

# UNA APROXIMACIÓN INTERNACIONAL PRIVATISTA A LAS ÓRDENES DE ACTUACIÓN CONTRA CONTENIDOS DIFAMATORIOS TRAS EL REGLAMENTO DE SERVICIOS DIGITALES

## *A PRIVATE INTERNATIONAL LAW APPROACH TO ORDERS TO ACT AGAINST DEFAMATORY CONTENT FOLLOWING THE DIGITAL SERVICES ACT*

ROSA PLA ALMENDROS\*

SUMARIO: I. INTRODUCCIÓN. II. LAS ÓRDENES DE ACTUACIÓN CONTRA CONTENIDOS ILÍCITOS EN EL CONTEXTO ACTUAL: RELEVANCIA Y CONCRECIÓN DE ANÁLISIS. III. LA REGULACIÓN DE LAS ÓRDENES DE ACTUACIÓN CONTRA CONTENIDOS DIFAMATORIOS ANTERIOR AL REGLAMENTO DE SERVICIOS DIGITALES. IV. LAS ÓRDENES DE ACTUACIÓN EN EL REGLAMENTO DE SERVICIOS DIGITALES. V. CONCLUSIONES Y PROPUESTAS DE SOLUCIÓN.

**RESUMEN:** La circulación de contenidos ilícitos en línea constituye uno de los riesgos más preocupantes de Internet, resultando primordial ofrecer una tutela eficaz a sus víctimas. Hasta febrero de 2024, en materia de difamación la única vía de protección legal se reducía a las órdenes judiciales de actuación contra contenidos ilícitos, cuyo elevado coste dejaba a las víctimas desprotegidas. Asimismo, su regulación nacional, que daba entrada a imprevisibles normas de Derecho Internacional privado, impedía su adecuado funcionamiento. El nuevo Reglamento (UE) 2022/2065 de servicios digitales (*Digital Services Act*), junto con otras medidas de tutela, ha instaurado por primera vez a nivel de la UE un régimen de armonización mínima de las órdenes judiciales de actuación contra todo tipo de contenidos ilícitos. El objetivo del presente trabajo de investigación es analizar esta nueva regulación para evaluar si mejora la eficacia de las órdenes en materia de difamación, ilustrando este aspecto a través de la sentencia del TJUE *Glawischnig-Piesczek*.

**ABSTRACT:** *The circulation of illegal content online is one of the most worrying risks of the internet, and effective protection for its victims is of paramount importance. Until February 2024, the only legal protection for defamation was limited to judicial orders to act against illegal content, the high cost of which left victims unprotected. Moreover, its national regulation, which allowed for unpredictable rules of Private International law, prevented it from functioning properly. The new Regulation (EU) 2022/2065 for Digital Services (Digital Services Act), together with other enforcement measures, has, for the first time at EU level, introduced a minimum harmonisation regime for orders to act against all types of illegal content. The aim of this paper is to analyse this new regulation in order to assess whether it improves the effectiveness of defamation orders, illustrating this aspect through the judgement of the CJEU Glawischnig-Piesczek.*

**PALABRAS CLAVE:** difamación, plataformas en línea, moderación de contenidos, órdenes judiciales, transfronterizo.

**KEYWORDS:** *defamation, online platforms, content moderation, judicial orders, cross-border.*

---

Fecha de recepción del trabajo: 26 de marzo de 2025. Fecha de aceptación de la versión final: 13 de mayo de 2025.

\* Investigadora predoctoral FPU de Derecho Internacional privado en la Universitat de València, Departamento de Derecho Internacional “Adolfo Miaja de la Muela”. Correo electrónico: rosa.pla@uv.es.

## I. INTRODUCCIÓN

En los últimos años, la presencia de contenidos ilícitos en Internet se ha disparado de forma exponencial debido a la creciente accesibilidad a las plataformas en línea, así como a las crisis de las democracias liberales actuales. En consecuencia, la Comisión Europea ha definido la retirada del contenido ilícito en línea como “un reto urgente para la sociedad digital actual”<sup>1</sup>.

Frente a este preocupante escenario protagonizado por los contenidos ilícitos, resulta necesario proteger a sus víctimas, quienes no suelen estar interesadas tanto en una compensación económica como en la eliminación de aquellos<sup>2</sup>. La primera opción para alcanzar la supresión del contenido sería solicitarla directamente al usuario digital que lo ha publicado. Sin embargo, ello no es posible en la mayoría de los supuestos<sup>3</sup>, en los que el autor es anónimo<sup>4</sup>. A la luz de esta dificultad por la que el destinatario del ilícito queda “particularmente indefenso”<sup>5</sup>, la única manera factible de conseguir la eliminación del contenido sería reclamarla a la plataforma en línea a través de la que se ha publicado. Una posibilidad que, como se verá, resultaría plausible incluso cuando aquella no sea responsable por la información publicada por un tercero.

Según el tipo de contenido ilícito, las vías de tutela legales para solicitar su supresión a las plataformas en línea han sido tradicionalmente distintas. La presente investigación se centrará en el supuesto de la difamación, perteneciente a los llamados “derechos de la personalidad”, consagrados en el art. 8.1 del Convenio Europeo de Derechos Humanos y art. 7 de la Carta de Derechos Fundamentales de la UE. Hasta ahora, en relación con este tipo de ilícito, la única vía legal para realizar aquella solicitud de retirada se reducía a las órdenes judiciales de actuación dirigidas a prestadores de servicios intermediarios como las plataformas en línea.

Esta posibilidad se introdujo en el año 2000 a través de una mínima referencia en el art. 18 de la Directiva 2000/31/CE de comercio electrónico (DCE)<sup>6</sup>, que obligó a los distintos países de la UE a regular aquellas órdenes, resultando en una respuesta legislativa puramente nacional. Este escenario jurídicamente fragmentado, unido al habitual carácter transfronterizo de las órdenes, exigía la aplicación de normas de Derecho Internacional privado, cuya eventual falta de adaptación a Internet podía obstaculizar la eficacia de las órdenes.

---

1 Comunicación de la Comisión, de 28 de septiembre de 2017, sobre la Lucha contra el contenido ilícito en línea. Hacia una mayor responsabilización de las plataformas en línea, COM (2017) 555 final.

2 ARDIA, D. S., “Freedom of speech, defamation, and injunctions”, *William & Mary Law Review*, vol. 55, núm. 1, 2013, pp. 1-84, p. 15.

3 Como excepción, véase la STEDH Alexandru Pătrașcu v. Romania, de 7 de enero de 2025, n.º 1847/21.

4 En caso de anonimidad, solo puede obligarse a los prestadores de acceso a revelar la identidad del supuesto infractor cuando medie una orden judicial en ese sentido. Orden judicial que debería quedar regida por lo dispuesto en el art. 15.2 DCE y no en el art. 18 DCE, toda vez que la averiguación de dicha identidad no es imprescindible para conseguir la cesación de la conducta ilícita, pues siempre se tiene la posibilidad de dirigirse contra el prestador de servicios de alojamiento de datos, que es, precisamente, el supuesto que aquí se estudia. Para más información en este sentido, véase GONZÁLEZ GONZALO, A., “La obligación de los prestadores de servicios en línea de revelar la identidad de los usuarios que infringen derechos de propiedad intelectual a través de redes P2P”, *Revista de propiedad intelectual*, núm. 20, 2005, pp. 77-134, pp. 98-100.

5 FFJJ 6.º de la STC de 4 de julio de 2023, núm. 83/2023, ECLI:ES:TC:2023:83

6 Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico). *DO* núm. 178, de 17 de julio de 2000.

Tras más de dos décadas, el legislador de la UE ha querido atajar la cuestión a través del Reglamento (UE) 2022/2065 de servicios digitales (RSD)<sup>7</sup>, que actualiza y complementa la Directiva de comercio electrónico. Esta nueva norma, que devino plenamente aplicable en febrero de 2024, ha incorporado medidas adicionales de tutela de las víctimas de contenidos ilícitos, entre las que incluye una nueva regulación de las órdenes de actuación contra todo tipo de contenidos ilícitos en línea en el art. 9 RSD. A la luz de lo anterior, nuestra finalidad es comparar los marcos legales de las mencionadas órdenes antes y después de la plena aplicación del RSD para dictaminar si la nueva regulación, tal y como pretende, resulta eficaz.

Bajo aquel propósito, el presente trabajo se estructura como sigue. Tras esta introducción, se examinará la importancia de las órdenes judiciales en el entorno digital actual y se delimitará cuáles serán objeto de análisis. A tal fin, se tomará como punto de partida la sentencia del Tribunal de Justicia de la Unión Europea (TJUE) *Glawischnig-Piesczek* C-18/18 (STJUE *Glawischnig-Piesczek*)<sup>8</sup>, que restringirá el examen a la tutela de las víctimas de contenidos difamatorios difundidos a través de una plataforma en línea (apartado II). Tras ello, se analizará el régimen legal de las órdenes antes del RSD, detallando el carácter nacional de su regulación sustantiva, así como la relevancia de las normas de Derecho Internacional privado, cuyas soluciones aplicadas a nuestro supuesto de hecho permitirán poner en duda el funcionamiento de las órdenes con anterioridad al RSD (apartado III). Más tarde, se analizará la nueva regulación de las órdenes incorporada en el RSD, que se aplicará al caso de estudio para comprender los avances (apartado IV). El último apartado servirá para concluir y presentar posibles propuestas de solución (apartado V).

## **II. LAS ÓRDENES DE ACTUACIÓN CONTRA CONTENIDOS ILÍCITOS EN EL CONTEXTO ACTUAL: RELEVANCIA Y CONCRECIÓN DE ANÁLISIS**

Las órdenes judiciales de actuación contra contenidos ilícitos han gozado siempre de una singular relevancia, que se mantiene incluso tras la aplicación del RSD. Sin embargo, el espacio de que aquí se dispone impedirá analizar las particularidades de todos los tipos de órdenes, por lo que se limitará su examen a aquellas emitidas a propósito de supuestos como el descrito en la STJUE *Glawischnig-Piesczek*.

### **1. La relevancia de las órdenes de actuación en la tutela de las víctimas de contenidos difamatorios**

Con anterioridad a la entrada en funcionamiento del RSD, la regulación del entorno en línea en la UE era limitada, en consonancia con el enfoque de liberalismo digital de aquel momento:

---

7 Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales), *DO* núm. 277, de 27 de octubre de 2022.

8 STJUE de 3 de octubre de 2019, *Glawischnig-Piesczek*, C-18/18, ECLI:EU:C:2019:821.

se reducía a la DCE y a algunas pocas normas complementarias. En este contexto, las plataformas en línea no estaban obligadas a ello, pero en muchas ocasiones, de forma voluntaria<sup>9</sup>, perseguían, detectaban y eliminaban contenidos y actividades controvertidas llevadas a cabo por terceros sirviéndose de medidas de autorregulación. El objetivo era liberar el espacio en línea de peligros para mejorar su reputación, así como retener y atraer a nuevos usuarios.

Con dicho fin, las plataformas en línea, sobre todo las de muy gran tamaño, hacían uso de medidas de moderación de contenidos, y para los supuestos en que fueran insuficientes<sup>10</sup>, solían incorporar mecanismos de notificación y acción e incluso sistemas de solución extrajudicial<sup>11</sup>. Sin embargo, ninguna de estas medidas conseguía poner fin a la totalidad de ilícitos que se vertían en la red, toda vez que su verdadera meta no era proteger a los usuarios digitales, sino maximizar el beneficio de las plataformas<sup>12</sup>.

Así las cosas, la única forma fiable de conseguir la retirada del contenido ilícito era solicitar una orden de actuación contra el mismo dirigida al prestador de servicios intermediario a través del que se hubiera publicado, tomando como base el art. 18 DCE. No obstante, dado el elevado coste económico y la lentitud característica de los tribunales, las víctimas preferían no actuar, quedando desprotegidas.

Pese a estos inconvenientes, las órdenes de actuación gozaban de una significación especial, siendo la única herramienta que permitía atacar los contenidos difamatorios. Pero lamentablemente la tutela de las víctimas se tornaba insuficiente, al no brindárseles otras herramientas más ventajosas con el mismo fin<sup>13</sup>. Sobre el particular, hubo estudios que confirmaron que esta podía ser una razón que explicara la exigua notificación de contenidos de este tipo<sup>14</sup>.

9 Por todos, CORDERO ÁLVAREZ, C. I., “El régimen de responsabilidad de las plataformas online en la DSA ante contenidos ilícitos lesivos de derechos fundamentales: evolución de la figura de puerto seguro”, en J.J. CASTELLÓ PASTOR (Dir.), *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, pp. 69-105, p. 94.

10 Estos errores pueden ser de dos tipos: error de tipo I o falsos positivos si se retira un contenido lícito, y error de tipo II o falsos negativos si no se retira un contenido ilícito. Aunque ambos errores existen, la práctica pone de relieve que los falsos positivos son más frecuentes. Pese a ello, nuestra atención se centrará en los falsos negativos, pues son estos y no aquellos los que abordan las órdenes contra contenidos ilícitos analizadas. Para más información sobre los errores, véase SCHWEMER, S. F., “Decision Quality and Errors in Content Moderation”, *op.cit.*, p. 144.

11 SCHULZ, W., “Changing the Normative Order of Social Media from Within: Supervisory Bodies”, en CELESTE, E., HELDT, A., e IGLESIAS KELLER, C., *Constitutionalising Social Media*, Hart Publishing, Oxford, 2022, pp. 237-250, p. 242.

12 COTINO HUESO, L., “Quién, cómo y qué regular (o no regular) frente a la desinformación”, *Teoría y Realidad Constitucional*, núm. 49, 2022, pp. 199-238, p. 217.

13 ROJSZCZAK, M., “The Digital Services Act and the Problem of Preventive Blocking of (Clearly) Illegal Content”, *Journal of Administrative Sciences*, vol. 3, núm. 2, 2023, pp. 44-59, p. 45, y ZEYBEK, B., VAN HOBOKEN, J., y BURI, I., “Redressing Infringements of Individuals’ Rights Under the Digital Services Act”, *DSA Observatory*, 2022, versión en línea accesible en: <https://dsa-observatory.eu/2022/05/04/redressing-infringements-of-individuals-rights-under-the-digital-services-act/>, último acceso el 23 de marzo de 2025.

14 ICF, GRIMALDI STUDIO LEGALE y 21C CONSULTANCY, “Overview of the legal framework of notice-and-action procedures in Member States. SMART 2016/0039. Final report”, *Publications Office of the European Union*, 2018. Versión en línea disponible en: <https://op.europa.eu/en/publication-detail/-/publication/a56ceb47-2446-11e9-8d04-01aa75ed71a1>, último acceso el 23 de marzo de 2025, p. 125.

Aquel preocupante escenario, que dejaba a las víctimas al margen, junto con un entorno digital cada vez más plagado de contenidos ilícitos, falsos y engañosos<sup>15</sup>, generó una fuerte preocupación en el legislador de la UE, quien temía la obstaculización de la consolidación del Mercado Único Digital<sup>16</sup>. En consecuencia, este quiso atajar la cuestión de forma progresiva, para lo cual construyó un marco legal sobre la DCE, que se tradujo en ciertas medidas impuestas por la Directiva 2018/1808 y por otras normas dictadas a propósito de los cuatro tipos de contenidos ilícitos —en su mayoría, penales<sup>17</sup>— armonizados a nivel de la UE (terrorismo, pornografía infantil, racismo y derechos de autor)<sup>18</sup>. Sin embargo, la situación del resto de los sectores —incluyendo el difamatorio— se mantuvo invariable y anclada a la DCE.

