

Miércoles, 17 de abril de 2019

P8\_TA(2019)0421

### **Lucha contra la difusión de contenidos terroristas en línea \*\*\*I**

**Resolución legislativa del Parlamento Europeo, de 17 de abril de 2019, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo para la prevención de la difusión de contenidos terroristas en línea (COM(2018)0640 — C8-0405/2018 — 2018/0331(COD))**

**(Procedimiento legislativo ordinario: primera lectura)**

(2021/C 158/68)

*El Parlamento Europeo,*

- Vista la propuesta de la Comisión al Parlamento Europeo y al Consejo (COM(2018)0640),
  - Vistos el artículo 294, apartado 2, y el artículo 114 del Tratado de Funcionamiento de la Unión Europea, conforme a los cuales la Comisión le ha presentado su propuesta (C8-0405/2018),
  - Visto el artículo 294, apartado 3, del Tratado de Funcionamiento de la Unión Europea,
  - Visto el dictamen motivado presentado por la Cámara de Diputados checa, de conformidad con lo dispuesto en el Protocolo nº 2 sobre la aplicación de los principios de subsidiariedad y proporcionalidad, en el que se afirma que el proyecto de acto legislativo no respeta el principio de subsidiariedad,
  - Visto el dictamen del Comité Económico y Social Europeo de 12 de diciembre de 2018 <sup>(1)</sup>,
  - Visto el artículo 59 de su Reglamento interno,
  - Vistos el informe de la Comisión de Mercado Interior y Protección del Consumidor y las opiniones de la Comisión de Cultura y Educación, y de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (A8-0193/2019),
1. Aprueba la Posición en primera lectura que figura a continuación;
  2. Pide a la Comisión que le consulte de nuevo si sustituye su propuesta, la modifica sustancialmente o se propone modificarla sustancialmente;
  3. Encarga a su presidente que transmita la Posición del Parlamento al Consejo y a la Comisión, así como a los Parlamentos nacionales.

---

### **P8\_TC1-COD(2018)0331**

**Posición del Parlamento Europeo aprobada en primera lectura el 17 de abril de 2019 con vistas a la adopción del Reglamento (UE) 2019/... del Parlamento Europeo y del Consejo para la ~~prevención de~~ **lucha contra la difusión de contenidos terroristas en línea [Enm. 1]****

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 114,

Vista la propuesta de la Comisión Europea,

---

<sup>(1)</sup> DO C 110 de 22.3.2019, p. 67.

Miércoles, 17 de abril de 2019

Previa transmisión del proyecto de acto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo <sup>(1)</sup>,

De conformidad con el procedimiento legislativo ordinario <sup>(2)</sup>,

Considerando lo siguiente:

- (1) El presente Reglamento tiene por objetivo garantizar el correcto funcionamiento del mercado único digital en una sociedad abierta y democrática, ~~evitando~~ **luchando contra** el uso indebido de los servicios de alojamiento de datos con fines terroristas **y contribuyendo a la seguridad pública en las sociedades europeas**. El funcionamiento del mercado único digital debe mejorarse mediante el refuerzo de la seguridad jurídica para los prestadores de servicios de alojamiento de datos, el refuerzo de la confianza de los usuarios en el entorno en línea y el fortalecimiento de las garantías de la libertad de expresión, **la libertad de recibir y comunicar información e ideas en una sociedad abierta y democrática y la libertad y el pluralismo de los medios de comunicación**. [Enm. 2]
- (1 bis) **La regulación de los prestadores de servicios de alojamiento de datos solo puede complementar las estrategias de los Estados miembros destinadas a la lucha contra el terrorismo, que deben centrarse en las medidas al margen de Internet, como la inversión en trabajo social, las iniciativas de desradicalización y la colaboración con las comunidades afectadas para prevenir de forma sostenible la radicalización en la sociedad**. [Enm. 3]
- (1 ter) **Los contenidos terroristas forman parte del problema más amplio de los contenidos ilícitos en línea, que incluyen otros tipos de contenidos como la explotación sexual infantil, prácticas comerciales ilícitas y la violación de los derechos de propiedad intelectual. A menudo, el tráfico de contenidos ilícitos lo llevan a cabo organizaciones terroristas y otras organizaciones delictivas con el fin de proceder al blanqueo de capitales y obtener capital inicial para financiar sus operaciones. Este problema requiere una combinación de medidas legislativas, no legislativas y voluntarias basadas en la colaboración entre autoridades y proveedores, por la que se respeten plenamente los derechos fundamentales. Aunque el peligro que presentan los contenidos ilícitos se ha visto mitigado por iniciativas exitosas como el Código de conducta para la lucha contra la incitación ilegal al odio en internet, adoptado por la industria, y la Alianza Mundial WePROTECT para acabar con el abuso sexual de menores en línea, es necesario establecer un marco legislativo de cooperación transfronteriza entre las autoridades reguladoras nacionales a fin de eliminar los contenidos ilícitos**. [Enm. 4]
- (2) Los prestadores de servicios de alojamiento de datos activos en Internet desempeñan un papel esencial en la economía digital, consistente en conectar a las empresas y los ciudadanos, **en proporcionar oportunidades de aprendizaje** y en facilitar el debate público y la distribución y recepción de la información, las opiniones y las ideas, lo que contribuye de forma importante a la innovación, el crecimiento económico y la creación de empleo en la Unión. No obstante, en ocasiones algunos terceros hacen un uso abusivo de sus servicios para llevar a cabo actividades ilícitas en línea. Es particularmente preocupante el uso indebido de los servicios de alojamiento de datos por parte de grupos terroristas y sus seguidores para difundir contenidos terroristas en línea, con el fin último de propagar su mensaje, de radicalizar y reclutar a personas y de facilitar y dirigir actividades terroristas. [Enm. 5]
- (3) **Aunque no se trate del único factor**, la presencia de contenidos terroristas en línea **ha demostrado ser un catalizador para la radicalización de individuos que han perpetrado actos terroristas y, por tanto**, tiene graves consecuencias negativas para los usuarios, los ciudadanos y la sociedad en general, así como para los prestadores de servicios en línea que alojan esos contenidos, dado que menoscaba la confianza de sus usuarios y daña sus modelos de negocio. En vista de su papel esencial y **en proporción a** los medios y capacidades tecnológicos asociados a los servicios que prestan, los prestadores de servicios en línea tienen una responsabilidad social particular que los obliga a proteger sus servicios del uso indebido por parte de los terroristas y a ayudar **a las autoridades competentes** a evitar la difusión de contenidos terroristas a través de sus servicios, **al tiempo que tienen en cuenta la importancia fundamental de la libertad de expresión y la libertad de recibir y comunicar información en una sociedad abierta y democrática**. [Enm. 6]

<sup>(1)</sup> DO C 110 de 22.3.2019, p. 67.

<sup>(2)</sup> Posición del Parlamento Europeo de 17 de abril de 2019.

Miércoles, 17 de abril de 2019

- (4) La labor a escala de la Unión destinado a combatir los contenidos terroristas en línea comenzó en 2015, con un marco de cooperación voluntaria entre Estados miembros y prestadores de servicios de alojamiento de datos, y es necesario complementarlo con un marco legislativo claro para seguir reduciendo la accesibilidad de los contenidos terroristas en línea y abordar adecuadamente un problema que evoluciona con rapidez. Ese marco legislativo pretende basarse en esfuerzos voluntarios, reforzados por la Recomendación (UE) 2018/334 de la Comisión <sup>(3)</sup>, y responde a los llamamientos realizados por el Parlamento Europeo para reforzar las medidas de lucha contra los contenidos ilícitos y nocivos, **de conformidad con el marco horizontal establecido por la Directiva 2000/31/CE**, y por el Consejo Europeo para mejorar la detección automática y la retirada de los contenidos que incitan actos terroristas. [Enm. 7]
- (5) La aplicación del presente Reglamento no debe afectar a la aplicación del artículo 14 de la Directiva 2000/31/CE <sup>(4)</sup>. ~~En particular, las medidas tomadas por un prestador de servicios de alojamiento de datos en cumplimiento del presente Reglamento, incluidas medidas proactivas cualesquiera, no deben suponer, por sí mismas, que ese prestador de servicios deje de beneficiarse de la exención de responsabilidad que le concede esa disposición. El presente Reglamento no afecta a los poderes de que están revestidos las autoridades y los órganos jurisdiccionales nacionales de establecer la responsabilidad de los prestadores de servicios de alojamiento de datos en casos específicos en los que no se cumplan las condiciones para la exención de responsabilidad con arreglo al artículo 14 de la Directiva 2000/31/CE.~~ [Enm. 8]
- (6) Las normas para ~~evitar~~ **luchar contra** el uso indebido de los servicios de alojamiento de datos para la difusión de contenidos terroristas en línea, con el fin de garantizar el correcto funcionamiento del mercado interior, se establecen en el presente Reglamento ~~con pleno respeto de~~ **deben respetar plenamente** los derechos fundamentales protegidos en el ordenamiento jurídico de la Unión, en particular los garantizados en la Carta de los Derechos Fundamentales de la Unión Europea. [Enm. 9]
- (7) El presente Reglamento ~~contribuye~~ **pretende contribuir** a la protección de la seguridad pública ~~a la vez que establece~~ **debe establecer** garantías adecuadas y sólidas para velar por la protección de los derechos fundamentales afectados. Dichos derechos son el respeto de la vida privada y de la protección de los datos de carácter personal; el derecho a la tutela judicial efectiva; el derecho a la libertad de expresión, incluido el derecho de recibir y transmitir información; el derecho a la libertad de empresa y el principio de no discriminación. Las autoridades competentes y los prestadores de servicios de alojamiento de datos únicamente deben adoptar medidas que sean necesarias, adecuadas y proporcionadas en una sociedad democrática, teniendo en cuenta la importancia particular concedida a la libertad de expresión ~~y de~~ **la libertad de recibir y comunicar** información ~~e ideas, los derechos al respeto de la vida privada y familiar y la protección de los datos personales, que constituye uno de~~ **constituyen** los pilares esenciales de una sociedad democrática y pluralista ~~y uno de~~ **son** los valores en que se fundamenta la Unión. ~~Las medidas que constituyan una interferencia~~ **Toda medida debe evitar interferir** con la libertad de expresión y de información ~~deben ser muy específicas, en el sentido de que deben~~ **en la medida de lo posible, debe** servir para ~~evitar~~ **luchar contra** la difusión de contenidos terroristas **aplicando un enfoque dotado de objetivos muy estrictos**, sin por ello afectar, no obstante, al derecho a recibir y transmitir información lícitamente, teniendo en cuenta el papel esencial de los prestadores de servicios de alojamiento de datos en el fomento del debate público y la distribución y recepción de hechos, opiniones e ideas de conformidad con la ley. **Las medidas efectivas de lucha contra el terrorismo en línea y la protección de la libertad de expresión no son objetivos incompatibles, sino complementarios y se refuerzan mutuamente.** [Enm. 10]
- (8) El derecho a una tutela judicial efectiva está consagrado en el artículo 19 del TUE y el artículo 47 de la Carta de los Derechos Fundamentales de la Unión Europea. Toda persona física o jurídica tiene derecho a una tutela judicial efectiva por parte del órgano jurisdiccional nacional competente contra cualquier medida tomada con arreglo al presente Reglamento que pueda afectar negativamente a sus derechos. Este derecho incluye, en particular, la

<sup>(3)</sup> Recomendación (UE) 2018/334 de la Comisión, de 1 de marzo de 2018, sobre medidas para combatir eficazmente los contenidos ilícitos en línea (DO L 63 de 6.3.2018, p. 50).

<sup>(4)</sup> Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) (DO L 178 de 17.7.2000, p. 1).

Miércoles, 17 de abril de 2019

posibilidad de que los prestadores de servicios de alojamiento de datos y los proveedores de contenidos impugnen de manera efectiva las órdenes de retirada ante el órgano jurisdiccional del Estado miembro cuyas autoridades hayan emitido la orden de retirada, **así como las posibilidades de que los proveedores de contenidos impugnen las medidas específicas adoptadas por el prestador de servicios de alojamiento de datos.** [Enm. 11]

- (9) Con el fin de aportar claridad sobre las acciones que tanto los prestadores de servicios en línea como las autoridades competentes deben emprender para ~~evitar~~ **luchar contra** la difusión de contenidos terroristas en línea, el presente Reglamento debe establecer una definición de contenidos terroristas a efectos preventivos, basada en la definición de delitos de terrorismo de la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo <sup>(5)</sup>. Dada la necesidad de ~~luchar contra la propaganda terrorista~~ **hacer frente a los contenidos terroristas** en línea más ~~no cívicos~~, la definición debe incluir el material y la información que incite ~~o inste~~ **a la comisión de delitos de terrorismo o a la contribución a ellos, las fomente o las defienda; facilite instrucciones para la comisión de dichos delitos o promueva la participación en las actividades de un grupo terrorista, provocando el peligro de que puedan cometerse intencionadamente uno o más de esos delitos. La definición también debe cubrir los contenidos que instruyan sobre la fabricación y el uso de explosivos, armas de fuego o cualesquiera otras armas o sustancias nocivas o peligrosas, así como de sustancias químicas, biológicas, radiológicas y nucleares (QBRN), y cualquier otra orientación sobre otros métodos y técnicas, entre ellas la selección de objetivos, a fin de cometer delitos de terrorismo.** Dicha información incluye, en particular, texto, imágenes, grabaciones de sonido y vídeos. Al evaluar si los contenidos constituyen contenidos terroristas en el sentido del presente Reglamento, las autoridades competentes y los prestadores de servicios de alojamiento de datos deben tener en cuenta factores como la naturaleza y la literalidad de las declaraciones, el contexto en el que se realizaron y su potencial de conllevar consecuencias nocivas que afecten a la seguridad y la integridad de las personas. El hecho de que el material haya sido producido por una organización o persona incluida en la lista de terroristas de la UE, sea atribuible a ella o se haya difundido en su nombre constituye un factor importante en esa evaluación. Los contenidos difundidos con fines educativos, periodísticos o de investigación, **o con fines de sensibilización contra actividades terroristas**, deben ser adecuadamente protegidos. **Especialmente en los casos en que el proveedor de contenidos asuma una responsabilidad editorial, cualquier decisión relativa a la retirada de material difundido debe tener en cuenta las normas periodísticas establecidas por la regulación de prensa o de los medios de comunicación coherentes con la legislación de la Unión y la Carta de los Derechos Fundamentales de la Unión Europea.** Además, la expresión de puntos de vista radicales, polémicos o controvertidos en el debate público sobre cuestiones políticas sensibles no debe considerarse contenido terrorista. [Enm. 12]

