



Bruselas, 7 de diciembre de 2018
(OR. en)

15336/18

**Expediente interinstitucional:
2018/0331(COD)**

CT 198
ENFOPOL 605
JAI 1264
COTER 175
CYBER 313
TELECOM 461
FREMP 222
AUDIO 121
DROIPEN 199
CODEC 2270

RESULTADO DE LOS TRABAJOS

De:	Secretaría General del Consejo
Fecha:	6 de diciembre de 2018
A:	Delegaciones
N.º doc. prec.:	14978/18 + COR 1
N.º doc. Ción.:	12129/18 + ADD 1-3
Asunto:	Propuesta de Reglamento del Parlamento Europeo y del Consejo para la prevención de la difusión de contenidos terroristas en línea - Orientación general

En su sesión del 6 de diciembre de 2018, el Consejo adoptó la orientación general recogida en el anexo.

Los cambios respecto a la propuesta de la Comisión se indican en *negrita itálica* para los añadidos y mediante el signo [...] para las supresiones.

[...]

[...] *Proyecto de*

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

sobre la prevención de la difusión de contenidos terroristas en línea

[...]

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,

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

Visto el dictamen del Comité Económico y Social Europeo¹,

De conformidad con el procedimiento legislativo ordinario,

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 el uso indebido de los servicios de alojamiento de datos con fines terroristas. 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 y de información.

¹ DO C [...] de [...], p. [...].

- (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 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.
- (3) La presencia de contenidos terroristas en línea 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 de 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 evitar la difusión de contenidos terroristas a través de sus servicios.
- (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 Comisión², y responde a los llamamientos realizados por el Parlamento Europeo para reforzar las medidas de lucha contra los contenidos ilícitos y nocivos y por el Consejo Europeo para mejorar la detección automática y la retirada de los contenidos que incitan actos terroristas.

² 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).

- (5) La aplicación del presente Reglamento no debe afectar a la aplicación del artículo 14 de la Directiva 2000/31/CE³. 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. ***El presente Reglamento no se aplica a las actividades relacionadas con la seguridad nacional, que siguen siendo responsabilidad exclusiva de cada Estado miembro.***
- (6) Las normas para evitar 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 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.

³ 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).

- (7) El presente Reglamento contribuye a la protección de la seguridad pública a la vez que establece 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 información, **así como a la libertad de prensa y al pluralismo de los medios de comunicación**, que constituyen [...] los pilares esenciales de una sociedad democrática y pluralista y uno de los valores en que se fundamenta la Unión. Las medidas que constituyan una interferencia con la libertad de expresión y de información deben ser muy específicas, en el sentido de que deben servir para evitar la difusión de contenidos terroristas 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.
- (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 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 **y de que los prestadores de servicios de alojamiento de datos impugnen una decisión por la que se impongan sanciones o medidas proactivas ante el órgano jurisdiccional del Estado miembro en el que estén establecidos o tengan un representante legal.**

- (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 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 Consejo⁴. Dada la necesidad de luchar contra la propaganda terrorista en línea más nociva, la definición debe incluir el material [...] que incite a la comisión de delitos de terrorismo o a la contribución a ellos, las fomente o las defiendan [...] o promueva la participación en las actividades de un grupo terrorista. [...] **La definición incluye los contenidos que instruyen sobre la fabricación y el uso de explosivos, armas de fuego u otras armas o sustancias nocivas o peligrosas, así como de sustancias QBRN, o sobre otros métodos y técnicas, entre ellas la selección de objetivos, a fin de cometer delitos de terrorismo.** Dicho [...] **material** 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, [...] **de contranarrativa** o de investigación deben protegerse adecuadamente **para lograr un justo equilibrio entre los derechos fundamentales, y en particular entre la libertad de expresión y de información y la necesidad de garantizar la seguridad pública. Cuando el material difundido se publique bajo la responsabilidad editorial del proveedor de contenidos, toda resolución relativa a la supresión de este tipo de contenidos debe tener en cuenta aquellos estándares periodísticos establecidos por la prensa o los medios de comunicación que sean compatibles con el Derecho de la Unión, el derecho a la libertad de expresión y el derecho a la libertad y el pluralismo de los medios de comunicación consagrados en el artículo 11 de la Carta de los Derechos Fundamentales.** Además, la expresión de puntos de vista radicales, polémicos o controvertidos en el debate público sobre cuestiones políticas sensibles no debe considerarse contenido terrorista.