Con el objetivo de cubrir el vacío regulatorio, el legislador europeo ha dado un último y reciente paso a través del nuevo Reglamento de Servicios Digitales. Este instrumento, cuya principal finalidad es alcanzar un entorno en línea seguro y fiable en el que se protejan los derechos fundamentales (art. 1 RSD), ha adoptado medidas que regulan por primera vez en la UE la moderación de contenidos ilícitos, y que pretenden disminuir la cantidad de todo tipo de contenidos ilícitos en línea<sup>19</sup>.

Entre ellas, destacan la figura del alertador fiable del art. 22, y la evaluación de riesgos sistémicos del art. 34 RSD, que obliga a las plataformas en línea de muy gran tamaño a examinar con periodicidad semestral el riesgo provocado en sus servicios por la difusión de contenidos ilícitos y a reducirlo con medidas como la moderación de contenidos en virtud del art. 35 RSD. Asimismo, conviene señalar la incorporación de la conocida como “cláusula del buen samaritano” del art. 7 RSD, que pretende promover la moderación de contenidos activa sin miedo a perder las exenciones de los arts. 4 a 6 RSD<sup>20</sup>.

Sin duda, estas medidas potenciarán la moderación de contenidos llevada a cabo voluntariamente por las plataformas. Sin embargo, por el momento, esta no podrá erradicar los ilícitos

---

15 COMISIÓN EUROPEA, “Standard Eurobarometer 100: Media use in the European Union”, *Eurobarometer Report*, octubre-noviembre 2023, pp. 27 y 61. Disponible en: <https://europa.eu/eurobarometer/surveys/detail/3053>, último acceso el 23 de marzo de 2025.

16 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 6 de mayo de 2015, Una Estrategia para el Mercado Único Digital de Europa, COM (2015) 192 final.

17 CORDERO ÁLVAREZ, C. I., “El régimen de responsabilidad de las plataformas online en la DSA ante contenidos ilícitos lesivos de derechos fundamentales: evolución de la figura de puerto seguro”, en J.J. CASTELLÓ PASTOR (Dir.), *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, pp. 69-105, p. 80.

18 Para más detalle, véase DE STREEL, A. et al, “Online Platforms’ Moderation of Illegal Content Online”, Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2020, pp. 18-34. Versión en línea accesible en: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648797/IPOL\\_STU%282020%29648797\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648797/IPOL_STU%282020%29648797_EN.pdf), último acceso el 21 de abril de 2025.

19 FROSIO, G. y GEIGER, C., “Taking fundamental rights seriously in the Digital Services Act’s Platform liability regime”, *European Law Journal*, vol. 29, núm. 1-2, 2023, pp. 31-77, pp. 63 y ss.

20 Con dudas, CASTELLÓ PASTOR, J.J., “Nuevo régimen de responsabilidad de los servicios digitales que actúan como intermediarios a la luz de la propuesta de Reglamento relativo a un mercado único de servicios digitales”, en CASTELLÓ PASTOR, J.J. (Dir.), *Desafíos jurídicos ante la integración digital: aspectos europeos e internacionales*, Aranzadi Thomson Reuters, 2021, versión en línea.

por completo. La razón es que las plataformas —especialmente si son de muy gran tamaño<sup>21</sup>— suelen confiar en medios automatizados para ejecutar sus medidas de moderación de contenidos<sup>22</sup>, y estos todavía quedan lejos de comprender los matices propios de la comunicación humana<sup>23</sup>. De este modo, aún existen errores inevitables en la moderación de contenidos, cuya tasa de error es explícitamente admitida por el art. 15.1.d) RSD.

Consciente de lo anterior, el RSD ha incluido nuevos medios de tutela que pone a disposición de las víctimas de contenidos ilícitos, con el objeto de mitigar las decisiones erróneas de moderación de contenidos (cdo. 26 RSD)<sup>24</sup>. En particular, las plataformas en línea deben incorporar, ahora con carácter obligatorio y salvaguardias mínimas, medios más rápidos y baratos que el recurso a los órganos judiciales, como el mecanismo de notificación y acción del art. 16 RSD, y los medios de solución extrajudicial tanto interno (art. 20 RSD) como externo a la plataforma (art. 21 RSD)<sup>25</sup>. Asimismo, el RSD introduce una nueva regulación de las órdenes de actuación contra contenido ilícito (art. 9 RSD)<sup>26</sup>.

Parece evidente que, si las víctimas tienen a su disposición medios gratuitos, fiables y más rápidos que los órganos judiciales para solicitar y conseguir la retirada del contenido ilícito, acudirán a aquellos antes que a estos. Sin embargo, ello no debe llevar a pensar que las órdenes han perdido relevancia práctica tras la implementación del RSD. Bien al contrario, siguen siendo sumamente necesarias; la supervisión judicial funciona como un contrapeso al poder privado de las plataformas, revisando sus decisiones de moderación de contenidos para evitar

- 
- 21 La *DSA Transparency Database* sitúa esta cifra en torno al 50% de las decisiones, si bien las plataformas en línea de muy gran tamaño exceden con creces este dato. Por ejemplo, del Informe de transparencia de Youtube se desprende que esta cifra fue del del 96,5% para el último semestre de 2024: retiró 9.456.987 videos de su plataforma, de las que 9.126.392 fueron automatizadas. Para más detalle, consúltese <https://transparencyreport.google.com/youtube-policy/removals>, último acceso el 11 de mayo de 2025.
- 22 CASTELLÓ PASTOR, J.J., “Inteligencia artificial aplicada por las plataformas en línea y motores de búsqueda de muy gran tamaño para mitigar los riesgos sistémicos en línea”, *Cuadernos de Derecho Transnacional*, vol. 17, núm. 1, 2025, pp. 308-328, p. 311, y FROSIO, G. y GEIGER, C., “Taking fundamental rights seriously in the Digital Services Act’s Platform liability regime”, *European Law Journal*, vol. 29, núm. 1-2, 2023, pp. 31-77, pp. 34-35.
- 23 KELLER, D., “Dolphins in the Net: Internet Content Filters and the Advocate General’s *Glawischnig-Piesczek v. Facebook Ireland* Opinion”, *Stanford Center for Internet and Society*, 2019, pp. 1-39, p. 22, y QUINTAIS, J. P., APPELMAN, N. y FATHAIGH, R., “Using Terms and Conditions to apply Fundamental Rights to Content Moderation”, *German Law Journal*, 2023, núm. 24, pp. 881-911, p. 882.
- 24 FILATOVA-BILOUS, N., “Content moderation in times of war: testing state and self-regulation, contract and human rights law in search of optimal solutions”, *International Journal of Law and Information Technology*, núm. 31, 2023, pp. 46-74, p. 64.
- 25 En realidad, las herramientas que deben incorporar las plataformas en línea no constituyen nuevas medidas de tutela, pues como mínimo los arts. 16 y 20 RSD se limitan a codificar legalmente —y a añadir garantías mínimas— a prácticas ya adoptadas de forma voluntaria con anterioridad por las plataformas.
- 26 El art. 86 RSD confiere al usuario digital la posibilidad de ejercer cualquiera de los mencionados medios de tutela de forma individual o a través de un organismo que le represente (p. ej. ONG). Y el art. 90 RSD también permite el uso de acciones colectivas cuando corresponda. No obstante, en materia de difamación, en la que el contenido afecta de modo más severo a individuos concretos, es más probable que la información controvertida sea notificada de modo directo y en exclusiva por estos. Así, ICF, GRIMALDI STUDIO LEGALE y 21C CONSULTANCY, “Overview of the legal framework...”, *op.cit.*, p. 125.

que sean ellas las que en exclusiva controlen la censura y la libertad de expresión<sup>27</sup>. Por tanto, se trata de una medida indispensable para garantizar una correcta ponderación entre derechos fundamentales<sup>28</sup>.

A la luz de lo anterior, resulta entonces sorprendente que el art. 9 RSD todavía no haya sido estudiado más allá de análisis meramente descriptivos. Una razón potencialmente justificativa es que, pese a que los informes de transparencia emitidos por las plataformas en línea al amparo de los arts. 15, 24 y 42 RSD confirman que ya se han dictado órdenes con arreglo al art. 9 RSD<sup>29</sup>, estas no suelen publicarse, dificultando ello su estudio<sup>30</sup>. En consecuencia, el presente análisis no se basará en una orden dictada en virtud del art. 9 RSD, sino emitida conforme a la regulación anterior al RSD, para así predecir los efectos que pensamos que la nueva normativa podría tener sobre las órdenes judiciales que se dicten a partir de ahora.

## 2. La STJUE *Glawischnig-Piesczek* como caso de estudio

Comparar en abstracto los marcos regulatorios de las órdenes de actuación contra contenidos ilícitos antes y después del RSD resultaría temerario e insensato por nuestra parte, toda vez que sería inabarcable examinar las singularidades de todas las órdenes. De este modo, se ofrecerá una visión general sobre las distintas clases de órdenes, para más tarde concretar, de todas ellas, en cuáles pondremos la atención.

En lo que aquí concierne, las órdenes de actuación contra contenidos ilícitos pueden clasificarse con arreglo a los siguientes criterios.

---

27 MCGONAGLE, T., “Free Expression and Internet Intermediaries: The Changing Geometry of European Regulation”, en FROSIO, G., *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, Oxford, 2020, pp. 467-485, p. 483, y GEIST, M., “The *Equustek* Effect: A Canadian Perspective on Global Takedown Orders in the Age of the Internet”, en FROSIO, G., *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, Oxford, 2020, pp. 709-726, p. 725

28 KUCZERAWY, A., “Remedying Overremoval”, en VAN HOBOKEN, J. et al., *Putting the DSA into Practice: Enforcement, Access to Justice, and Global Implications*. Verfassungsbooks, Berlín, 2023, pp. 167-182, p. 179.

29 A título de ejemplo, el Informe de transparencia del segundo semestre de 2024 elaborado por Tiktok señala que en este periodo de tiempo recibió un total de 701 órdenes judiciales de actuación contra contenidos ilícitos (p. 20 del Informe accesible en <https://www.tiktok.com/transparency/en/dsa-transparency/>, último acceso el 11 de mayo de 2025), mientras que la misma cifra se sitúa en 6 para LinkedIn (p. 18 del Informe accesible en <https://www.linkedin.com/help/linkedin/answer/a1678508>, último acceso el 11 de mayo de 2025), y 0 para Bing (p. 1 del Informe accesible en <https://www.microsoft.com/en-us/corporate-responsibility/eu-dsa-report-bing>, último acceso el 11 de mayo de 2025).

30 La información sobre las órdenes del art. 9 RSD también debería incluirse en los informes anuales que, con arreglo al art. 55 RSD, deben publicar los coordinadores de servicios digitales con carácter anual, que deberían aparecer en la página web oficial de la Comisión Europea, y también en la siguiente página web de carácter semipúblico: <https://dscdb.edri.org/>, último acceso el 12 de mayo de 2025. En esta fecha, los informes en cuestión todavía no se han difundido. Tan solo las entidades designadas como coordinadores de servicios digitales en Bélgica, Irlanda y Luxemburgo han emitido informes correspondientes a sus actividades en 2023. Sin embargo, en aquel momento ni siquiera el RSD había entrado en funcionamiento.

- i) Según la autoridad que tenga competencia para emitirla, la orden puede ser judicial o administrativa. En materia de difamación, el tribunal competente se determinará principalmente por el Reglamento (UE) 1215/2012 Bruselas I bis (RB I bis)<sup>31</sup>.
- ii) Desde el punto de vista material, las órdenes pueden obligar a suprimir cualquier tipo de ilicitudes, incluyendo ilícitos de propiedad intelectual, difamaciones, pornografía infantil, discursos de odio o terrorismo, entre otros.
- iii) En función del destinatario, las órdenes pueden dirigirse contra cualquier prestador de servicios intermediarios, ya sea de mera transmisión, de memoria caché o de alojamiento de datos. Sin embargo, habida cuenta de que la relación técnica de cada uno de ellos con el contenido es distinta<sup>32</sup>, en la práctica es más frecuente solicitar una orden a los prestadores de servicios de alojamiento de datos (p. ej. plataformas en línea) o a los de mera transmisión (p. ej. proveedores de acceso a Internet). Mientras que los primeros son capaces de conseguir la eliminación del contenido suprimiéndolo de sus servidores, los segundos tan solo podrían bloquear el acceso al mismo<sup>33</sup>, sin eliminarlo por completo. Por ese motivo, de todos los potenciales destinatarios de una orden (esto es, cualquier prestador de servicios intermediarios), las plataformas en línea y los motores de búsqueda, especialmente de muy gran tamaño<sup>34</sup> (arts. 3.i) y j) RSD), son aquellos a los que las víctimas suelen demandar con mayor frecuencia para solicitar supresión del contenido<sup>35</sup>.
- iv) Las órdenes de actuación se pueden dirigir contra los prestadores de servicios intermediarios, con independencia de que estos se eximan o no de responsabilidad por el contenido ilícito difundido por terceros. Ello es así gracias a los puertos seguros de los arts. 12 a 14 DCE, ahora reproducidos de forma prácticamente intacta —con críticas<sup>36</sup>— en los arts. 4 a 6 RSD<sup>37</sup>. En este sentido, habida cuenta de la indispensable

---

31 Reglamento (UE) n.º 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil. *DO* núm. L 351 de 20 de diciembre de 2012.

32 VAN DER DONK, B. B. E., “How dynamic is a dynamic injunction?...”, *op.cit.*, p. 602.

33 LODDER, A. R., y POLTER, P., “ISP blocking and filtering: on the shallow justification in case law regarding effectiveness of measures”, *European Journal of Law and Technology*, vol. 8, núm. 2, 2017, pp. 1-20, p. 3.

34 Según el art. 33 RSD, las plataformas en línea de muy gran tamaño son aquellas que cuentan con “un promedio mensual de destinatarios del servicio activos en la Unión igual o superior a cuarenta y cinco millones” y sean designadas como tales por la Comisión Europea.

35 HUSOVEC, M., *Injunctions against intermediaries in the European Union: Accountable but Not Liable?*, Cambridge University Press, Cambridge, 2017, p. 53.

36 BUITEN, M.C., “The Digital Services Act. From Intermediary Liability to Platform Regulation”, *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, vol. 12, núm. 5, pp. 361-380, p. 379.

37 Sobre este régimen de responsabilidad, que explicó buena parte del éxito de la Directiva de comercio electrónico, véase CASTELLÓ PASTOR, J.J., “Nuevo régimen de responsabilidad de los servicios digitales...”, versión en línea, y CORDERO ÁLVAREZ, C. I., “El régimen de responsabilidad de las plataformas online en la DSA ante contenidos ilícitos lesivos de derechos fundamentales: evolución de la figura de puerto seguro”, en J.J. Castelló Pastor (Dir.), *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024, pp. 69-105, pp. 84-92.

colaboración de los intermediarios para eliminar los ilícitos en línea, los arts. 12.3, 13.2 y 14.3 DCE —actuales arts. 4.3, 5.2 y 6.4 RSD— estipulan que, aun cuando las exenciones de responsabilidad sean aplicables a los prestadores de servicios intermediarios, estos pueden seguir siendo destinatarios de las órdenes de actuación contra contenidos ilícitos.