- (10) Con objeto de abarcar aquellos servicios de alojamiento de datos en que se difunden contenidos terroristas, el presente Reglamento debe ser aplicable a los servicios de la sociedad de la información que almacenen información proporcionada por un receptor del servicio a petición de este y pongan la información almacenada a disposición ~~de~~ **terceros del público**, independientemente de que esa actividad sea de naturaleza meramente técnica, automática o pasiva. Esos prestadores de servicios de la sociedad de la información incluyen, a modo de ejemplo, las plataformas de redes sociales, los servicios de emisión de vídeo en tiempo real, los servicios de distribución de vídeo, imágenes y audio, los servicios de intercambio de archivos y otros servicios en la nube, en la medida en que ponen información a disposición ~~de terceros del público~~, y los sitios web en los que los usuarios pueden hacer comentarios o colgar reseñas. El Reglamento debe también ser aplicable a los prestadores de servicios de alojamiento de datos establecidos fuera de la Unión pero que ofrecen servicios dentro de la Unión, dado que una proporción significativa de los prestadores de servicios de alojamiento de datos expuestos a contenidos terroristas en sus servicios están establecidos en terceros países. Con ello se busca garantizar que todas las empresas con actividad en el mercado único digital cumplan los mismos requisitos, independientemente de su país de establecimiento. La determinación de si un prestador de servicios ofrece dichos servicios en la Unión requiere evaluar si el prestador permite a las personas físicas o jurídicas que se encuentren en uno o más Estados miembros utilizar sus servicios. Sin embargo, la mera accesibilidad del sitio web de un prestador de servicios o de una dirección de correo electrónico y otros datos de contacto en uno o más Estados miembros no debe ser, por sí sola, una condición suficiente para que el presente Reglamento resulte de aplicación. **No debe aplicarse a los servicios en la nube, incluidos los servicios de empresa a empresa en la nube, para los cuales el prestador de servicios no tenga**

<sup>(5)</sup> Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo (DO L 88 de 31.3.2017, p. 6).

Miércoles, 17 de abril de 2019

**ningún derecho contractual respecto a los contenidos que se almacenan o a la forma en que sus clientes o los usuarios finales de dichos clientes los tratan o ponen a disposición del público, y cuando el prestador de servicios no tenga capacidad técnica para retirar contenidos específicos almacenados por sus clientes o los usuarios finales de sus servicios.** [Enm. 13]

- (11) Para determinar el ámbito de aplicación del presente Reglamento, debe resultar relevante una conexión sustancial con la Unión. Debe considerarse que existe tal conexión sustancial con la Unión cuando el prestador de servicios tenga un establecimiento en la Unión o, en ausencia de este, cuando exista un número significativo de usuarios en uno o más Estados miembros, o se orienten actividades hacia uno o más Estados miembros. La orientación de las actividades hacia uno o más Estados miembros puede determinarse en función de todas las circunstancias pertinentes, incluidos factores como el uso de una lengua o una moneda utilizada generalmente en ese Estado miembro, o la posibilidad de encargar bienes o servicios. La orientación de las actividades hacia un Estado miembro también puede derivarse de la disponibilidad de una aplicación para móvil en la tienda de aplicaciones nacional correspondiente, de la existencia de publicidad local o publicidad en la lengua utilizada en dicho Estado miembro, o de una gestión de las relaciones con los clientes que incluya por ejemplo la prestación de servicios a los clientes en la lengua comúnmente utilizada en tal Estado miembro. También se presumirá que existe una conexión sustancial cuando el prestador de servicios dirija sus actividades hacia uno o más Estados miembros, como establece el artículo 17, apartado 1, letra c), del Reglamento (UE) n.º 1215/2012 del Parlamento Europeo y del Consejo <sup>(6)</sup>. Por otro lado, la prestación del servicio con el mero objeto de cumplir la prohibición de discriminación establecida en el Reglamento (UE) 2018/302 del Parlamento Europeo y del Consejo <sup>(7)</sup> no puede, por esa única razón, considerarse como dirección u orientación de las actividades hacia un determinado territorio dentro de la Unión. [Enm. 14]
- (12) Los prestadores de servicios de alojamiento de datos deben aplicar ciertos deberes de diligencia, con el fin de ~~evitar~~ **luchar contra** la difusión de contenidos terroristas en sus servicios **al público**. Dichos deberes de diligencia no deben convertirse en una obligación general de supervisión ~~para los prestadores de servicios de alojamiento de datos de supervisar los datos que almacenan, ni en una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas~~. Entre los deberes de diligencia debe incluirse que, al aplicar el presente Reglamento, los prestadores de servicios de alojamiento de datos actúen de forma **transparente**, resuelta, proporcionada y no discriminatoria en relación con los contenidos que almacenen, en particular al aplicar sus propios términos y condiciones, con vistas a evitar la retirada de contenidos que no sean terroristas. La retirada o el bloqueo del acceso ha de realizarse en observancia de la libertad de expresión ~~y de~~ **la libertad de recibir y comunicar información e ideas en una sociedad abierta y democrática y la libertad y el pluralismo de los medios de comunicación**. [Enm. 15]
- (13) Deben armonizarse el procedimiento y las obligaciones resultantes de las órdenes ~~legales~~ **de retirada** que exijan a los prestadores de servicios de alojamiento de datos retirar los contenidos terroristas o bloquear el acceso a ellos, previa evaluación por las autoridades competentes. Los Estados miembros deben ser libres para designar ~~las autoridades competentes~~ **la autoridad competente** para esas funciones, que ~~pueden~~ **puede** ser autoridades administrativas, policiales o judiciales **una autoridad judicial o una autoridad administrativa o policial funcionalmente independiente**. Dada la velocidad con la que se difunden los contenidos terroristas por los servicios en línea, esta disposición impone obligaciones a los prestadores de servicios en línea para garantizar que se retiran los contenidos terroristas a que se refiere la orden de retirada, o que se bloquea el acceso a ellos, en el plazo de una hora desde la recepción de la orden de retirada. ~~Son los prestadores de servicios en línea los que deben decidir si retiran los contenidos en cuestión o bloquean el acceso a ellos para los usuarios de la Unión.~~ [Enm. 16]
- (14) Las autoridades competentes deben transmitir el orden de retirada directamente ~~al destinatario~~ y al punto de contacto **del proveedor de servicios de alojamiento de datos y, cuando el establecimiento principal del proveedor de servicios de alojamiento de datos se encuentre en otro Estado miembro, a la autoridad competente de ese Estado miembro** por cualquier medio electrónico capaz de producir un registro escrito en unas condiciones que permitan al prestador de servicios determinar la autenticidad, incluidas la fecha y hora precisas de envío y recepción de la orden, como correos electrónicos y plataformas seguros u otros canales seguros, incluidos aquellos dispuestos

<sup>(6)</sup> Reglamento (UE) n.º 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (DO L 351 de 20.12.2012, p. 1).

<sup>(7)</sup> Reglamento (UE) 2018/302 del Parlamento Europeo y del Consejo, de 28 de febrero de 2018, sobre medidas destinadas a impedir el bloqueo geográfico injustificado y otras formas de discriminación por razón de la nacionalidad, del lugar de residencia o del lugar de establecimiento de los clientes en el mercado interior y por el que se modifican los Reglamentos (CE) n.º 2006/2004 y (UE) 2017/2394 y la Directiva 2009/22/CE (DO L 601 de 2.3.2018, p. 1).

Miércoles, 17 de abril de 2019

por el prestador de servicios con arreglo a las normas de protección de los datos de carácter personal. Este requisito puede cumplirse, en particular, mediante el uso de servicios cualificados de entrega electrónica certificada, de conformidad con el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo<sup>(8)</sup>. [Enm. 17]

- (15) ~~Los requerimientos por parte de las autoridades competentes o de Europol constituyen un medio eficaz y rápido para poner a los prestadores de servicios de alojamiento de datos sobre aviso acerca de contenidos específicos en sus servicios. Este mecanismo para alertar a los prestadores de servicios de alojamiento de datos acerca de información que puede considerarse contenido terrorista, para que el prestador tome en consideración voluntariamente la compatibilidad de esa información con sus términos y condiciones, debe seguir estando disponible junto a las órdenes de retirada. Es importante que los prestadores de servicios de alojamiento de datos evalúen esos requerimientos de manera prioritaria e informen rápidamente sobre las medidas que hayan adoptado. La decisión final sobre la retirada o no de los contenidos por su incompatibilidad con los términos y condiciones sigue correspondiendo al prestador de servicios de alojamiento de datos. La aplicación del presente Reglamento en lo que se refiere a los requerimientos no afecta al mandato de Europol de conformidad con el Reglamento (UE) 2016/794<sup>(9)</sup>. [Enm. 18]~~
- (16) Dadas la escala y la velocidad necesarias para detectar y retirar eficazmente los contenidos terroristas, la adopción de medidas ~~proactivas~~**específicas** proporcionadas, ~~que incluso se sirvan de medios automatizados en ciertos casos,~~ constituye un elemento esencial para luchar contra los contenidos terroristas en línea. Con el fin de reducir la accesibilidad de los contenidos terroristas en sus servicios, los prestadores de servicios de alojamiento de datos deben evaluar si resulta adecuado tomar medidas ~~proactivas~~**específicas**, atendiendo a los riesgos y el nivel de exposición a los contenidos terroristas, así como a los efectos sobre los derechos de terceros y el interés público de ~~recibir y comunicar~~ información, **en particular cuando exista un nivel elevado de exposición a contenidos terroristas y de recepción de órdenes de retirada**. En consecuencia, los prestadores de servicios de alojamiento de datos deben determinar qué medida ~~proactiva~~ adecuada, **específica**, eficaz y proporcionada debe emplearse. Esta exigencia no conlleva una obligación general de supervisión. **Esas medidas específicas pueden incluir la presentación de informes periódicos a las autoridades competentes, el aumento de los recursos humanos a cargo de las medidas de protección de los servicios contra la difusión pública de contenidos terroristas y el intercambio de mejores prácticas**. En el contexto de esta evaluación, la ausencia de órdenes de retirada ~~y de requerimientos dirigidos~~**dirigidas** a un prestador de servicios de alojamiento de datos es una indicación de un bajo nivel de exposición a los contenidos terroristas. [Enm. 19]
- (17) Al poner en marcha medidas ~~proactivas~~**específicas**, los prestadores de servicios de alojamiento de datos deben garantizar que se respeta el derecho de los usuarios a la libertad de expresión y ~~de información, incluida~~ la libertad de recibir y transmitir información ~~libremente~~**ideas en una sociedad abierta y democrática**. Además de cumplir las exigencias que establece la ley, en particular la legislación sobre protección de los datos de carácter personal, los prestadores de servicios de alojamiento de datos deben actuar con la diligencia debida e implementar garantías, incluidas en particular la supervisión y las verificaciones por personas, ~~cuando proceda,~~ para evitar que cualquier decisión no intencionada y errónea derive en la retirada de contenidos que no sean terroristas. ~~Esto reviste especial importancia cuando los prestadores de servicios de alojamiento de datos usen medios automatizados para detectar los contenidos terroristas. Cualquier decisión de uso de medios automatizados, haya sido tomada por el prestador de servicios de alojamiento de datos por su propia iniciativa o previa solicitud de la autoridad competente, debe evaluarse en relación con la fiabilidad de la tecnología subyacente y las consiguientes repercusiones sobre los derechos fundamentales.~~ [Enm. 20]
- (18) Con objeto de garantizar que los prestadores de servicios de alojamiento de datos expuestos a contenidos terroristas tomen medidas adecuadas para evitar el uso indebido de sus servicios, ~~las autoridades competentes deben~~**la autoridad competente debe** exigir la presentación de informes sobre las medidas **específicas** tomadas a los prestadores de servicios de alojamiento de datos que hayan recibido ~~una orden~~**un número significativo de órdenes definitivas** de retirada ~~que se haya convertido en definitiva~~. Dichas medidas pueden consistir en medidas para evitar que vuelvan a subirse contenidos terroristas retirados o cuyo acceso haya sido bloqueado como resultado de una orden de retirada o un requerimiento recibidos por el prestador de servicios de alojamiento de datos, en relación con instrumentos de titularidad pública o privada que contengan contenidos terroristas conocidos. También pueden incluir el empleo de instrumentos técnicos fiables, ~~tanto disponibles en el mercado como desarrollados por~~

<sup>(8)</sup> Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (DO L 257 de 28.8.2014, p. 73).

<sup>(9)</sup> Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo (DO L 135 de 24.5.2016, p. 53).