⁴ 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).

- (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 **y el material** que almacenen información proporcionada por un receptor del servicio a petición de este y pongan la información **y el material** almacenados a disposición de terceros, independientemente de que esa actividad sea de naturaleza meramente técnica, automática o pasiva. [...] ***El almacenamiento de contenidos consiste en conservar datos en la memoria de un servidor físico o virtual; ello excluye del ámbito de aplicación los servicios dedicados a la mera transmisión y otros servicios de comunicación electrónica en el sentido del [Código Europeo de las Comunicaciones Electrónicas] o los prestadores de servicios de almacenamiento temporal, así como otros servicios facilitados en otros niveles de la infraestructura de Internet, como los registros y los registradores, el sistema de nombres de dominio (DNS) o servicios adyacentes, tales como los servicios de pago o los servicios de protección contra ataques de denegación de servicio distribuido (DDoS). Además, la información debe almacenarse a petición del prestador de contenidos; únicamente entran dentro del ámbito de aplicación los servicios en los que el prestador de contenidos es el receptor directo. Por último, la información almacenada se pone a disposición de terceros, es decir a cualquier usuario tercero que no sea prestador de contenidos. No entran dentro del ámbito de aplicación los servicios de comunicación interpersonal que permiten el intercambio interpersonal directo e interactivo de información entre un número limitado de personas, mediante los cuales las personas que inician la comunicación o participan en ella determinan el receptor o receptores. Esos prestadores de servicios de alojamiento de datos [...] 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 y servicios de almacenamiento [...]. El presente Reglamento se aplica a la actividad de prestación de servicios de alojamiento de datos y no al prestador concreto ni a su actividad principal, en la que se podrían combinar servicios de alojamiento de datos con otros servicios que no entren dentro del ámbito de aplicación del presente Reglamento.***

(10 bis) 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.

- (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 n.º 1215/2012 del Parlamento Europeo y del Consejo⁵. 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 Consejo⁶ no puede, por esa única razón, considerarse como dirección u orientación de las actividades hacia un determinado territorio dentro de la Unión.

⁵ 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).

⁶ 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).

- (12) Los prestadores de servicios de alojamiento de datos deben aplicar ciertos deberes de diligencia, con el fin de evitar la difusión de contenidos terroristas en sus servicios. Dichos deberes de diligencia no deben convertirse en una obligación general de supervisión. Entre los deberes de diligencia debe incluirse que, al aplicar el presente Reglamento, los prestadores de servicios de alojamiento de datos actúen de forma 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 **contenidos** terroristas. La retirada o el bloqueo del acceso ha de realizarse en observancia de la libertad de expresión y de información.
- (13) Deben armonizarse el procedimiento y las obligaciones resultantes de las órdenes legales 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 para esas funciones, que pueden ser autoridades administrativas, policiales o judiciales. 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 retiren los contenidos terroristas a que se refiere la orden de retirada, o que se bloquee el acceso a ellos, en el plazo de una hora desde la recepción de la orden de retirada. ***Sin perjuicio de la obligación de conservar los datos en virtud del artículo 7 del presente Reglamento, o en virtud [del proyecto de legislación sobre las pruebas electrónicas], 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. Esto debe tener como efecto impedir el acceso o, como mínimo, dificultarlo y disuadir seriamente a los internautas que recurren a sus servicios de acceder a los contenidos cuyo acceso ha sido bloqueado.***

(13 bis) La orden de retirada debe incluir una clasificación de los contenidos correspondientes en tanto que contenidos terroristas y debe contener información suficiente para localizar los contenidos, facilitando una dirección URL y cualquier otra información adicional, por ejemplo una captura de pantalla de los contenidos en cuestión. Previa petición, la autoridad competente debe facilitar una motivación complementaria para explicar por qué los contenidos se consideran contenidos terroristas. No es preciso que los motivos aducidos contengan información sensible que pudiera poner en riesgo las investigaciones. No obstante, la motivación debe permitir al prestador de servicios de alojamiento de datos y, en última instancia, al prestador de contenidos, ejercer de forma efectiva su derecho a interponer recursos judiciales.