- v) Según su alcance material, las órdenes pueden ser estáticas o dinámicas. Las primeras son aquellas cuyo objeto se limita a eliminar un contenido ilícito concreto, de modo que son fácilmente superables para el autor del contenido (basta con volver a subirlo a la plataforma). Para evitar la ineffectividad de aquellas, en los últimos años se ha hablado de órdenes “dinámicas” (*dynamic injunctions*), que obligan a las plataformas a retirar o bloquear el acceso al contenido infractor, pero también a todo aquel que se publique con posterioridad por el mismo u otro autor con el mismo mensaje<sup>38</sup>.

La posibilidad de dictar órdenes dinámicas no se ha previsto en las legislaciones nacionales ni de la UE —tampoco en el RSD—. Tan solo el TJUE se ha pronunciado sobre ellas, precisamente a propósito de la STJUE *Glawischnig-Piesczek*. De hecho, este es el aspecto de la sentencia que más discusión doctrinal ha suscitado, dada la potencial incompatibilidad con la prohibición general de búsqueda del art. 15 DCE (actual art. 8 RSD)<sup>39</sup>, si bien en este caso no ocupará nuestra atención.

De acuerdo con lo señalado, tan solo nos centraremos en las órdenes de actuación dictadas en escenarios como el de la STJUE *Glawischnig-Piesczek*, cuyo relato fáctico se resume a continuación.

En abril de 2016, un periódico en línea austriaco publicó un artículo sobre la entonces diputada y portavoz del grupo parlamentario austriaco “Los Verdes”, la Sra. Eva Glawischnig-Piesczek<sup>40</sup>. El mencionado artículo fue republicado el mes siguiente por un usuario a través de un perfil falso en Facebook, añadiendo un comentario sobre la diputada austriaca, calificándola de “miserable traidora al pueblo”, “idiota corrupta” o perteneciente a un “partido de fascistas”<sup>41</sup>.

Dada la anonimidad del usuario, la Sra. Glawischnig-Piesczek no tuvo otra opción que dirigirse contra Facebook Ireland —encargado de gestionar la plataforma para todos los usuarios situados fuera de Estados Unidos y Canadá— para solicitar la eliminación del comentario. Para ello, primero reclamó la supresión del contenido directamente a la plataforma, siendo lo más probable que se sirviera para ello del sistema de notificación ofrecido voluntariamente por Facebook. Ante la negativa de retirar el contenido de este, la afectada interpuso demanda ante el Tribunal de lo Mercantil de Viena ejerciendo, conjuntamente, una acción indemnizatoria y una acción de cesación que obligara a Facebook a retirar a nivel mundial la imagen de

38 VAN DER DONK, B. B. E., “How dynamic is a dynamic injunction?...”, *op.cit.*, pp. 603-604.

39 RAUCHEGGER, C y KUCZERAWY, A. «Injunctions to remove illegal content online under the eCommerce Directive: *Glawischnig-Piesczek*». *Common Market Law Review*. 2020, vol. 57, 1495-1526, pp. 6-15.

40 <https://www.oe24.at/oesterreich/politik/gruene-mindestsicherung-fuer-fluechtlinge-soll-bleiben/230318208>, último acceso el 23 de marzo de 2025.

41 Este pasaje fue redactado originalmente en un idioma distinto del español. Esta y el resto de las traducciones que presenta el trabajo son las propias de quien escribe estas líneas.

la demandante y los comentarios injuriosos que la acompañaban, así como cualesquiera otros comentarios idénticos o similares publicados por ese usuario o por un tercero. La orden contra los comentarios se solicitó como medida de fondo, pero también cautelar.

El Tribunal de lo Mercantil de Viena estimó la demanda, considerando que el comentario vulneraba el derecho al honor de la demandante y ordenando la supresión a nivel mundial de las fotografías de la demandante acompañadas del contenido difamatorio o cualquier otro idéntico o similar<sup>42</sup>. Finalmente, el caso acabó llegando al TJUE tras la elevación de una cuestión prejudicial por parte del Tribunal Supremo austriaco. La resolución del TJUE se dictó en octubre de 2019 y, tras ella, el Alto Tribunal austriaco acabó poniendo fin al procedimiento en septiembre de 2020<sup>43</sup>.

De lo anterior se desprende que, siguiendo los criterios de clasificación antes expuestos, la STJUE *Glawischnig-Piesczek* obligará a focalizarnos en tan solo aquellas órdenes judiciales transfronterizas dictadas contra contenidos difamatorios y dirigidas a una plataforma en línea de muy gran tamaño establecida en la UE. Un supuesto práctico bien conocido por todos dada su frecuencia práctica<sup>44</sup>.

### III. LA REGULACIÓN DE LAS ÓRDENES DE ACTUACIÓN CONTRA CONTENIDOS DIFAMATORIOS ANTERIOR AL REGLAMENTO DE SERVICIOS DIGITALES

A fin de exponer el func0ra más tarde estudiar las cuatro cuestiones paradigmáticas en Derecho Internacional privado, cuya aplicación al caso *Glawischnig-Piesczek* servirá para ilustrar el ineficaz funcionamiento de las órdenes judiciales de actuación contra contenidos difamatorios antes del RSD.

#### 1. Regulación sustantiva

La primera referencia que se hizo en la UE a las órdenes contra contenidos ilícitos en línea se redujo al art. 18 DCE, que obligaba a los Estados miembros a regularlas a nivel nacional. Con posterioridad, la progresiva proliferación de determinados contenidos ilícitos en Internet provocó que el legislador de la UE incrementara el grado de armonización de las órdenes en ciertas materias, como los derechos de autor o el terrorismo.

No obstante, la difamación nunca ha constituido uno de esos sectores, probablemente porque implica no solo intereses privados sino también públicos<sup>45</sup>. En consecuencia, hasta la apro-

---

42 OGH (Oberster Gerichtshof), sentencia de 25 de octubre de 2017, *Glawischnig-Piesczek*, núm. 6Ob116/17b, ECLI:AT:OGH:2017:6Ob116/17b

43 OGH (Oberster Gerichtshof), sentencia de 15 de septiembre de 2020, *Glawischnig-Piesczek*, núm. 6Ob195/19a, ECLI:AT:OGH:2020:6Ob195/19a

44 WAGNER, B., “Governing Internet Expression: How Public and Private Regulation Shape Expression Governance”, *Journal of Information Technology and Politics*, vol. 10, núm. 4, 2013, pp. 389-403, p. 399.

45 MILLS, A., “The law applicable to cross-border defamation on social media: whose law governs free speech in “Facebookistan”?”, *Journal of Media Law*, vol. 7, núm. 1, 2015, pp. 1-35, p. 13.

bación del RSD, la regulación de las órdenes contra contenido difamatorio quedaba limitada a la referencia del art. 18 DCE, así como a las leyes nacionales complementarias<sup>46</sup>. Y pese a que estas compartían límites comunes<sup>47</sup>, como la prohibición de búsqueda general del art. 15 DCE (actual art. 8 RSD) o la aplicación de la CDFUE<sup>48</sup>, divergían de manera significativa. Sobre este particular, el régimen nacional aplicable a las órdenes podía encontrar diferencias considerables en función del país.

Primero de todo, el contenido podía ser considerado difamatorio en un Estado miembro y lícito en otro. Asimismo, la CDFUE nunca ha constituido un impedimento para que las legislaciones nacionales emitieran órdenes en sentido contrario ante un mismo contenido. De hecho, ni siquiera el TJUE ha guiado la ponderación de los derechos en juego con base en la CDFUE<sup>49</sup>, como sí ha hecho en otras materias<sup>50</sup> —aunque sea de forma insatisfactoria<sup>51</sup>—. De otro lado, no debe perderse de vista que, incluso en el supuesto de que el contenido fuera concebido como difamatorio en distintos Estados al mismo tiempo, las legislaciones de estos diferían en gran medida en aspectos relacionados con la prueba del daño, la causalidad o la cuantificación de la compensación económica<sup>52</sup>.

En resumidas cuentas, las legislaciones nacionales aplicables a las órdenes de actuación contra contenidos difamatorios presentaban diferencias significativas.

## 2. El estado de las cuestiones internacional privatistas de las órdenes con anterioridad al RSD

El carácter transfronterizo de las órdenes, junto con su regulación nacional, otorgaban un inquestionable protagonismo a las cuestiones esenciales del Derecho Internacional privado: el

---

46 En el caso español, la ley de transposición de la DCE (Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico) no se pronunció sobre esta cuestión, tal y como afirma DE MIGUEL ASENSIO, P. A., *Derecho Privado de Internet*, 5.ª ed., Thomson Reuters Aranzadi, Pamplona, 2015, versión en línea. Ante esta ausencia, la doctrina y la jurisprudencia nacionales consideraron que las órdenes de actuación contra contenidos difamatorios quedaban subsumidas bajo el sistema general, que comprendería la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, junto con el art. 9.2 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Así lo confirma CORDERO ÁLVAREZ, C. I., *Litigios internacionales sobre difamación y derechos de la personalidad: adaptado a la LO 7/2015*, Dyckinson, Madrid, 2015, pp. 59, 209 y 257.

47 CORDERO ÁLVAREZ, C. I., *Litigios internacionales sobre difamación y derechos de la personalidad...*, *op.cit.*, pp. 257 y ss.

48 A este respecto debe mencionarse el ap. 60 de la STJUE de 26 de febrero de 2013, *Melloni*, C-399/11, ECLI:EU:C:2013:107: “el artículo 53 de la Carta confirma que, cuando un acto del Derecho de la Unión requiere medidas nacionales para su ejecución, las autoridades y tribunales nacionales siguen estando facultados para aplicar estándares nacionales de protección de los derechos fundamentales, siempre que esa aplicación no afecte al nivel de protección previsto por la Carta, según su interpretación por el Tribunal de Justicia, ni a la primacía, la unidad y la efectividad del Derecho de la Unión”.

49 RAUCHEGGER, C y KUCZERAWY, A. “Injunctions to remove illegal content online...”, *op.cit.*, p. 1516.

50 STJUE de 27 de marzo de 2014, *UPC Telekabel*, C-314/12, ECLI:EU:C:2014:192

51 HUSOVEC, M., *The Principles of the Digital Services Act*, *op.cit.*, pp. 90-91 y VAN DER DONK, B. B. E., “How dynamic is a dynamic injunction?...”, *op.cit.*, pp. 611-615.

52 CORDERO ÁLVAREZ, C. I., *Litigios internacionales sobre difamación y derechos de la personalidad...*, *op.cit.*, p. 261.

tribunal competente para dictar la orden, el alcance territorial de la misma, la ley aplicable encargada de precisar si el contenido era difamatorio o no, y su eficacia extraterritorial. Resolver estas cuestiones resultaba pues indispensable al dictar una orden transfronteriza. Igualmente, constituía una tarea complicada y singularmente crucial, pues permitía entender por qué el funcionamiento de las órdenes antes de la entrada en funcionamiento del RSD no resultaba del todo socialmente deseable.

Ante la relevancia y complejidad de las cuatro cuestiones *iusprivatistas*, resulta sorprendente que las sentencias publicadas sobre el supuesto de hecho analizado no las abordaran de forma explícita, a salvo del alcance territorial<sup>53</sup>. En su lugar, se limitaron a dar por sentados aspectos como el tribunal competente y la ley aplicable, sin concretar qué normas aplicaron para responder a dichos interrogantes. El siguiente epígrafe se ocupará de especular sobre la respuesta que debe ofrecerse en el caso de examen a las cuatro cuestiones planteadas. El punto de partida es que el contenido difamatorio publicado a través de plataformas en línea constituye un ilícito extracontractual —como ocurre en nuestro ejemplo—, aunque en casos excepcionales debiera calificarse de infracción contractual<sup>54</sup>.

#### A) LA COMPETENCIA JUDICIAL INTERNACIONAL

Si, como en nuestro ejemplo, el domicilio del demandado se encuentra en un país de la UE (la demandada es la filial de Facebook domiciliada en Irlanda), el Reglamento (UE) 1215/2012 Bruselas I bis (RB I bis) se ocupa de determinar el órgano competente para dictar una orden contra contenido ilícito, también en materia de difamación<sup>55</sup>.

Dada la no aplicabilidad del art. 24 RB I bis, el tribunal competente para conocer de las órdenes de retirada de contenido difamatorio sería, en primer lugar, el tribunal elegido expresa o tácitamente por las partes (arts. 25 y 26). En este sentido, resulta habitual que plataformas como Facebook introduzcan en sus términos y condiciones normas sobre jurisdicción y ley aplicable en caso de conflicto<sup>56</sup>. No obstante, en el caso de estudio no se puede asumir que existiera un acuerdo de sumisión expresa, pues este argumento pierde validez si la Sra. Glawischnig-Piesczek no era una usuaria de Facebook, en cuyo caso no quedaría vinculada por sus términos y condiciones. Parece que no se puede asumir que en 2016 tuviera perfil de esta red social —ahora no lo tiene—, sobre todo teniendo en cuenta que las sentencias publicadas no aluden a este extremo.

53 Conviene aclarar que el sistema de información legal oficial austriaco (*Rechtsinformationssystem des Bundes* (RIS)) no publica con carácter general las sentencias de primera y segunda instancia, tal y como ocurre con el caso de la Sra. Glawischnig-Piesczek, salvo error por nuestra parte. En consecuencia, la referencia que en el trabajo se haga a las “sentencias publicadas” no incluirá las sentencias de primera y segunda instancia, sino tan solo las dos emitidas por el Tribunal Supremo austriaco antes y después de la solución prejudicial ofrecida por la STJUE *Glawischnig-Piesczek*, así como esta última.

54 CORDERO ÁLVAREZ, C. I., *Litigios internacionales sobre difamación y derechos de la personalidad...*, *op.cit.*, pp. 237-240.

55 Ap. 83 STUE de 17 de octubre de 2017, *Bolagsupplysningen*, C-194/16, ECLI:EU:C:2017:766

56 Por ejemplo: <https://es-la.facebook.com/legal/terms/>, último acceso el 23 de marzo de 2025.

Descartada la sumisión, serían alternativamente competentes los siguientes tribunales.

- i) El tribunal del Estado miembro donde radique el domicilio del demandado (art. 4) (Irlanda), que permitiría al demandante solicitar la orden y, además, la indemnización de la totalidad del daño sufrido. Sin embargo, en materia de derechos de la personalidad, este foro no suele resultar atractivo para la víctima, pues el daño reputacional no se produciría en aquel Estado, sino en el que radica su vida<sup>57</sup>.
- ii) El tribunal del Estado miembro donde se produzca el hecho dañoso, que en materia “*delictual o cuasidelictual*” (art. 7.2) —precepto al que se debe acudir en los ilícitos extracontractuales como el analizado<sup>58</sup>—, permitiría litigar ante el “*órgano jurisdiccional del lugar donde se haya producido o pueda producirse el hecho dañoso*”. En lo relativo a los daños en derechos de la personalidad a través de internet, el TJUE ha aplicado la “teoría de la ubicuidad”, interpretando que por “lugar del daño” deben entenderse todos los siguientes, cuyos tribunales serán alternativamente competentes<sup>59</sup>:

Primero. El lugar de origen del daño, que sería aquel donde se ha producido el hecho causante del daño. En materia de plataformas en línea, se ha adaptado la STJUE *Shevill* C-68/93<sup>60</sup>, dictada en materia de contenido editorial, para equiparar este lugar al de establecimiento del emisor de los contenidos<sup>61</sup>.