Miércoles, 17 de abril de 2019

~~el propio prestador de servicios de alojamiento de datos~~, para la detección de nuevos contenidos terroristas. El prestador de servicios debe presentar informes sobre las medidas ~~proactivas~~ específicas puestas en marcha, con el fin de permitir a la autoridad competente juzgar si las medidas son **necesarias**, eficaces y proporcionadas y si, en caso de que se usen medios automatizados, el prestador de servicios de alojamiento de datos posee las capacidades necesarias para la supervisión y la verificación por personas. En su examen de la eficacia, **la necesidad** y la proporcionalidad de las medidas, las autoridades competentes deben tener en cuenta parámetros pertinentes, entre ellos el número de órdenes de retirada ~~y de requerimientos enviados~~ **enviadas** al prestador, **su tamaño** y su capacidad económica y los efectos de su servicio en la difusión de contenidos terroristas (por ejemplo, tomando en consideración el número de usuarios en la Unión), **así como las garantías establecidas para proteger la libertad de expresión y de información y el número de incidentes relativos a la restricción de contenidos lícitos**. [Enm. 21]

- (19) Tras la solicitud, la autoridad competente debe entablar un diálogo con el prestador de servicios de alojamiento de datos sobre las medidas ~~proactivas~~ **específicas** que deben adoptarse. En caso necesario, la autoridad competente debe ~~imponer~~ **pedir al proveedor de alojamiento de datos que reevalúe las medidas necesarias o solicitar** la adopción de medidas **específicas** adecuadas, eficaces y proporcionadas cuando considere que las medidas adoptadas **no respetan los principios de necesidad y proporcionalidad** o son insuficientes para atenuar los riesgos. **La autoridad competente solo debe pedir medidas específicas cuya adopción pueda esperarse del proveedor de servicios de alojamiento de datos, teniendo en cuenta, entre otros factores, los recursos financieros y de otra índole de dicho prestador.** La ~~decisión~~ **petición** de ~~imponer~~ **adoptar** dichas medidas ~~proactivas~~ específicas no debe, ~~en principio,~~ conllevar la imposición de una obligación general de supervisión, en el sentido del artículo 15, apartado 1, de la Directiva 2000/31/CE. Teniendo ~~en cuenta los riesgos particularmente graves asociados a la~~ difusión de contenidos terroristas, las decisiones adoptadas por las autoridades competentes sobre la base del presente Reglamento pueden constituir excepciones al criterio establecido en el artículo 15, apartado 1, de la Directiva 2000/31/CE, en el caso de ciertas medidas específicas y concretas cuya adopción sea necesaria por razones imperiosas de seguridad pública. Antes de adoptar esas decisiones, la autoridad competente debe establecer un justo equilibrio entre los objetivos de interés público y los derechos fundamentales afectados, en particular la libertad de expresión y de información y la libertad de empresa, y aportar una justificación adecuada. [Enm. 22]
- (20) La obligación de los prestadores de servicios de alojamiento de datos de conservar los contenidos retirados y los datos conexos debe fijarse con fines específicos y limitarse al tiempo necesario. Es menester ampliar la exigencia de conservación a los datos conexos en la medida en que cualquiera de esos datos pudiera perderse, de otro modo, como consecuencia de la retirada del contenido correspondiente. Los datos conexos pueden consistir en datos tales como «datos de los abonados», que incluyen, en particular, datos correspondientes a la identidad del proveedor de contenidos, o «datos de acceso», ~~que incluyen,~~ por ejemplo, datos sobre la fecha y hora de uso por parte del proveedor de contenidos o la conexión y desconexión del servicio, junto con la dirección IP asignada por el prestador de servicios de acceso a Internet al proveedor de contenidos. [Enm. 23]
- (21) La obligación de conservar el contenido para procedimientos de revisión administrativa o judicial **o de recurso** es necesaria, y se justifica por el fin de garantizar medidas eficaces de recurso para el proveedor de contenidos cuyos contenidos hayan sido retirados o a los cuales se haya bloqueado el acceso, así como para garantizar el restablecimiento de dichos contenidos en la forma en que se encontraban antes de la retirada, en función del resultado del procedimiento de revisión. La obligación de conservar los contenidos a efectos de investigación y enjuiciamiento es necesaria, y se justifica por el valor que este material podría aportar a efectos de interrumpir o evitar las actividades terroristas. Si las empresas retiran el material o bloquean su acceso, ~~en particular~~ a través de sus propias medidas ~~proactivas,~~ y ~~no informan a la autoridad correspondiente por entender que no entra en el~~ ámbito de aplicación del artículo 13, apartado 4, del presente Reglamento, **específicas, deben informar sin demora** a las autoridades policiales ~~pueden quedar sin conocimiento de la existencia de esos contenidos~~ **competentes**. ~~Por tanto,~~ La conservación del contenido a efectos de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo también está justificada. A esos efectos, **los contenidos terroristas y los datos relacionados deben almacenarse durante un período específico que permita a las autoridades policiales comprobar su contenido y decidir si sería necesario para esos fines específicos. Dicho período no debe exceder de seis meses. A los efectos de prevención, detección, investigación y enjuiciamiento de delitos terroristas,** la conservación de datos exigida se limita a los datos que puedan tener un vínculo con los delitos de terrorismo y, por lo tanto, puedan ser de utilidad para el enjuiciamiento de los delitos de terrorismo o para evitar graves riesgos para la seguridad pública. [Enm. 24]
- (22) Para garantizar la proporcionalidad, el plazo de conservación debe limitarse a seis meses, con objeto de dejar a los proveedores de contenidos el tiempo suficiente para iniciar el proceso de revisión y de permitir el acceso de las autoridades policiales a los datos relevantes para la investigación y el enjuiciamiento de los delitos de terrorismo.

Miércoles, 17 de abril de 2019

- Sin embargo, este plazo puede prorrogarse el tiempo que sea necesario en caso de que se inicien procedimientos de revisión **o de recurso** y no se completen en el plazo de seis meses, a petición de la autoridad que lleve a cabo la revisión. Esta duración debe ser suficiente **también** para permitir a las autoridades policiales conservar ~~las pruebas necesarias~~ **el material necesario** en relación con las investigaciones **y el enjuiciamiento**, garantizando el equilibrio con los derechos fundamentales afectados.. [Enm. 25]
- (23) El Reglamento no afecta a las garantías procedimentales ni a las medidas de investigación procedimentales relacionadas con el acceso a los contenidos y los datos conexos conservados a efectos de investigación y enjuiciamiento de delitos de terrorismo, las cuales se regulan en la normativa nacional de los Estados miembros y en la normativa de la Unión.
- (24) La transparencia de las políticas de los prestadores de servicios de alojamiento de datos en relación con los contenidos terroristas es esencial para reforzar la rendición de cuentas con respecto a sus usuarios y reforzar la confianza de los ciudadanos en el mercado único digital. **Solo** los prestadores de servicios de alojamiento de datos **sujetos a órdenes de retirada durante ese año** deben **estar obligados a** publicar informes anuales de transparencia que contengan información relevante sobre la actuación relacionada con la detección, la identificación y la retirada de los contenidos terroristas. [Enm. 26]
- (24 bis) **Las autoridades competentes para emitir órdenes de retirada deben también publicar informes transparentes que incluyan información sobre el número de dichas órdenes, el número de denegaciones, el número de contenidos terroristas detectados que llevaron a la investigación y enjuiciamiento de delitos terroristas y el número de casos de contenidos considerados erróneamente terroristas.** [Enm. 27]
- (25) Los procedimientos de reclamación constituyen una garantía necesaria contra la retirada errónea de contenidos protegidos en virtud de la libertad de expresión y de **la libertad de recibir y comunicar** información **e ideas en una sociedad abierta y democrática**. Los prestadores de servicios de alojamiento de datos deben, en consecuencia, diseñar mecanismos de reclamación fáciles de usar y garantizar que las reclamaciones se tratan con celeridad y plena transparencia para con el proveedor de contenidos. La exigencia de que el prestador de servicios de alojamiento de datos restablezca los contenidos cuando se hayan retirado por error no afecta a la posibilidad que tiene de hacer cumplir sus términos y condiciones por otros motivos. [Enm. 28]
- (26) La tutela judicial efectiva a tenor del artículo 19 del TUE y el artículo 47 de la Carta de los Derechos Fundamentales de la Unión Europea exige que las personas puedan cerciorarse de los motivos por los que los contenidos que hayan subido han sido retirados o tienen su acceso bloqueado. A esos efectos, el prestador de servicios de alojamiento de datos debe facilitar al proveedor de contenidos información relevante, **por ejemplo, los motivos para la retirada o el bloqueo del acceso y la base jurídica de la acción**, que permita al proveedor de contenidos impugnar la decisión. ~~Sin embargo, esto no implica necesariamente la obligatoriedad de una notificación al proveedor de contenidos. Dependiendo de las circunstancias, los prestadores de servicios de alojamiento de datos pueden sustituir contenidos que se consideren contenidos terroristas por el mensaje de que han sido retirados o bloqueados de conformidad con el presente Reglamento. Si así se solicita, debe facilitarse más información sobre los motivos y las posibilidades de que dispone el proveedor de contenidos para impugnar la decisión.~~ Si las autoridades competentes deciden que, por razones de seguridad pública y en particular en el contexto de una investigación, se considera inadecuado o contraproducente notificar directamente al proveedor de contenidos la retirada o bloqueo de los contenidos, deben informar al prestador de servicios de alojamiento de datos. [Enm. 29]
- (27) Con objeto de evitar duplicidades y posibles interferencias con las investigaciones, **y para minimizar los gastos de los prestadores de servicios afectados**, las autoridades competentes deben informarse mutuamente, coordinarse y cooperar entre sí y, cuando proceda, con Europol cuando emitan órdenes de retirada ~~o envíen requerimientos~~ **destinadas** a los prestadores de servicios de alojamiento de datos. Al aplicar las disposiciones del presente Reglamento, Europol puede proporcionar apoyo en consonancia con su mandato actual y con el marco jurídico vigente. [Enm. 30]
- (27 bis) **Los requerimientos por parte de Europol constituyen un medio eficaz y rápido para poner a los prestadores de servicios de alojamiento de datos sobre aviso acerca de contenidos específicos en sus servicios. Este mecanismo**

Miércoles, 17 de abril de 2019

*para alertar a los prestadores de servicios de alojamiento de datos acerca de información que puede considerarse contenido terrorista, para que el prestador tome en consideración voluntariamente la compatibilidad de esa información con sus términos y condiciones, debe seguir estando disponible junto a las órdenes de retirada. Por eso es importante que los prestadores de servicios de alojamiento de datos colaboren con Europol y evalúen sus requerimientos de manera prioritaria e informen rápidamente sobre las medidas que hayan adoptado. La decisión final sobre la retirada o no de los contenidos por su incompatibilidad con los términos y condiciones sigue correspondiendo al prestador de servicios de alojamiento de datos. La aplicación del presente Reglamento no afecta al mandato de Europol de conformidad con el Reglamento (UE) 2016/794 <sup>(10)</sup>. [Enm. 31]*

- (28) Con vistas a garantizar una aplicación eficaz y suficientemente coherente de las medidas ~~proactivas~~ **por parte de los prestadores de servicios de alojamiento de datos**, las autoridades competentes de los Estados miembros deben constituir enlaces mutuos relativos a los debates que mantengan con los prestadores de servicios de alojamiento de datos en lo que se refiere a **las órdenes de retirada** y la determinación, la aplicación y el examen de las medidas ~~proactivas~~ específicas. ~~Del mismo modo~~, Esta cooperación también es necesaria en relación con la adopción de normas relativas a sanciones, incluidas las que regulen su aplicación y su cumplimiento. [Enm. 32]
- (29) Es crucial que la autoridad competente del Estado miembro responsable de la imposición de sanciones esté plenamente informada de la emisión de órdenes de retirada ~~y requerimientos~~ y de las conversaciones posteriores entre el prestador de servicios de alojamiento de datos y ~~la autoridad competente pertinente~~ **las autoridades competentes pertinentes de otros Estados miembros**. A esos efectos, los Estados miembros deben garantizar unos canales y mecanismos de comunicación adecuados **y seguros** que permitan compartir la información pertinente a su debido tiempo. [Enm. 33]
- (30) Con el fin de facilitar los intercambios rápidos entre las autoridades competentes y entre estas y los prestadores de servicios de alojamiento de datos, y de impedir la duplicación del trabajo, los Estados miembros pueden utilizar instrumentos desarrollados por Europol, como la actual Aplicación de Gestión de los Requerimientos de Internet o los instrumentos que lo han sucedido.
- (31) Dadas las consecuencias particularmente graves de determinados contenidos terroristas, los prestadores de servicios de alojamiento de datos deben informar con celeridad a las autoridades del Estado miembro pertinente, o a las autoridades competentes en su lugar de establecimiento o en el que tengan un representante legal, acerca de la existencia de cualquier indicio de delitos de terrorismo del que hayan tenido conocimiento. Para garantizar la proporcionalidad, esta obligación se limita a los delitos de terrorismo en el sentido del artículo 3, apartado 1, de la Directiva (UE) 2017/541. La obligación de informar no implica para los prestadores de servicios de alojamiento de datos una obligación de búsqueda activa de dichos indicios. El Estado miembro pertinente es el Estado miembro que tenga jurisdicción para investigar y enjuiciar los delitos de terrorismo con arreglo a la Directiva (UE) 2017/541, en función de la nacionalidad del infractor o de la posible víctima del delito o de la ubicación del objetivo del acto terrorista. En caso de duda, los prestadores de servicios de alojamiento de datos pueden transmitir la información a Europol, que puede dar curso al asunto con arreglo a su mandato o remitirlo a las autoridades nacionales correspondientes.
- (32) Las autoridades competentes de los Estados miembros deben poder usar esa información para adoptar medidas de investigación disponibles con arreglo a la normativa de la Unión o del Estado miembro, incluida la emisión de una orden europea de entrega a tenor del Reglamento sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal <sup>(11)</sup>.
- (33) Tanto los prestadores de servicios de alojamiento de datos como los Estados miembros deben crear puntos de contacto para facilitar el tratamiento rápido de las órdenes de retirada ~~y los requerimientos~~. Al contrario que el representante legal, el punto de contacto tiene funciones operativas. El punto de contacto del prestador de servicios de alojamiento de datos debe consistir en cualquier medio específico que permita la presentación electrónica de órdenes de retirada ~~y requerimientos~~ y en los medios técnicos y personales que permitan el procesamiento rápido de estas. El punto de contacto del prestador de servicios de alojamiento de datos no tiene que estar situado en la Unión y el prestador de servicios de alojamiento de datos es libre de nombrar un punto de contacto ya existente, siempre que este sea capaz de cumplir las funciones encomendadas en virtud del presente Reglamento. Con vistas a garantizar que los contenidos terroristas se retiren o que el acceso a ellos se bloquee en el plazo de una hora desde la recepción de una orden de retirada, los prestadores de servicios de alojamiento de datos deben garantizar que el punto de contacto está disponible ininterrumpidamente. La información sobre el punto de contacto debe incluir información sobre la lengua que puede utilizarse para dirigirse al punto de contacto. Para facilitar la comunicación

<sup>(10)</sup> **Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo (DO L 135 de 24.5.2016, p. 53).**

<sup>(11)</sup> COM(2018)0225.

