Recopilación de la Jurisprudencia

CONCLUSIONES DEL ABOGADO GENERAL
SR. MACIEJ SZPUNAR
presentadas el 4 de junio de 2019 [1]

Asunto C-18/18

Eva Glawischnig-Piesczek
contra
Facebook Ireland Limited

[Petición de decisión prejudicial planteada por el Oberster Gerichtshof (Tribunal Supremo de lo Civil y Penal, Austria)]

«Procedimiento prejudicial — Libre prestación de servicios — Directiva 2000/31/CE — Servicios de la sociedad de la información — Responsabilidad de los prestadores de servicios intermedios — Obligación de un prestador de servicios de alojamiento de sitios de Internet (Facebook) de retirar datos ilícitos — Alcance»

I. Introducción

1. «En Internet no se escribe a lápiz, se escribe con tinta», afirma un personaje de una película americana de 2010. Me refiero, no por casualidad, a la cinta *The Social Network*.

2. En efecto, el meollo del presente asunto es si un proveedor de servicios de alojamiento que explota una plataforma de red social en línea puede estar obligado a hacer desaparecer, mediante un borratintas metafórico, determinados contenidos publicados en línea por los usuarios de dicha plataforma.

3. Más concretamente, mediante sus cuestiones prejudiciales, el órgano jurisdiccional remitente solicita al Tribunal de Justicia que precise el alcance personal y material de las obligaciones que pueden imponerse a un prestador de servicios de alojamiento de datos, sin que ello lleve a imponer una obligación general de supervisión, prohibida por el artículo 15, apartado 1, de la Directiva 2000/31/CE. [2] El órgano jurisdiccional remitente también pregunta al Tribunal de Justicia si, en el marco de un requerimiento judicial formulado por un órgano jurisdiccional de un Estado miembro, puede obligarse a un prestador de servicios de alojamiento de datos a retirar ciertos contenidos no solo frente a los internautas de ese Estado miembro, sino también a nivel mundial.

1 Lengua original: francés.

2 Directiva 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 2000, L 178, p. 1).

II. Marco jurídico

A. Derecho de la Unión

4. Los artículos 14 y 15 de la Directiva 2000/31 figuran en la sección 4, titulada «Responsabilidad de los prestadores de servicios intermediarios», del capítulo II de la mencionada Directiva.

5. El artículo 14, apartados 1 y 3, de la Directiva 2000/31, con el título «Alojamiento de datos», dispone:

«1. Los Estados miembros garantizarán que, cuando se preste un servicio de la sociedad de la información consistente en almacenar datos facilitados por el destinatario del servicio, el prestador de servicios no pueda ser considerado responsable de los datos almacenados a petición del destinatario, a condición de que:

a) el prestador de servicios no tenga conocimiento efectivo de que la actividad [o] la información es ilícita y, en lo que se refiere a una acción por daños y perjuicios, no tenga conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito,

   o de que

b) en cuanto tenga conocimiento de estos puntos, el prestador de servicios actúe con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible.

[…]

3. El presente artículo no afectará la posibilidad de que un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados miembros, exijan al prestador de servicios […] poner fin a una infracción o impedirla, ni a la posibilidad de que los Estados miembros establezcan procedimientos por los que se rija la retirada de datos o impida el acceso a ellos.»

6. Según el artículo 15, apartado 1, de la Directiva 2000/31, titulado «Inexistencia de obligación general de supervisión»:

«Los Estados miembros no impondrán a los prestadores de servicios una obligación general de supervisar los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas, respecto de los servicios contemplados en los artículos 12, 13 y 14.»

B. Derecho austriaco

7. A tenor del artículo 18, apartado 1, de la E-Commerce-Gesetz (Ley de Comercio Electrónico), mediante la cual el legislador austriaco transpuso la Directiva 2000/31, los prestadores de servicios de alojamiento de datos no tienen una obligación general de supervisar los datos que almacenan, transmiten o facilitan, ni de realizar por sí mismos búsquedas de hechos o circunstancias que indiquen actividades ilícitas.

8. Conforme al artículo 1330, apartado 1, del Allgemeines Bürgerliches Gesetzbuch (Código Civil General; en lo sucesivo, «ABGB), quien haya sufrido un perjuicio efectivo o un lucro cesante a consecuencia de una lesión a su honor tendrá derecho a exigir una indemnización. En virtud del apartado 2 de dicho artículo, existirá ese mismo derecho cuando alguien difunda hechos que menoscaben la reputación, la situación económica y las perspectivas de futuro de un tercero y cuya falsedad conocía o debía haber conocido. En este caso, también se podrá pedir la rectificación y la publicación de esta.

9. De conformidad con el artículo 78, apartado 1, de la Urheberrechtsgesetz (Ley de Propiedad Intelectual; en lo sucesivo, «UrhG»), no está permitido exponer públicamente ni difundir de otro modo al público imágenes de personas cuando ello vulnere intereses legítimos del interesado o, en caso de haber fallecido este sin haber autorizado ni ordenado la publicación, de un pariente cercano.

III. Hechos y procedimiento principal

10. La Sra. Eva Glawischnig-Piesczek fue diputada del Nationalrat (Cámara Baja del Parlamento, Austria), presidenta del grupo parlamentario Die Grünen («Los Verdes») y portavoz federal de dicho partido.

11. Facebook Ireland Limited, sociedad registrada en Irlanda y con domicilio social en Dublín, es una filial de la sociedad estadounidense Facebook Inc. Facebook Ireland explota una plataforma de red social en línea para los usuarios que se encuentran fuera de Estados Unidos y Canadá, a la que puede accederse a través de la dirección www.facebook.com. Esa plataforma permite a los usuarios crear perfiles y publicar comentarios.

12. El 3 de abril de 2016, un usuario de la citada plataforma compartió en su página personal un artículo recogido en la publicación austriaca en línea *oe24.at* y titulado «Los Verdes: a favor del mantenimiento de unos ingresos mínimos para los refugiados». Mediante esa acción se generó en la citada plataforma una imagen en miniatura del sitio de origen, en la que se incluía el título y un breve resumen del citado artículo, al igual que una fotografía de la demandante. Asimismo, dicho usuario publicó, en relación con ese artículo, un comentario humillante referido a la demandante, tildándola de «miserable traidora al pueblo», «idiota corrupta» y militante de un «partido de fascistas». Cualquier usuario de la plataforma podía acceder a los contenidos publicados por ese usuario.

13. Mediante escrito de 7 de julio de 2016, la demandante solicitó a Facebook Ireland, en particular, que eliminara ese comentario.

14. Como Facebook Ireland no suprimió el comentario controvertido, la demandante interpuso una demanda ante el Handelsgericht Wien (Tribunal de lo Mercantil de Viena, Austria) solicitando que se dictara un auto de medidas provisionales en el que se ordenara a Facebook Ireland que dejara de mostrar o difundir fotografías de la demandante que fueran acompañadas de alegaciones idénticas o de «contenido similar», es decir, que la demandante era una «miserable traidora al pueblo», una «idiota corrupta» y una militante de un «partido de fascistas».

15. El 7 de diciembre de 2016, el Handelsgericht Wien (Tribunal de lo Mercantil de Viena) dictó el auto de medidas provisionales solicitado.

16. A continuación, Facebook Ireland impidió el acceso desde Austria al contenido inicialmente publicado.

17. En fase de apelación, el Oberlandesgericht Wien (Tribunal Superior Regional de Viena, Austria), confirmó el auto dictado en primera instancia en lo tocante a las alegaciones idénticas. Así, dicho tribunal no estimó la pretensión de Facebook Ireland de que se limitaran los efectos del auto de medidas provisionales a la República de Austria. El citado órgano jurisdiccional consideró, en cambio, que la obligación de dejar de difundir alegaciones de contenido similar solamente se refería a aquellas que hubieran sido puestas en conocimiento de Facebook Ireland por la demandante en el litigio principal, por terceros o de cualquier otro modo.

18. Los órganos jurisdiccionales de primera y segunda instancia basaron sus decisiones en el artículo 78 de la UrhG y en el artículo 1330 de la ABGB, al considerar, en particular, que el comentario publicado contenía declaraciones que lesionaban de forma excesiva el honor de la demandante y daba a entender que esta había tenido un comportamiento delictivo sin aportar la más mínima prueba de ello. Además, según dichos tribunales, en lo que respecta a las manifestaciones formuladas contra un político fuera del ámbito de un debate político o de interés general, cualquier referencia al derecho a la libertad de expresión también sería inadmisible.

19. Ambas partes en el procedimiento principal interpusieron un recurso ante el Oberster Gerichtshof (Tibunal Supremo de lo Civil y Penal, Austria), el cual entendió que las declaraciones controvertidas tenían por objeto atentar contra el honor de la demandante, injuriarla y difamarla.

20. El órgano jurisdiccional remitente debe pronunciarse sobre la cuestión de si la orden de cesación, dictada contra el prestador de servicios de alojamiento de datos que explota una red social que cuenta con multitud de usuarios, puede ampliarse también, a nivel mundial, a las declaraciones literalmente idénticas o de contenido similar de las que no tenga conocimiento.