En supuestos como el analizado, en el que se consideró a la plataforma responsable —por hecho propio— por el contenido difamatorio, el lugar de origen del daño se corresponde con el lugar de establecimiento de la plataforma responsable<sup>62</sup> (Irlanda). Sin perjuicio de ello, el lugar de origen del daño no suele resultar relevante en la práctica, puesto que a menudo coincide con el lugar del domicilio del demandado del art. 4<sup>63</sup> —como ocurre en el caso—. Y este solapamiento se resolvería a favor de

57 FERACI, O., “Digital Rights and Jurisdiction: The European Approach to Online Defamation and IPRs Infringements”, en CARPANELLI, E. y LAZZERINI, N. (eds.), *Use and misuse of new technologies: contemporary challenges in international and European law*, Springer International Publishing AG, Cham, Switzerland, 2019, pp. 277-304, p. 284.

58 PALAO MORENO, G., “Responsabilidad civil y Derecho Internacional Privado”, en CLEMENTE MEORRO, M. y COBAS COBIELLA, M.E., *Derecho de Daños*, Tirant lo Blanch, Valencia, 2021, pp. 2007-2078, p. 2017, y ÁLVAREZ RUBIO, J.J., “Jurisdicción, competente y ley aplicable en materia de difamación y protección de los derechos de la personalidad”, *AEDIPr*, t. XI, 2011, pp. 89-118, p. 100.

59 Sin detenernos en detalle en esta cuestión, así se deriva de la STJUE *Mines de potasse d’Alsace*, 21-76, la STJUE *Shevill* C-68/93 y la STJUE *eDate Advertising*, C-509/09 y C-161/10. Para más detalle, véase ÁLVAREZ RUBIO, J.J., “Jurisdicción, competente y ley aplicable...”, pp. 101-108.

60 Aps. 23-24 STJUE de 7 de marzo de 1995, *Shevill*, C-68/93, ECLI:EU:C:1995:61

61 CORDERO ÁLVAREZ, C. I., *Litigios internacionales sobre difamación y derechos de la personalidad...*, *op.cit.*, pp. 142-143.

62 Tal y como afirma CARBAJO CASCÓN, se trataría de una responsabilidad indirecta en virtud de la cual el prestador de la plataforma en línea es sancionado porque ha contribuido a difundir el ilícito cometido por otro sujeto. Para más detalle, véase CARBAJO CASCÓN, F., “La responsabilidad de las plataformas digitales por infracciones a derechos de la personalidad”, en CARBAJO CASCÓN, F. y CURTO POLO, M.M., *Derecho Digital y Mercado*, Tirant lo Blanch, Valencia, 2024, pp. 77-133, pp. 127-131.

63 Ap. 26 STJUE *Shevill* C-68/93

este último precepto, que además permitiría solicitar la indemnización del daño sin limitación territorial.

Segundo. El Estado miembro donde se ha producido el resultado del hecho dañoso, que es aquel donde el hecho causal “ha producido sus efectos dañosos en relación con las víctimas”<sup>64</sup>. En materia de contenidos ilícitos en Internet, el TJUE ha confirmado que es lugar del daño todo aquel desde el que se pueda acceder al contenido ilícito<sup>65</sup>, con independencia de que la víctima sea conocida en ese estado y de que en ese país se haya accedido efectivamente al contenido (efecto mosaico)<sup>66</sup>.

A la luz de lo anterior, y ante el alcance global de Internet, los tribunales de cualquier Estado miembro tendrían competencia bajo el art. 7.2 siempre que el daño haya tenido lugar en él<sup>67</sup>, pero solo para ordenar la reparación de la parte del daño que se hubiera materializado dentro de su jurisdicción, no el daño en su totalidad<sup>68</sup>. En el mismo sentido, debe añadirse que los tribunales que solo estén habilitados para conocer del daño producido bajo su jurisdicción tampoco tienen capacidad para ordenar la retirada de un contenido ilícito debido a “la naturaleza ubicua de los datos y los contenidos puestos en línea en un sitio de Internet y de que el alcance de su difusión es, en principio, universal”<sup>69</sup>. El resultado final es que los tribunales del lugar del hecho dañoso no serán competentes para dictar una orden de retirada, salvo que ostenten competencia con base en algún otro foro<sup>70</sup>.

Tercero. Los tribunales del lugar del centro de intereses de la víctima<sup>71</sup>, que se equipara<sup>72</sup> al lugar donde la víctima ha sufrido un mayor daño reputacional<sup>73</sup>. Si bien suele corresponderse con su residencia habitual, puede también manifestarse en cualquier otro que refleje el centro de gravedad de su vida<sup>74</sup>. El tribunal de este lugar (Austria)

64 Ap. 28 STJUE *Shevill* C-68/93

65 Ap. 46 STJUE *eDate Advertising* C-509/09 y C-161/10

66 CARRASCOSA GONZÁLEZ, J. *The Internet – Privacy and rights relating to personality*, Volumen 378 Recueil des cours Académie de Droit International de La Haye. The Hague: Martinus Nijhoff, 2016, p. 337. Una fuerte crítica al efecto mosaico se encuentra en BIZER, A., “International Jurisdiction for Violations of Personality Rights on the Internet: Bolagsupplysningen”, *Common Market Law Review*, núm. 55, 2018, pp. 1941-1957, pp. 1950-1952.

67 Aps. 21 a 26 y ap. 36 STJUE *Wintersteiger*, C-523/10.

68 Ap. 33 STJUE *Shevill* C-68/93.

69 Ap. 48 STJUE, *Bolagsupplysningen*, C-194/16.

70 Con base en la STJUE de 21 de diciembre de 2021, *Gtflifx Tv*, C-251/20, ECLI:EU:C:2021:1036, así lo confirma también DE MIGUEL ASENSIO, P. A., Derechos de la personalidad y reputación en medios digitales transfronterizos, *Derecho Privado y Constitución*, núm. 40, 2022, pp. 171-205, p. 187.

71 Aps. 48 a 50, STJUE *eDate Advertising* C-509/09 y C-161/10.

72 CARRASCOSA GONZÁLEZ, J. *The Internet – Privacy and rights relating to personality*, *op.cit.*, p. 363.

73 Si bien en un primer momento el TJUE se pronunció sobre este foro de conexión en materia de derechos de la personalidad, también se ha pronunciado más recientemente sobre la (im)posibilidad de aplicarlo en infracciones relacionadas de propiedad intelectual. Véase HESS, B., “The Protection of Privacy in the Case of Law of the Court of Justice of the European Union”, en HESS B y MARIOTTINI, C. (eds.), *Protecting Privacy in International and Procedural Law and by Data Protection European and American Developments*, 2015, Baden-Baden: Ashgate-Nomos, pp. 81-113, pp. 95-99.

74 HÖRNLE, J. *Internet Jurisdiction Law and Practice*. Oxford: Oxford University Press, 2021, p. 374.

será competente con independencia de que se pueda acceder al contenido y de que la víctima tenga reputación en ese estado<sup>75</sup>, y tendría potestad para conocer de la acción de cesación e indemnizatoria, esta vez, por la totalidad del daño<sup>76</sup>.

- iii) El foro cautelar (art. 35), interpretado juntamente con la ya expuesta STJUE *Bolagsupplysningen* C-194/16<sup>77</sup>, que permitiría solicitar una orden de retirada como medidas cautelares ante los tribunales que tengan competencia para conocer de la totalidad del fondo del asunto (Irlanda o Austria), siempre y cuando sus leyes nacionales lo permitan.
- iv) El foro del codemandado (art. 8.1), que posibilitaría demandar conjuntamente al usuario autor del contenido y a la plataforma en el lugar del domicilio de cualquiera de ellos (Austria o Irlanda), siempre que ambos estén domiciliados en un Estado miembro<sup>78</sup>, y que ello resulte oportuno para evitar sentencias contradictorias si se les juzgara por separado. Sin embargo, esta no suele ser una situación muy común, pues se suele solicitar la retirada a la plataforma precisamente cuando el usuario es anónimo o ilocalizable.

De acuerdo con lo señalado, la competencia para dictar la orden de retirada correspondería, alternativamente, a distintos tribunales: los tribunales de Irlanda, por ser lugar del domicilio del demandado (art. 4 RB I bis), o Austria, por constituir el lugar del centro de intereses de la víctima (art. 7.2 RB I bis)<sup>79</sup>. En el caso concreto, la Sra. Gławischnig-Piesczek optó por ejer-

---

75 Sobre el particular, debe matizarse que la STJUE *Mittelbayerischer Verlag* C-800/19 pareció sugerir que el centro de intereses de la víctima tan solo sería un foro competente si el contenido potencialmente difamatorio permite identificar a la víctima demandante, ya sea directa o indirectamente. La razón justificativa fue la falta de previsibilidad y seguridad jurídica que podría acarrear una solución distinta. Sin embargo, voces doctrinales admitieron que, en realidad, este requisito ya se encontraba implícito en la jurisprudencia anterior del TJUE relacionada (STJUE *eDate Advertising* C-509/09 y C-161/10), pero no hubo necesidad de explicitarlo porque los demandantes estuvieron desde el primer momento identificados. Para una interpretación y crítica más detallada sobre la referida sentencia, véase ÁLVAREZ GONZÁLEZ, S., “Una nueva, provisional y discutible delimitación de la competencia judicial internacional en materia de atentados a los derechos de la personalidad”, *La Ley Unión Europea*, núm. 95, 2021, pp. 1-15.

76 Al respecto, debe traerse a colación una diferencia significativa. En materia de acción de responsabilidad por daños, la STJUE *eDate Advertising* C-509/09 y C-161/10 no condiciona la posibilidad de que el foro del centro de intereses de la víctima conozca de la totalidad del daño causado, pudiendo pronunciarse sobre todo este con independencia del lugar donde se haya manifestado (ap. 52). Por el contrario, en materia de acción de cesación de contenidos ilícitos, la STJUE *Gławischnig-Piesczek* somete el alcance territorial global de la orden a la coherencia entre las normas de la UE y del derecho internacional, lo cual deberá ser concretado por el Estado miembro competente (aps. 51 y 52).

77 Para más detalle sobre los hechos y la discusión de la sentencia, véase BIZER, A., “International Jurisdiction for Violations of Personality Rights on the Internet: Bolagsupplysningen”, *Common Market Law Review*, núm. 55, 2018, pp. 1941-1957.

78 HEREDIA CERVANTES, I., “Artículo 8”, en PÉREZ-LLORCA, J.P., *Comentario al Reglamento (UE) n.º 1215/2012 relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil: Reglamento Bruselas I refundido*, Aranzadi, Cizur Menor (Navarra), 2016, versión en línea.

79 A esta misma conclusión llega BIZER, A., “International Jurisdiction for Violations of Personality Rights on the Internet: Bolagsupplysningen”, *Common Market Law Review*, núm. 55, 2018, pp. 1941-1957, p. 1957.

citar la acción, también como medida cautelar, en Austria, por ser la jurisdicción de su centro de intereses principal. Así lo confirmó posteriormente el abogado general del caso<sup>80</sup>.

Con todo, las opciones aparentemente disponibles a la luz del RB I bis eran plurales, lo cual ocasionaba una intolerable imprevisibilidad a Facebook (contraria al cdo. 16 RB I bis), a quien predecir el tribunal competente le resultaba complicado hasta que la demandante no lo eligiera<sup>81</sup>. En realidad, dicha imprevisibilidad se debe a la falta de adaptación del RB I bis al entorno digital, en el que los daños no se pueden ubicar geográficamente<sup>82</sup>. Por el momento, ha sido el TJUE el que ha ido intentando adaptar el RB I bis a la realidad de Internet. Sin embargo, ya se ha visto que las soluciones no han devenido del todo satisfactorias. Frente a esta problemática, las propuestas doctrinales han resultado vastas y diversas<sup>83</sup>, defendiéndose una simplificación del sistema de foros competentes e incluso la creación de un auténtico *forum actoris* digital<sup>84</sup>.

## B) EL ALCANCE TERRITORIAL

Una vez analizados los tribunales competentes para dictar la orden, debe precisarse el alcance territorial con que la pueden emitir. A efectos aclaratorios, implica determinar en qué países puede el tribunal competente ordenar la supresión. Se trata de una cuestión que, pese a su relevancia, ni está regulada en la ley, ni ha llamado demasiado la atención de la doctrina<sup>85</sup>.

Ante la ausencia de regulación legal, la respuesta a aquel interrogante se encuentra en la jurisprudencia del TJUE, traducida en pronunciamientos tardíos y discordantes. La primera sentencia fue la STJUE *Google LLC C-507/17* que, aunque dictada a propósito del derecho al

80 Ap. 84 Opinión AG Spuznar *Glawischnig-Piesczek*.

81 En el mismo sentido y para más detalle, véase PALAO MORENO, G., *Responsabilidad civil extracontractual en el derecho europeo*, Tirant lo Blanch, Valencia, 2008, p. 349.

82 LINDROOS-HOVINHEIMO, S., “Jurisdiction and personality rights – in which Member State should harmful online content be assessed?”, *Maastricht Journal of European and Comparative Law*, vol. 29, núm. 2, 2022, pp. 201-214, 204.

83 A título de ejemplo, algunas voces doctrinales propugnan una solución multilateral (SVANTESSON, D. J. B. y SYMEONIDES, S. C. “Cross-border internet defamation conflicts and what to do about them: Two Proposals”. *Journal of Private International Law*. 2023, vol. 19, núm. 2, 137-185) o una solución de cooperación transnacional que implique a actores públicos y privados (LA CHAPELLE, B. y FEHLINGER, P., “Jurisdiction on the Internet...”, *op.cit.*). Otros defienden el criterio del *targeting*, que otorgaría competencia en exclusiva al Estado en que la actividad ilícita tenga intención de provocar efectos (SCHULTZ, T. “Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface”. *The European Journal of International Law*. 2008, vol. 19, núm. 4, 799-839), si bien se ha criticado porque esta cuestión es difícil de demostrar en internet (OSTER, J., “Rethinking *Shevill*. Conceptualising the EU private international law of Internet torts against personality rights”, *International Review of Law, Computers and Technology*, vol. 26, núms. 2-3, 2016, pp. 113-128, p. 118).

84 Destaca, al respecto, CASTELLÓ PASTOR, J.J., “Por un foro de competencia judicial internacional para favorecer al vulnerable de los comportamientos lesivos a los derechos de la personalidad en internet”, en BLASCO GARCÍA, A. I. (dir.), *Protección multidisciplinar del vulnerable en la sociedad digital*, Cizur Menor (Navarra), Aranzadi, pp. 37-80, pp. 75-76.

85 SVANTESSON, J. B., *Solving the Internet Jurisdiction Puzzle*, Oxford University Press, Oxford, 2017, p. 171.

olvido, puede resultar orientativa en nuestro caso difamatorio<sup>86</sup>. En esencia, el TJUE concluyó que el alcance territorial de las órdenes destinadas a restringir contenido ilícito debe equivaler a la totalidad de la UE o solo a un Estado miembro según la legislación en la materia esté armonizada o no, respectivamente (ap. 66). Excepcionalmente, la orden podría gozar de un alcance mundial (ap. 72), acentuándose en este caso la importancia de una correcta ponderación entre derechos y la consideración de las diferencias de regulación entre los distintos Estados (aps. 59-60).