Miércoles, 17 de abril de 2019

- entre los prestadores de servicios de alojamiento de datos y las autoridades competentes, se anima a los prestadores de servicios de alojamiento de datos a habilitar la comunicación en una de las lenguas oficiales de la Unión Europea en la que se puedan consultar sus términos y condiciones. [Enm. 34]
- (34) A falta de la exigencia general a los prestadores de servicios de garantizar una presencia física en el territorio de la Unión, es necesario velar por la claridad en lo que respecta al Estado miembro a cuya jurisdicción pertenece el prestador de servicios de alojamiento de datos que ofrece servicios dentro de la Unión. Como norma general, el prestador de servicios de alojamiento de datos pertenece a la jurisdicción del Estado miembro en el que tenga su establecimiento principal o en el que haya designado un representante legal. ~~Sin embargo, cuando otro Estado miembro emita una orden de retirada, sus autoridades deben poder hacer cumplir sus órdenes mediante medidas coercitivas de carácter no punitivo, como multas sancionadoras.~~ En lo que respecta a los prestadores de servicios de alojamiento de datos que no tengan establecimientos en la Unión y no hayan designado un representante legal, cualquier Estado miembro debe, no obstante, tener la posibilidad de imponer sanciones, siempre que se respete el principio de *non bis in idem*. [Enm. 35]
- (35) Aquellos prestadores de servicios de alojamiento de datos que no estén establecidos en la Unión deben designar un representante legal por escrito para garantizar la aplicación y el cumplimiento de las obligaciones que impone el presente Reglamento. **Los prestadores de servicios de alojamiento de datos pueden recurrir a un representante legal existente, siempre que este pueda desempeñar las funciones que se establecen en el presente Reglamento.** [Enm. 36]
- (36) El representante legal debe tener la capacidad legal de actuar en representación del prestador de servicios de alojamiento de datos.
- (37) A efectos del presente Reglamento, los Estados miembros deben designar ~~a las autoridades competentes~~ **una única autoridad judicial o administrativa funcionalmente independiente.** ~~La~~ Esta exigencia de designar a las autoridades competentes ~~la autoridad competente no necesariamente implicar~~ **requiere** la creación de ~~nuevas autoridades~~ **una nueva autoridad**, sino que pueden encomendarse las funciones a las que obliga el presente Reglamento a ~~organismos~~ **un organismo** ya ~~existentes~~ **existente**. El presente Reglamento requiere la designación de ~~autoridades competentes~~ **una autoridad competente** para emitir órdenes de retirada y ~~requerimientos~~, para supervisar las medidas ~~proactivas~~ **específicas** y para imponer sanciones. ~~Se~~ Los Estados miembros ~~los que deciden a cuántas autoridades desean designar para ejercer esas funciones~~ **deben comunicar la autoridad competente designada con arreglo al presente Reglamento a la Comisión, que debe publicar en línea una relación de las autoridades competentes de cada Estado miembro. El registro en línea debe ser fácilmente accesible, a fin de facilitar la rápida verificación de la autenticidad de las órdenes de retirada por parte de los prestadores de servicios de alojamiento de datos.** [Enm. 37]
- (38) Las sanciones son necesarias para garantizar el cumplimiento efectivo por los prestadores de servicios de alojamiento de datos de las obligaciones derivadas del presente Reglamento. Los Estados miembros deben adoptar normas sobre sanciones, incluidas, cuando proceda, directrices para la imposición de multas. ~~Deben imponerse~~ **Deben imponerse** sanciones ~~particularmente rigurosas~~ en los casos en que ~~el prestador~~ **los prestadores** de servicios de alojamiento de datos ~~incumpla sistemáticamente la obligación de retirada de los contenidos terroristas o de bloqueo del acceso a ellas en el plazo de una hora desde la recepción de una orden de retirada. El incumplimiento en casos concretos puede ser sancionado, con respeto de los principios de *non bis in idem* y de proporcionalidad, y con la garantía de que esas sanciones tienen en cuenta la inobservancia sistemática. Para garantizar la seguridad jurídica, el Reglamento debe fijar la medida en que las obligaciones pertinentes pueden ser objeto de sanciones~~ **incumplan de forma sistemática y persistente las obligaciones derivadas del presente Reglamento.** Las sanciones por el incumplimiento de lo dispuesto en el artículo 6 solo pueden imponerse en relación con las obligaciones derivadas de una solicitud de ~~presentar informes con arreglo al artículo 6, apartado 2, o de una decisión que imponga~~ **aplicación de** medidas ~~proactivas~~ **específicas** adicionales con arreglo al artículo 6, apartado 4. Al determinar si se deben imponer o no sanciones económicas, deben tenerse debidamente en cuenta los recursos económicos del prestador. **Además, la autoridad competente debe tener en cuenta si el prestador de servicios de alojamiento de datos es una empresa emergente o una pequeña y mediana empresa y determinar, caso por caso, si tiene capacidad para cumplir adecuadamente la orden emitida.** Los Estados miembros deben garantizar que las sanciones no incentiven la retirada de contenidos que no sean terroristas. [Enm. 38]
- (39) El uso de plantillas normalizadas facilita la cooperación y el intercambio de información entre las autoridades competentes y los prestadores de servicios, y les permite comunicarse con mayor rapidez y eficacia. Es de particular importancia garantizar una actuación rápida tras la recepción de una orden de retirada. Las plantillas reducen los costes de traducción y contribuyen a un alto nivel de calidad. Del mismo modo, los formularios de respuesta deben permitir un intercambio de información normalizado, lo cual reviste especial importancia cuando los prestadores

Miércoles, 17 de abril de 2019

de servicios no pueden cumplir las exigencias que se les imponen. Los canales de envío autenticado pueden asegurar la autenticidad de la orden de retirada, incluida la precisión de la fecha y la hora de envío y de recepción de la orden.

- (40) Con el fin de permitir una modificación rápida, cuando sea necesario, del contenido de las plantillas que deben utilizarse a efectos del presente Reglamento, debe delegarse en la Comisión el poder de adoptar actos con arreglo al artículo 290 del Tratado de Funcionamiento de la Unión Europea para modificar los anexos I, II y III del presente Reglamento. Con objeto de poder tener en cuenta el desarrollo tecnológico y el del marco jurídico conexo, la Comisión debe también estar facultada para adoptar actos delegados que completen el presente Reglamento con requisitos técnicos para los medios electrónicos que deben usar las autoridades competentes a efectos de la transmisión de las órdenes de retirada. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos, y que esas consultas se realicen de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación<sup>(12)</sup>. En particular, a fin de garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo reciben toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus expertos tienen acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados.
- (41) Los Estados miembros deben recabar información relativa a la aplicación de la legislación, **incluida información sobre el número de casos de detección, investigación y enjuiciamiento satisfactorios de delitos de terrorismo como consecuencia de la aplicación del presente Reglamento**. Debe elaborarse un programa detallado para el seguimiento de las realizaciones, los resultados y las repercusiones del presente Reglamento, con objeto de servir de base a una evaluación de la legislación. [Enm. 39]
- (42) Fundamentándose en los hallazgos y conclusiones del informe de aplicación y el resultado de la actividad de seguimiento, la Comisión debe llevar a cabo una evaluación del presente Reglamento ~~cuando hayan transcurrido al menos tres años desde su entrada en vigor~~ **un año después de su entrada en vigor**. La evaluación debe basarse en los ~~cinco~~ **siete** criterios de eficiencia, **necesidad, proporcionalidad**, eficacia, pertinencia, coherencia y valor añadido de la UE. ~~Evaluará~~ **Debe evaluar** el funcionamiento de las diferentes medidas operativas y técnicas previstas con arreglo al Reglamento, incluidas la eficacia de las medidas de refuerzo de la detección, la identificación y la retirada de contenidos terroristas, la eficacia de los mecanismos de garantía y las repercusiones sobre los derechos **fundamentales que puedan resultar afectados, incluida la libertad de expresión y la libertad de recibir y comunicar información, la libertad y el pluralismo de los medios de comunicación, la libertad de empresa y el derecho a la privacidad y la protección de los datos personales**. **La Comisión debe también evaluar la repercusión sobre los** intereses de terceros que puedan resultar afectados, la que incluye una revisión de la exigencia de informar a los proveedores de contenidos. [Enm. 40]
- (43) Dado que el objetivo del presente Reglamento, a saber, garantizar el correcto funcionamiento del mercado único digital evitando la difusión de contenidos terroristas en línea, no pueden ser alcanzado de manera suficiente por los Estados miembros y, por consiguiente, debido a las dimensiones y los efectos de la limitación, puede lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad enunciado en dicho artículo, el presente Reglamento no excede de lo necesario para alcanzar ese objetivo.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

## SECCIÓN I

### DISPOSICIONES GENERALES

#### Artículo 1

##### Objeto y ámbito de aplicación

1. El presente Reglamento establece normas uniformes **específicas** con el fin de ~~evitar~~ **luchar contra** el uso indebido de los servicios de alojamiento de datos para la difusión **pública** de contenidos terroristas en línea. En particular, establece: [Enm. 41]

<sup>(12)</sup> DO L 123 de 12.5.2016, p. 1.

Miércoles, 17 de abril de 2019

- (a) normas sobre los deberes **razonables y proporcionados** de diligencia que deben aplicar los prestadores de servicios de alojamiento de datos para ~~evitar~~ **luchar contra** la difusión **pública** de contenidos terroristas a través de sus servicios y garantizar, cuando sea necesario, su retirada rápida; [Enm. 42]
- (b) una serie de medidas que deben poner en marcha los Estados miembros para identificar los contenidos terroristas, para permitir su retirada rápida por parte de los prestadores de servicios de alojamiento, **de conformidad con la legislación de la Unión que establece salvaguardas adecuadas de la libertad de expresión y la libertad de recibir y comunicar información e ideas en una sociedad abierta y democrática**, y para facilitar la cooperación con las autoridades competentes de otros Estados miembros, los prestadores de servicios de alojamiento de datos y, cuando proceda, los organismos de la Unión pertinentes. [Enm. 43]

2. El presente Reglamento será de aplicación a los prestadores de servicios de alojamiento de datos que ofrecen servicios **al público** en la Unión, independientemente de su lugar de establecimiento principal. [Enm. 44]

**2 bis.** *El presente Reglamento no se aplicará a los contenidos difundidos con fines educativos, artísticos, periodísticos o de investigación o con fines de sensibilización contra las actividades terroristas ni a contenidos que representen la expresión de puntos de vista polémicos o controvertidos en el curso del debate público.* [Enm. 45]

**2 ter.** *El presente Reglamento no tendrá el efecto de modificar la obligación de respetar los derechos, libertades y principios contemplados en el artículo 6 del Tratado de la Unión Europea y se aplicará sin perjuicio de los principios fundamentales del Derecho de la Unión y nacional relativos a la libertad de expresión, la libertad de prensa y la libertad y el pluralismo de los medios de comunicación.* [Enm. 46]

**2 quater.** *El presente Reglamento se entenderá sin perjuicio de lo dispuesto en la Directiva 2000/31/CE.* [Enm. 47]

## Artículo 2

### Definiciones

A los efectos del presente Reglamento, se entenderá por:

- 1) **«servicios de la sociedad de la información»** los servicios según la definición del artículo 2, letra a), de la Directiva 2000/31/CE; [Enm. 48]
- (1) «prestador de servicios de alojamiento de datos» un prestador de servicios de la sociedad de la información consistentes en el almacenamiento de información facilitada por el proveedor de contenidos a petición de este y en la puesta a disposición de ~~terceros~~ **del público** de la información almacenada. **Esto se aplica a los servicios prestados al público en la capa de aplicación. Los proveedores de infraestructura en la nube y los prestadores de servicios en la nube no se consideran prestadores de servicios de alojamiento de datos. Tampoco se aplica a los servicios de comunicaciones electrónicas según la definición de la Directiva (UE) 2018/1972;** [Enm. 49]
- (2) «proveedor de contenidos» un usuario que ha suministrado información que esté o haya estado almacenada **y puesta a disposición del público**, a petición suya, por un prestador de servicios de alojamiento de datos; [Enm. 50]
- (3) «ofrecer servicios en la Unión» permitir a las personas físicas o jurídicas de uno o más Estados miembros usar los servicios del prestador de servicios de alojamiento de datos que tenga una conexión sustancial con ese Estado miembro o esos Estados miembros, por ejemplo:
- a) un establecimiento del prestador de servicios de alojamiento de datos en la Unión;
  - b) un número de usuarios significativo en uno o más Estados miembros;
  - c) la orientación de actividades hacia uno o más Estados miembros.
- (4) ~~«delitos de terrorismo» los delitos definidos en el artículo 3, apartado 1, de la Directiva (UE) 2017/541;~~ [Enm. 51]