21. A este respecto, el Oberster Gerichtshof (Tribunal Supremo de lo Civil y Penal) señala que, con arreglo a su propia jurisprudencia, una obligación de este tipo debe considerarse proporcionada cuando el prestador de servicios ya ha tenido conocimiento de, al menos, una vulneración de los intereses de la persona afectada causada por la actuación de un destinatario de sus servicios y cuando quede acreditado que existe el riesgo de que se cometan nuevas infracciones.

IV. Cuestiones prejudiciales y procedimiento ante el Tribunal de Justicia

22. En estas circunstancias, mediante resolución de 25 de octubre de 2017, recibida en el Tribunal de Justicia el 10 de enero de 2018, el Oberster Gerichtshof (Tribunal Supremo de lo Civil y Penal) decidió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

«1) ¿Se opone el artículo 15, apartado 1, de la Directiva [2000/31], con carácter general, a alguna de las siguientes obligaciones de un prestador de servicios de alojamiento de datos que no haya retirado con prontitud datos ilícitos, obligaciones que consisten no solo en retirar los datos en el sentido del artículo 14, apartado 1, letra a), de [dicha] Directiva, sino en retirar también otros datos idénticos:

   a) en todo el mundo?

   b) en el Estado miembro en cuestión?

   c) del destinatario en cuestión del servicio en todo el mundo?

   d) del destinatario en cuestión del servicio en el Estado miembro en cuestión?

2) En caso de respuesta negativa a la primera cuestión: ¿Se aplica lo anterior también a datos similares?

3) ¿Se aplica lo anterior también a datos similares, tan pronto como el explotador tenga conocimiento de esta circunstancia?»

23. Han presentado observaciones escritas la demandante, Facebook Ireland, los Gobiernos austriaco, letón, portugués y finlandés y la Comisión Europea. Todas esas partes, a excepción del Gobierno portugués, estuvieron representadas en la vista celebrada el 13 de febrero de 2019.

V. Análisis

A. Sobre las cuestiones prejudiciales primera y segunda

24. Mediante sus cuestiones prejudiciales primera y segunda, que procede examinar conjuntamente, el órgano jurisdiccional remitente solicita al Tribunal de Justicia que determine el alcance material y personal de la obligación de supervisión que, mediante requerimiento judicial, puede imponerse a un prestador de un servicio de la sociedad de la información consistente en almacenar datos facilitados por un destinatario de ese servicio (prestador de servicios de alojamiento de datos), sin que ello lleve a imponer una obligación general de supervisión, prohibida por el artículo 15, apartado 1, de la Directiva 2000/31.

25. Es cierto que las dos primeras cuestiones prejudiciales se refieren más a la retirada de datos difundidos a través de una plataforma de red social en línea que a su supervisión o filtrado. Sin embargo, ha de señalarse que las plataformas de red social constituyen medios de comunicación cuyo contenido no procede de las sociedades que las han creado y las operan, sino principalmente de sus usuarios. Además, dicho contenido, reproducido y modificado entretanto, es objeto de permanentes interacciones entre usuarios.

26. Para que un prestador de servicios de alojamiento de datos pueda eliminar un dato difundido a través de una plataforma de este tipo o impedir el acceso a él, al margen de quién sea el autor de dicho dato y de su contenido, debe identificar con carácter previo ese dato de entre todos los que se encuentran almacenados en sus servidores. Para ello, debe supervisar o filtrar esos datos de un modo u otro. Pues bien, según el artículo 15, apartado 1, de la Directiva 2000/31, mencionado en las cuestiones prejudiciales, ningún Estado miembro puede imponer a un prestador de servicios de alojamiento de datos una obligación general de supervisión. Todo ello implica que, mediante sus dos primeras cuestiones prejudiciales, el órgano jurisdiccional remitente se pregunta, en esencia, sobre el alcance personal y material de una obligación de ese tipo, que sea conforme con las exigencias de la Directiva 2000/31.

27. Mediante su primera cuestión prejudicial, el órgano jurisdiccional remitente solicita asimismo al Tribunal de Justicia que precise si puede obligarse a un prestador de servicios de alojamiento de datos a retirar, a nivel mundial, informaciones difundidas a través de una plataforma de red social.

28. Para responder a esas dos cuestiones prejudiciales, analizaré en primer lugar, por un lado, el régimen de la Directiva 2000/31 que resulta aplicable a Facebook Ireland en su condición de prestador de servicios de alojamiento de datos y, por otro lado, las implicaciones que puede tener el hecho de calificar a esa entidad como prestador de servicios de alojamiento de datos a efectos de los requerimientos judiciales que se le dirijan. En segundo lugar, analizaré las exigencias que plantea el Derecho de la Unión en lo que atañe al alcance material y personal de la obligación de supervisión que puede imponerse a un prestador de servicios de alojamiento de datos mediante un requerimiento judicial, sin que ello lleve a imponer una obligación general en esta materia. Por último, en tercer lugar abordaré la cuestión del alcance territorial de una obligación de retirada.

1. Requerimientos judiciales dirigidos a los prestadores de servicios de alojamiento de datos a la luz de la Directiva 2000/31

29. Conviene recordar que, para que el almacenamiento efectuado por el prestador de un servicio de la sociedad de la información quede incluido en el artículo 14 de la Directiva 2000/31, es preciso que su comportamiento se ciña al de un «prestador intermediario» en el sentido que el legislador ha querido dar a esta expresión en la sección 4 de esta Directiva. Además, del considerando 42 de la citada Directiva se desprende que su actividad debe ser meramente técnica, automática y pasiva, lo que implica que el prestador no tiene conocimiento ni control de la información almacenada y que el papel que desempeña es neutro. [3]

30. El Tribunal de Justicia ya ha tenido la oportunidad de aclarar que el explotador de una plataforma de red social en línea que almacena en sus servidores información facilitada por usuarios de dicha plataforma, relativa a su perfil, es un prestador de servicios de alojamiento de datos en el sentido del artículo 14, de la Directiva 2000/31. [4] Al margen de las dudas que podrían albergarse a este respecto, de la petición de decisión prejudicial se desprende que el órgano jurisdiccional remitente considera acreditado que Facebook Ireland es un prestador de servicios de alojamiento de datos cuyo comportamiento se ciñe al de un prestador intermediario.

31. En el régimen de la Directiva 2000/31, un prestador de servicios de alojamiento de datos cuyo comportamiento se ciñe al de un prestador intermedio goza de una inmunidad relativa en lo que respecta a la responsabilidad por los datos que almacena. En efecto, esa inmunidad se concede únicamente si el prestador de servicios de alojamiento de datos no tenía conocimiento del carácter ilegal de los datos almacenados o de la actividad que se desarrollaba mediante esos datos y a condición de que, una vez informado de dicha ilegalidad, actúe con prontitud para retirar los datos en cuestión o impedir el acceso a ellos. En cambio, si dicho prestador no cumple estos requisitos, esto es, si tenía conocimiento de la ilegalidad de los datos almacenados pero no actuó para retirarlos o impedir el acceso a ellos, la Directiva 2000/31 no se opone a que pueda ser considerado responsable indirecto respecto de dichos datos. [5]

32. Además, del artículo 14, apartado 3, de la Directiva 2000/31 se desprende que la inmunidad que se concede a un prestador intermediario no impide que un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados miembros, exijan al prestador poner fin a una infracción o impedirla. De esa disposición resulta que puede emitirse un requerimiento judicial frente al prestador intermediario incluso cuando, según los requisitos establecidos en el artículo 14, apartado 1, de dicha Directiva, dicho prestador no sea él mismo responsable de los datos almacenados en sus servidores. [6]

33. Los requisitos y los elementos de tales requerimientos judiciales emitidos frente a los prestadores intermediarios se rigen por el Derecho nacional. [7] Sin embargo, las reglas que establezcan los Estados miembros deben respetar las exigencias que plantea el Derecho de la Unión, en particular, la Directiva 2000/31.

3 Véase, en particular, la sentencia de 23 de marzo de 2010, Google France y Google (C-236/08 a C-238/08, EU:C:2010:159), apartados 112 y 113.

4 Véase la sentencia de 16 de febrero de 2012, SABAM (C-360/10, EU:C:2012:85), apartado 27.

5 Véase el artículo 14 de la Directiva 2000/31. Véanse también mis conclusiones presentadas en el asunto Stichting Brein (C-610/15, EU:C:2017:99), puntos 67 y 68.

6 Véase la sentencia de 7 de agosto de 2018, SNB-REACT (C-521/17, EU:C:2018:639), apartado 51. Véase asimismo, en el mismo sentido, Lodder, A.R., Polter, P., «ISP blocking and filtering: on the shallow justifications in case law regarding effectiveness of measures», *European Journal of Law and Technology*, 2017, vol. 8, n.º 2, p. 5.