(14) Las autoridades competentes deben transmitir la orden de retirada directamente al destinatario y al punto de contacto 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 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 Consejo⁷.

⁷ 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).

- (15) [...] El [...] mecanismo de **requerimiento** para alertar a los prestadores de servicios de alojamiento de datos acerca de la información **y el material** que pueden considerarse contenido terrorista, para que el prestador tome en consideración voluntariamente la compatibilidad de esa información *con* sus términos y condiciones, **constituye un medio [...] particularmente eficaz, rápido y proporcionado para poner a los prestadores de servicios de alojamiento de datos sobre aviso acerca de contenidos específicos en sus servicios** [...]. 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) 2016/794⁸.
- (16) Dadas la escala y la velocidad necesarias para detectar y retirar eficazmente los contenidos terroristas, la adopción de medidas proactivas 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, 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 la información. En consecuencia, los prestadores de servicios de alojamiento de datos deben determinar qué medida proactiva adecuada, eficaz y proporcionada debe emplearse. Esta exigencia no conlleva una obligación general de supervisión. En el contexto de esta evaluación, la ausencia de órdenes de retirada y de requerimientos dirigidos a un prestador de servicios de alojamiento de datos es una indicación de un bajo **riesgo o** nivel de exposición a los contenidos terroristas.

⁸ 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).

- (17) Al poner en marcha medidas proactivas, 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. 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.
- (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 exigir la presentación de informes sobre las medidas tomadas a los prestadores de servicios de alojamiento de datos que hayan recibido una orden 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 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 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 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 al prestador, 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).

- (19) Tras la solicitud, la autoridad competente debe entablar un diálogo con el prestador de servicios de alojamiento de datos sobre las medidas proactivas que deben adoptarse. En caso necesario, la autoridad competente debe imponer la adopción de medidas adecuadas, eficaces y proporcionadas cuando considere que las medidas adoptadas son insuficientes para atenuar los riesgos. La decisión de imponer 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.
- (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, **en «datos de transacciones» y en «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.

- (21) La obligación de conservar el contenido para procedimientos de revisión administrativa o judicial 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, las autoridades policiales pueden quedar sin conocimiento de la existencia de esos contenidos. 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, 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.
- (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. Sin embargo, este plazo puede prorrogarse el tiempo que sea necesario en caso de que se inicien procedimientos de revisión 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 para permitir a las autoridades policiales conservar las pruebas necesarias en relación con las investigaciones, garantizando el equilibrio con los derechos fundamentales afectados.
- (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. Los prestadores de servicios de alojamiento de datos, ***expuestos a contenidos terroristas***, deben 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, ***cuando ello no contravenga el propósito de las medidas adoptadas***.
- (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 información, ***efectuada a consecuencia de medidas adoptadas con arreglo a los términos y condiciones de los prestadores de servicios de alojamiento de datos***. 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. ***Además, los proveedores de contenidos cuyos contenidos hayan sido retirados en virtud de una orden de retirada deben tener derecho a la tutela judicial efectiva, de conformidad con lo dispuesto en el artículo 19 del TUE y en el artículo 47 de la Carta de los Derechos Fundamentales de la Unión Europea***.