Miércoles, 17 de abril de 2019

- (5) «contenidos terroristas» uno o más de los ~~elementos de información~~ **materiales** siguientes: [Enm. 52]
- a) los que inciten a la comisión de **uno de los delitos enumerados en el artículo 3, apartado 1, letras a) a i), de la Directiva (UE) 2017/541, cuando tal conducta defienda de manera directa o indirecta la comisión de delitos de terrorismo o los defiendan, incluidos los que hagan apología de ellos, por ejemplo, mediante la apología de los actos terroristas**, provocando con ello un peligro de ~~comisión de dichos actos~~ **que se puedan cometer intencionadamente uno o más de esos delitos**; [Enm. 53]
  - b) ~~los que fomenten la contribución a los~~ **que induzcan a otra persona o grupo de personas a cometer o contribuir a cometer uno de los delitos de terrorismo enumerados en el artículo 3, apartado 1, letras a) a i), de la Directiva (UE) 2017/541, provocando con ello un peligro de que se puedan cometer intencionadamente uno o más de esos delitos**; [Enm. 54]
  - c) ~~los que promuevan~~ **los que induzcan a otra persona o grupo de personas a participar en** las actividades de un grupo terrorista, en particular fomentando la participación en un grupo terrorista o el apoyo al mismo, **incluida las consistentes en el suministro de información o medios materiales, o en cualquier forma de financiación de sus actividades** en el sentido del artículo 2, ~~apartado 3,4~~ de la Directiva (UE) 2017/541, **provocando con ello un peligro de que se puedan cometer intencionadamente uno o más de esos delitos**; [Enm. 55]
  - d) ~~los que instruyan~~ **los que faciliten instrucción sobre la fabricación o el uso de explosivos, armas de fuego u otras armas o sustancias nocivas o peligrosas o sobre otros métodos o técnicas específicos** para la comisión ~~o la contribución a la comisión de cualquiera de los~~ **delitos de terrorismo enumerados en el artículo 3, apartado 1, letras a) a i), de la Directiva (UE) 2017/541**; [Enm. 56]
- d bis) los que describan la comisión de uno o más de los delitos enumerados en el artículo 3, apartado 1, letras a) a i), de la Directiva (UE) 2017/541, provocando con ello un peligro de que se puedan cometer intencionadamente uno o más de esos delitos**; [Enm. 57]
- (6) «difusión de contenidos terroristas» la puesta a disposición ~~de terceros~~ **del público** de contenidos terroristas en los servicios de los prestadores de servicios de alojamiento de datos; [Enm. 58]
- (7) «términos y condiciones» todos los términos, condiciones y cláusulas, independientemente de su nombre o forma, que rigen la relación contractual entre el prestador de servicios de alojamiento de datos y sus usuarios;
- (8) «requerimiento» una notificación de una autoridad competente o, cuando proceda, de un organismo de la Unión pertinente a un prestador de servicios de alojamiento de datos con información que pueda considerarse contenido terrorista, para la toma en consideración voluntaria por parte del prestador de la compatibilidad con sus propios términos y condiciones destinados a evitar la difusión de contenidos terroristas; [Enm. 59]
- (9) «establecimiento principal» la sede central u el domicilio social en que se ejerzan las principales funciones financieras y el control operativo.
- 9 bis) «autoridad competente» una única autoridad judicial o autoridad administrativa funcionalmente independiente designada en el Estado miembro.** [Enm. 60]

Miércoles, 17 de abril de 2019

## SECCIÓN II

## MEDIDAS PARA EVITAR LA DIFUSIÓN DE CONTENIDOS TERRORISTAS EN LÍNEA

## Artículo 3

## Deberes de diligencia

1. Los prestadores de servicios de alojamiento de datos actuarán ~~de manera adecuada, razonable y proporcionada~~ en consonancia con el presente Reglamento para ~~hacer frente a la difusión de contenidos terroristas y~~ proteger a los usuarios de los contenidos terroristas. ~~Al hacerlo, actuarán~~ **Lo harán** de manera resuelta, proporcionada y no discriminatoria, con la debida consideración **en toda circunstancia** a los derechos fundamentales de los usuarios y teniendo en cuenta la importancia capital de la libertad de expresión y ~~de la libertad de recibir y comunicar~~ información ~~e ideas~~ en una sociedad abierta y democrática **y procurando evitar la retirada de contenidos que no sean terroristas.** [Enm. 61]

**1 bis. Dichos deberes de diligencia no se convertirán en una obligación general para los prestadores de servicios de alojamiento de supervisar los datos que transmiten o almacenan, ni en un deber general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas.** [Enm. 62]

~~2. Los prestadores de servicios de alojamiento de datos incluirán en sus términos y condiciones disposiciones para evitar la difusión de contenidos terroristas y las aplicarán.~~ [Enm. 63]

**2 bis. Cuando los prestadores de servicios de alojamiento de datos tengan conocimiento o se percaten de la existencia de contenido terrorista en sus servicios, informarán a las autoridades competentes de tal contenido y lo eliminarán rápidamente.** [Enm. 64]

**2 ter. Los prestadores de servicios de alojamiento de datos que cumplan los criterios de la definición de prestador de plataforma de intercambio de vídeos contemplados en la Directiva (UE) 2018/1808, adoptarán las medidas adecuadas para combatir la difusión de contenidos terroristas de conformidad con el artículo 28 ter, apartado 1, letra c), y apartado 3, de la Directiva (UE) 2018/1808.** [Enm. 65]

## Artículo 4

## Órdenes de retirada

1. La autoridad competente **del Estado miembro en el que esté situado el establecimiento principal del prestador de servicios de alojamiento de datos** estará facultada para emitir una ~~decisión~~ **orden de retirada** que exija al prestador de servicios de alojamiento de datos retirar contenidos terroristas **ilícitos** o bloquear el acceso a ellos **en todos los Estados miembros.** [Enm. 66]

**1 bis. La autoridad competente de un Estado miembro en el que el prestador de servicios de alojamiento de datos no tenga su establecimiento principal o no cuente con un representante legal podrá solicitar el bloqueo del acceso al contenido terrorista y ejecutar esa petición en su propio territorio.** [Enm. 67]

**1 ter. Si la autoridad competente pertinente no ha emitido previamente una orden de retirada dirigida a un prestador de servicios de alojamiento de datos, se pondrá en contacto con el prestador de servicios para facilitarle información sobre los procedimientos y plazos aplicables, al menos doce horas antes de emitir la orden de retirada.** [Enm. 68]

2. Los prestadores de servicios de alojamiento de datos retirarán los contenidos terroristas o bloquearán el acceso a ellos **tan pronto como sea posible y** en el plazo de una hora desde la recepción de la orden de retirada. [Enm. 69]

3. Las órdenes de retirada contendrán los elementos siguientes de conformidad con la plantilla establecida en el anexo I:

a) la identificación **mediante una firma electrónica** de la autoridad competente que emite la orden de retirada y la autenticación de la orden de retirada por la autoridad competente; [Enm. 70]

Miércoles, 17 de abril de 2019

- b) una motivación **detallada** que explique por qué los contenidos se consideran contenidos terroristas, ~~al menos por y una~~ referencia **específica** a las categorías de contenidos terroristas enumeradas en el artículo 2, apartado 5; [Enm. 71]
- c) un localizador uniforme de recursos (URL) **exacto** y, cuando sea necesario, información adicional que permita la identificación de los contenidos de que se trate; [Enm. 72]
- d) una referencia al presente Reglamento como base jurídica de la orden de retirada;
- e) la marca de fecha y hora de la emisión;
- f) información ~~sobre los recursos disponibles~~ **de fácil comprensión** para el prestador de servicios de alojamiento de datos y el proveedor de contenidos **sobre los recursos disponibles, incluidos los recursos ante la autoridad competente y ante los tribunales, y los correspondientes plazos de recurso**; [Enm. 73]
- g) cuando sea ~~pertinente~~ **necesario y proporcionado**, la decisión de no divulgar información sobre la retirada de contenidos terroristas o el bloqueo del acceso a ellos a que se refiere el artículo 11. [Enm. 74]

4. ~~A petición del prestador de servicios de alojamiento de datos o del proveedor de contenidos, la autoridad competente facilitará una motivación detallada, sin perjuicio de la obligación que tiene el prestador de servicios de alojamiento de datos de cumplir con la orden de retirada en el plazo establecido en el apartado 2.~~ [Enm. 75]

5. ~~Las autoridades competentes dirigirán~~ **La autoridad competente dirigirá** las órdenes de retirada al establecimiento principal del prestador de servicios de alojamiento de datos o al representante legal designado por el prestador de servicios de alojamiento de datos con arreglo al artículo 16 y las ~~transmitirá~~ **transmitirá** al punto de contacto al que se refiere el artículo 14, apartado 1. Dichas órdenes se enviarán por medios electrónicos capaces de producir un registro escrito en condiciones que permitan determinar la autenticación del remitente, incluidas la fecha y la hora precisas de envío y recepción de la orden. [Enm. 76]

6. Los prestadores de servicios de alojamiento de datos ~~acusarán recibo e~~ informarán, sin demora indebida, a la autoridad competente acerca de la retirada de los contenidos terroristas o del bloqueo del acceso a ellos, indicando en particular la hora de la actuación, mediante la plantilla establecida en el anexo II. [Enm. 77]

7. Si el prestador de servicios de alojamiento de datos no puede cumplir con la orden de retirada por causa de fuerza mayor o imposibilidad de hecho no atribuible a él, **incluidas razones técnicas u operativas**, informará sin demora indebida a la autoridad competente, exponiendo los motivos, mediante la plantilla establecida en el anexo III. El plazo fijado en el apartado 2 se aplicará desde el momento en que dejen de concurrir los motivos expuestos. [Enm. 78]

8. ~~Si~~ El prestador de servicios de alojamiento de datos ~~no puede cumplir~~ **podrá negarse a ejecutar** la orden de retirada ~~por contener~~ **si esta contiene** errores manifiestos o no ~~contiene~~ **contiene** información suficiente ~~para la ejecución de la orden~~. Informará a la autoridad competente sin demora indebida y pedirá las aclaraciones necesarias, mediante la plantilla establecida en el anexo III. El plazo fijado en el apartado 2 se aplicará desde el momento en que se faciliten las aclaraciones. [Enm. 79]

9. La autoridad competente que haya emitido la orden de retirada informará a la autoridad competente encargada de supervisar la aplicación de las medidas ~~proactivas~~ **específicas** a que se refiere el artículo 17, apartado 1, letra c), cuando la orden de retirada se convierta en definitiva. Una orden de retirada se convierte en definitiva cuando no haya sido impugnada en el plazo al efecto conforme a la normativa nacional aplicable o cuando haya sido confirmada después de una impugnación. [Enm. 80]

Miércoles, 17 de abril de 2019

**Artículo 4 bis****Procedimiento de consulta para las órdenes de retirada**

1. La autoridad competente que emita una orden de retirada en virtud del artículo 4, apartado 1 bis, remitirá una copia de dicha orden a la autoridad competente a que se refiere el artículo 17, apartado 1, letra a), del Estado miembro en el que esté situado el establecimiento principal del prestador de servicios de alojamiento de datos, al mismo tiempo que se la transmite al prestador de servicios de alojamiento de datos con arreglo al artículo 4, apartado 5.

2. Cuando la autoridad competente del Estado miembro en el que esté situado el establecimiento principal del prestador de servicios de alojamiento de datos tenga motivos razonables para considerar que la orden de retirada puede afectar a los intereses fundamentales de dicho Estado miembro, informará a la autoridad competente emisora. La autoridad emisora tendrá en cuenta dichas circunstancias y, cuando proceda, retirará o adaptará la orden de retirada. [Enm. 81]

**Artículo 4 ter****Procedimiento de cooperación para la emisión de una orden de retirada adicional**

1. Cuando una autoridad competente haya emitido una orden de retirada en virtud del artículo 4, apartado 1 bis, dicha autoridad podrá ponerse en contacto con la autoridad competente del Estado miembro en el que el prestador de servicios de alojamiento de datos tenga su establecimiento principal para solicitar que esta última autoridad también expida una orden de retirada de conformidad con el artículo 4, apartado 1.

2. La autoridad competente del Estado miembro en el que esté situado el establecimiento principal del proveedor de servicios de alojamiento de datos expedirá una orden de retirada o se negará a emitirla a la mayor brevedad y, en cualquier caso, no más tarde de una hora después de haber sido contactada con arreglo al apartado 1, e informará de su decisión a la autoridad competente que haya dictado la primera orden.

3. En los casos en que la autoridad competente del Estado miembro del establecimiento principal necesite más de una hora para realizar su propia evaluación del contenido, enviará un requerimiento al proveedor de servicios de alojamiento de datos de que se trate para desactivar temporalmente el acceso al contenido durante un máximo de 24 horas, período durante el cual la autoridad competente realizará la evaluación y enviará la orden de retirada o retirará el requerimiento de desactivación del acceso. [Enm. 82]

**Artículo 5****Requerimientos**

1. La autoridad competente o el organismo de la Unión pertinente podrá enviar un requerimiento al prestador de servicios de alojamiento de datos.

2. Los prestadores de servicios de alojamiento de datos pondrán en funcionamiento medidas operativas y técnicas que faciliten la evaluación con celeridad de los contenidos objeto del requerimiento enviado por las autoridades competentes y, cuando proceda, los organismos de la Unión pertinentes para su toma en consideración voluntaria.

3. Los requerimientos se dirigirán al establecimiento principal del prestador de servicios de alojamiento de datos o al representante legal designado por el prestador de servicios de alojamiento de datos de conformidad con el artículo 16 y se transmitirán al punto de contacto al que se refiere el artículo 14, apartado 1. Dichos requerimientos se enviarán por medios electrónicos.

4. El requerimiento contendrá información suficientemente detallada, incluidos los motivos por los que los contenidos se consideran contenidos terroristas, una URL y, cuando sea necesario, información adicional que permita la identificación de los contenidos terroristas objeto del requerimiento.

5. El prestador de servicios de alojamiento de datos evaluará, con carácter prioritario, los contenidos identificados en el requerimiento en relación con sus propios términos y condiciones y decidirá si los retira o bloquea el acceso a ellos.