Sin embargo, poco después el TJUE abandonó esa postura y decidió cambiar de enfoque en materia de difamación. En particular, la siguiente —y última— sentencia que pronunció en materia de alcance territorial de órdenes contra contenidos difamatorios fue, precisamente, la STJUE *Glawischnig-Piesczek*. Contra todo pronóstico —incluso contra el del Abogado General<sup>87</sup>—, en dicha sentencia el Tribunal de Luxemburgo optó por un planteamiento abierto y escueto, limitándose a reconocer que la Directiva de comercio electrónico “no limita en modo alguno, en particular territorialmente, el alcance de las medidas que los Estados miembros pueden adoptar” (ap. 49).

De este modo, el alcance global de la orden no está prohibido por la DCE y será una cuestión que dependerá de la legislación nacional, que a la hora de determinarlo deberá tener en cuenta “la coherencia de las normas de la Unión en ese ámbito con las normas aplicables a nivel internacional” (aps. 49-52). Por supuesto, se trata de una solución que añade más ambigüedad e impredecibilidad al destinatario de una orden, toda vez que su alcance territorial de aquella no podrá conocerse hasta que lo concrete el tribunal competente.

En el caso de estudio, el tribunal austriaco consideró que para proteger el derecho al honor de la Sra. Glawischnig-Piesczek era necesario ordenar la retirada del contenido difamatorio no solo en Austria sino a nivel mundial<sup>88</sup>, en consonancia con la legislación austriaca (ley aplicable).

### C) LA LEY APLICABLE

De todas las cuestiones internacional privatistas, la determinación de la ley aplicable al fondo del asunto es la que goza de mayor relevancia práctica, pues será la que determine si existe o no una vulneración del derecho al honor y, en caso afirmativo, las consecuencias de esta.

En los supuestos relativos a las obligaciones extracontractuales transfronterizas, los tribunales de los Estados miembros concretan la ley aplicable a través de normas de conflicto armonizadas a nivel europeo en el Reglamento (CE) 864/2007 Roma II (en adelante, Roma II)<sup>89</sup>. Sin embargo, las obligaciones extracontractuales derivadas de los derechos de la personalidad

86 STJUE de 24 de septiembre de 2019, *Google LLC*, C-507/17, ECLI:EU:C:2019:772.

87 Ap. 100 Opinión AG Spuznar *Glawischnig-Piesczek*.

88 FJ 5.º OGH *Glawischnig-Piesczek*, núm. 6Ob195/19a

89 Reglamento (CE) n.º 864/2007 del Parlamento Europeo y del Consejo, de 11 de julio de 2007, relativo a la ley aplicable a las obligaciones extracontractuales («Roma II»). *DO L* 199, de 31 de julio de 2007.

quedaron desde el principio excluidas del ámbito de aplicación del citado instrumento por falta de acuerdo sobre el criterio de conexión (art. 1.2.g) Roma II)<sup>90</sup>. La consiguiente ausencia<sup>91</sup> provoca que los tribunales de cada Estado miembro deban concretar la ley aplicable a dichos supuestos según sus normas nacionales de Derecho Internacional privado.

En el supuesto de hecho, el tribunal competente radicaba en Austria, y debía aplicar sus normas nacionales de conflicto para determinar la ley aplicable. A diferencia de España, donde las normas de esta disciplina no están codificadas, el Estado austriaco cuenta con una Ley de Derecho Internacional privado desde 1978<sup>92</sup>. Esta no prevé una norma de conflicto específica para vulneraciones de derechos de la personalidad, debiéndose subsumir en la norma conflictual sobre obligaciones extracontractuales.

Según el art. 48.2 del mencionado instrumento, la ley que debe aplicar el tribunal austriaco sería la ley elegida por las partes y, en su defecto, la ley del lugar donde se haya producido la conducta causante del daño. No obstante, si las partes están más vinculadas a otro país, se aplicaría la ley de este último.

Con respecto a la existencia de un pacto sobre la ley aplicable entre las partes, aunque Facebook suele incorporar en sus términos y condiciones una cláusula en este sentido, no se puede presumir que exista un pacto sobre la ley aplicable, haciendo aquí extensivo el razonamiento que se expuso más arriba.

Ante esta ausencia, el tribunal austriaco acabó aplicando la ley austriaca al fondo del asunto, probablemente por ser Austria el lugar donde se había producido la conducta causante del daño. Pese a que la determinación de este lugar puede resultar compleja, es posible que se siguiera la línea jurisprudencial austriaca consistente en equipararlo al lugar de la residencia habitual de la víctima. Así lo confirma CORDERO ÁLVAREZ, que atribuye la siguiente afirmación a la jurisprudencia austriaca: “incluso en aquellos sistemas nacionales en los que no se prevé expresamente este criterio [lugar del daño], la práctica generalizada en este tipo de litigios permite afirmar que en la mayoría de los supuestos el tribunal termina aplicando la ley del Estado de residencia habitual de la víctima como concreción del *locus delicti comissi*”<sup>93</sup>.

Al final, la ley austriaca fue la encargada de precisar que el contenido controvertido vulneró el derecho al honor y de concretar los medios de tutela de la víctima, incluyendo la acción de cesación. En particular, la normativa austriaca reguladora de aquellas cuestiones comprendía

---

90 Según el Anexo de Roma II, la intención del legislador de la UE era armonizar la norma de conflicto aplicable a los derechos de la personalidad más adelante, en concreto, “a más tardar en diciembre de 2008”, lo cual supondría hacerlo tan solo un año después de la aprobación de Roma II. Sin embargo, dicha reforma todavía no ha tenido lugar.

91 Para más información sobre el motivo de exclusión, véase ÁLVAREZ RUBIO, J.J., “Jurisdicción, competente y ley aplicable en materia de difamación y protección de los derechos de la personalidad”, *AEDIPr*, t. XI, 2011, pp. 89-118, pp. 112-116.

92 Gesetz über das internationale Privatrecht – IPR-Gesetz. *Bundesgesetzblatt*, 15 Juni 1978, Nr. 304

93 CORDERO ÁLVAREZ, C. I., *Litigios internacionales sobre difamación y derechos de la personalidad...*, *op.cit.*, p. 367.

el art. 1330 del Código Civil General<sup>94</sup>, el art. 78 de la Ley de Propiedad Intelectual<sup>95</sup> y el art. 18.1 de la Ley de comercio electrónico<sup>96</sup>.

Sin duda, Facebook se encontraba de nuevo en una situación de impredecibilidad. La existencia de 27 normas de conflicto nacionales distintas<sup>97</sup>, en vez de una única para el conjunto de la UE, provocaba que hasta que no conociera el tribunal competente, no podía predecir el derecho aplicable que determinaría si se le podría obligar a retirarlo.

Frente a este escenario, que obstaculiza la consolidación del mercado interior, tanto el legislador europeo como la doctrina llevan exigiendo una armonización conflictual europea desde que Roma II la aplazara (art. 30.2)<sup>98</sup>. Ante la urgencia de reforma, las iniciativas de nuevo han sido múltiples, oscilando desde mantener la situación invariable hasta una armonización material. De todas ellas, debemos mostrar nuestro apoyo a la presentada por el Comité de asuntos extrajeros del Parlamento Europeo de mayo de 2012, que apuesta por aplicar la ley del lugar de residencia habitual de la víctima, siempre que no exista otra más vinculada con el caso. Propuesta que, pese a sus ventajas<sup>99</sup>, no salió adelante<sup>100</sup>.

Aun así, conviene poner de relieve que, en enero de 2025, la Comisión Europea emitió un informe en el que evalúa por primera vez la aplicación del Reglamento Roma II desde 2009<sup>101</sup>, y en el que admite que la mayoría de los Estados miembros defienden la incorporación de los litigios relacionados con los derechos de la personalidad en el ámbito de aplicación del Reglamento. Aunque esta realidad esté cada vez más cerca, el Informe también admite la dificultad de seleccionar un punto de conexión que equilibre todos los intereses en juego<sup>102</sup>.

---

94 *Allgemeines Bürgerliches Gesetzbuch, Bundesgesetzblatt*, 1 Januar 1812, Nr. 1.

95 *Urheberrechtsgesetz, Bundesgesetzblatt*, 9 März 1936, Nr. 111.

96 *E-Commerce-Gesetz, Bundesgesetzblatt*, 21 Dezember 2001, Nr. 152.

97 Las normas de conflicto nacionales en materia de derechos de la personalidad suelen aplicar puntos de conexión distintos o, incluso aplicando los mismos, es posible que los interpreten de forma distinta. CORDE-RO ÁLVAREZ, C. I., *Litigios internacionales sobre difamación y derechos de la personalidad...*, *op.cit.*, pp. 323-324 y SAKOLCIOVÁ, S., “Defamation on social media – challenges of Private International Law”, *Bratislava Law Review*, vol. 5, núm. 1, 2021, pp. 121-134, p. 126.

98 PALAO MORENO, G., “El Reglamento Roma II y el sistema español de Derecho internacional privado: primeras impresiones y algunas reflexiones para el debate”, en *El agua como factor de cooperación y de conflicto en las relaciones internacionales contemporáneas (XXII Jornadas de la Asociación Española de Profesores de Derecho Internacional y Relaciones Internacionales)*, Instituto Euro Mediterráneo del Agua, Murcia, 2009, pp. 411-434, p. 414, y MILLS, A., “The law applicable to cross-border defamation on social media...”, *op.cit.*, pp. 13-17.

99 MEIER, F.M., “Unification of choice-of-law rules for defamation claims”, *Journal of Private International Law*, vol. 12, núm. 3, 2016, pp. 492-520, pp. 514-515.

100 Para más información sobre la conveniencia de armonizar las normas de conflicto a nivel europeo, véase PALAO MORENO, G., *Responsabilidad civil extracontractual en el derecho europeo*, *op.cit.*, pp. 172 y ss.

101 Informe de la Comisión Europea, de 31 de enero de 2025, sobre la aplicación del Reglamento (CE) n.º 864/2007, relativo a la ley aplicable a las obligaciones extracontractuales (Reglamento Roma II), COM(2025) 20 final.

102 *Ídem*, p. 7.

## D) RECONOCIMIENTO Y EJECUCIÓN

En nuestro caso, el punto de partida es que tras la sentencia de primera instancia el demandado ya bloqueó el acceso a los comentarios lesivos en Austria<sup>103</sup>, y es probable que también a nivel mundial<sup>104</sup>, deviniendo innecesario su reconocimiento y ejecución forzosa en otro estado. Para conseguirlo, lo más verosímil es que retirara el contenido directamente del servidor en el que lo almacenaba, que por razones de cumplimiento normativo (principalmente, RGPD<sup>105</sup>) es probable que fuera alguno de los servidores de la plataforma en Europa, que radican en Irlanda, Suecia y Dinamarca<sup>106</sup>.

Pese a lo anterior, no podemos dejar de realizar algunas precisiones en materia de reconocimiento y ejecución, que serían por supuesto hipotéticas. Deben diferenciarse dos escenarios.

- i) Si Facebook no hubiera retirado los comentarios en algún país de la UE, la Sra. Glawischnig-Piesczek debería instar el reconocimiento y ejecución de la resolución en los Estados miembros que considere. El régimen aplicable sería el RB I bis, que a diferencia del Reglamento Roma II, no excluye la vulneración de derechos de la personalidad de su ámbito de aplicación. Si bien parte de un reconocimiento y ejecución automáticas —sin *exequatur*—, salvo que concurra alguna de las causas excepcionales de denegación de los arts. 45 y 52, es posible que los Estados miembros debieran adaptar sus sistemas para lograr la ejecución<sup>107</sup>.

Así las cosas, lo más idóneo sería instar la ejecución en el país de la UE donde, habiendo incumplido Facebook su obligación de supresión, esté ubicado el servidor en el que la plataforma almacena el contenido controvertido. Con un único procedimiento se podría obligar a Facebook a suprimir el contenido a nivel mundial. Aunque más arriba se intentó adivinar en qué país está el servidor en cuestión (Suecia e Irlanda), este lugar es totalmente imprevisible al estar por completo desligado de la controversia<sup>108</sup>. Al final, si por ello la solicitud de ejecución se acaba realizando en un Estado distinto al del lugar del servidor que almacena el contenido, solo se podría conseguir el bloqueo en ese Estado miembro, pero no en el resto<sup>109</sup>. Bajo estas cir-

103 Ap. 15 STJUE *Glawischnig-Piesczek*.

104 SUZOR, N. P., *Lawless. The Secret Rules That Govern Our Digital Lives*, *op.cit.*, p. 85.

105 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 (Reglamento general de protección de datos). *DO* L 119 de 4 de mayo de 2016.

106 <https://datacenters.atmeta.com/europe-es/>, último acceso el 23 de marzo de 2025.

107 HESS, B., “Protecting Privacy by Cross-border Injunction”, *Rivista di Diritto Internazionale Privato e Processuale*, vol. 55, núm. 2, 2019, pp. 284-301, p. 295.

108 CARRASCOSA GONZÁLEZ, J. *The Internet – Privacy and rights relating to personality*, *op.cit.*, p. 369.

109 Con base en la interpretación que la STJUE de 12 de abril de 2011, *DHL Express France C-235/09 ECLI:EU:C:2011:238* (ap. 59) vierte sobre el art. 39 RB I bis, LUNDSTED confirma que el reconocimiento y la ejecución de la orden dictada por un tribunal de un Estado miembro se puede solicitar en otro Estado miembro (p. ej. el de establecimiento) aunque el contenido en cuestión esté almacenado en un servidor localizado fuera de la UE. LUNDSTED, L., “Putting Right Holders in the Centre: Bolagsupplysningen and

cunstances, alcanzar la supresión en todos los Estados miembros requeriría ejecutar la sentencia en cada uno de ellos por separado, lo cual supondría un coste inasumible.

- ii) Distinta habría sido la situación en que los comentarios difamatorios no hubieran sido retirados por Facebook en Estados terceros. En este caso, el régimen de reconocimiento y ejecución, en defecto de convenio internacional, depende de las normas nacionales del Estado tercero. Tomando como ejemplo a Estados Unidos —donde se encuentran la mayoría de los servidores de Facebook—, allí la libertad de expresión goza de una protección constitucional superior a la de los derechos de la personalidad<sup>110</sup>. En consecuencia, sería altamente probable que el país denegara la ejecución de la resolución judicial austriaca<sup>111</sup>, como ya ha ocurrido con otras soluciones provenientes de tribunales europeos en el ámbito digital (p. ej. una sentencia californiana sobre Yahoo rechazó el reconocimiento de una sentencia francesa, tal y como explica SVANTESSON<sup>112</sup>).

### **3. Una breve y crítica recapitulación**

A modo de síntesis, la aplicación de las normas de Derecho Internacional privado al supuesto de la Sra. Glawischnig-Piesczek permitió responder a los aspectos de Derecho Internacional privado en el siguiente sentido: el tribunal competente radicaba en Austria, el alcance territorial fue global, y la ley aplicable al fondo fue la austriaca.

Precisamente, esta solución resulta plenamente ilustrativa de la problemática que acompañaba a las órdenes de actuación contra contenidos difamatorios con anterioridad al Reglamento de Servicios Digitales. En particular, tras ella subyacen dos fuertes problemas que, sin embargo, ninguno de los tribunales implicados en el caso apreció.

La primera problemática está relacionada con el alcance global de la orden. El tribunal austriaco estimó oportuno que los comentarios difamatorios se debían eliminar no solo en Austria, sino a nivel global, en consonancia con la tendencia promulgada por tribunales de todo el mundo<sup>113</sup>. De este modo, el contenido se eliminó también en países como Estados Unidos, donde los comentarios probablemente serían perfectamente lícitos, dada la fuerte protección constitucional otorgada al derecho al honor.