7 Véanse mis conclusiones en el asunto Mc Fadden (C-484/14, EU:C:2016:170). Véase también Husovec, M., *Injunctions Against Intermediaires in the European Unión. Accountable But Not Liable*?, Cambridge University Press, Cambridge, 2017, pp. 57 y 58.

34. Todo ello pone de manifiesto la voluntad del legislador de la Unión de lograr, a través de dicha Directiva, un equilibro entre los intereses de los prestadores de servicios de alojamiento de datos cuyo comportamiento se ciñe al de un prestador intermediario, los de los usuarios de sus servicios y los de las personas víctimas de cualquier infracción cometida en el marco de la utilización de dichos servicios. En consecuencia, en el momento de aplicar las medidas de adaptación del ordenamiento jurídico a la Directiva 2000/31, corresponde a los Estados miembros no solo respetar las exigencias que establece, sino también procurar que la interpretación que tomen como base no entre en conflicto con los derechos fundamentales de que se trata o con otros principios generales del Derecho de la Unión, como el principio de proporcionalidad. [8]

2. Exigencias en cuanto al alcance personal y material de una obligación de supervisión

a) Prohibición de establecer una obligación general de supervisión

35. Conviene señalar que el artículo 15, apartado 1, de la Directiva 2000/31 prohíbe a los Estados miembros imponer, en particular a los prestadores de servicios cuya actividad consista en almacenar datos, una obligación general de supervisar los datos que almacenen o una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas. Además, de la jurisprudencia se desprende que dicha disposición se opone, en particular, a que un prestador de servicios de alojamiento de datos cuyo comportamiento se ciñe al de un prestador intermediario se vea obligado a proceder a una supervisión de la totalidad [9] o de la casi totalidad [10] de los datos respecto de todos sus clientes con el fin de evitar cualquier futura infracción.

36. Si, a diferencia de lo que establece esa disposición, un Estado miembro pudiera imponer mediante un requerimiento judicial una obligación general de supervisión a un prestador de servicios de alojamiento de datos, no puede excluirse que este perdiera su condición de prestador intermediario y, por consiguiente, la inmunidad que ese estatuto trae consigo. En efecto, el papel que desempeñaría un prestador de servicios de alojamiento de datos que ejerciese una supervisión general ya no sería neutro. La actividad de dicho prestador de servicios de alojamiento de datos no mantendría su naturaleza técnica, automática y pasiva, lo que implicaría que tendría conocimiento de la información almacenada y ejercería un control sobre esta.

37. Además, aunque no existiera ese riesgo, un prestador de servicios de alojamiento de datos que ejerciese una supervisión general en principio podría ser considerado responsable de toda actividad o información ilícita, sin que se cumplan efectivamente los requisitos establecidos en el artículo 14, apartado 1, letras a) y b), de dicha Directiva.

38. Es cierto que el artículo 14, apartado 1, letra a), de la Directiva 2000/31 supedita la responsabilidad de todo prestador intermediario al conocimiento efectivo de la actividad o de la información ilícita. Sin embargo, ante una obligación general de supervisión, cabría considerar que el prestador intermediario tiene conocimiento de oficio del carácter ilícito de cualquier actividad o información y que debería retirar esa información o impedir el acceso a ella, aunque no hubiera apreciado el contenido ilícito. [11] En consecuencia, la lógica de la inmunidad de responsabilidad relativa por los datos almacenados por un prestador intermediario se invertiría sistemáticamente, lo cual menoscabaría el efecto útil del artículo 14, apartado 1, de la Directiva 2000/31.

8 Véase, en ese sentido, en lo que respecta al respeto de los derechos fundamentales y del principio de proporcionalidad, la sentencia de 29 de enero de 2008, Promusicae (C-275/06, EU:C:2008:54), apartado 68.

9 Véanse las sentencias de 12 de julio de 2011, L'Oréal y otros (C-324/09, EU:C:2011:474), apartados 139 y 144, y de 24 de noviembre de 2011, Scarlet Extended (C-70/10, EU:C:2011:771), apartados 36 y 40.

10 Véase la sentencia de 16 de febrero de 2012, SABAM (C-360/10, EU:C:2012:85), apartado 37 y 38.

11 Véanse, en ese sentido, las conclusiones del Abogado General Jääskinen presentadas en el asunto L'Oréal y otros (C-324/09, EU:C:2010:757), punto 143.

39. En resumen, el papel de un prestador de servicios de alojamiento de datos que ejerciese esa supervisión general dejaría de ser neutro en la medida en que su actividad ya no mantendría su carácter técnico, automático y pasivo, lo cual entrañaría que el citado prestador de servicios tendría conocimiento de los datos almacenados y ejercería un control sobre ellos. Por consiguiente el establecimiento de una obligación general de supervisión, impuesta a un prestador de servicios de alojamiento de datos en el marco de un requerimiento judicial autorizado, en principio, por el artículo 14, apartado 3, de la Directiva 2000/31, podría suponer que el artículo 14 de dicha Directiva resultase inaplicable a dicho prestador.

40. Deduzco pues de la interpretación del artículo 14, apartado 3, en relación con el artículo 15, apartado 1, de la Directiva 2000/31, que ninguna obligación que se imponga a un prestador intermediario mediante requerimiento judicial puede dar lugar a que su papel, en lo que respecta a la totalidad o a la casi totalidad de los datos almacenados, deje de ser neutro, en el sentido indicado en el punto anterior.

b) Obligación de supervisión en casos específicos

41. Como establece el considerando 47 de la Directiva 2000/31, la prohibición de imponer obligaciones de carácter general, prevista en el artículo 15, apartado 1, de dicha Directiva, no se refiere a las obligaciones de supervisión *en casos específicos*. En efecto, del tenor literal del artículo 14, apartado 3, de la Directiva 2000/31 resulta que un prestador de servicios de alojamiento de datos puede estar obligado a *prevenir* una infracción, lo cual lógicamente entraña, como señala la Comisión, una cierta forma de supervisión en el futuro, supervisión que no puede transformarse en una obligación de supervisión general.[12] Además, el artículo 18 de dicha Directiva exige a los Estados miembros velar por que los recursos judiciales existentes en virtud de la legislación nacional en relación con las actividades de servicios de la sociedad de la información permitan adoptar rápidamente medidas destinadas, en particular, *a evitar que se produzcan nuevos perjuicios* contra los intereses afectados.

42. Asimismo, de la sentencia L'Oréal y otros[13] resulta que un prestador de servicios de alojamiento de datos puede ser obligado a adoptar medidas que contribuyan a evitar que se produzcan *nuevas lesiones* de la misma naturaleza por el mismo usuario.

43. En dicha sentencia, el Tribunal de Justicia no interpretó exclusivamente las disposiciones de la Directiva 2000/31, sino también las de la Directiva 2004/48/CE.[14] Pues bien, en ese contexto, el Tribunal de Justicia definió una obligación de supervisión conforme a las exigencias de ambas directivas, en contraposición con la obligación prohibida por el artículo 15, apartado 1, de la Directiva 2000/31, es decir, de supervisión activa del conjunto —o de la casi totalidad— de los datos dirigida a evitar cualquier futura lesión.[15] Al margen del contexto específico de la sentencia L'Oréal y otros[16] y de las referencias a la Directiva 2004/48, las consideraciones efectuadas en esa sentencia en relación con las obligaciones de los prestadores de servicios de alojamiento de datos conformes al Derecho de la Unión, en función de que sean de carácter general o no, son de naturaleza transversal y, por consiguiente, extrapolables, en mi opinión, al presentes asunto.

12 Véase asimismo, en ese sentido, Rosati, E., *Copyright and the Court of Justice of the European Unión*, Oxford University Press, Oxford, 2019, p. 158.

13 Sentencia de 12 de julio de 2011 (C-324/09, EU:C:2011:474), apartado 144.

14 Directiva del Parlamento Europeo y del Consejo, de 29 de abril de 2004, relativa al respeto de los derechos de propiedad intelectual (DO 2004, L 157, p. 45).

15 Sentencia de 12 de julio de 2011, L'Oréal y otros (C-324/09, EU:C:2011:474), apartados 139 y 144.

16 Sentencia de 12 de julio de 2011 (C-324/09, EU:C:2011:474).

44. Por lo tanto, con el fin de prevenir cualquier infracción futura, puede obligarse a un prestador de servicios de alojamiento de datos, mediante requerimiento judicial, a retirar información ilícita que aún no haya sido difundida en el momento de la adopción de dicho requerimiento, sin necesidad de que la difusión de dicha información se ponga en su conocimiento de nuevo y al margen de la solicitud inicial.

45. Sin embargo, para que ello no suponga imponer una obligación general, según parece desprenderse de la sentencia L'Oréal y otros,[17] toda obligación de supervisión debe respetar determinados requisitos adicionales, es decir, que las lesiones sean de la *misma naturaleza*, provengan del *mismo usuario* y vayan dirigidas *contra los mismos derechos*, en ese asunto, el derecho de marcas.

46. Así, llego a la conclusión de que la supervisión activa no es inconciliable con la Directiva 2000/31, a diferencia de la supervisión activa cuyo objeto no se centra en el caso específico de una lesión.