Miércoles, 17 de abril de 2019

~~6. El prestador de servicios de alojamiento de datos informará con celeridad a la autoridad competente o el organismo de la Unión pertinente sobre el resultado de la evaluación y el momento de cualquier actuación emprendida como consecuencia del requerimiento.~~

~~7. Cuando el prestador de servicios de alojamiento de datos considere que el requerimiento no contiene información suficiente para evaluar los contenidos objeto del requerimiento, informará sin demora a las autoridades competentes o al organismo de la Unión pertinente y determinará la información adicional o las aclaraciones que necesita. [Enm. 83]~~

## Artículo 6

### Medidas ~~proactivas~~específicas [Enm. 84]

~~1. Sin perjuicio de lo dispuesto en la Directiva (UE) 2018/1808 y la Directiva 2000/31/CE, los proveedores de servicios de alojamiento de datos tomarán, cuando proceda, podrán tomar medidas ~~proactivas~~específicas para proteger sus servicios frente a la difusión pública de contenidos terroristas. Las medidas serán eficaces, selectivas y proporcionadas, teniendo en cuenta el prestando especial atención al riesgo y el nivel de exposición a contenidos terroristas, los derechos fundamentales de los usuarios y la importancia capital ~~del derecho a~~ la libertad de expresión y ~~la libertad de información~~recibir o de comunicar informaciones o ideas en una sociedad abierta y democrática. [Enm. 85]~~

~~2. Cuando haya sido informada con arreglo al artículo 4, apartado 9, la autoridad competente a que se refiere el artículo 17, apartado 1, letra c), solicitará al prestador de servicios de alojamiento de datos que presente un informe en el plazo de tres meses desde la recepción de la solicitud, y posteriormente con una periodicidad al menos anual, sobre las medidas proactivas específicas que haya tomado, incluidas las que hayan supuesto el uso de instrumentos automatizados, con el fin de:~~

~~a) evitar que vuelvan a subirse contenidos que hayan sido retirados o cuyo acceso haya sido bloqueado previamente por considerarse que se trataba de contenidos terroristas;~~

~~b) detectar e identificar los contenidos terroristas y retirarlos o bloquear el acceso a ellos con celeridad.~~

~~Dicha solicitud se enviará al establecimiento principal del prestador de servicios de alojamiento de datos o al representante legal designado por el prestador de servicios.~~

~~Los informes incluirán toda la información pertinente que permita a la autoridad competente a que se refiere el artículo 17, apartado 1, letra c), evaluar si las medidas proactivas son eficaces y proporcionadas, y en particular evaluar el funcionamiento de todos los instrumentos automatizados que se hayan utilizado y de los mecanismos de supervisión y verificación por personas que se hayan empleado. [Enm. 86]~~

~~3. Cuando la autoridad competente a que se refiere el artículo 17, apartado 1, letra c), considere que las medidas proactivas tomadas y notificadas de conformidad con el apartado 2 son insuficientes para atenuar y gestionar el riesgo y el nivel de exposición, podrá solicitar al prestador de servicios de alojamiento de datos que tome medidas proactivas adicionales específicas. A tal efecto, el prestador de servicios de alojamiento de datos cooperará con la autoridad competente a que se refiere el artículo 17, apartado 1, letra c), con vistas a determinar las medidas proactivas específicas que el prestador de servicios de alojamiento de datos debe poner en funcionamiento y fijar sus objetivos e indicadores fundamentales y los calendarios de aplicación. [Enm. 87]~~

~~4. Cuando no pueda alcanzarse un acuerdo en el plazo de tres meses desde la solicitud a que se refiere el apartado 3Una vez que se haya constatado que un prestador de servicios de alojamiento de datos ha recibido un número sustancial de órdenes de retirada, la autoridad competente a que se refiere el artículo 17, apartado 1, letra c), podrá emitir una decisión que imponga medidas ~~proactivas~~específicas adicionales específicas que sean necesarias y proporcionadas y eficaces que el prestador de servicios de alojamiento de datos deberá aplicar. La autoridad competente no impondrá una obligación general de seguimiento ni el uso herramientas automatizadas. La ~~decisión~~solicitud tendrá en cuenta, en particular, la viabilidad técnica, el tamaño y la capacidad económica del prestador de servicios de alojamiento de datos, el efecto de dichas medidas sobre los derechos fundamentales de los usuarios y la importancia capital de la libertad de expresión y la libertad de ~~información~~recibir o comunicar información o ideas en una sociedad abierta y democrática. Dicha ~~decisión~~solicitud se enviará al establecimiento principal del prestador de servicios de alojamiento de datos o al representante legal designado por el prestador de servicios. El prestador de servicios de alojamiento de datos informará periódicamente sobre la aplicación de las medidas especificadas por la autoridad competente a que se refiere el artículo 17, apartado 1, letra c). [Enm. 88]~~

Miércoles, 17 de abril de 2019

5. Un prestador de servicios de alojamiento de datos podrá, en cualquier momento, solicitar a la autoridad competente a que se refiere el artículo 17, apartado 4, letra c), una revisión y, cuando proceda, la revocación de una solicitud o ~~decisión~~ derivada de los apartados 2, 3 ~~y del apartado 4, respectivamente~~. La autoridad competente facilitará una decisión motivada en un plazo razonable tras la recepción de la solicitud del prestador de servicios de alojamiento de datos. [Enm. 89]

#### Artículo 7

##### Conservación de los contenidos y los datos conexos

1. Los prestadores de servicios de alojamiento de datos conservarán los contenidos terroristas que hayan sido retirados o cuyo acceso haya sido bloqueado como consecuencia de una orden de retirada o ~~un requerimiento~~ o de medidas ~~proactivas~~ **específicas** a tenor de los artículos 4, 5 y 6 y los datos conexos retirados como consecuencia de la retirada de los contenidos terroristas y que sean necesarios para: [Enm. 90]

a) procedimientos **administrativos o judiciales** de revisión ~~administrativa o judicial~~ **recurso**; [Enm. 91]

b) la prevención, la detección, la investigación o el enjuiciamiento de delitos de terrorismo **por las autoridades encargadas de hacer cumplir la ley**. [Enm. 92]

2. Los contenidos terroristas y los datos conexos a que se refiere el apartado 1, **letra a)**, se conservarán durante seis meses **y se suprimirán transcurrido dicho plazo**. Los contenidos terroristas se conservarán, a solicitud de la autoridad o del órgano jurisdiccional competente, durante un **nuevo** plazo ~~más largo~~ **especificado únicamente** cuando sea necesario para procedimientos **judiciales o administrativos** de revisión ~~administrativa o judicial~~ **recurso**, en el sentido del apartado 1, letra a), que se encuentren en curso. **Los prestadores de servicios de alojamiento de datos conservarán los contenidos terroristas y los datos conexos a que se refiere el apartado 1, letra b), hasta que la autoridad encargada de hacer cumplir la ley reaccione a la notificación efectuada por el prestador de servicios de alojamiento de datos de conformidad con el artículo 13, apartado 4, pero en ningún caso durante más de seis meses.** [Enm. 93]

3. Los prestadores de servicios de alojamiento de datos velarán por que los contenidos terroristas y los datos conexos conservados en consonancia con los apartados 1 y 2 estén sujetos a garantías técnicas y organizativas adecuadas.

Estas garantías técnicas y organizativas asegurarán que solo sea posible el acceso a los contenidos terroristas conservados y los datos conexos, y el procesamiento de dichos contenidos y datos, para los fines enumerados en el apartado 1, y asegurarán por un alto nivel de seguridad de los datos de carácter personal afectados. Los prestadores de servicios de alojamiento de datos revisarán y actualizarán dichas garantías cuando sea necesario.

### SECCIÓN III

#### GARANTÍAS Y RENDICIÓN DE CUENTAS

#### Artículo 8

##### Obligaciones de transparencia **para los prestadores de servicios de alojamiento de datos** [Enm. 94]

1. **En su caso**, los prestadores de servicios de alojamiento de datos establecerán **claramente** en sus términos y condiciones su política destinada a evitar la difusión de contenidos terroristas, incluida, ~~cuando proceda~~ **en su caso**, una explicación sustanciosa del funcionamiento de las medidas proactivas, ~~entre ellas el uso de instrumentos automatizados~~ **específicas**. [Enm. 95]

2. Los prestadores de servicios de alojamiento de datos ~~publicarán~~ **que estén sujetos o que hayan estado sujetos a órdenes de retirada ese año harán público** informes anuales de transparencia sobre las actuaciones llevadas a cabo contra la difusión de contenidos terroristas. [Enm. 96]

3. Los informes de transparencia incluirán al menos la siguiente información:

a) información sobre las medidas del prestador de servicios de alojamiento de datos en relación con la detección, la identificación y la retirada de contenidos terroristas;

Miércoles, 17 de abril de 2019

- b) información sobre las medidas del prestador de servicios de alojamiento de datos destinadas a evitar que vuelvan a subirse contenidos que hayan sido retirados o cuyo acceso haya sido bloqueado previamente por considerarse que se trataba de contenidos terroristas, **en particular cuando se haya utilizado tecnología automatizada**; [Enm. 97]
- c) número de elementos de contenido terrorista retirados o cuyo acceso haya sido bloqueado como consecuencia de órdenes de retirada, ~~requerimientos~~ o medidas ~~proactivas~~ **específicas**, respectivamente, **y número de órdenes cuando no se hayan retirado los contenidos de conformidad con el artículo 4, apartados 7 y 8, junto con los motivos de la negativa**; [Enm. 98]
- d) ~~resumen~~ **número** y resultados de los procedimientos de reclamación **y los recursos judiciales, incluido el número de casos en que se determinó que los contenidos se habían considerado erróneamente contenidos terroristas**. [Enm. 99]

#### Artículo 8 bis

##### Obligaciones de transparencia de las autoridades competentes

1. **Las autoridades competentes publicarán informes anuales de transparencia que incluirán, como mínimo, la siguiente información:**
  - a) **número de órdenes de retirada emitidas, número de retiradas y número de órdenes de retirada a las que se opuso una negativa o que no se cumplieron;**
  - b) **número de contenidos considerados terroristas que hayan dado lugar a investigaciones y enjuiciamientos, y número de casos en que se consideró erróneamente que los contenidos eran terroristas;**
  - c) **descripción de las medidas solicitadas por las autoridades competentes con arreglo al artículo 6, apartado 4.** [Enm. 100]

#### Artículo 9

##### Garantías en relación con el uso y la aplicación de medidas ~~proactivas~~ **específicas** [Enm. 101]

1. Cuando los prestadores de servicios de alojamiento de datos usen instrumentos automatizados ~~de conformidad con el presente Reglamento~~ en relación con los contenidos que hayan almacenado, aplicarán garantías eficaces y adecuadas para garantizar que las decisiones tomadas en relación con dichos contenidos, en particular las decisiones de retirar los contenidos considerados terroristas o bloquear el acceso a ellos, sean precisas y bien fundamentadas. [Enm. 102]
2. Dichas garantías consistirán, en particular, en la supervisión y verificación ~~uando proceda y, en cualquier caso, cuando se precise una evaluación detallada del contexto pertinente para determinar si los contenidos deben considerarse~~ **de la idoneidad de la decisión de retirar** contenidos terroristas **o no denegar el acceso a estos, en particular por lo que respecta al derecho a la libertad de expresión y la libertad de recibir o de comunicar informaciones o ideas en una sociedad abierta y democrática**. [Enm. 103]

#### Artículo 9 bis

##### Vías de recurso efectivas

1. **Los proveedores de contenidos cuyos contenidos hayan sido retirados o el acceso a los cuales haya sido bloqueado como consecuencia de una orden de retirada y los prestadores de servicios de alojamiento de datos que hayan recibido una orden de retirada tendrán derecho a la tutela judicial efectiva. Los Estados miembros establecerán procedimientos efectivos para ejercer este derecho.** [Enm. 104]

Miércoles, 17 de abril de 2019

## Artículo 10

## Mecanismos de reclamación

1. Los prestadores de servicios de alojamiento de datos establecerán ~~mecanismos eficaces~~ **un mecanismo eficaz y accesible** que ~~permitan~~ **permita** a los proveedores de contenidos cuyos contenidos hayan sido retirados o hayan visto bloqueado su acceso como consecuencia ~~de un requerimiento con arreglo al artículo 5 o~~ de medidas ~~proactivas~~ **específicas** con arreglo al artículo 6 presentar una reclamación contra la actuación del prestador de servicios de alojamiento de datos en la que se solicite el restablecimiento del contenido. [Enm. 105]
2. Los prestadores de servicios de alojamiento de datos deben examinar rápidamente todas las reclamaciones que reciban y restablecer el contenido sin demora indebida cuando la retirada o el bloqueo del acceso no estuviese justificado. Informarán al reclamante sobre el resultado del examen **en el plazo de dos semanas desde la recepción de la reclamación, con una explicación en los casos en que los prestadores de servicios de alojamiento de datos decidan no restablecer el contenido. El restablecimiento del contenido no impedirá la adopción de otras medidas judiciales contra la decisión del prestador de servicios de alojamiento de datos o de la autoridad competente.** [Enm. 106]

## Artículo 11

## Información a los proveedores de contenidos

1. Cuando los prestadores de servicios de alojamiento de datos ~~hayan retirado~~ **retiren** contenidos terroristas **ilegales** o ~~bloqueen~~ **bloqueen** el acceso a ellos, pondrán a disposición del proveedor de contenidos información **completa y concisa** sobre la retirada de los contenidos terroristas o el bloqueo del acceso a ellos, **que incluirá las posibilidades de impugnación de la decisión, y le proporcionarán una copia de la orden de retirada emitida en virtud del artículo 4.** [Enm. 107]
2. ~~A petición del proveedor de contenidos, el prestador de servicios de alojamiento de datos informará al proveedor de contenidos sobre los motivos de la retirada o del bloqueo del acceso y las posibilidades de impugnación de la decisión.~~ [Enm. 108]
3. La obligación fijada en ~~los apartados~~ **el apartado** 1 ~~y 2~~ no será de aplicación cuando la autoridad competente decida, **con base en pruebas objetivas y teniendo en cuenta la proporcionalidad y la necesidad de dicha decisión**, que no debe revelarse esa información por razones de seguridad pública, como la prevención, la investigación, la detección y el enjuiciamiento de los delitos de terrorismo, durante el tiempo necesario, sin que exceda las [cuatro] semanas a partir de dicha decisión. En esos casos, el prestador de servicios de alojamiento de datos no revelará información alguna acerca de la retirada de contenidos terroristas o del bloqueo de su acceso. [Enm. 109]