- (26) **En términos más generales, 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 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.**
- (27) Con objeto de evitar duplicidades y posibles interferencias con las investigaciones, las autoridades competentes deben informarse mutuamente, coordinarse y cooperar entre sí, y cuando proceda con Europol, [...] **antes** de emitir órdenes de retirada o **cuando** envíen requerimientos a los prestadores de servicios de alojamiento de datos. A la hora de decidir la emisión de una orden de retirada, la autoridad competente debe tener debidamente en cuenta toda notificación de injerencia en una investigación («prevención de conflictos»). [...] **A la hora de decidir la emisión de una orden de retirada, la autoridad competente debe tener debidamente en cuenta toda notificación de injerencia en una investigación («prevención de conflictos»). Cuando una autoridad competente sea informada por la autoridad competente de otro Estado miembro de la emisión de una orden de retirada, no debe emitir una orden duplicada.** Al aplicar las disposiciones del presente Reglamento, Europol puede proporcionar apoyo en consonancia con su mandato actual y con el marco jurídico vigente.

- (28) Con vistas a garantizar una aplicación eficaz y suficientemente coherente de las medidas proactivas, 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 la determinación, la aplicación y el examen de las medidas proactivas específicas. Del mismo modo, es necesario ese tipo de cooperación en relación con la adopción de normas relativas a sanciones, incluidas las que regulen su aplicación y su cumplimiento. ***La Comisión debe facilitar esta coordinación y cooperación.***
- (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. A esos efectos, los Estados miembros deben garantizar unos canales y mecanismos de comunicación adecuados que permitan compartir la información pertinente a su debido tiempo.
- (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, ***se anima a*** los Estados miembros [...] a utilizar los instrumentos ***específicos*** 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 penal⁹.
- (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, **interno o externalizado**, que permita la presentación electrónica de órdenes de retirada y requerimientos y en los medios técnicos [...] o 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, **aquellos prestadores de servicios de alojamiento de datos expuestos a contenidos terroristas según evidencie la recepción de una orden de retirada** deben garantizar que el punto de contacto esté disponible de forma ininterrumpida. 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 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.
- (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. **No obstante, por motivos de aplicación efectiva, urgencia u orden público, cualquier Estado miembro debe tener jurisdicción sobre las órdenes de retirada y los requerimientos.**

⁹ COM(2018) 225 final.

- (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 ya existente, siempre que este pueda desempeñar las funciones que se establecen en el presente Reglamento.***
- (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. La exigencia de designar a las autoridades competentes no necesariamente implica la creación de nuevas autoridades, sino que pueden encomendarse las funciones a las que obliga el presente Reglamento a organismos ya existentes. El presente Reglamento requiere la designación de autoridades competentes para emitir órdenes de retirada y requerimientos, para supervisar las medidas proactivas y para imponer sanciones. Son los Estados miembros los que deciden a cuántas autoridades desean designar para ejercer esas funciones.

- (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, **que pueden ser de carácter administrativo o penal**, incluidas, cuando proceda, directrices para la imposición de multas. Deben imponerse sanciones particularmente rigurosas en los casos en que el prestador 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. 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 medidas proactivas adicionales con arreglo al artículo 6, apartado 4. **Al determinar el carácter de la infracción y decidir imponer sanciones, deben tenerse debidamente en cuenta los derechos fundamentales, como la libertad de expresión.** Al determinar si se deben imponer o no sanciones económicas, deben tenerse debidamente en cuenta los recursos económicos del prestador. Los Estados miembros deben garantizar que las sanciones no incentiven la retirada de contenidos que no sean terroristas.
- (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 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 legislación¹⁰. 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. ***Los Estados miembros pueden utilizar los informes de transparencia de los prestadores de servicios de alojamiento de datos y complementarlos, cuando sea necesario, con información más pormenorizada.*** 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.

¹⁰ DO L 123 de 12.5.2016, p. 1.

