GA_P
Gómez-Acebo & Pombo

ANÁLISIS

Comercio electrónico

Excepciones al principio de control en origen de los servicios de la sociedad de la información y supervisión algorítmica de los contenidos alojados por un intermediario

(Sentencia del Tribunal de Justicia de 16 de junio del 2016, ass. acs. C-188/24 y C-190/24)

La Sentencia del Tribunal de Justicia de 16 de junio del 2026 (ass. acs. C-188/24 y C-190/24) aborda dos cuestiones centrales del régimen jurídico de los servicios de la sociedad de la información: el alcance de las excepciones al principio de control en origen por razones de orden y seguridad públicos, y la responsabilidad de las plataformas digitales cuando ejercen un control algorítmico sobre los contenidos.

ÁNGEL GARCÍA VIDAL
Catedrático de Derecho Mercantil
de la Universidad de Santiago de Compostela
Consejero académico (asesor externo) de Gómez-Acebo & Pombo

Julio 2026

El Tribunal de Justicia ha dictado una reciente sentencia en la que sienta dos importantes pautas en relación con la interpretación de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio, 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). Se trata de la Sentencia de 16 de junio del 2026, en los asuntos acumulados C-188/24 y C-190/24, *WebGroup Czech Republic y Coyote System*, ECLI:EU:C:2026:492.

1. Los principios de control en origen y de reconocimiento mutuo en materia de servicios de la sociedad de la información y las excepciones basadas en el orden público

1.1. *El marco normativo*

La Directiva 2000/31/CE parte del principio del control en origen de los servicios de la sociedad de la información. De conformidad con este principio (recogido en el artículo 3 de la directiva), el control de la legalidad de estos servicios debe producirse en el Estado de origen de dicha actividad, debiendo los demás Estados de la Union Europea impedir la libre prestación en su territorio de los servicios de la sociedad de la información de otros Estados miembros. Ahora bien, estos principios de control en origen y de reconocimiento mutuo operan en el denominado *ámbito coordinado*, esto es, en relación con las disposiciones normativas sobre las exigencias que el prestador debe cumplir en lo que respecta al acceso a la actividad de los servicios de la sociedad de la información —como las exigencias relativas a las cualificaciones y a los regímenes de autorización o notificación— y en lo que respecta al ejercicio de dicha actividad —como las exigencias relativas al comportamiento del prestador, a la calidad o al contenido del servicio, o a la responsabilidad del prestador—.

Con todo, excepcionalmente se prevé que estos principios no operan en relación con determinados ámbitos recogidos en el anexo de la directiva: derechos de autor, derechos afines y derechos de propiedad industrial, emisión de moneda electrónica, organismos de inversión colectiva, actividad aseguradora, libertad de elección de la ley aplicable al contrato, obligaciones contractuales en contratos celebrados por consumidores, validez formal de los contratos sobre derechos inmobiliarios y comunicaciones comerciales no solicitadas por correo electrónico.

De igual modo, los Estados miembros podrán tomar medidas que constituyan excepciones a dichos principios respecto de un determinado servicio de la sociedad de la información si las medidas son necesarias por motivos de orden público (en particular, la prevención, la investigación, el descubrimiento y el procesamiento del delito, incluidas la protección de menores y la lucha contra la instigación al odio por motivos de raza, sexo, religión o nacionalidad, así como las violaciones de la dignidad humana de personas individuales), protección de la salud pública, protección de los consumidores o seguridad pública, comprendidas la salvaguarda de la seguridad y la defensa

nacionales. Además, dichas medidas —que deben ser tomadas en contra de un servicio de la sociedad de la información que vaya en detrimento de objetivos o que presente un riesgo serio y grave de ir en detrimento de dichos ellos— han de ser proporcionadas a tales objetivos y, antes de adoptarlas, el Estado miembro deberá haber pedido al Estado miembro de origen que tome medidas y este último no haberlas tomado, o no haber resultado suficientes, haber notificado a la Comisión y al Estado miembro de origen su intención de adoptar dichas medidas.