---

Iljan (C-194/16): What Does It Mean for International Jurisdiction over Transborder Intellectual Property Infringement Disputes?”, *IIC*, núm. 49, 2018, pp. 1022-1047, p. 1038.

110 SVANTESSON, D. J. B., “Recent developments in Private International Law applicable to the Internet”, *Journal of Internet Law*, diciembre, 2011, pp. 26-35, p. 32.

111 En este contexto, ha habido autoridades que han confirmado la dificultad de eliminar el material ilegal alojado en el extranjero en ausencia de cooperación por parte del proveedor de alojamiento de datos. Véase ICF, GRIMALDI STUDIO LEGALE y 21C CONSULTANCY, “Overview of the legal framework...”, *op.cit.*, pp. 113 y ss.

112 SVANTESSON, D. J. B., “Recent developments in Private International Law...”, *op.cit.*, pp. 32-33.

113 SUZOR, N. P., *Lawless. The Secret Rules That Govern Our Digital Lives*, *op.cit.*, p. 85.

En otras palabras, el alcance global de una orden de retirada trae como resultado la protección del derecho de una persona en Austria (derecho al honor), y al mismo tiempo la restricción ilegítima de derechos de personas ubicadas en terceros Estados (libertad de expresión). De ahí que haya autores que defiendan una “postura comedida” de estas decisiones<sup>114</sup>, si bien se ha argumentado que, en casos como el expuesto, permitir la retirada en toda la Unión Europea sería como mínimo necesaria<sup>115</sup>.

El segundo de los problemas tenía que ver con la impredecibilidad que las normas de Derecho Internacional privado crean cuando se aplican al ámbito digital. Tal y como hubo ocasión de detallar, la Sra. Glawischnig-Piesczek, ante la multiplicidad de foros competentes, podía solicitar la retirada del contenido no solo ante los tribunales de un Estado miembro, sino ante los de distintos, que en este caso se reducían a Irlanda y Austria. A su vez, la determinación del tribunal competente era clave para delimitar la ley aplicable al fondo del asunto, pues la norma de conflicto en materia de difamación es nacional y, en consecuencia, los criterios para la determinación de la ley aplicable varían de un foro competente a otro.

De lo anterior se deriva que, hasta que la demandante no eligiera el tribunal competente, el demandado, Facebook, no podía predecir ni el tribunal competente ni, por extensión, la ley aplicable que determinaría la ilicitud del contenido y el éxito de la acción de cesación. Por supuesto, esta impredecibilidad provocada por la potencial aplicación de leyes nacionales distintas a nivel mundial ocasionaba una fuerte incertidumbre jurídica a Facebook, traducida en costes. Con el propósito de reducirla, el riesgo era que Facebook acabara anticipándose a este tipo de decisiones, adaptando para ello sus términos y condiciones globales a la ley nacional que fuera más restrictiva de la libertad de expresión.

Lejos de ser impensable, este riesgo constituye un fenómeno común entre las plataformas en línea. Se bautizó como “censura colateral” (*collateral censorship*) y de él se pueden encontrar múltiples ejemplos en Internet, como la prohibición de las imágenes de desnudos<sup>116</sup>. De forma simple, el concepto implica que las plataformas en línea aplican de forma voluntaria los estándares de la ley nacional que sea más restrictiva, de modo que eliminan globalmente todo aquel contenido que, aunque sea lícito, puede parecer mínimamente ilícito con base a una sola ley nacional, evitando así consecuencias legales como las órdenes de actuación contra contenidos ilícitos. En la misma línea, se ha sugerido que las plataformas adoptan sus propios estándares a nivel global, dejando de lado las exigencias legales salvo riesgo elevado de incumplimiento<sup>117</sup>.

---

114 MORENO BLESA, L., “La retirada de contenidos ilícitos por los prestadores de servicios en línea”, *THÉMIS Revista de Derecho*, núm. 79, 2021, pp. 73-86, p. 83.

115 HESS, B., “Protecting Privacy by Cross-border Injunction”, *op.cit.*, p. 291.

116 Este alcance global es explicado por la plataforma Facebook en sus términos y condiciones: “Facebook restringe la exhibición de desnudos y actividad sexual para no importunar a determinados sectores de nuestra *comunidad global* con una especial sensibilidad ante este tipo de contenido, en particular, por su contexto cultural o su edad” (énfasis añadido). <https://www.facebook.com/business/help/725672454452774?id=208060977200861>, último acceso el 23 de marzo de 2025.

117 GOANTA, C., BERTAGLIA, T. y IAMNITCHI, A., “The Case for a Legal Compliance API for the Enforcement of the EU’s Digital Services Act on Social Media Platforms”, *Proceedings of the 2022 AC; Conference on Fairness, Accountability and Transparency, Seoul, 2022*, pp. 1341-1349, p. 1342.

Al final, ya fuera por una decisión judicial con alcance global, ya fuera por una decisión voluntaria de las plataformas ejerciendo la censura colateral, existía el riesgo de que los estándares nacionales de la ley más protectora de un derecho (derecho al honor) se expandieran globalmente a otros países, aun cuando dicho derecho no fuera objeto de una protección tan elevada en aquellos, pudiendo así vulnerar ilegítimamente derechos de terceros (libertad de expresión). En sentido más abstracto, el riesgo era que Internet pasara a permitir en exclusiva el contenido que cumpliera con las leyes de todos los países, eliminando la multiculturalidad<sup>118</sup> y provocando conflictos entre Estados soberanos<sup>119</sup>.

A la luz de lo anterior, el caso práctico seleccionado es perfectamente representativo de la problemática suscitada por las órdenes de actuación contra contenidos difamatorios con anterioridad al RSD. En resumen, la complejidad de las normas de Derecho Internacional privado era responsable del funcionamiento ineficaz de las órdenes: además de resultar demasiado gravosas para su destinatario (imprevisibilidad), podían acabar vulnerando ilegítimamente derechos de terceros (censura y censura colateral).

#### **IV. LAS ÓRDENES DE ACTUACIÓN EN EL REGLAMENTO DE SERVICIOS DIGITALES**

Veinte años después de la DCE, el legislador de la UE ha abordado por primera vez las órdenes de actuación contra contenidos ilícitos en el RSD. En particular, se ha servido del art. 9 RSD —que no deroga el art. 18 DCE— con el fin de facilitar el cumplimiento de las órdenes transfronterizas, cuya problemática suscitada hasta el momento y expuesta con anterioridad admite conocer. Así lo explica de forma clara el cdo. 31 RSD, al estipular que el RSD debe facilitar la efectividad, la eficiencia y el cumplimiento de las órdenes transfronterizas, reduciendo las “cargas desproporcionadas” de los destinatarios y “sin afectar indebidamente a los derechos e intereses legítimos de terceros”.

La cuestión que surge es, por tanto, si realmente el art. 9 RSD constituye un avance en la materia, mejorando el funcionamiento de las órdenes transfronterizas de actuación. Para responder a este interrogante, primero se analizará el art. 9 RSD en detalle, para más tarde poner de relieve los avances que la nueva regulación representa con respecto a la anterior a la luz del caso *Glawischnig-Piesczek*.

##### **1. El ámbito de aplicación del art. 9 RSD**

El primer paso para analizar el art. 9 RSD es comprobar que las órdenes judiciales de actuación dirigidas a las plataformas en línea contra contenidos difamatorios se encuentran dentro

---

118 SVANTESSON, J. B., *Solving the Internet Jurisdiction Puzzle*, *op.cit.*, p. 214.

119 GEIST, M., “The *Equustek* Effect: A Canadian Perspective on Global Takedown Orders in the Age of the Internet”, en FROSIO, G. (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, Oxford, 2020, pp. 709-726, p. 726

del ámbito de aplicación de aquel precepto. En esta línea, los requisitos que deben cumplir las órdenes para quedar bajo el art. 9 RSD son los tres siguientes.

- i) En primer lugar, desde el punto de vista material, deben ser órdenes cuyo objetivo sea ordenar una actuación contra uno o varios elementos concretos de contenido ilícito. Deben realizarse tres precisiones al respecto.

Primero, las órdenes deben referirse a uno o varios elementos específicos de contenido ilícito, pues una solución opuesta vulneraría la prohibición de búsqueda general del art. 8 RSD. En realidad, este aspecto ya era exigido por el art. 15 DCE. Ahora, la novedad es que el art. 9.2.a.iv exige expresamente que la orden incluya “*uno o varios URL exactos y, en su caso, información adicional*”. Con ello, se pretenden evitar órdenes que acaben imponiendo una obligación desproporcionada al destinatario consistente en identificar de forma autónoma nuevos contenidos ilícitos. Es posible que el TJUE deba pronunciarse sobre la interpretación de la última coetilla de “*información adicional*” para dilucidar el grado de concreción que requiere. En este sentido, la STJUE *Glawischnig-Piesczek* puede servir de inspiración, pues su ap. 45 exige que la autoridad emisora de la orden identifique elementos concretos (p. ej. nombre de la víctima o circunstancias de la infracción).

Segundo, el objetivo de las órdenes debe consistir en ordenar la “*actuación*” contra el contenido ilícito, pudiendo tener cabida dentro de esta expresión tanto la retirada del contenido como su bloqueo, pero no medidas que vayan más allá, como pudiera ser la suspensión de la cuenta del usuario<sup>120</sup>. En sentido más amplio, de una interpretación *sensu contrario* se deriva que las órdenes del art. 9 RSD no pueden tener como finalidad el restablecimiento de un contenido eliminado erróneamente por un prestador de servicios intermediarios (falsos positivos). Pese a ello, el RSD reconoce que el derecho nacional puede prever este tipo de órdenes de restablecimiento y las acoge favorablemente por considerarlas necesarias para respetar el derecho a la tutela judicial efectiva (cdo. 39).

Para finalizar, conviene dilucidar qué se entiende por contenido ilícito. En este sentido, el art. 3.h) RSD, siguiendo la línea de la Recomendación 2018/334<sup>121</sup>, evita ofrecer una definición, limitándose a aplicar el principio de que es ilícito en línea todo aquello que lo es fuera de línea según las leyes de la UE o nacionales (cdo. 12 RSD). Este precepto, consonante con el principio “*procedure before substance*” que se predica del RSD<sup>122</sup>, provoca que la definición de contenido difamatorio se mantenga intacta: continúa siendo nacional y distinta de un país a otro.

- ii) El segundo requisito exigido por el art. 9 RSD es que las órdenes sean vinculantes y no meras recomendaciones. Ello exige que exista una base legal que active el po-

120 WILMAN, F., KALĀDA, S. L., LOEWENTHAL, P. *The EU Digital Services Act*. Oxford: Oxford University Press, 2024 p. 83

121 Recomendación (UE) 2018/334 de la Comisión, de 1 de marzo de 2018, sobre medidas para combatir eficazmente los contenidos ilícitos en línea, *DO L 63*, de 6 de marzo de 2018

122 ORTOLANI, P., “Moderation made in Europe...”, *op.cit.*, p. 6.

der sancionador estatal otorgándole competencias para dictar la orden vinculante<sup>123</sup>. Igual que ocurría con el art. 18 DCE, el art. 9 RSD no constituye el fundamento para dictar una orden de actuación contra el contenido ilícito, sino que será la ley de la UE o nacional aplicable la que determine, no solo la ilicitud del contenido, sino también si la orden tiene cabida o no (cdos. 31, 32 y 34 RSD).

- iii) En tercer lugar, el art. 9 RSD exige que las órdenes sean dictadas por autoridades nacionales judiciales o administrativas, si bien en materia de difamación en España solo son competentes las primeras. Bajo este marco, se discute si las autoridades competentes pueden solo ser nacionales o también de la UE. En este sentido, una interpretación literal del art. 9.1 RSD y del cdo. 31 conduce a considerar que solo se admiten las primeras.

A mayor abundamiento, parece difícil concebir la emisión de este tipo de órdenes por autoridades de la UE. Por ejemplo, aunque los arts. 51.2.b) y 73.3 RSD otorgan competencia a los coordinadores de servicios digitales y a la Comisión Europea para dictar órdenes por medio de las que obliguen a cesar infracciones, estas no pueden equipararse a las órdenes del art. 9 RSD, pues aquellas se prevén para garantizar el cumplimiento de las obligaciones instauradas por el RSD, entre las que no se incluye la eliminación del contenido considerado ilícito por una ley nacional. Ello no quita que, si la plataforma en línea destinataria de la orden incumple con las exigencias impuestas por el art. 9 RSD, pueda ser objeto de medidas de ejecución públicas como las mencionadas en los arts. 51.2.b) o 73.3 RSD.

Por último, y sin perjuicio de todo lo anterior, las órdenes del art. 9 RSD, igual que las previstas en el art. 18 DCE, se pueden dirigir contra cualquier prestador de servicios intermediarios, con independencia de que se eximan o no de responsabilidad por el contenido cuya restricción se solicita. Si no se pueden eximir de responsabilidad, se les puede exigir cualquier cosa — también las órdenes del art. 9 RSD—<sup>124</sup>, y si la exención sí resulta aplicable, los arts. 4.3, 5.2 y 6.4 RSD permiten dirigir a los intermediarios órdenes como las del art. 9 RSD, emitidas por una autoridad con la finalidad de poner fin o impedir una infracción. De hecho, HUSOVEC considera que el art. 9 RSD constituye un ejemplo de las órdenes dictadas al amparo de aquellos preceptos<sup>125</sup>.

Siguiendo con los prestadores de servicios intermediarios como destinatarios de la orden y en consonancia con el amplio ámbito de aplicación territorial del RSD<sup>126</sup>, conviene aclarar que estos pueden estar establecidos tanto en un Estado miembro de la UE como en un tercer Estado. Pero en este último caso, habría primero que garantizar que la autoridad emisora tenga competencia para obligar al demandado establecido en un tercer Estado; cuestión que, al estar

---

123 HUSOVEC, M., *The Principles of the Digital Services Act*, *op.cit.*, p. 153.

124 HUSOVEC, M., *Injunctions against intermediaries in the European Union...*, *op.cit.*, p. 59.

125 HUSOVEC, M., *The Principles of the Digital Services Act*, *op.cit.*, p. 146.

126 Distanciándose de la DCE, el RSD se aplica a cualquier prestador de servicios intermediarios que dirija sus servicios a los usuarios digitales situados en la UE, con independencia del lugar de establecimiento de aquel (arts. 2, 3 y cdos. 7, 8 y 15). En términos prácticos, el RSD y sus significativas obligaciones se exigirán a cualquier servicio intermediario establecido en la UE (p. ej. Facebook Ireland), pero también fuera de la UE cuando sea ofrecido a los usuarios europeos (p. ej. Wikipedia).

el demandado domiciliado fuera de la UE, no se resolvería por el RB I bis, sino por la normativa convencional o nacional (en España, art. 22 quinqués LOPJ<sup>127</sup>).

En resumidas cuentas, se puede afirmar que las órdenes judiciales transfronterizas de actuación contra contenidos difamatorios concretos dirigidas a una plataforma en línea establecida en la UE quedan dentro del ámbito de aplicación del art. 9 RSD. Por consiguiente, si la orden solicitada por la Sra. Glawischnig-Piesczek se hubiera dictado con posterioridad al 17 de febrero de 2024, se le debería haber aplicado el art. 9 RSD.