## SECCIÓN IV

## COOPERACIÓN ENTRE LAS AUTORIDADES COMPETENTES, LOS ORGANISMOS DE LA UNIÓN Y LOS PRESTADORES DE SERVICIOS DE ALOJAMIENTO DE DATOS

## Artículo 12

## Capacidades de las autoridades competentes

Los Estados miembros garantizarán que sus autoridades competentes tienen la capacidad necesaria y los recursos suficientes para alcanzar los objetivos del presente Reglamento y cumplir las obligaciones que este les impone, **con garantías sólidas de independencia.** [Enm. 110]

## Artículo 13

Cooperación entre los prestadores de servicios de alojamiento de datos, las autoridades competentes y, cuando proceda, los organismos de la Unión ~~pertinentes~~ **competentes** [Enm. 111]

1. Las autoridades competentes de los Estados miembros se informarán mutuamente, se coordinarán y cooperarán entre sí y, cuando proceda, con ~~los organismos de la Unión pertinentes, como~~ Europol, en relación con las órdenes de retirada y ~~los requerimientos~~ para evitar duplicidades, mejorar la coordinación y evitar las interferencias con las investigaciones en diferentes Estados miembros. [Enm. 112]

Miércoles, 17 de abril de 2019

2. Las autoridades competentes de los Estados miembros informarán a la autoridad competente a que se refiere el artículo 17, apartado 1, letras c) y d), y se coordinarán y cooperarán con ella en lo relativo a las medidas tomadas con arreglo al artículo 6 y las medidas de garantía del cumplimiento con arreglo al artículo 18. Los Estados miembros asegurarán que la autoridad competente a que se refiere el artículo 17, apartado 1, letras c) y d), está en posesión de toda la información pertinente. A tal efecto, los Estados miembros dispondrán canales o mecanismos de comunicación adecuados **y seguros** para velar por que la información pertinente se comparta a su debido tiempo. [Enm. 113]

3. Los Estados miembros ~~y los prestadores de servicios de alojamiento de datos~~ podrán elegir hacer uso de instrumentos específicos, incluidos, ~~cuando proceda, los establecidos por organismos de la Unión pertinentes como~~ Europol, para facilitar, en particular: [Enm. 114]

a) el procesamiento y la información en relación con las órdenes de retirada de conformidad con el artículo 4;

b) ~~el procesamiento y la información en relación con los requerimientos de conformidad con el artículo 5;~~ [Enm. 115]

c) la cooperación con vistas a la determinación y la aplicación de medidas ~~proactivas~~ **específicas** de conformidad con el artículo 6. [Enm. 116]

4. Cuando los prestadores de servicios de alojamiento de datos tengan conocimiento de ~~cualquier indicio de delitos de terrorismo~~ **contenidos terroristas**, informarán rápidamente a las autoridades competentes para investigar y enjuiciar infracciones penales en el Estado miembro correspondiente ~~o~~. **Cuando resulte imposible identificar el Estado miembro correspondiente, los prestadores de servicios de alojamiento de datos lo notificarán** al punto de contacto del Estado miembro de conformidad con el artículo ~~14~~ **17**, apartado 2, en el que tengan su establecimiento principal o un representante legal. ~~Los prestadores de servicios de alojamiento de datos podrán, en caso de duda,~~ **y transmitirán también** transmitir esa información a Europol para que se le dé el curso adecuado. [Enm. 117]

**4 bis. Los prestadores de servicios de alojamiento de datos cooperarán con las autoridades competentes.** [Enm. 118]

#### Artículo 14

##### Puntos de contacto

1. Los prestadores de servicios de alojamiento de datos **que ya hayan recibido una o varias órdenes de retirada** establecerán un punto de contacto que permita la recepción de órdenes de retirada ~~y requerimientos~~ por medios electrónicos y garantice su procesamiento ~~rápido~~ **expeditivo** de conformidad con ~~los artículos~~ **el artículo 4 y 5**. Velarán por que esta información esté disponible al público. [Enm. 119]

2. La información mencionada en el apartado 1 especificará la lengua oficial o lenguas oficiales de la Unión, previstas en el Reglamento 1/58, en que sea posible dirigirse al punto de contacto y en que tendrán lugar las subsiguientes conversaciones en relación con las órdenes de retirada ~~y los requerimientos~~ a que se ~~refieren los artículos~~ **refiere el artículo 4 y 5**. Entre ellas estará al menos una de las lenguas oficiales del Estado miembro en el que el prestador de servicios de alojamiento de datos tenga su establecimiento principal o en el que resida o esté establecido su representante legal con arreglo al artículo 16. [Enm. 120]

3. ~~Los Estados miembros establecerán un punto de contacto para gestionar las solicitudes de aclaraciones e información en relación con las órdenes de retirada y los requerimientos que hayan emitido. La información sobre el punto de contacto estará disponible al público.~~ [Enm. 121]

Miércoles, 17 de abril de 2019

SECCIÓN V  
APLICACIÓN Y EJECUCIÓN

## Artículo 15

## Jurisdicción

1. La jurisdicción a efectos de los artículos 6, 18 y 21 corresponderá al Estado miembro en el que esté ubicado el establecimiento principal del prestador de servicios de alojamiento de datos. Se considerará que un prestador de servicios de alojamiento de datos que no tenga su establecimiento principal en uno de los Estados miembros se encuentra bajo la jurisdicción del Estado miembro en el que resida o esté establecido su representante legal con arreglo al artículo 16.
2. Cuando un prestador de servicios de alojamiento de datos **que no tenga su establecimiento principal en uno de los Estados miembros** no designe un representante legal, la jurisdicción corresponderá a todos los Estados miembros. **Cuando un Estado miembro decida ejercer esta jurisdicción informará de ello a todos los demás Estados miembros.** [Enm. 122]
3. ~~Cuando una autoridad de otro Estado miembro haya emitido una orden de retirada con arreglo al artículo 4, apartado 1, dicho Estado miembro tendrá jurisdicción para tomar medidas coercitivas con arreglo a su normativa nacional destinadas a hacer cumplir la orden de retirada.~~ [Enm. 123]

## Artículo 16

## Representante legal

1. Los prestadores de servicios de alojamiento de datos que no tengan un establecimiento en la Unión, pero que ofrezcan servicios en la Unión, designarán por escrito a una persona física o jurídica como representante legal en la Unión a efectos de la recepción, el cumplimiento y la ejecución de las órdenes de retirada, ~~los requerimientos,~~ **y** las solicitudes ~~y las decisiones emitidas~~ **emitidas** por las autoridades competentes con arreglo al presente Reglamento. El representante legal deberá residir o estar establecido en uno de los Estados miembros en los que el prestador de servicios de alojamiento de datos ofrezca los servicios. [Enm. 124]
2. El prestador de servicios de alojamiento de datos encomendará al representante legal la recepción, el cumplimiento y la ejecución de las órdenes de retirada, ~~los requerimientos,~~ **y** las solicitudes ~~y las decisiones~~ a que se refiere el apartado 1 en nombre del prestador de servicios de alojamiento de datos correspondiente. Los prestadores de servicios de alojamiento de datos otorgarán a su representante legal los poderes y recursos necesarios para cooperar con las autoridades competentes y cumplir esas decisiones y órdenes. [Enm. 125]
3. El representante legal designado puede ser considerado responsable del incumplimiento de las obligaciones fijadas en el presente Reglamento, sin perjuicio de la responsabilidad del prestador de servicios de alojamiento de datos y de las acciones legales que podrían iniciarse contra este.
4. El prestador de servicios de alojamiento de datos notificará la designación a la autoridad competente a que se refiere el artículo 17, apartado 1, letra d), del Estado miembro en el que resida o esté establecido el representante legal. La información sobre el representante legal estará disponible al público.

## SECCIÓN VI

## DISPOSICIONES FINALES

## Artículo 17

## Designación de las autoridades competentes

1. Los Estados miembros designarán ~~la~~ **una** autoridad ~~o autoridades competentes~~ **judicial o a una autoridad administrativa funcionalmente independiente que será competente** para: [Enm. 126]
  - a) emitir órdenes de retirada con arreglo al artículo 4;

Miércoles, 17 de abril de 2019

- b) ~~detectar e identificar contenidos terroristas y enviar requerimientos respecto de ellos a los prestadores de servicios de alojamiento de datos con arreglo al artículo 5;~~ [Enm. 127]
- c) supervisar la aplicación de las medidas ~~proactivas~~**específicas** con arreglo al artículo 6; [Enm. 128]
- d) hacer cumplir las obligaciones que impone el presente Reglamento mediante sanciones con arreglo al artículo 18.

**1 bis.** *Los Estados miembros designarán un punto de contacto en el seno de las autoridades competentes para tramitar las solicitudes de aclaraciones e información en relación con las órdenes de retirada que hayan emitido. La información sobre el punto de contacto estará disponible al público.* [Enm. 129]

2. A más tardar [seis meses después de la fecha de entrada en vigor del presente Reglamento], los Estados miembros notificarán a la Comisión cuáles son las autoridades competentes a que se refiere el apartado 1. **La Comisión creará un registro en línea en el que figurarán todas las autoridades competentes y el punto de contacto designado para cada una de ellas.** La Comisión publicará la notificación, y sus eventuales modificaciones, en el *Diario Oficial de la Unión Europea*. [Enm. 130]

#### Artículo 18

##### Sanciones

1. Los Estados miembros determinarán el régimen de sanciones aplicable a las infracciones **sistemáticas y persistentes** de las obligaciones impuestas a los prestadores de servicios de alojamiento de datos en el presente Reglamento y tomarán todas las medidas necesarias para garantizar su aplicación. Dichas sanciones se limitarán a las infracciones de las obligaciones que imponen: [Enm. 131]

- a) ~~el artículo 3, apartado 2 (términos y condiciones de los prestadores de servicios de alojamiento de datos);~~ [Enm. 132]
- b) el artículo 4, apartados 2 y 6 (aplicación de las órdenes de retirada e información sobre ellas);
- e) ~~el artículo 5, apartados 5 y 6 (evaluación de los requerimientos e información sobre ellos);~~ [Enm. 133]
- d) el artículo 6, ~~apartados 2 y~~**apartado 4** (informes sobre medidas ~~proactivas~~**específicas** y adopción de medidas tras una ~~decisión~~**solicitud** que imponga medidas ~~proactivas~~ específicas **adicionales**); [Enm. 134]
- e) el artículo 7 (conservación de datos);
- f) el artículo 8 (transparencia **para los prestadores de servicios de alojamiento de datos**); [Enm. 135]
- g) el artículo 9 (garantías en relación con ~~las~~**la aplicación de** medidas ~~proactivas~~**específicas**); [Enm. 136]
- h) el artículo 10 (procedimientos de reclamación);
- i) el artículo 11 (información a los proveedores de contenidos);
- j) el artículo 13, apartado 4 (información sobre ~~indicios de delitos de terrorismo~~**contenidos terroristas**); [Enm. 137]
- k) el artículo 14, apartado 1 (puntos de contacto);
- l) el artículo 16 (designación de un representante legal).

2. Las sanciones ~~que se impongan~~**contempladas en el apartado 1** serán eficaces, proporcionadas y disuasorias. A más tardar [seis meses desde la entrada en vigor del presente Reglamento], los Estados miembros notificarán dichas normas y medidas a la Comisión, y le notificarán sin demora toda modificación posterior de estas. [Enm. 138]

Miércoles, 17 de abril de 2019

3. Los Estados miembros garantizarán que, al determinar el tipo y el nivel de las sanciones, las autoridades competentes tengan en cuenta todas las circunstancias pertinentes, entre ellas:

- a) la naturaleza, la gravedad y la duración de la infracción;
- b) el carácter doloso o culposo de la infracción;
- c) las infracciones previas de la persona jurídica considerada responsable;
- d) la solidez financiera de la persona jurídica considerada responsable;
- e) el nivel de cooperación del prestador de servicios de alojamiento de datos con las autoridades competentes; [Enm. 139]

***e bis) la naturaleza y el tamaño de los prestadores de servicios de alojamiento de datos, en particular las microempresas o pequeñas empresas en el sentido de la Recomendación 2003/361/CE de la Comisión <sup>(13)</sup>. [Enm. 140]***

4. Los Estados miembros garantizarán que el incumplimiento sistemático **y persistente** de las obligaciones impuestas en virtud del artículo 4, apartado 2, se someta a sanciones económicas de hasta el 4 % del volumen de negocio mundial del prestador de servicios de alojamiento de datos en el último ejercicio. [Enm. 141]

#### Artículo 19

Requisitos técnicos, ***criterios para evaluar la importancia*** y modificaciones de las plantillas de órdenes de retirada [Enm. 142]

1. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 20 con el fin de complementar el presente Reglamento con requisitos técnicos ***necesarios*** para los medios electrónicos que deben usar las autoridades competentes para la transmisión de las órdenes de retirada. [Enm. 143]

***1 bis. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 20 por los que se complete el presente Reglamento con criterios y cifras que deberán usar las autoridades competentes para determinar a qué corresponde el número significativo de órdenes de retirada no impugnadas a que se refiere el presente Reglamento. [Enm. 144]***

2. La Comisión estará facultada para adoptar actos delegados de modificación de los anexos I, II y III con el fin de abordar de forma efectiva la posible necesidad de mejoras en lo que concierne al contenido de los formularios de orden de retirada y de los formularios que deben utilizarse para facilitar información sobre la imposibilidad de ejecutar la orden de retirada.

#### Artículo 20

##### Ejercicio de la delegación

1. Se otorgan a la Comisión poderes para adoptar actos delegados en las condiciones establecidas en el presente artículo.