1.2. *La sentencia del Tribunal de Justicia de 16 de junio del 2026: la importancia de la distinción entre normativa general y su aplicación concreta*

Sobre esta base normativa, en la citada sentencia de 16 de junio del 2026, el Tribunal de Justicia ha analizado si se ajustan a la Directiva de comercio electrónico y a los referidos principios de control en origen y de reconocimiento mutuo dos normativas francesas aplicables a servicios digitales establecidos en otros Estados miembros. Se trata, en primer lugar, de la normativa que establece la obligación de los sitios pornográficos de implantar sistemas eficaces de verificación de edad para impedir el acceso de menores y, en segundo lugar, de la que establece la prohibición temporal de difundir información sobre determinados controles policiales y de tráfico mediante aplicaciones de asistencia a la conducción. En concreto, y por motivos de orden público, seguridad pública y protección de las personas, se establece un mecanismo que permite a la autoridad administrativa competente prohibir a los operadores de este segundo tipo de servicios difundir, durante un periodo y dentro de un ámbito geográfico limitados, los mensajes de sus usuarios que puedan revelar la localización de controles de alcoholemia o de consumo de estupefacientes, así como de determinadas operaciones de policía judicial, por ejemplo, dirigidas contra personas buscadas por infracciones penales graves (incluidos actos terroristas) o por haberse fugado de un establecimiento psiquiátrico.

Pues bien, lo primero que hace el Tribunal de Justicia es analizar si las referidas normativas encajan en el ya mencionado *ámbito coordinado* de la directiva, que es donde, como regla general, operan los principios de control en origen y de reconocimiento mutuo. Y la conclusión a la que llega el tribunal es que las disposiciones penales destinadas a garantizar la protección de los menores, así como las medidas que imponen la implantación de mecanismos técnicos para bloquear el acceso de los menores a contenidos pornográficos, entran en el *ámbito coordinado* y constituyen una *exigencia* relativa al ejercicio de la actividad de los servicios de la sociedad de la información en el sentido de la Directiva 2000/31.

A este respecto, el Tribunal de Justicia sienta algunas pautas relevantes, entre las que destacan las siguientes:

1) el ámbito coordinado no se limita a las materias expresamente

reguladas y armonizadas en la Directiva de comercio electrónico;

2) el carácter general y abstracto de una norma no puede tener como efecto excluirla del ámbito coordinado;

3) las normativas nacionales (formen o no parte del Derecho penal) que persiguen objetivos de orden público, seguridad pública o protección de las personas no quedan excluidas, por ese solo hecho, del ámbito coordinado. En efecto, únicamente las normas adoptadas en los ámbitos fiscal, de protección de datos, de prácticas colusorias (Derecho de la competencia), de la actividad notarial, de la representación procesal y de los juegos de azar están expresamente excluidas del ámbito de aplicación de dicha directiva por su artículo 1, apartado 5. Por ello, concluye el Tribunal de Justicia que, siempre que no se refieran a los sectores excluidos por dicha disposición, las normas pertenecientes al Derecho penal o que persigan objetivos de orden público, seguridad pública o protección de las personas pueden estar comprendidas en el ámbito de aplicación de la directiva y, por tanto, en el ámbito coordinado.

Ahora bien, aunque esas disposiciones nacionales encajen en el ámbito coordinado de la directiva, es posible, como ya se ha recordado, que los Estados miembros adopten, respecto de un servicio concreto de la sociedad de la información, medidas que constituyan una excepción a los principios de control en origen y de reconocimiento mutuo cuando sean necesarias para garantizar el orden público, la protección de la salud pública, la seguridad pública o la protección de los consumidores, se adopten respecto de un servicio de la sociedad de la información que perjudique efectivamente esos objetivos o constituya un riesgo serio y grave de perjuicio para ellos, y sean proporcionadas a dichos objetivos.

Según el Tribunal de Justicia, los objetivos perseguidos por la primera normativa controvertida encajan en el concepto de *orden público*, pues éste comprende, en particular, la protección de los menores y la lucha contra las vulneraciones de la dignidad de la persona humana, así como la prevención, investigación, detección y persecución de infracciones penales. De igual modo, motivos de orden público, así como de seguridad pública o protección de las personas pueden justificar prohibiciones de difusión de información relativa a controles de tráfico o carreteros, como las previstas en esa normativa.

Con todo, en este punto es muy relevante el matiz que señala el Tribunal de Justicia al destacar que estas normas no quedan excluidas automáticamente del principio del control en origen por el mero hecho de ser normas penales o de seguridad pública. Según el Tribunal de Justicia, la directiva se opone a que un Estado miembro imponga directamente a todos los

operadores establecidos en otro Estado una obligación general de impedir el acceso de menores a contenidos pornográficos así como una prohibición general de difundir determinada información sobre controles policiales. Por el contrario, lo que sí es posible es que, en aplicación de dicha normativa general, un Estado miembro adopte medidas —individuales y específicas— contra un prestador establecido en otro Estado. Y, sobre esa base, el Tribunal de Justicia constata que en las referidas normativas francesas, además de las correspondientes prohibiciones generales, se prevé que la autoridad administrativa remitirá un requerimiento individualizado a cada operador para instarle al cumplimiento de la normativa.