47. En esa línea, en mis conclusiones presentadas en el asunto Mc Fadden,[18] relativo a un proveedor de acceso a una red de comunicaciones, en el sentido del artículo 12 de la Directiva 2000/31, basándome en los trabajos preparatorios de la Directiva 2000/31, señalé que para que una obligación pueda considerarse aplicable *en casos específicos*, debe limitarse, en particular, en función del *objeto* y de la *duración* de la supervisión.

48. En mi opinión, esas exigencias generales formuladas de forma abstracta son extrapolables a circunstancias como las del litigio principal, a pesar de que, cuando se aplican por analogía a los prestadores de servicios de alojamiento de datos como Facebook Ireland determinadas consideraciones sobre obligaciones de supervisión relativas a proveedores de acceso a una red de comunicaciones como Internet, los papeles que desempeñan esos prestadores intermediarios son diferentes. Por ejemplo, si se parte de un prestador de servicios de alojamiento de datos como Facebook Ireland, los contenidos de su plataforma parecen constituir la totalidad de los datos almacenados, mientras que, para un proveedor de acceso a Internet, esos datos representan solo una ínfima parte de los datos transmitidos. En cambio, el carácter y la intensidad de la implicación de un prestador de servicios de alojamiento de datos en el tratamiento de los contenidos digitales difieren sustancialmente de los de un proveedor de acceso a Internet. Como señala la Comisión, un prestador de servicios de alojamiento de datos está en mejor disposición para adoptar medidas para buscar y eliminar información ilícita que un proveedor de acceso.

49. Además, la exigencia relativa a la limitación temporal de toda obligación de supervisión está plasmada en varias sentencias del Tribunal de Justicia.[19] Aunque, conforme a la jurisprudencia, la limitación temporal de la obligación impuesta mediante un requerimiento judicial guarda relación más bien con la problemática de los principios generales del Derecho de la Unión,[20] creo que una obligación de supervisión permanente sería difícilmente conciliable con el concepto de obligación en casos específicos en el sentido del considerando 47 de la Directiva 2000/31.

17 Sentencia de 12 de julio de 2011, L'Oréal y otros (C-324/09, EU:C:2011:474), apartados 141 y 144.

18 C-484/14, EU:C:2016:170, punto 132.

19 Más concretamente, en su sentencia de 12 de julio de 2011, L'Oréal y otros (C-324/09, EU:C:2011:474), apartado 140, el Tribunal de Justicia señaló que el requerimiento que tiene por objeto evitar posibles lesiones provocadas a marcas en el marco del servicio de la sociedad de la información, a saber, un mercado electrónico, no puede tener por objeto o efecto imponer una prohibición general y *permanente* de poner a la venta productos de estas marcas. En ese mismo sentido, el Tribunal de Justicia observó en su sentencia de 16 de febrero de 2012, SABAM (C-360/10, EU:C:2012:85), apartado 45, que el Derecho de la Unión se opone, en particular, a que una obligación de supervisión impuesta mediante un requerimiento judicial dirigido a un prestador sea *ilimitada en el tiempo*.

20 Ese fue el planteamiento que adoptó el Abogado General Jääskinen en sus conclusiones presentadas en el asunto L'Oréal y otros (C-324/09, EU:C:2010:757), punto 181, que, en mi opinión, inspiraron en gran medida la redacción de los pasajes correspondiente de la sentencia dictada por el Tribunal de Justicia en dicho asunto.

50. Por consiguiente, el carácter selectivo de una obligación de supervisión debería apreciarse teniendo en cuenta la duración de dicha supervisión, así como las precisiones relativas a la naturaleza de las lesiones, su autor y su objeto. Todos esos elementos son interdependientes y están vinculados entre sí. Por tanto, conviene analizarlos de forma global para determinar si un requerimiento judicial respeta o no la prohibición establecida en el artículo 15, apartado 1, de la Directiva 2000/31.

c) Conclusiones provisionales

51. Para recapitular esta parte de mi análisis, en primer lugar, de la interpretación del artículo 14, apartado 3, en relación con el artículo 15, apartado 1, de la Directiva 2000/31, se desprende que ninguna obligación que se imponga a un prestador intermediario mediante requerimiento judicial puede dar lugar a una situación en la que su papel, en lo que respecta a la totalidad o a la casi totalidad de los datos almacenados, deje de ser técnico, automático y pasivo, lo cual entrañaría que el citado prestador de servicios de alojamiento de datos tendría conocimiento de los datos almacenados y ejercería un control sobre ellos. [21]

52. En segundo lugar, la supervisión activa no es inconciliable con la Directiva 2000/31, a diferencia de la supervisión activa cuyo objeto no se centra en el caso específico de una lesión. [22]

53. En tercer lugar, el carácter selectivo de una obligación de supervisión debería apreciarse teniendo en cuenta la duración de dicha supervisión, así como las precisiones relativas a la naturaleza de las lesiones, su autor y su objeto. [23]

54. El alcance personal y material de la obligación de supervisión de un prestador de servicios que explota una plataforma de red social debe examinarse a la luz de las anteriores consideraciones. En el presente caso, ello entraña buscar e identificar, entre los contenidos almacenados, datos idénticos a los declarados ilícitos por el órgano jurisdiccional que conoció del correspondiente procedimiento, así como buscar datos similares.

d) Aplicación en el caso de autos

1) Datos idénticos a los declarados ilícitos

55. A excepción de Facebook Ireland, todas los interesados sostienen que debe ser posible ordenar a un prestador de servicios de alojamiento de datos que suprima o bloquee el acceso a declaraciones idénticas a las que hayan sido declaradas ilícitas, que sean publicadas por el mismo usuario. La demandante, los Gobiernos austriaco y letón y la Comisión consideran, en esencia, que lo mismo debe suceder con las que sean publicadas por otros usuarios.

56. De la resolución de remisión se desprende que el órgano jurisdiccional de segunda instancia considera «datos idénticos» las publicaciones de fotografías de la recurrente *con un texto de acompañamiento idéntico*. En la misma línea, el órgano jurisdiccional remitente expone que su duda se refiere a si el requerimiento judicial dirigido a Facebook Ireland puede extenderse a *declaraciones (mensajes de acompañamiento) textualmente idénticas* y a las de contenido similar. Yo interpreto esa referencia a «datos idénticos» en el sentido de que el órgano jurisdiccional remitente se refiere a las reproducciones manuales y exactas de los datos que ha declarado ilícitos y, como señala el Gobierno austriaco, a las reproducciones automatizadas realizadas a través de la función «compartir».

21 Véase el punto 39 de las presentes conclusiones.

22 Véase el punto 46 de las presentes conclusiones.

23 Véase el punto 50 de las presentes conclusiones.

57. A este respecto, opino que un prestador de servicios de alojamiento de datos que explota una plataforma de red social puede ser obligado, en el marco de un requerimiento judicial emitido por un órgano jurisdiccional de un Estado miembro, a buscar e identificar todos los datos idénticos a aquellos que hayan sido declarados ilícitos por ese órgano jurisdiccional.

58. En efecto, tal y como se desprende de mi análisis, un prestador de servicios de alojamiento de datos puede ser obligado a evitar que se produzcan nuevas lesiones del mismo tipo y del mismo destinatario de un servicio de la sociedad de la información.[24] En ese caso, se trata efectivamente de un caso específico de una lesión identificada de forma concreta, de modo que la obligación de identificar datos idénticos a los declarados ilícitos de entre los procedentes de un mismo usuario no constituye una obligación general de supervisión.

59. Desde mi punto de vista, lo mismo ocurriría con los datos idénticos a los declarados ilícitos procedentes de otros usuarios. Soy consciente de que ese razonamiento da pie a que el alcance personal de una obligación de supervisión comprenda a todo usuario y, por consiguiente, a todos los datos que se difundan a través de una plataforma.

60. Sin embargo, la obligación de buscar e identificar datos idénticos a los declarados ilícitos por el órgano jurisdiccional que conoce del asunto sigue estando centrada en el caso específico de una lesión. Además, en este caso se trata de una obligación impuesta en el marco de un auto de medidas provisionales que surte efecto hasta el cierre definitivo del procedimiento. Así, esa obligación impuesta al prestador de servicios de alojamiento de datos es, por la propia naturaleza de las cosas, limitada en el tiempo.

61. Por otra parte, creo que, con carácter general, la reproducción del mismo contenido por cualquier usuario de una plataforma de red social puede detectarse con la ayuda de herramientas informáticas sin que el prestador de servicios de alojamiento de datos esté obligado a realizar un filtrado activo y no automático de la totalidad de los datos difundidos mediante su plataforma.

62. Además, imponer la obligación de buscar e identificar todos los datos idénticos a los declarados ilícitos permite garantizar un equilibrio justo entre los derechos fundamentales en juego.