## 2. El contenido del art. 9 RSD

A diferencia de la mayoría de los preceptos del RSD, que gozan de armonización plena, el art. 9 adopta un enfoque de armonización mínima (cdo. 31 RSD)<sup>128</sup>, limitándose a sentar requisitos mínimos que deben cumplir las órdenes subsumidas en su ámbito de aplicación. Como consecuencia, la base legal y la regulación de las órdenes de actuación siguen siendo de carácter nacional incluso tras el art. 9 RSD. La única novedad de este precepto es que, con independencia de cuál sea el derecho aplicable, las órdenes deberán cumplir ciertos requisitos mínimos, referidos a aspectos de derecho tanto sustantivo como conflictual.

### A) ARMONIZACIÓN SUSTANTIVA

Las exigencias mínimas de derecho sustantivo con las que deben cumplir las órdenes del art. 9 RSD se pueden clasificar en tres grupos: requisitos de fondo, requisitos de forma y requisitos de comunicación. Téngase en cuenta que solo los requisitos de comunicación resultan aplicables al prestador destinatario de la orden, mientras que los dos primeros quedarán a cargo de la autoridad emisora, que deberá cumplirlos a más tardar en el momento en que transmita la orden al intermediario destinatario (cdo. 35 RSD).

#### a) *Requisitos de fondo*

Las órdenes del art. 9 RSD deben incorporar el contenido mínimo señalado en el art. 9.2.a), que incluye los siguientes extremos.

- i) El fundamento jurídico sobre el que se dicta la orden, así como la base jurídica que explica la ilicitud del contenido.
- ii) La identidad de la autoridad emisora—incluyendo los datos de su punto de contacto (cdo. 35)— y, en su caso, de la autoridad a la que el prestador de servicios intermediario debe notificar el curso dado a la orden.

---

127 Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. BOE núm. 157, de 2 de julio de 1985 (última versión de 5 de agosto de 2024).

128 WILMAN, F., KALĀDA, S. L., LOEWENTHAL, P., *The EU Digital Services Act*, *op.cit.*, p. 18.

- iii) La identificación del contenido ilícito concreto —URL e información adicional—.
- iv) Información sobre los medios de recurso disponibles tanto para el prestador de servicios intermediario como para el usuario digital que ha proporcionado el contenido controvertido.

Estos medios de recurso, que están previstos en la legislación nacional o europea, no solo incluyen los recursos judiciales sino también los mecanismos administrativos de gestión de reclamaciones, que podrán ser desarrollados o explicados por los Coordinadores de servicios digitales nacionales en sus respectivos Estados miembros (cdo. 39 RSD). Sin embargo, no se deben entenderse incluidos los medios de solución extrajudicial de los arts. 20 y 21 RSD, a los que solo se podría acudir tras una restricción del contenido acometida por el intermediario en línea de forma voluntaria, pero no obligada<sup>129</sup>.

*b) Requisitos de forma*

El art. 9.2.c) regula la lengua en que deben dictarse las órdenes, ofreciendo tres alternativas. En primer lugar, las autoridades nacionales pueden dictar la orden en cualquiera de las lenguas que el prestador de servicios intermediarios a quien vaya dirigida la orden haya especificado públicamente conforme al art. 11.3 RSD.

En segundo lugar, la orden también se puede emitir en la lengua acordada bilateralmente por la autoridad emisora y el prestador de servicios intermediario destinatario, siempre y cuando sea una lengua oficial de un Estado miembro (cdo. 35).

Por último, si la orden no está redactada en ninguna de las dos lenguas anteriores, la autoridad nacional deberá acompañarla de una traducción a cualquiera de las dos. No obstante, la traducción no se exige de la totalidad de la orden, sino tan solo de los requisitos de fondo más arriba expuestos. Esta limitación podría desembocar en situaciones absurdas en las que se traduzca la orden de forma parcial, solo en los aspectos exigidos por el art. 9 RSD, que no incluyen algunos como el plazo para la retirada del contenido ilícito. Ahora bien, cabe pensar que estos supuestos serían ínfimos, sobre todo si se emplean herramientas informáticas en la traducción de las órdenes, para las que traducir tan solo parte de ellas puede resultar más complejo.

*c) Requisitos de comunicación*

Una vez el intermediario destinatario de la orden la recibe, este se enfrenta a dos exigencias. Además de contar con la obligación de actuar contra el contenido ilícito siguiendo las indicaciones de la orden, el art. 9 RSD le impone la obligación de comunicarla a distintos sujetos, tanto públicos (art. 9.1) como privados (art. 9.5).

---

129 Ídem., p. 98.

Así, por un lado, el intermediario debe informar a la autoridad emisora de la orden o a la autoridad que en su caso se haya especificado en ella del curso que le haya dado a la orden y de cuándo lo haya hecho (art. 9.1). Se trata de una obligación de respuesta, que según algunos, constituye el principal objetivo del art. 9 RSD<sup>130</sup>.

La comunicación intermediario-autoridad debería realizarse “sin dilación indebida”, es decir, en los plazos que establezca el derecho nacional que ha servido de base para dictar la orden (cdo. 33). Tras esta comunicación, la autoridad receptora debe transmitirla, junto con la orden, al coordinador de servicios digitales de su Estado miembro (art. 9.3), quien deberá enviar una copia al resto de coordinadores de servicios digitales (art. 9.4).

Por otro lado, el prestador de servicios intermediario destinatario de la orden también debe comunicarla, a más tardar cuando se dé curso (cdo. 34), a los destinatarios del servicio afectados por la misma (art. 9.5). Dentro de esta categoría debe necesariamente incluirse al usuario digital que ha proporcionado el contenido cuya retirada se requiere (art. 9.2.a) —si bien puede resultar difícil localizarlo si es anónimo—, y probablemente también al destinatario del servicio que solicitó la orden. Por el contrario, no parece razonable incardinar al resto de destinatarios del servicio afectados de forma más indirecta por la restricción del contenido. Ello desembarcaría en un exceso de obligaciones de comunicación que sobrecargaría a las plataformas, que es lo que precisamente quiere evitar el RSD (cdo. 31 RSD).

Por último, el art. 9.5 RSD exige que la orden comunicada al usuario digital afectado cumpla con los requisitos del art. 9.2, que incluye los requisitos de fondo y de forma antes expuestos. Sin embargo, esta exigencia no se reproduce en los arts. 9.1, 9.3 y 9.4 RSD. Esta diferencia no debe interpretarse en el sentido de que solo la orden que se transmita a los afectados, y no la dirigida a las autoridades, debe cumplir con los mínimos del art. 9.2. Por el contrario, en ambos casos la orden que se comunique debe incorporar dichas condiciones; se trata de una misma y única orden, transmitida a dos sujetos distintos.

## B) ARMONIZACIÓN CONFLICTUAL

Al haber tomado conciencia de la creciente relevancia y problemática suscitada por las órdenes transfronterizas, lo lógico habría sido que el art. 9 RSD se hubiera pronunciado sobre dichos interrogantes, muchos de los cuales hubo ocasión de exponer con anterioridad. Más bien al contrario, el precepto los deja al margen (cdo. 31). Aun así, pueden encontrarse algunas referencias —mínimas— a cuestiones de Derecho Internacional privado, que a continuación se discuten.

### a) *El alcance territorial de las órdenes*

Se anticipó que el cdo. 31 RSD estipula que el alcance territorial de las órdenes del art. 9 RSD no está regulado por el RSD, sino por el Derecho de la UE o nacional aplicable que sirva de

---

130 HUSOVEC, M., *The Principles of the Digital Services Act*, *op.cit.*, p. 146.

base para dictarlas (cdo. 36). Con todo, el art. 9.2.b) RSD establece un límite al alcance territorial de la orden: que no se exceda del estrictamente necesario para alcanzar su objetivo, de conformidad con todo el Derecho de la UE y el derecho nacional, incluyendo la CDFUE y los principios generales del derecho internacional.

El mencionado art. 9.2.b) debe interpretarse según el cdo. 36 RSD, del que se deriva que la regla general debería ser que el alcance territorial de las órdenes se circunscriba al territorio de la autoridad emisora. De este modo, las órdenes serían con carácter general de bloqueo y no de retirada<sup>131</sup>. Y solo cabría extender el alcance territorial en dos supuestos: o bien cuando la ilicitud del contenido provenga de una norma del Derecho de la UE, de forma que su eliminación en toda la UE sea aconsejable, o bien cuando la autoridad emisora lo estime pertinente teniendo en cuenta el Derecho de la UE, el Derecho Internacional y los intereses de la cortesía internacional.

Así las cosas, la elevación de estos límites jurisprudenciales a rango legal debe valorarse positivamente al poner fin a una jurisprudencia vacilante<sup>132</sup>. Sin embargo, la reforma es insuficiente. Habrá ocasión de argumentar que habría sido preferible una solución más ambiciosa de carácter vinculante.

#### *b) La coordinación con otras normas*

Junto con el alcance territorial, la coordinación del art. 9 RSD con otros instrumentos legales es el otro aspecto internacional privatista atendido por la nueva normativa europea. En concreto, la coordinación se prevé tanto respecto de instrumentos tanto nacionales como de la UE.

En cuanto a las normas de corte nacional, es posible que regulen órdenes cuyo ámbito de aplicación coincida total o parcialmente con las previstas en el art. 9 RSD, en consonancia con el enfoque de armonización mínima adoptado por este. Para estos supuestos, el art. 9.6 RSD establece que “*Las condiciones y los requisitos establecidos en el presente artículo se entenderán sin perjuicio del Derecho procesal penal y civil nacional*”. Según el cdo. 34, el solapamiento entre los requisitos del art. 9 RSD y los que pudiera establecer el derecho procesal nacional, aun cuando sean compatibles, debería resolverse a favor de este último.

El resultado de interpretar en este sentido el art. 9.6 RSD y el cdo. 34 RSD permitiría que los Estados miembros se desvíen de los requisitos del art. 9 RSD, eliminando su efecto armonizador. Por consiguiente, debemos mostrar nuestra conformidad con aquel sector doctrinal que, con base en una interpretación teleológica, rechaza la literalidad del cdo. 34 y propone concebir el art. 9.6 RSD como un límite al derecho procesal nacional<sup>133</sup>. Ello significa que,

---

131 DE MIGUEL ASENSIO, P.A., “Obligaciones de diligencia y responsabilidad de los intermediarios: el Reglamento (UE) de Servicios Digitales”, *La Ley Unión Europea*, núm. 109, 2022, pp. 1-47, p. 15.

132 PALAO MORENO, G., “Las órdenes de actuación contra contenidos ilícitos en el nuevo reglamento europeo de servicios digitales”, en CASTELLÓ PASTOR, J. J. (dir.), *Análisis del reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, Cizur Menor (Navarra), 2024, pp. 109-134, p. 134

133 WILMAN, F., KALÁDA, S. L., LOEWENTHAL, P., *The EU Digital Services Act*, *op.cit.*, pp. 98 y 100.

cuando los requisitos del derecho procesal nacional sean compatibles con los del art. 9 RSD, se deberán aplicar ambos de forma conjunta. Por el contrario, los Estados miembros no podrán imponer a las órdenes que estén bajo la aplicación del art. 9 RSD requisitos contrarios a este precepto, salvo que el RSD lo permita.

Con respecto a la coordinación entre el art. 9 RSD y otros instrumentos de la UE, conviene recordar que las órdenes del art. 9 RSD se aplican a todo tipo de ilícitos, mientras que al mismo tiempo existen otras normas europeas dedicadas a regular las órdenes en sectores específicos. Lo anterior puede desembocar en solapamientos entre los ámbitos de aplicación de unas y otras órdenes. Con arreglo al cdo. 34, ello ocurre con “el Reglamento (UE) 2021/784, el Reglamento (UE) 2019/1020 o el Reglamento (UE) 2017/2394”, y también con “otros actos de la Unión que establecen sistemas similares de actuación contra determinados tipos de contenidos ilícitos”, dentro de los que debemos considerar incluidas las ya mencionadas Directivas en materia de derechos de autor.

Para resolver los mencionados solapamientos, la literalidad del cdo. 34 exige entender que el art. 9 RSD se aplica “sin perjuicio” de dichas regulaciones. En el mismo sentido que antes, los requisitos previstos en el art. 9 RSD deben añadirse a los instaurados en las regulaciones sectoriales si son compatibles. En cambio, si se contradicen, deberían prevalecer las normas sectoriales frente al RSD por el principio de *lex specialis*.

Bajo el paraguas de la compatibilidad entre el RSD y otras normas europeas, es destacable que el cdo. 38 RSD aborde la complementariedad entre el art. 9 RSD y el principio de control en origen del art. 3 DCE. Según el citado considerando, exigir desde otro Estado miembro tan solo la restricción de un contenido ilícito no limita la libertad de los prestadores de servicios intermediarios. Dicho de otro modo, el art. 3 DCE no se aplica a las órdenes del art. 9 RSD<sup>134</sup>, pese a que hay quien sostiene que esta exclusión debería analizarse caso por caso<sup>135</sup>.

### 3. El incumplimiento de las condiciones del art. 9 RSD

Por su parte, surge la cuestión de qué ocurre en caso de que las órdenes previstas en el art. 9 RSD no cumplan con los requisitos previstos por el precepto.

A este respecto, debe primero descartarse la interpretación de aquellos que consideran que el art. 9 RSD no es vinculante y se limita a representar “cómo debe ser una buena orden”<sup>136</sup>, pudiendo la autoridad emisora elegir si aplicar o no el precepto en cuestión a las órdenes que emita. Pese a que esta conclusión se deriva necesariamente del tenor literal del art. 9 RSD, así como de su falta de coordinación con el art. 6.4 RSD, una aplicación voluntaria del precepto obstaculizaría su objetivo armonizador<sup>137</sup>. Por consiguiente, debemos abogar por su carácter

---

134 PALAO MORENO, G., “Las órdenes de actuación contra contenidos ilícitos...”, *op.cit.*, p. 129.

135 HUSOVEC, M., *The Principles of the Digital Services Act*, *op.cit.*, p. 152.

136 *Ídem*, p. 153.

137 WILMAN, F., KALĀDA, S. L., LOEWENTHAL, P., *The EU Digital Services Act*, *op.cit.*, p. 98.

vinculante: siempre que se dicte una orden que se halle bajo el ámbito de aplicación del art. 9 RSD, debería cumplir sus exigencias.

Sentado lo anterior, debemos enfrentarnos a las consecuencias de incumplir sus exigencias. Conviene recordar que parte de los requisitos del art. 9 RSD se exigen al prestador de servicios intermediarios destinatario de la orden, y la otra parte a la autoridad nacional que la emite. Habida cuenta de que el ámbito de aplicación subjetivo del RSD queda restringido a los primeros, tan solo los incumplimientos de estos quedan regulados por el RSD. En este marco, habría que distinguir dos supuestos.

Por un lado, si la plataforma en línea retira el contenido señalado por la orden, podría ocurrir que posteriormente no comunique su cumplimiento a la autoridad pertinente o a los usuarios digitales afectados, o lo comunique, pero sin los elementos mínimos del art. 9.2 RSD. En estos supuestos, estaríamos ante un incumplimiento de obligaciones exigidas por el RSD, de modo que se activarían sus mecanismos de supervisión y ejecución del Cap. IV, que pueden ser de tutela jurídico-pública<sup>138</sup> o jurídico-privada<sup>139</sup>.