Medidas individuales pueden justificar excepciones al principio de origen

Por lo tanto, aunque las disposiciones generales no, los requerimientos individuales dirigidos a los prestadores de servicios de comunicación al público que difunden contenidos pornográficos o las decisiones de prohibición dirigidas a los operadores de un servicio determinado para que no difundan ciertas informaciones sí pueden calificarse de medidas relativas a un servicio concreto de la sociedad de la información a efectos del artículo 3, apartado 4, letra *a*, de la Directiva 2000/31, permitiendo así que el Estado de destino excepcione el principio de control en origen, siempre que se respeten las exigencias de proporcionalidad y las garantías procedimentales establecidas por el Derecho de la Unión.

2. El control por medio de un algoritmo sobre la información almacenada y la pérdida de la exención de responsabilidad para los prestadores del servicio de *hosting*

Otra de las cuestiones que analiza el Tribunal de Justicia es si la normativa francesa que impide a los operadores de servicios electrónicos de ayuda a la conducción o a la navegación mediante geolocalización difundir determinadas informaciones sobre controles en carretera en realidad no supone imponerles una obligación general de supervisar la información que transmiten; tal obligación general de supervisión la prohíbe el artículo 15 de la directiva (artículo hoy derogado por el Reglamento (UE) 2022/2065, de Servicios Digitales, que sienta tal prohibición en su artículo 8).

En primer lugar, el tribunal recuerda su jurisprudencia previa (Sentencia de 3 de octubre del 2019, *Glawischnig-Piesczek*, C-18/18) según la cual la prohibición impuesta a los Estados miembros de establecer para los prestadores intermediarios de servicios una obligación general de supervisión no afecta a las obligaciones de supervisión en «casos concretos» y, en particular, deja intactas las órdenes dictadas por las autoridades nacionales con arreglo a sus respectivas legislaciones y relativas a un caso de esa naturaleza. Una orden

de este tipo no obliga al prestador a realizar una evaluación autónoma del contenido almacenado, puesto que puede limitarse a identificar los contenidos afectados por la orden mediante búsquedas automatizadas.

Con estos presupuestos, la prohibición de control general se aplica a los prestadores intermediarios de servicios, y una cuestión previa sería la de determinar si el prestador del servicio de ayuda a la conducción tiene tal condición. Es ésta una cuestión cuya determinación el Tribunal de Justicia deja al juez nacional. Pero, en todo caso, hace una consideración muy relevante para determinar si es de aplicación la exención de responsabilidad de los intermediarios de *hosting*, regulada inicialmente en el artículo 14 de la directiva (y en la actualidad en el artículo 6 del Reglamento de Servicios Digitales). Según esta exención, 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 *a*) de que el prestador de servicios no tenga conocimiento efectivo de que la actividad o la información sea 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 *b*) de que, 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.

Pues bien, según el Tribunal de Justicia, las condiciones de conocimiento y control deben entenderse como alternativas y autónomas entre sí. Por consiguiente, el operador de un servicio de la sociedad de la información que controle la información almacenada queda excluido del beneficio, incluso aunque no llegue a conocer esa información debido a la automatización de su tratamiento.

Y, a este respecto, es especialmente relevante el hecho de que en la sentencia ahora comentada el Tribunal de Justicia declare que el control puede ejercerse por medio de un algoritmo, afirmando que es precisamente mediante el algoritmo utilizado como dicho operador ejerce un control sobre la información almacenada. En consecuencia, mientras haya predeterminado, mediante ese algoritmo, las condiciones conforme a las cuales dicha información será o no difundida, carece de relevancia que el operador no realice por sí mismo intervenciones adicionales destinadas a promover, modificar o eliminar la información almacenada para su difusión.

El control algorítmico puede excluir la exención de responsabilidad

Por lo tanto, si, más allá de una mera clasificación e indexación de la información para facilitar su accesibilidad, el algoritmo utilizado determina, en interés del operador o de su servicio, en qué condiciones,

de qué manera y con qué orden de prioridad se difunde o no dicha información, ese operador ejerce un control sobre ella. En consecuencia, el servicio que presta no puede calificarse de «servicio de la sociedad de la información consistente en el almacenamiento de información proporcionada por un destinatario del servicio», por lo que no sería de aplicación la exención de responsabilidad.