63. En primer lugar, la búsqueda y la identificación de datos idénticos a los declarados ilícitos por un órgano jurisdiccional no requieren medios técnicos sofisticados, que puedan constituir una carga extraordinaria. Por lo tanto, no parece que esa obligación lesione de forma excesiva el derecho a la libertad de empresa que ampara a un prestador de servicios de alojamiento de datos que explota una plataforma de red social como Facebook Ireland con arreglo al artículo 16 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»).

64. En segundo lugar, habida cuenta de lo fácil que resulta reproducir datos en el entorno de Internet, la búsqueda y la identificación de datos idénticos a los declarados ilícitos es necesaria para garantizar una protección eficaz de la intimidad y de los derechos de la personalidad.

65. Por último, esa obligación respeta el derecho fundamental de los usuarios de Internet a la libertad de expresión y de información consagrada en el artículo 11 de la Carta, en la medida en la que la protección de esa libertad no debe garantizarse forzosamente de forma absoluta, sino ponerse en equilibrio con la protección de otros derechos fundamentales. En lo que respecta a los datos idénticos a los declarados ilícitos, tales datos constituyen, *a priori* y por regla general, reiteraciones de una lesión declarada ilícita en el caso concreto. Esas reiteraciones deben ser objeto de la misma calificación, si bien matizada en función, en particular, del contexto de una supuesta declaración ilícita. A este propósito conviene señalar que los terceros que podrían verse directamente afectados por

24 Véanse los puntos 42 y 45 de las presentes conclusiones.

requerimientos judiciales no son parte en los procedimientos en los que se dictan esos requerimientos. Ese es el motivo principal por el que es preciso garantizar a esos terceros la posibilidad de oponerse ante un juez a medidas de ejecución adoptadas por un prestador de servicios de alojamiento de datos sobre la base de un requerimiento judicial,[25] sin supeditar esa posibilidad a tener la condición de parte en un procedimiento principal.[26]

2) Datos similares

66. En lo que concierne al alcance material de una obligación de supervisión, la demandante sostiene que un prestador de servicios de alojamiento de datos puede estar sujeto a la obligación de retirar declaraciones similares a la declarada ilícita que sean publicadas por el mismo usuario. En cambio, el Gobierno austriaco y la Comisión estiman que la posibilidad de imponer esa obligación depende de la puesta en equilibrio de los intereses en juego. La demandante es la única que considera posible requerir a un prestador de servicios de alojamiento de datos para que retire declaraciones similares a la considerada ilícita publicadas por otros usuarios.

67. Las expresiones «datos similares» o «de contenido similar» generan dificultades interpretativas en la medida en la que el órgano jurisdiccional remitente no precisa su significado. Sin embargo, de la petición de decisión prejudicial cabe deducir que la mención datos «similares» se refiere a datos que *difieren ligeramente* de los datos iniciales o a situaciones en las que el *mensaje permanece básicamente inalterado*. Interpreto esas indicaciones en el sentido de que la reproducción de datos declarados ilícitos que incluyan un error de mecanografía o que tengan una sintaxis o puntuación matizada constituyen «datos similares». Sin embargo, no es evidente que la similitud a que se refiere la segunda cuestión prejudicial no vaya más allá de esos casos.

68. Es cierto que de la sentencia L'Oréal y otros[27] se desprende que el prestador de un servicio de la sociedad de la información puede ser obligado a adoptar medidas que contribuyan a evitar *nuevas lesiones* del *mismo tipo* a los mismos derechos.

69. Sin embargo, no debe perderse de vista el contexto fáctico en el que se desarrolló la jurisprudencia pertinente, a saber, el de violaciones del derecho de propiedad intelectual. Por regla general, esas violaciones consisten en la difusión de contenido protegido o, al menos, de un contenido parecido al protegido, pues las eventuales modificaciones de este, a veces difíciles de aportar, requieren una intervención específica.

70. En cambio, no es común que un acto difamatorio reproduzca los mismos términos que otro acto de la misma naturaleza. Ello deriva, en parte, del carácter personalizado del modo de expresar las ideas. Además, a diferencia de lo que ocurre con las vulneraciones del derecho de propiedad intelectual, los actos difamatorios cometidos después del acto difamatorio inicial reproducen más bien el hecho de realizar afirmaciones que atentan contra el honor de una persona, antes que la forma del acto inicial. Por esa razón, en materia de difamación, la mera referencia a actos de la misma naturaleza no puede desempeñar la misma función que en ámbito de vulneraciones del derecho de propiedad intelectual.

25 Véase, por analogía, la sentencia de 27 de marzo de 2014, UPC Telekabel Wien (C-314/12, EU:C:2014:192), apartado 57.

26 Véanse, por analogía, las sentencias de 25 de mayo de 2016, Meroni (C-559/14, EU:C:2016:349), apartado 49 y 50, y de 21 de diciembre de 2016, Biuro podróży «Partner» (C-119/15, EU:C:2016:987), apartado 40. Sobre la problemática del principio de tutela judicial efectiva frente a terceros, véase también Kalėda, S. L., «The Role of the Principle of Effective Judicial Protection in Relation to Website Blocking Injunctions», *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2017, pp. 222 y 223.

27 Sentencia de 12 de julio de 2011 (C-324/09, EU:C:2011:474).

71. En cualquier caso, la interpretación de la expresión «datos similares» puede incidir en el alcance de una obligación de supervisión y en el ejercicio de los derechos fundamentales de que se trata. Por tanto, un órgano jurisdiccional que se pronuncie en el marco de un requerimiento judicial sobre la retirada de «datos similares» debe respetar el principio de seguridad jurídica y velar por que los efectos de dicho requerimiento sean claros, precisos y previsibles. A ese propósito, dicho órgano jurisdiccional debe poner en equilibro los derechos fundamentales en cuestión y tener en cuenta el principio de proporcionalidad.

72. Sin perjuicio de lo anterior y basándome de nuevo en la sentencia L'Oréal y otros,[28] considero con mayor razón que puede obligarse a un prestador de servicios de alojamiento de datos a identificar datos similares a los declarados ilícitos que procedan del mismo usuario. También en este caso, debe garantizarse a dicho usuario la posibilidad de oponerse ante un juez a las medidas de ejecución adoptadas por un prestador de servicios de alojamiento de datos para cumplir un requerimiento judicial.

73. En cambio, para identificar datos similares a los declarados ilícitos que procedan de otros usuarios sería preciso supervisar todos los datos difundidos a través de una plataforma de red social. Pues bien, a diferencia de lo que sucede con los datos idénticos a los declarados ilícitos, un prestador de servicios de alojamiento de datos no puede identificar los datos similares a los declarados ilícitos sin recurrir a soluciones sofisticadas. En consecuencia, no solo el papel que desempeña el prestador que ejerce una supervisión general dejaría de ser neutro, al no tener carácter meramente técnico, automático y pasivo, sino que además, dicho prestador, al aplicar una forma de censura, pasaría a contribuir de forma activa en dicha plataforma.

74. Además, imponer una obligación de identificar datos similares a los declarados ilícitos procedentes de cualquier usuario no garantizaría un justo equilibrio entre la protección de la intimidad y los derechos de la personalidad, la de la libertad de empresa y la de la libertad de expresión e información. Por un lado, la búsqueda e identificación de esos datos precisaría de soluciones costosas, que deberían ser desarrolladas e implantadas por el prestador de servicios de alojamiento de datos. Por otro lado, la aplicación de esas soluciones daría lugar a una censura, de modo que la libertad de expresión y de información podría verse sistemáticamente limitada.

75. A la luz de las consideraciones anteriores, propongo que se responda a las cuestiones prejudiciales primera y segunda, en la medida en que versan sobre el alcance personal y material de una obligación se supervisión, que el artículo 15, apartado 1, de la Directiva 2000/31 debe interpretarse en el sentido de que no se opone a que, mediante un requerimiento judicial, se obligue a un prestador de servicios de alojamiento de datos que explota una plataforma de red social a buscar e identificar, entre todos los datos difundidos por los usuarios de esa plataforma, datos idénticos a los declarados ilícitos por el órgano jurisdiccional que haya dictado dicho requerimiento. Mediante ese requerimiento judicial puede obligarse a un prestador de servicios de alojamiento de datos a buscar e identificar datos similares a los declarados ilícitos únicamente de entre los datos difundidos por el usuario que publicó tales datos. Un órgano jurisdiccional que se pronuncie sobre la retirada de esos datos similares debe garantizar que los efectos de su requerimiento son claros, precisos y previsibles. A ese propósito, debe poner en equilibro los derechos fundamentales en juego y tener en cuenta el principio de proporcionalidad.

28 Sentencia de 12 de julio de 2011 (C-324/09, EU:C:2011:474).

3. Sobre la retirada a nivel mundial

a) Observaciones preliminares

76. A continuación abordaré las dudas del órgano jurisdiccional remitente sobre el alcance territorial de una obligación de retirada. Dichas dudas versan, en esencia, sobre si puede obligarse a un prestador de servicios de alojamiento de datos a retirar contenidos declarados ilícitos con arreglo al Derecho nacional de un Estado miembro no solo en el ámbito de dicho Estado miembro, sino también a nivel mundial.