Por otro lado, si la plataforma no restringe el contenido ilícito, necesariamente adquiere conocimiento efectivo del mismo. Al no retirarlo, no se podría aplicar la exención de responsabilidad del art. 6 RSD, debiendo la ley aplicable dilucidar si la plataforma es responsable. A su vez, el incumplimiento del art. 9 RSD activaría los mecanismos de tutela del Cap. IV RSD.

#### **4. Los avances del art. 9 RSD a la luz del caso *Glawischnig-Piesczek***

Si la Sra. Glawischnig-Piesczek se hubiera enfrentado a la misma situación fáctica tras la entrada en funcionamiento del RSD, es posible que antes de acudir a los órganos judiciales, aquella se hubiera servido de los mecanismos de tutela de los arts. 16, 20 y 21 RSD para lograr la retirada del contenido de forma más rápida y económica<sup>140</sup>. Aun así, si el caso hubiera escalado a los tribunales, el RSD ha incorporado un precepto específico dedicado a mejorar el funcionamiento de las órdenes que emiten (art. 9 RSD).

A tal efecto, los principales cambios que sufriría la orden dirigida contra Facebook, agrupados en función del encargado de implementarlos, habrían sido los siguientes.

---

138 El coordinador de servicios digitales del lugar de establecimiento de la plataforma —o del representante si está fuera de la UE—, o la Comisión Europea si la plataforma es de muy gran tamaño (art. 56 RSD), tras realizar una investigación (arts. 51.1 y 66 RSD), podrían ordenarle que cumpla con el contenido del art. 9 RSD (arts. 52.2.b) y 73 RSD) e imponerle multas (arts. 52.2.c) RSD y 74), y multas coercitivas hasta que cumpla (art. 52.2.d) RSD).

139 Las víctimas del incumplimiento del art. 9 RSD, que serían los usuarios digitales afectados por la orden, también tendrían vías para instar el cumplimiento. Podrían interponer una reclamación administrativa ante el coordinador de servicios digitales de su establecimiento para activar los mecanismos de supervisión pública del RSD (art. 53 RSD), así como solicitar una indemnización de daños y perjuicios ante los tribunales (art. 54 RSD).

140 En el supuesto práctico, antes de acudir a los tribunales, la demandante solo pudo servirse de un mecanismo de notificación y acción ofrecido de forma voluntaria y sesgada por Facebook. Por el contrario, el RSD obliga a Facebook a implementar aquel mecanismo con garantías mínimas.

## A) NOVEDADES PARA LA AUTORIDAD EMISORA

Según el art. 9 RSD, la autoridad emisora de la orden, que en el caso fue el Tribunal de lo Mercantil de Viena, tiene la obligación de identificar el contenido difamatorio a retirar mediante el URL exacto, así como la información adicional pertinente.

Igualmente, el tribunal austriaco debería incorporar en la orden los extremos del art. 9.2.a). Ahora bien, resulta lógico pensar que la mayoría de ellos ya formaban parte de las órdenes con anterioridad al RSD, siendo tal vez la única novedad los datos del punto de contacto de la autoridad emisora. Como se decía, el resto del contenido mínimo exigido (fundamento jurídico de la orden y de la ilicitud del contenido, identidad de la autoridad emisora, identificación del contenido cuya retirada se ordena y vías de recurso) ya estaba incorporado en las órdenes emitidas antes del RSD por así exigirlo un proceso con todas las garantías<sup>141</sup>.

En cuanto al idioma de la orden, es probable que tampoco represente un cambio antes y después del art. 9 RSD. Con carácter previo, la regulación europea relativa al traslado y notificación de documentos judiciales (tanto el Reglamento (CE) 1393/2007 vigente al dictar la STJUE *Glawischnig-Piesczek* (art. 4.3)<sup>142</sup>, como el posterior Reglamento (UE) 2020/1784 que lo derogó (art. 8.2)<sup>143</sup>) exigía que la notificación de un documento judicial a una parte establecida en otro Estado miembro fuera acompañada de una traducción a la lengua oficial de ese Estado miembro. En consecuencia, la orden que dictó el Tribunal de lo Mercantil de Viena, aun redactada en alemán, tuvo que ser acompañada de una traducción al inglés por ser esta la lengua oficial del lugar donde está establecido el demandado Facebook Ireland. Si la orden se dictara bajo el RSD, el art. 9 RSD conduciría al mismo resultado: el tribunal austriaco transmitiría la orden en alemán y la acompañaría de la traducción al inglés, lengua esta elegida por Facebook para recibir comunicaciones de las autoridades al amparo del art. 11.3 RSD<sup>144</sup>.

Sin embargo, sí constituye una novedad para la autoridad emisora la necesidad de enviar la orden y la información previamente recibida de Facebook al coordinador de servicios digitales austriaco (*Kommunikationsbehörde Austria*).

La última implicación del art. 9 RSD para el tribunal austriaco tendría que ver con el alcance territorial de la orden. En principio, lo debería haber limitado a Austria, salvo que, teniendo en cuenta los principios del Derecho Internacional, considerara que el alcance global era más acertado para preservar el honor de la Sra. Glawischnig-Piesczek (art. 9.2.b) y cdo. 36 RSD). En realidad, el carácter no vinculante del cdo. 36, junto con la vaguedad e imprecisión del art.

---

141 En España, véase arts. 208, 209 y 728 LEC.

142 Reglamento (CE) n.º 1393/2007 del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, relativo a la notificación y al traslado en los Estados miembros de documentos judiciales y extrajudiciales en materia civil o mercantil («notificación y traslado de documentos») y por el que se deroga el Reglamento (CE) n.º 1348/2000 del Consejo. *DO L* 324, de 10 de diciembre de 2007.

143 Reglamento (UE) 2020/1784 del Parlamento Europeo y del Consejo de 25 de noviembre de 2020 relativo a la notificación y traslado en los Estados miembros de documentos judiciales y extrajudiciales en materia civil o mercantil («notificación y traslado de documentos»). *DO L* 405 de 2 de diciembre de 2020, última rectificación *DO L* 90073 de 2 de febrero de 2024.

144 [https://www.facebook.com/help/678741677600131?ref=spoc&helpref=faq\\_content](https://www.facebook.com/help/678741677600131?ref=spoc&helpref=faq_content), último acceso el 23 de marzo de 2025.

9.2.b), provocan que el tribunal austriaco hubiera podido dictar una orden con exactamente el mismo alcance territorial global que la orden de 2017, siempre que justificara su necesidad.

## B) NOVEDADES PARA EL PRESTADOR DE SERVICIOS INTERMEDIARIO DESTINATARIO

Con respecto al destinatario de la orden (Facebook), la novedad más notoria sería el deber de respuesta que le impone el art. 9 RSD, debiendo comunicar al Tribunal de Viena el curso dado y cuándo lo ha hecho. Asimismo, debería notificar la orden y sus consecuencias a los usuarios digitales afectados. En este caso, serían la Sra. Glawischnig-Piesczek, y el autor del contenido, quien, a la vista de su anonimato, sería difícil de localizar.

## C) EN RESUMEN: MUCHO TEXTO Y POCA MEJORÍA

El ejercicio de someter la orden de retirada impulsada por la Sra. Glawischnig-Piesczek al art. 9 RSD constituye una clara prueba de que las novedades incorporadas por el Reglamento de Servicios Digitales en materia de órdenes de actuación contra contenidos ilícitos no modifican en absoluto su funcionamiento anterior al RSD. Se trata de medidas insignificantes y meramente procedimentales<sup>145</sup>. A lo sumo, las obligaciones de comunicación constituirían la principal novedad, que permitirían difundir la orden a un público más extenso.

Por el contrario, el art. 9 RSD mantiene invariables la base legal y la regulación nacional de las órdenes, así como la respuesta a las cuestiones internacional privatistas. En efecto, guarda silencio sobre la autoridad competente para dictar las órdenes, aplicándose el RB I bis (art. 2.4.h)). En la misma línea, no se hace referencia a ninguna norma de conflicto. Con respecto a la ejecución transfronteriza, el cdo. 32 RSD la excluye del ámbito de aplicación del RSD. Y en el mismo sentido, el art. 9.2 aborda el alcance territorial de las órdenes de forma incompleta.

En definitiva, pese a la considerable extensión del art. 9 RSD —una página en la versión oficial del Diario Oficial de la UE— y de los considerandos 31 a 39 concordantes —más de dos páginas—, el régimen legal de las órdenes de actuación contra contenidos ilícitos se conserva esencialmente intacto tras el RSD. Se mantiene la regulación eminentemente nacional de las órdenes, así como el funcionamiento indeseable de las mismas, que, si se recuerda, en materia de difamación se debe principalmente a la impredecibilidad ocasionada por las normas internacional privatistas, que podrían derivar en una vulneración ilegítima de los derechos de terceros.

## V. CONCLUSIONES Y PROPUESTAS DE SOLUCIÓN

A la luz de lo expuesto, ha quedado patente que las órdenes de actuación contra contenidos ilícitos dirigidas a las plataformas en línea han resultado tradicionalmente imprescindibles para

---

145 SAVIN, A., “The EU Digital Services Act: Towards a More Responsible Internet”, *Copenhagen Business School, CBS LAW Research Paper*, vol. 21, núm. 4, 2021, pp. 1-17, p. 6.

restringir la presencia de contenidos difamatorios en el entorno digital, toda vez que antes de aprobar el Reglamento de Servicios Digitales constituían la única vía legal prevista para alcanzar dicho fin. Sin embargo, en aquel momento, el funcionamiento de las órdenes en materia de difamación distaba de ser eficaz. En particular, las normas de Derecho Internacional privado, cuya aplicación era exigida por un escenario jurídicamente fragmentado, ofrecía respuestas complejas e imprevisibles, que podían desembocar en una orden impredecible y gravosa para el destinatario, y en una posible vulneración ilegítima de derechos de terceros.

El Reglamento de Servicios Digitales, consciente del escenario de desprotección de las víctimas y de la problemática suscitada por aquellas órdenes, ha instaurado nuevas vías de tutela para las víctimas de contenidos ilícitos (p. ej. arts. 16, 20 y 21 RSD) y, junto con ello, ha ofrecido una nueva regulación de las órdenes en el art. 9 RSD. En este contexto, se ha aclarado que la incorporación de nuevos medios de protección no ha eliminado la relevancia de las órdenes, que son todavía cruciales para controlar la moderación de contenidos de las plataformas. Ahora bien, pese a esta importancia innegable, la nueva regulación de las órdenes no ha devenido significativa, al menos en materia de contenidos difamatorios. Por el contrario, mantiene su funcionamiento legal prácticamente invariable, no pudiendo afirmarse que el RSD incremente su eficacia.

A pesar de la incontestabilidad de lo señalado, no se puede concluir que las víctimas de contenidos difamatorios sigan igual de desprotegidas tras el nuevo marco legal de la UE. Habría que analizar en detalle el resto de las herramientas de protección que este incorpora (en especial, el mecanismo de notificación y acción del art. 16 RSD y los medios de solución extrajudicial de los arts. 20 y 21 RSD) con la finalidad de dictaminar si, con ellos, se consigue mejorar la tutela frente a una potencial difamación. Se trata de una cuestión que, no obstante, sería merecedora de otra investigación.

Sentado lo anterior, es turno ahora de proponer las soluciones que debería haber incorporado el RSD para verdaderamente alcanzar su loable objetivo del cdo. 31 RSD, consistente en mejorar el funcionamiento de las órdenes transfronterizas.

En este ambicioso escenario, el punto de partida es que resulta difícil armonizar de forma plena las órdenes de actuación a nivel horizontal, pues para ello sería necesario homogeneizar a su vez los distintos tipos de contenidos ilícitos todavía no armonizados a nivel de la UE. Mientras ello podría ser concebible en un futuro en ciertas materias como el consumo<sup>146</sup>, a nuestro modo de ver no lo sería con relación al contenido difamatorio, que, como se dijo, involucra intereses privados, pero también públicos<sup>147</sup>. Precisamente, es posible que argumentos como este expliquen el enfoque de armonización mínima adoptado por el legislador de la UE de forma excepcional con respecto al art. 9 RSD. En consecuencia, las órdenes transfronterizas contra este tipo de contenidos seguirán involucrando inevitablemente a distintos ordenamientos jurídicos nacionales, debiéndose dar respuesta a las cuestiones del Derecho Internacional privado<sup>148</sup>.

---

146 SAVIN, A., "The EU Digital Services Act: Towards a More Responsible Internet", *op.cit.*, p. 16.

147 También VON DANWITZ, L., "The Contribution of EU Law to the Regulation of Online Speech", *Michigan Technology Law Review*, vol. 27, 2020, pp. 167-211, pp. 193-194.

148 Acerca de la práctica imposibilidad de unificar el régimen sustantivo de las obligaciones extracontractuales, véase PALAO MORENO, G., *Responsabilidad civil extracontractual en el derecho europeo*, *op.cit.*,

Con relación a esta ineludible disciplina, lo idóneo sería reducir la impredecibilidad que acarrea cuando se aplican sus normas genéricas al entorno digital. Sin embargo, somos plenamente conscientes de que ni el RSD es el lugar para acometer dichas reformas, ni —aunque se reclamen— son concebibles por el momento.

Ahora bien, lo anterior no significa que el art. 9 RSD no pudiera haber hecho más por mejorar el funcionamiento de las órdenes. En particular, habría resultado conveniente incorporar una (mínima) armonización material que reste importancia a las soluciones de Derecho Internacional privado, incluyendo para ello un marco de salvaguardias procesales mínimas, tal y como ha señalado algún sector doctrinal<sup>149</sup>.

Estas garantías, además de una mayor transparencia —a la que alude el art. 9.2 RSD—, deberían referirse a aspectos relacionados con la proporcionalidad, eficacia, plazo para dictar las órdenes, efectos suspensivos, legitimación activa o criterios para ponderar los derechos fundamentales en juego. De modo particular, resultaría especialmente oportuno trasladar el contenido del cdo. 36 al art. 9.2.b) RSD para dotarlo de carácter vinculante. Así, su contenido también se tornaría obligatorio, forzando —y no solo sugiriendo— a los tribunales de los Estados miembros a dictar órdenes con un alcance territorial limitado al territorio de su jurisdicción.

En virtud de la propuesta efectuada, aunque la regulación de las órdenes continuaría siendo nacional, los tribunales nacionales seguirían criterios mínimos comunes al dictar las órdenes, reduciéndose la impredecibilidad para los prestadores de servicios intermediarios destinatarios. Podría esgrimirse que esta propuesta de reforma legislativa resultaría excesiva, pudiéndose alcanzar la misma meta si el TJUE —en vez de una ley— se pronunciara en ese sentido. Sin embargo, ya se apuntó que la experiencia demuestra que los estándares mínimos por este dictados a propósito de las órdenes contra contenidos infractores de derechos de autor no han sido seguidos por la jurisprudencia nacional. Ello justifica la necesidad de una reforma de corte legal.

En definitiva, el conjunto de las propuestas anteriores conseguiría que, con independencia de la ley aplicable, existieran unos estándares mínimos comunes en la emisión de órdenes judiciales contra contenidos difamatorios en toda la UE, entre los que se incluiría un alcance territorial limitado. Así se ofrecería una mayor previsibilidad a todas las partes, incluyendo las plataformas en línea, que potencialmente podrían minimizar la aplicación de normativas y valores nacionales a nivel mundial.

---

pp. 250 y ss.

149 HUSOVEC, M., *The Principles of the Digital Services Act*, *op.cit.*, p. 157.

