado, la cual lo tendrá en cuenta a la hora de determinar si iniciar operaciones de investigación contra el proveedor o responsable de despliegue el sistema de IA. Además, la presentación de estas peticiones resulta obstaculizada por la

---

<sup>34</sup> Vid. BARRIO ANDRÉS, Moisés, “Consideraciones sobre el ámbito extraterritorial del Reglamento Europeo de Inteligencia Artificial”, en *Derecho Digital e Innovación. Digital Law and Innovation Review*, N° 20, 2024, pp. 1-3.

compleja distribución de competencias entre las autoridades de vigilancia del mercado que se deriva del artículo 74 del propio Reglamento europeo de IA.

*Segunda.— Necesaria (“difícil”) cohabitación entre los foros de competencia judicial internacional previsto en el Reglamento “Bruselas I bis” y el binomio RGPD + Reglamento europeo de IA.* Así las cosas, vista la disposición de los foros de competencia judicial internacional otorgados por los diferentes instrumentos normativos, es evidente que “son los detalles los que definen el cuadro”, pero cabría reflexionar y preguntarnos: si ¿no hubiera sido más apropiado regular las reglas de competencia judicial internacional en el Reglamento “Bruselas I Bis” en vez de hacerlo en el propio RGPD y/o en el Reglamento europeo de IA?

La coexistencia de los artículos 7.2 de Reglamento “Bruselas I Bis”, y el 79.2 del RGPD y los artículos 85 a 87 del Reglamento europeo de IA se encuentra en entredicho. Podemos observarlo en los foros especiales del artículo 79.2 del RGPD en los que se permite demandar: 1) ante los tribunales del Estado en el que esté domiciliado algún establecimiento tanto del responsable como del encargado; o, 2) ante los tribunales del Estado de la residencia habitual del afectado por un supuesto tratamiento ilícito de los datos personales que genera una responsabilidad extracontractual. Estos foros estipulados por el RGPD están redactados para adecuarse al supuesto concreto. En cambio, los foros del Reglamento “Bruselas I bis” tienen como objeto cubrir supuestos generales de responsabilidad civil extracontractual. Es decir, los principios que subyacen de ambos Reglamentos son diferentes y excluyentes entre sí, y uno de debe imponer su justicia sobre el otro<sup>35</sup>, por lo que el artículo 79.2 del RGPD debe prevalecer sobre el artículo 7.2 del Reglamento “Bruselas I bis”<sup>36</sup> (a los que habría que añadir los mecanismos de reclamación contemplados en los artículos 85 a 87 del Reglamento europeo de IA), teniendo en cuenta que la jurisdicción general (el Reglamento “Bruselas I Bis”) es “neutral” y la jurisdicción específica (el RGPD) al menos indica que ya hay algún tipo de conexión significativa entre el foro y la cuestión jurídica a decidir<sup>37</sup>, para, a su vez, mantener coherencia entre ambos Reglamentos<sup>38</sup>...pero bueno, en definitiva, llegados a este punto querido lector, parece que la realidad a la que nos enfrentamos en este juego de normas (RGPD, Reglamento “Bruselas I Bis” y Reglamento europeo de IA) es compleja...o, como decía Johan Cruyff: “si yo hubiera querido que me entendieras, me hubiera explicado mucho mejor”...

<sup>35</sup> Vid. REVOLIDIS, Ioanis, “Judicial jurisdiction over Internet privacy violations and the GDPR: a case of privacy tourism?”, *Masaryk University Journal of Law and Technology*, 2017, núm. 1, vol. 11, p. 23.

<sup>36</sup> Vid. CALVO CARAVACA, Alfonso Luis y CARRASCOSA GONZÁLEZ, Javier, *Derecho internacional privado*, Vol. II, 17ª ed., Comares, Granada, 2017, p. 1528.

<sup>37</sup> Vid. VON HEIN, Jan, “Social Media and the Protection of Privacy”, *European Data Science Conference*, 2016, p. 24.

<sup>38</sup> Vid. BRKAN, Maja, “Data protection and European private international law: observing a bull in a China shop”, *International Data Privacy Law*, 2015, núm. 4º, vol. 5, p. 275.