77. Con carácter preliminar, es cierto que Facebook Ireland, en su condición de filial de Facebook, explota una plataforma electrónica únicamente para usuarios situados fuera del territorio de los Estados Unidos y de Canadá. Sin embargo, no creo que esa circunstancia excluya la retirada a nivel mundial de los datos difundidos a través de esa plataforma. En efecto, Facebook Ireland no niega que pueda garantizar esa retirada a nivel mundial.

78. Sin embargo, es preciso señalar que el legislador de la Unión no ha armonizado las normas sustantivas en materia de violación de la intimidad o de los derechos relacionados con la personalidad, en particular, la difamación. [29] Además, a falta de consenso en el ámbito de la Unión, [30] el legislador de la Unión tampoco ha armonizado las normas de conflicto en la materia. [31] Así, para resolver sobre acciones en materia de difamación, los órganos jurisdiccionales de la Unión recurren a la ley designada como aplicable en virtud de las normas de conflicto nacionales.

79. La situación controvertida en el litigio principal es, *a priori*, distinta de aquella de la que partí al realizar mi análisis sobre el alcance territorial de la retirada de enlaces de los resultados obtenidos al utilizar un motor de búsqueda en el asunto Google, [32] citado por Facebook Ireland y el Gobierno letón. Dicho asunto guarda relación con la Directiva 95/46/CE, [33] que armoniza en el ámbito de la Unión ciertas normas en materia de protección de datos. En particular, el hecho de que existan normas armonizadas en esa materia me llevó a concluir que un prestador debía estar obligado a suprimir los resultados obtenidos como consecuencia de una búsqueda realizada no solo desde un Estado miembro, sino también desde un lugar situado en la Unión. [34] Sin embargo, en mis conclusiones presentadas en ese asunto, no excluí que pudieran surgir situaciones en las que el interés de la Unión exigiese aplicar las disposiciones de la Directiva 95/46 más allá del territorio de la Unión. [35]

80. En consecuencia, en lo que respeta a los casos de difamación, la imposición en un Estado miembro de una obligación que consiste en retirar ciertos datos a nivel mundial, con respecto a todos los usuarios de una plataforma electrónica, a raíz de la ilicitud de dichos datos declarada en virtud de una ley aplicable, daría lugar a que la constatación de su carácter ilícito surtiera efecto en otros Estados. Dicho de otro modo, la constatación del carácter ilícito de los datos controvertidos se extendería a los territorios de esos otros Estados. Sin embargo, no puede excluirse que, con arreglo a las leyes designadas aplicables en virtud de las normas de conflicto nacionales de tales Estados, dichos datos puedan considerarse lícitos.

29 Véase Savin, A., *EU Internet law*, Elgar European Law, Cheltenham — Northampton, 2017, p. 130.

30 Véase Van Calster, G., *European Private International Law*, Hart Publishing, Oxford, Portland, 2016, p. 248 a 251.

31 Véase el artículo 1, apartado 2, del 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 2007, L 199, p. 40).

32 Me refiero a mis conclusiones presentadas en el asunto Google (alcance territorial de la retirada de enlaces de una lista de resultados) (C-507/17, EU:C:2019:15).

33 Directiva del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO 1995, L 281, p. 31).

34 Véanse mis conclusiones presentadas en el asunto Google (alcance territorial de la retirada de enlaces de una lista de resultados) (C-507/17, EU:C:2019:15), puntos 47, 55, 76 y 77.

35 Véanse mis conclusiones presentadas en el asunto Google (alcance territorial de la retirada de enlaces de una lista de resultados) (C-507/17, EU:C:2019:15), punto 62.

81. Como pone de manifiesto el debate entre las partes, por un lado, la reticencia a otorgar esos efectos extraterritoriales a los requerimientos judiciales refleja la postura de Facebook Ireland y la de los Gobiernos letón, portugués y finlandés. Por otro lado, a excepción del Gobierno portugués, esas partes también parecen albergar dudas sobre el alcance territorial de la competencia de los tribunales de un Estado miembro. En esencia, dichas partes parecen considerar que los tribunales de un Estado miembro no pueden pronunciarse, en el contexto de un requerimiento judicial dirigido a un prestador de servicios de alojamiento de datos, sobre la retirada de contenidos fuera del territorio de dicho Estado miembro. Por consiguiente, resulta preciso analizar esos dos aspectos, a saber, el alcance territorial de una obligación de retirada y el alcance de la competencia de los tribunales de un Estado miembro, examinando, en primer lugar, el relativo a la competencia, que, con carácter general, suele ser previo a las cuestiones de fondo.

b) Sobre el alcance territorial de la competencia

82. La Directiva 2000/31 no regula la competencia para dictar requerimientos judiciales. En cambio, según se desprende de la sentencia eDate Advertising y otros,[36] en caso de supuesta lesión de los derechos de la personalidad mediante el contenido publicado en un sitio de Internet, la persona que se considere lesionada puede ejercitar una acción ante los órganos jurisdiccionales de los Estados miembros competentes en virtud del Reglamento (UE) n.º 1215/2012.[37] En efecto, aunque las normas de conflicto en materia de difamación no están armonizadas en el ámbito de la Unión, no ocurre lo mismo en cuanto a las normas de competencia.

83. A este respecto ha de añadirse que las normas de competencia del Reglamento n.º 1215/2012 también se aplican a los litigios en materia de eliminación de contenidos difamatorios publicados en línea.[38] Además, carece de importancia que, en el presente asunto, esa solicitud no se dirija contra el emisor, sino contra un prestador de servicios de alojamiento de los contenidos publicados en línea. Dicho esto, no creo que proceda proponer al Tribunal de Justicia que reformule las cuestiones prejudiciales, en la medida en que únicamente los interesados albergan dudas sobre el alcance territorial de la competencia. Sin embargo, desearía efectuar algunas observaciones a ese respecto.

84. Según la sentencia eDate Advertising y otros,[39] una persona que se considera perjudicada puede ejercitar una acción, en particular, ante los órganos jurisdiccionales del Estado miembro en el que se encuentra su centro de intereses. Dichos órganos jurisdiccionales son competentes para pronunciarse sobre la totalidad del daño causado. Al parecer, en este caso, el órgano jurisdiccional ante el que la demandante ha ejercitado la acción es el de su centro de intereses.[40]

85. Es cierto que en la sentencia eDate Advertising y otros,[41] el Tribunal de Justicia indicó que, en virtud del lugar en el que se hubiera producido el daño ocasionado en la Unión, la persona que se consideraba perjudicada podía acudir a un fuero por la totalidad de dicho daño. Ciertamente, lo anterior puede dar pie a considerar que el alcance territorial de la competencia de ese fuero no engloba los hechos acaecidos en el territorio de terceros Estados. No obstante, esa consideración guarda más bien relación con el hecho de que, para ser competente con arreglo al Reglamento

36 Sentencia de 25 de octubre de 2011 (C-509/09 y C-161/10, EU:C:2011:685), apartados 43 y 44.

37 Reglamento 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 2012, L 35, p. 1).

38 Sentencia de 17 de octubre de 2017, Bolagsupplysningen e Ilsjan (C-194/16, EU:C:2017:766), apartado 44.

39 Sentencia de 25 de octubre de 2011 (C-509/09 y C-161/10, EU:C:2011:685), apartado 48.

40 Por consiguiente, pese al hecho de que el órgano jurisdiccional remitente debe pronunciarse sobre un auto de medidas provisionales, no procede preguntarse sobre las implicaciones del artículo 35 del Reglamento n.º 1215/2012 en el alcance territorial de la competencia y sobre el alcance territorial de una obligación de retirada impuesta mediante requerimiento judicial.

41 Sentencia de 25 de octubre de 2011 (C-509/09 y C-161/10, EU:C:2011:685), apartado 48.

n.º 1215/2012, en virtud del lugar de materialización del daño, ese fuero debe ser un órgano jurisdiccional de un Estado miembro. Asimismo, dejando al margen esa consideración, el Tribunal de Justicia indicó en muchas ocasiones en esa sentencia que dicho fuero es competente para resolver sobre la totalidad de los daños ocasionados por esa difamación. [42]

86. De ello se desprende, a mi juicio, que, en contra de lo que sostienen Facebook Ireland y los Gobiernos letón y finlandés, los tribunales de un Estado miembro pueden resolver, en principio, sobre la retirada de contenidos fuera del territorio del citado Estado miembro, pues tienen competencia territorial universal. [43] Cabe que los órganos jurisdiccionales de un Estado miembro no puedan pronunciarse sobre una retirada a nivel mundial no ya por un tema de competencia, sino, en su caso, por una cuestión de fondo.

87. A continuación conviene analizar la cuestión de los efectos extraterritoriales de los requerimientos dirigidos a los prestadores de servicios de alojamiento de datos que, en el presente asunto, como ya he señalado en el punto 81 de las presentes conclusiones, se refiere básicamente a la cuestión del alcance territorial de una obligación de retirada.

c) Sobre el alcance territorial de una obligación de retirada

88. En primer lugar, debe destacarse que, como admite el Gobierno finlandés, el artículo 15, apartado 1, de la Directiva 2000/31 no regula los efectos territoriales de los requerimientos dirigidos a prestadores de servicios de la sociedad de la información. Además, siempre que se cumplan las exigencias que establece la Directiva 2000/31, las obligaciones de retirada impuestas a esos prestadores mediante requerimientos judiciales están sujetas al Derecho nacional.