2. Los poderes para adoptar los actos delegados a que se refiere el artículo 19 se otorgarán a la Comisión por un período de tiempo indefinido a partir del [fecha de aplicación del presente Reglamento].

3. La delegación de poderes a que se refiere el artículo 19 podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La Decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La Decisión surtirá efecto el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior indicada en la misma. No afectará a la validez de los actos delegados que ya estén en vigor.

4. Antes de la adopción de un acto delegado, la Comisión consultará a los expertos designados por cada Estado miembro de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación .

---

<sup>(13)</sup> Recomendación de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas (DO L 124 de 20.5.2003, p. 36).

Miércoles, 17 de abril de 2019

5. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.

6. Los actos delegados adoptados en virtud del artículo 19 entrarán en vigor únicamente si, en un plazo de dos meses desde su notificación al Parlamento Europeo y al Consejo, ni el Parlamento Europeo ni el Consejo formulan objeciones o si, antes del vencimiento de dicho plazo, tanto el uno como el otro informan a la Comisión de que no las formularán. El plazo se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.

#### Artículo 21

##### Seguimiento

1. Los Estados miembros recabarán de sus autoridades competentes y de los prestadores de servicios de alojamiento de datos bajo su jurisdicción información sobre las actuaciones que hayan llevado a cabo de conformidad con el presente Reglamento, y la enviarán a la Comisión a más tardar el [31 de marzo] de cada año. Dicha información incluirá los elementos siguientes:

a) información sobre el número de órdenes de retirada ~~y de requerimientos emitidos~~ **emitidas**, el número de elementos de contenido terrorista que se hayan retirado o cuyo acceso se haya bloqueado, incluidos los períodos correspondientes con arreglo ~~a los artículos~~ **al artículo 4 y 5, e información sobre el número de casos correspondientes de detección, investigación y enjuiciamiento satisfactorios de delitos del terrorismo;** [Enm. 145]

b) información sobre las medidas proactivas específicas tomadas en virtud del artículo 6, incluida la cantidad de contenidos terroristas que se hayan retirado o cuyo acceso se haya bloqueado y los períodos correspondientes;

**b bis) información sobre el número de solicitudes de acceso emitidas por las autoridades competentes en relación con los contenidos conservados por los prestadores de servicios de alojamiento de datos con arreglo al artículo 7;** [Enm. 146]

c) información sobre el número de procedimientos de reclamación iniciados y las actuaciones emprendidas por los prestadores de servicios de alojamiento de datos con arreglo al artículo 10;

d) información sobre el número de procedimientos de recurso iniciados y las decisiones tomadas por la autoridad competente de conformidad con la normativa nacional.

2. A más tardar [un año después de la fecha de aplicación del presente Reglamento], la Comisión elaborará un programa detallado para el seguimiento de las realizaciones, los resultados y las repercusiones del presente Reglamento. El programa de seguimiento establecerá los indicadores que se tendrán en cuenta en la recopilación de datos y otras pruebas necesarias, los medios por los que se recopilarán y la periodicidad de dicha recopilación. Especificará las acciones que deben adoptar la Comisión y los Estados miembros al recopilar y analizar los datos y otras pruebas necesarias a efectos del seguimiento de los avances y la evaluación del presente Reglamento de conformidad con el artículo 23.

#### Artículo 22

##### Informe de aplicación

A más tardar [dos años después de la fecha de entrada en vigor del presente Reglamento], la Comisión presentará un informe al Parlamento Europeo y al Consejo acerca de la aplicación del presente Reglamento. En el informe de la Comisión se tendrán en cuenta la información sobre el seguimiento con arreglo al artículo 21 y la información que se derive de las obligaciones de transparencia con arreglo al artículo 8. Los Estados miembros facilitarán a la Comisión la información necesaria para la preparación del informe.

#### Artículo 23

##### Evaluación

~~No antes del [tres años desde~~ **Un año después de** la fecha de aplicación del presente Reglamento], la Comisión llevará a cabo una evaluación del presente Reglamento y presentará un informe al Parlamento Europeo y al Consejo sobre la aplicación del presente Reglamento, que entre otros asuntos trate el funcionamiento y la eficacia de los mecanismos de garantía, **así como el impacto sobre los derechos fundamentales, en particular la libertad de expresión, la libertad de recibir o de comunicar información y el derecho al respeto de la intimidad. En el contexto de esta evaluación, la Comisión informará también sobre la necesidad, la viabilidad y la eficacia de la creación de una plataforma europea sobre contenidos terroristas en**

Miércoles, 17 de abril de 2019

***línea, que permitiría a todos los Estados miembros utilizar un canal de comunicación seguro para enviar las órdenes de retirada de contenidos terroristas a los prestadores de servicios de alojamiento de datos.*** En su caso, el informe irá acompañado de propuestas legislativas. Los Estados miembros facilitarán a la Comisión la información necesaria para la preparación del informe. [Enm. 147]

## Artículo 24

## Entrada en vigor

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

Será aplicable a partir del ~~seis~~**doce** meses después de su entrada en vigor. [Enm. 148]

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en ..., el

*Por el Parlamento Europeo*

*El Presidente*

*Por el Consejo*

*El Presidente*

---

Miércoles, 17 de abril de 2019

**ANEXO I****ORDEN DE RETIRADA DE CONTENIDOS TERRORISTAS [Artículo 4 del Reglamento (UE) xxx]**

De conformidad con el artículo 4 del Reglamento (UE) ... <sup>(1)</sup>, el destinatario de la orden de retirada retirará los contenidos terroristas o bloqueará el acceso a ellos en el plazo de una hora desde la recepción de la orden de retirada de la autoridad competente.

De conformidad con el artículo 7 del Reglamento (UE) ... <sup>(2)</sup>, los destinatarios deben conservar los contenidos que hayan sido retirados o cuyo acceso haya sido bloqueado y los datos conexos durante seis meses, o un período más largo en caso de que así se lo soliciten las autoridades u órganos jurisdiccionales competentes.

La orden de retirada debe enviarse en una de las lenguas designadas por el destinatario de conformidad con el artículo 14, apartado 2.

**SECCIÓN A:**

Estado miembro emisor: .....

Nota: los datos de la autoridad emisora se facilitan al final (Secciones E y F).

Destinatario (representante legal):

.....

Destinatario (punto de contacto):

.....

Estado miembro de jurisdicción del destinatario [si es diferente del Estado emisor]: .....

Fecha y hora de emisión de la orden de retirada:

.....

Número de referencia de la orden de retirada: .....

<sup>(1)</sup> Reglamento del Parlamento Europeo y del Consejo para la prevención de la difusión de contenidos terroristas en línea (DO L ...).

<sup>(2)</sup> Reglamento del Parlamento Europeo y del Consejo para la prevención de la difusión de contenidos terroristas en línea (DO L ...).

SECCIÓN B: contenidos que deben retirarse o cuyo acceso debe ser bloqueado ~~en el plazo de una hora~~ **sin demora indebida** [Enm. 162]

URL y cualquier otra información que posibilite la identificación y localización exacta de los contenidos afectados:

.....

Motivo o motivos por los que los contenidos se consideran contenidos terroristas con arreglo al artículo 2, punto 5, del Reglamento (UE) xxx. Los contenidos (marque la casilla o casillas pertinentes):

- incitan a la comisión de delitos de terrorismo **enumerados en el artículo 3, apartado 1, letras a) a i), de la Directiva (UE) 2017/541** la defienden hacen apología de ella (artículo 2, apartado 5, letra a)) [Enm. 149]
- ~~fomentan la contribución a~~ **inducen a otra persona o grupo de personas a que cometan o contribuyan a la comisión de** delitos de terrorismo **enumerados en el artículo 3, apartado 1, letras a) a i), de la Directiva (UE) 2017/541** (artículo 2, apartado 5, letra b)) [Enm. 150]
- ~~promueven las~~ **inducen a otra persona o grupo de personas a que participen en** actividades de un grupo terrorista **enumeradas en el artículo 3, apartado 1, letras a) a i), de la Directiva (UE) 2017/541** (artículo 2, apartado 5, letra c)) [Enm. 151]
- facilitan **instrucciones o técnicas para la fabricación o el uso de explosivos, armas de fuego u otras armas o sustancias nocivas o peligrosas, o sobre otros métodos específicos,** instrucciones o técnicas para la comisión de delitos de terrorismo **enumerados en el artículo 3, apartado 1, letras a) a i), de la Directiva (UE) 2017/541** (artículo 2, apartado 5, letra d)) [Enm. 152]
- representan la comisión de delitos de terrorismo enumerados en el artículo 3, apartado 1, letras a) a i), de la Directiva (UE) 2017/541** (artículo 2, apartado 5, letra e)) [Enm. 153]

Información adicional sobre los motivos por los que los contenidos se consideran contenidos terroristas (opcional):

.....

.....

SECCIÓN C: información para el proveedor de contenidos

Téngase en cuenta que (marcar, en su caso):

- por razones de seguridad pública, el destinatario **debe abstenerse de informar al proveedor de contenidos** cuyos contenidos se han retirado o a los cuales se ha bloqueado el acceso.

De lo contrario: datos de las posibilidades de impugnación de la orden de retirada en el Estado miembro emisor (que pueden facilitarse al proveedor de contenidos, si lo solicita) con arreglo a la normativa nacional; véase la Sección G.

SECCIÓN D: Estado miembro de jurisdicción que informa

- Márquese si el Estado de jurisdicción del destinatario es diferente del Estado miembro emisor
- Se envía una copia de la orden de retirada a la autoridad competente pertinente del Estado de jurisdicción

Miércoles, 17 de abril de 2019

SECCIÓN E: datos de la autoridad emisora de la orden de retirada

Tipo de autoridad que ha emitido la orden de retirada (marque la casilla correspondiente):

- juez, tribunal o juez de instrucción
- autoridad policial
- otra autoridad competente → rellene también la Sección (F)

Datos de la autoridad emisora y/o de su representante que certifica la orden de retirada como precisa y correcta:

Nombre de la autoridad: .....

Nombre del representante: .....

Cargo que ocupa (título/grado): .....

Expediente n.º: .....

Dirección:

N.º de teléfono: (prefijo de país) (prefijo de ciudad/región) .....

N.º de fax: (prefijo de país) (prefijo de ciudad/región) .....

Correo electrónico: .....

Fecha:

.....

Sello oficial (en su caso) y firma <sup>(1)</sup>: .....

SECCIÓN F: datos de contacto para el seguimiento

Datos de contacto de la autoridad emisora para la recepción de información sobre la hora de la retirada o el bloqueo del acceso, o para la solicitud de aclaraciones adicionales:

.....

Datos de contacto de la autoridad del Estado de jurisdicción del destinatario [si es diferente del Estado miembro emisor]:

.....

SECCIÓN G: información sobre posibilidades de recurso

Información sobre el organismo u órgano jurisdiccional competente, los plazos y los procedimientos, **incluidos los requisitos formales**, para impugnar la orden de retirada: [Enm. 154]

Organismo u órgano jurisdiccional ante el que impugnar la orden de retirada:

.....

Plazo para impugnar la decisión:

Xxx meses a partir de xxxx

Enlace a las disposiciones nacionales:

.....

<sup>(1)</sup> Puede no ser necesaria la firma si el envío se realiza mediante canales de transmisión autenticada.

Miércoles, 17 de abril de 2019

ANEXO II

FORMULARIO DE INFORMACIÓN POSTERIOR A LA RETIRADA DE CONTENIDOS TERRORISTAS O EL BLOQUEO DE SU ACCESO

[artículo 4, apartado 5, del Reglamento (UE) xxx]

SECCIÓN A:

Destinatario de la orden de retirada:  
.....

Autoridad emisora de la orden de retirada:  
.....

Referencia de la autoridad emisora:  
.....

Referencia del destinatario:  
.....

Fecha y hora de recepción de la orden de retirada:  
.....

SECCIÓN B:

Los contenidos terroristas / el acceso a los contenidos terroristas objeto de la orden de retirada ha(n) sido objeto de (marque la casilla correspondiente)

retirada

bloqueo

Fecha y hora de la retirada o el bloqueo del acceso: .....

SECCIÓN C: datos del destinatario

Nombre del prestador de servicios de alojamiento de datos / representante legal:  
.....

Estado miembro del establecimiento principal o de establecimiento del representante legal:  
.....

Nombre de la persona autorizada:  
.....

Datos del punto de contacto (correo electrónico): .....

Fecha:  
.....

Miércoles, 17 de abril de 2019

## ANEXO III

## INFORMACIÓN SOBRE LA IMPOSIBILIDAD DE EJECUTAR LA ORDEN DE RETIRADA [artículo 4, apartados 6 y 7, del Reglamento (UE) xxx]

## SECCIÓN A:

Destinatario de la orden de retirada:

.....

Autoridad emisora de la orden de retirada:

.....

Referencia de la autoridad emisora: .....

.....

Referencia del destinatario: .....

.....

Fecha y hora de recepción de la orden de retirada:

.....

## SECCIÓN B: motivos de la inexecución

i) La orden de retirada no puede ejecutarse, o no puede ejecutarse en el plazo exigido, por el motivo o motivos siguientes:

- fuerza mayor o imposibilidad de hecho no atribuible al destinatario o al prestador de servicios, **también por motivos técnicos u operativos [Enm. 155]**
- la orden de retirada contiene errores manifiestos
- la orden de retirada no contiene suficiente información

ii) Facilite más información sobre los motivos de la inexecución:

.....

iii) Si la orden de retirada contiene errores manifiestos y/o no contiene suficiente información, especifique los errores y la información o aclaraciones adicionales necesarias:

.....

## SECCIÓN H: datos del prestador de servicios / representante legal

Nombre del prestador de servicios / representante legal:

.....

Nombre de la persona autorizada:

.....

Datos de contacto (correo electrónico):

.....

Firma:

.....

Fecha y hora: .....