89. Asimismo, a falta de normativa de la Unión en materia de intimidad y derechos de la personalidad, es difícil justificar los efectos territoriales de un requerimiento judicial invocando la protección de los derechos fundamentales que garantizan los artículos 1, 7 y 8 de la Carta. En efecto, el ámbito de aplicación de la Carta coincide con el ámbito de aplicación del Derecho de la Unión, y no al contrario, [44] y, en el presente asunto, en cuanto al fondo, la acción de la demandante no está basada en el Derecho de la Unión.

90. A este respecto, conviene señalar que no parece que la demandante invoque derechos en materia de protección de datos personales ni que reproche a Facebook Ireland haber «llevado a cabo» un tratamiento ilícito de sus datos, pues su demanda se basa en disposiciones generales de Derecho civil. Además, el órgano jurisdiccional remitente no invoca instrumentos jurídicos del Derecho de la Unión pertinentes en esa materia. Únicamente hace referencia a la Directiva 2000/31. Pues bien, del artículo 1, apartado 5, letra b), de dicha Directiva se desprende que esta no se aplica a cuestiones relacionadas con servicios de la sociedad de la información incluidas en las directivas en materia de protección de datos personales.

42 Sentencia de 25 de octubre de 2011, eDate Advertising y otros (C-509/09 y C-161/10, EU:C:2011:685), apartados 48, 51 y 52. Véase, asimismo, la sentencia de 17 de octubre de 2017, Bolagsupplysningen e Ilsjan (C-194/16, EU:C:2017:766), apartados 38 y 47. Asimismo, según las interpretaciones doctrinales de esa sentencia, el tribunal del lugar del centro de los intereses puede pronunciarse en todo el mundo sobre los daños ocasionados. Véase Mankowski, P., Magnus, U., y Mankowski, P. (bajo la dirección de), Brussels I *bis* Regulation — Commentary, Otto Schmidt, Colonia, 2016, Art. 7, apartado 364. Lo mismo ocurre con el alcance territorial de la competencia general del foro del demandado. En su sentencia de 1 de marzo de 2005, Owusu (C-281/02, EU:C:2005:120), apartado 26, el Tribunal de Justicia consideró que el Convenio de Bruselas [Convenio de 27 de septiembre de 1968 relativo a la competencia judicial y a la ejecución de resoluciones judiciales en materia civil y mercantil (DO 1972, L 299, p. 32)] puede aplicarse cuando demandante y demandado están domiciliados en un Estado miembro y los hechos controvertidos se han producido en un Estado tercero. De lo anterior deduzco que, en ese caso, el foro del deudor es competente para pronunciarse sobre tales hechos controvertidos. Véase, también, Van Calster, G., Luks, C., Extraterritoriality and private international law, Recht in beweging — 19de VRG Alumnidag 2012, MAKLU, Amberes, Apeldoorn, 2012, p. 132.

43 Se trata pues, en este caso, de una competencia denominada «global» o «general». Véase Larsen, T.B., «The extent of jurisdiction under the forum delicti rule in European trademark litigation», *Journal of Private International Law*, 2018, vol. 14, nº 3, pp. 550 y 551.

44 Véase la sentencia de 26 de febrero de 2013, Åkerberg Fransson (C-617/10, EU:C:2013:105), apartado 19. Véanse también mis conclusiones presentadas en el asunto Google (alcance territorial de la retirada de enlaces de una lista de resultados) (C-507/17, EU:C:2019:15), punto 55.

91. Por último, aunque cabe extraer del Reglamento n.º 1215/2012 ciertas enseñanzas en lo que respecta a los efectos que los requerimientos judiciales surten en los Estados miembros, no ocurre lo mismo con los que se producen fuera de la Unión. En efecto, dicho Reglamento no exige que un requerimiento judicial emitido por un órgano jurisdiccional de un Estado miembro surta efectos también en terceros Estados. Por lo demás, el hecho de que un tribunal sea competente para pronunciarse sobre el fondo en virtud de una norma de competencia del Derecho de la Unión no implica que, al hacerlo, solo aplique las normas sustantivas comprendidas en el ámbito de aplicación de dicho Derecho y, en consecuencia, de la Carta.

92. Por esos motivos, tanto la cuestión de los efectos extraterritoriales de un requerimiento judicial que impone una obligación de retirada, como la del alcance territorial de esa obligación, deberían ser objeto de un análisis realizado no ya a la luz del Derecho de la Unión, sino, en particular, del Derecho internacional público y privado no armonizado en el ámbito de la Unión. [45] En efecto, nada apunta a que la situación objeto del litigio principal pueda estar comprendida en el ámbito de aplicación del Derecho de la Unión y, por consiguiente, de las normas de derecho internacional que inciden en la interpretación del Derecho de la Unión. [46]

93. Por consiguiente, en lo que respecta al alcance territorial de una obligación de retirada impuesta a un prestador de servicios de alojamiento de datos mediante un requerimiento judicial, debe considerarse que no está regulado ni por el artículo 15, apartado 1, de la Directiva 2000/31 ni por ninguna otra de sus disposiciones, de modo que dicho artículo no se opone a que se obligue a un prestador de servicios de alojamiento de datos a retirar datos difundidos mediante una plataforma de red social a nivel mundial. Además, ese alcance territorial tampoco está regulado por el Derecho de la Unión en la medida en que, en el presente asunto, el recurso de la demandante no está basado en él.

94. Dicho esto, en aras de la exhaustividad, para el caso de que el Tribunal de Justicia no siga mi propuesta, formularé algunas observaciones adicionales en lo que respecta a la retirada de datos difundidos a través de una plataforma de red social a nivel mundial.

95. Con arreglo al Derecho internacional, no está excluido que un requerimiento judicial pueda surtir los llamados efectos «extraterritoriales». [47] Pues bien, como he señalado en el punto 80 de las presentes conclusiones, ese planteamiento implicaría que la constatación del carácter ilícito de los datos de que se trata se extendiese a los territorios de otros Estados miembros, al margen del carácter lícito o ilícito de dichos datos con arreglo a la ley designada como aplicable conforme a las normas de conflicto de tales Estados miembros.

96. En consecuencia, cabría alegar que el Tribunal de Justicia ya ha admitido implícitamente ese enfoque en la sentencia Bolagsupplysningen e Ilsjan. [48] Es cierto que en esa sentencia el Tribunal de Justicia no se pronunció en absoluto sobre la ley aplicable a una solicitud de eliminación de contenidos publicados en línea. Sin embargo, el Tribunal de Justicia consideró que, habida cuenta de *la naturaleza ubicua de los contenidos puestos en línea en un sitio de Internet* y de que *el alcance de su difusión es, en principio, universal*, una demanda que tenga por objeto la rectificación de esos

45 En cuanto a los efectos territoriales de las resoluciones judiciales, a veces resulta difícil trazar los límites entre el Derecho internacional público y el privado. Véase Maier, H.G,, «Extraterritorial Jurisdiction at a Crossroads: An Intersection between Public and Private International Law», *The American Journal of International Law*, vol. 76, n.º 2, p. 280, y Svantesson, D.J.B., *Solving the Internet Jurisdiction Puzzle*, Oxford University Press, Oxford, 2017, p. 40.

46 Véase, en ese sentido, el auto de 12 de julio de 2012, Currà y otros (C-466/11, EU:C:2012:465), apartado 19.

47 Véase Douglas, M., «Extraterritorial injunctions affecting the internet», *Journal of Equity* 2018, vol. 12, p. 48; Riordan, J., *The Liability of Internet Intermediaries*, Oxford University Press, Oxford, 2011, p. 418.

48 Sentencia de 17 de octubre de 2017 (C-194/16, EU:C:2017:766, apartado 44.

contenidos debe interponerse ante un tribunal competente para conocer íntegramente de una acción de indemnización del daño. Así, dicho tribunal aplicaría la ley o las leyes designadas como aplicables en virtud de sus normas de conflicto.[49] No puede excluirse que, en ese contexto, un tribunal de un Estado miembro aplique una única ley designada aplicable.

97. Sin embargo, si ese órgano jurisdiccional no pudiera pronunciarse sobre la eliminación de contenidos publicados en línea a nivel mundial, se plantearía entonces la cuestión de qué tribunal está mejor situado para resolver sobre dicha eliminación. De hecho, todos los órganos jurisdiccionales se enfrentarían a las dificultades mencionadas en el punto anterior. Por lo demás, ¿puede exigirse a un demandante que, a pesar de esas dificultades prácticas, demuestre que los datos declarados ilícitos conforme a la ley designada aplicable en virtud de las normas de conflicto del Estado miembro del órgano jurisdiccional que conoce del procedimiento son ilícitos también conforme a todas las leyes potencialmente aplicables?

98. Aun admitiendo que las consideraciones relativas al carácter territorial de la protección que se deriva de las normas sustantivas en materia de lesión de la intimidad y de los derechos de la personalidad no se oponen a esas exigencias, sería preciso tener en cuenta los derechos fundamentales reconocidos a nivel mundial.

99. En efecto, como he afirmado en otro contexto, el interés legítimo del público en acceder a determinada información varía forzosamente en función de su ubicación geográfica, de un Estado tercero a otro.[50] Por consiguiente, en el caso de una retirada a nivel mundial, existiría el riesgo de que su aplicación impidiera acceder a los datos a personas establecidas en Estados distintos de aquel en el que se encuentra el órgano jurisdiccional que conoce del procedimiento.

100. Como conclusión, de las consideraciones anteriores se desprende que, en teoría, los órganos jurisdiccionales de un Estado miembro pueden pronunciarse sobre la retirada de datos difundidos a través de Internet a nivel mundial. Sin embargo, a raíz de las diferencias que existen entre las leyes nacionales, por un lado, y la protección de la intimidad y de los derechos de la personalidad que dichas leyes establecen, por otro lado, y con el fin de respetar derechos fundamentales ampliamente reconocidos, conviene que dichos órganos jurisdiccionales adopten una postura comedida. Por consiguiente, por cortesía internacional,[51] invocada por el Gobierno portugués, dichos órganos jurisdiccionales deberían limitar, en la medida de lo posible, los efectos extraterritoriales de sus requerimientos en materia de lesión de la intimidad y de los derechos de la personalidad.[52] El cumplimiento de una obligación de retirada no debería ir más allá de lo necesario para lograr la protección de la persona lesionada. Así, en lugar de ordenar la eliminación del contenido controvertido, el citado órgano jurisdiccional podría instar a que se impidiera el acceso a dichos datos mediante bloqueo geográfico.

101. Esas consideraciones no quedan desvirtuadas por la alegación de la demandante de que el bloqueo geográfico de los datos ilícitos es fácilmente eludible mediante un servidor proxy o por otros medios.

49 Véase también, en lo que respecta a las implicaciones de esta sentencia, Lundstedt, L., «Putting Right Holders in the Centre: Bolagsupplysningen and Ilsjan (C-194/16): What Does It Mean for International Jurisdiction over Transborder Intellectual Property Infringement Disputes?», *International Review of Intellectual Property and Competition Law*, 2018, vol. 49, nº 9, p. 1030, y Svantesson, D.J.B., «European Unión Claims of Jurisdiction over the Internet — an Analysis of Three Recent Key Developments», *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2018, vol. 9, n.º 2, p. 122, apartado 59.

50 Véanse mis conclusiones presentadas en el asunto Google (alcance territorial de la retirada de enlaces de una lista de resultados) (C-507/17, EU:C:2019:15), punto 60.

51 Véanse, en particular, sobre las implicaciones prácticas de dicha cortesía internacional, Maier, H.G., *op. cit.*, p. 283.

52 Véase la doctrina citada en la nota 47. Véase también, en contextos muy diferentes al del presente asunto, Scott, J., «The New EU "Extraterritoriality"», *Common Market Law Review*, 2014, vol. 51, n.º 5, p. 1378.

102. Para retomar una reflexión formulada en el contexto de situaciones comprendidas en el ámbito del Derecho de la Unión: la protección de la intimidad y de los derechos de la personalidad no debe garantizarse forzosamente de forma absoluta, sino ponerse en equilibrio con la protección de otros derechos fundamentales.[53] Conviene pues evitar medidas exorbitantes que no respeten el afán por garantizar un justo equilibrio entre los distintos derechos fundamentales en juego.[54]

103. Sin perjuicio de las anteriores observaciones adicionales, en lo que respecta al alcance territorial de una obligación de retirada, mantengo la postura expuesta en el punto 93 de las presentes conclusiones.

B. Sobre la tercera cuestión prejudicial

104. Mediante su tercera cuestión prejudicial, el órgano jurisdiccional remitente solicita que se determine si el artículo 15 de la Directiva 2000/31 se opone a que se dicte frente a un prestador de servicios de alojamiento de datos un requerimiento judicial que le imponga la obligación de retirar de su plataforma datos similares a los declarados ilícitos en el marco de un procedimiento judicial, después de que haya tenido conocimiento de esos datos.

105. La demandante, al igual que los Gobiernos austriaco, letón, portugués y finlandés, considera, en esencia, que el artículo 15, apartado 1, de la Directiva 2000/31 no se opone a que se requiera a un prestador de servicios de alojamiento de datos para que retire datos similares a los declarados ilícitos cuando tenga conocimiento de ellos. A la luz de su análisis de la primera cuestión prejudicial, Facebook Ireland considera que no procede responder a la tercera cuestión prejudicial.

106. Comparto, en esencia, el punto de vista de la demandante y de todos los Gobiernos que han intervenido en el procedimiento.

107. En efecto, por cuanto que una obligación de retirada no constituye una obligación de supervisión general de los datos almacenados por un prestador de servicios de alojamiento de datos, sino que se deriva de una toma de conocimiento a partir de una notificación remitida por la persona afectada o por un tercero, no se vulnera la prohibición establecida en el artículo 15, apartado 1, de la Directiva 2000/31.

108. Por consiguiente, propongo responder a la tercera cuestión prejudicial que el artículo 15, apartado 1, de la Directiva 2000/31 debe interpretarse en el sentido de que no se opone a que se obligue a un prestador de servicios de alojamiento de datos a retirar datos similares a los declarados ilícitos, por cuanto que una obligación de retirada no constituye una obligación de supervisión general de los datos almacenados y se deriva de una toma de conocimiento a partir de una notificación efectuada por la persona afectada, por terceros o por otra fuente.

53 Véase, por analogía, en lo que respecta al equilibrio entre el derecho de propiedad intelectual y el respeto a la vida privada y familiar, garantizado por el artículo 7 de la Carta, la sentencia de 18 de octubre de 2018, Bastei Lübbe (C-149/17, EU:C:2018:841), apartados 44 a 47. Véanse asimismo mis conclusiones presentadas en el asunto Bastei Lübbe (C-149/17, EU:C:2018:400), puntos 37 a 39.

54 Véase, en ese sentido, en lo que respecta a la protección de la propiedad intelectual, la sentencia de 27 de marzo de 2014, UPC Telekabel Wien (C-314/12, EU:C:2014:192), apartados 58 a 63. Véanse también las conclusiones del Abogado General Cruz Villalón presentadas en el asunto UPC Telekabel Wien (C-314/12, EU:C:2013:781), puntos 99 a 101, y mis conclusiones presentadas en el asunto Stichting Brein (C-610/15, EU:C:2017:99), puntos 69 a 72.

VI. Conclusión

109. A la luz de todas las consideraciones anteriores, propongo al Tribunal de Justicia que responda del siguiente modo a las cuestiones prejudiciales planteadas por el Oberster Gerichtshof (Tribunal Supremo de lo Civil y Penal, Austria):

«1) El artículo 15, apartado 1, de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), debe interpretarse en el sentido de que no se opone a que, mediante un requerimiento judicial, se obligue a un prestador de servicios de alojamiento de datos que explota una plataforma de red social a buscar e identificar, entre todos los datos difundidos por los usuarios de esa plataforma, datos idénticos a los declarados ilícitos por el órgano jurisdiccional que haya dictado dicho requerimiento. Mediante ese requerimiento judicial puede obligarse a un prestador de servicios de alojamiento de datos a buscar e identificar datos similares a los declarados ilícitos únicamente de entre los datos difundidos por el usuario que publicó tales datos. Un órgano jurisdiccional que se pronuncie sobre la retirada de esos datos similares debe garantizar que los efectos de su requerimiento son claros, precisos y previsibles. A ese propósito, debe poner en equilibro los derechos fundamentales en juego y tener en cuenta el principio de proporcionalidad.

2) En lo que respecta al alcance territorial de una obligación de retirada impuesta a un prestador de servicios de alojamiento de datos mediante un requerimiento judicial, debe considerarse que no está regulado ni por el artículo 15, apartado 1, de la Directiva 2000/31 ni por ninguna otra de sus disposiciones, de modo que dicho artículo no se opone a que se obligue a un prestador de servicios de alojamiento de datos a retirar datos difundidos mediante una plataforma de red social a nivel mundial. Además, ese alcance territorial tampoco está regulado por el Derecho de la Unión en la medida en que, en el presente asunto, la acción de la demandante no está basada en él.

3) El artículo 15, apartado 1, de la Directiva 2000/31 debe interpretarse en el sentido de que no se opone a que se obligue a un prestador de servicios de alojamiento de datos a retirar datos similares a los declarados ilícitos, por cuanto que una obligación de retirada no constituye una obligación de supervisión general de los datos almacenados y se deriva de una toma de conocimiento a partir de una notificación efectuada por la persona afectada, por terceros o por otra fuente.»