- (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. La evaluación debe basarse en los cinco criterios de eficiencia, eficacia, pertinencia, coherencia y valor añadido de la UE. Evaluará 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 e intereses de terceros que puedan resultar afectados, la que incluye una revisión de la exigencia de informar a los proveedores de contenidos.
- (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 con el fin de evitar el uso indebido de los servicios de alojamiento de datos para la difusión de contenidos terroristas en línea. En particular, establece:
 - a) normas sobre los deberes de diligencia que deben aplicar los prestadores de servicios de alojamiento de datos para evitar la difusión de contenidos terroristas a través de sus servicios y garantizar, cuando sea necesario, su retirada rápida;
 - 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 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.
2. El presente Reglamento será de aplicación a los prestadores de servicios de alojamiento de datos que ofrecen servicios en la Unión, independientemente de su lugar de establecimiento principal.
3. ***El presente Reglamento no tendrá por efecto modificar la obligación de respetar los derechos fundamentales y los principios jurídicos fundamentales consagrados en el artículo 6 del Tratado de la Unión Europea.***

Artículo 2

Definiciones

A los efectos del presente Reglamento, se entenderá por:

- (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 de la información almacenada;

- (2) «proveedor de contenidos»: un usuario que ha suministrado información que esté o haya estado almacenada, a petición suya, por un prestador de servicios de alojamiento de datos;
- (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, un establecimiento del prestador de servicios de alojamiento de datos en la Unión;

A falta de tal establecimiento, la evaluación de una conexión sustancial se basará en criterios objetivos específicos, tales como:

- a) ***un*** número de usuarios significativo en uno o más Estados miembros;
- b) ***o*** la orientación de actividades hacia uno o más Estados miembros.
- (4) «delitos de terrorismo»: ***uno de los actos intencionados enumerados*** [...] en el artículo 3, apartado 1, de la Directiva (UE) 2017/541;
- (5) «contenidos terroristas»: ***material susceptible de contribuir a la comisión de los actos intencionados, enumerados en el artículo 3, apartado 1, letras a) a i), de la Directiva 2017/541, pues:***
- a bis) amenaza de cometer un delito terrorista;***
- a) incitar a la comisión [...] de delitos de terrorismo o defenderlos, ***por ejemplo, [...] haciendo apología de actos terroristas***, provocando con ello un peligro de comisión de dichos actos;
- b) ***pedir a personas o a un grupo de personas que cometan o [...] contribuyan [...] a cometer delitos de terrorismo;***

- c) promover las actividades de un grupo terrorista, en particular *pidiendo a personas o a un grupo de personas que apoyen o participen las actividades delictivas de* [...] un grupo terrorista, en el sentido del artículo 2, apartado 3, de la Directiva (UE) 2017/541;

instruir sobre métodos o técnicas para la comisión de delitos de terrorismo;

- (6) «difusión de contenidos terroristas» la puesta a disposición de terceros de contenidos terroristas en los servicios de los prestadores de servicios de alojamiento de datos;
- (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;
- (9) «establecimiento principal» la sede central o el domicilio social en que se ejerzan las principales funciones financieras [y el control operativo] *en la Unión*.

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 de manera resuelta, proporcionada y no discriminatoria, con la debida consideración a los derechos fundamentales de los usuarios y teniendo en cuenta la importancia capital de la libertad de expresión y de información en una sociedad abierta y democrática.
2. Los prestadores de servicios de alojamiento de datos incluirán en sus términos y condiciones **que no almacenarán contenidos terroristas** y disposiciones para evitar la difusión de contenidos terroristas y las aplicarán.

Artículo 4

Órdenes de retirada

1. La autoridad competente estará facultada para emitir una [...] **orden de retirada** que exija al prestador de servicios de alojamiento de datos retirar contenidos terroristas o bloquear el acceso a ellos.
2. Los prestadores de servicios de alojamiento de datos retirarán los contenidos terroristas o bloquearán el acceso a ellos en el plazo de una hora desde la recepción de la orden de retirada.
3. Las órdenes de retirada contendrán los elementos siguientes de conformidad con la plantilla establecida en el anexo I:
 - a) la identificación de la autoridad competente que emite la orden de retirada y la autenticación de la orden de retirada por la autoridad competente; [...] **una evaluación de los contenidos**, al menos por referencia a las categorías **pertinentes** de contenidos terroristas enumeradas en el artículo 2, apartado 5;

- b) un localizador uniforme de recursos (URL) y, cuando sea necesario, información adicional que permita la identificación de los contenidos de que se trate;
 - c) una referencia al presente Reglamento como base jurídica de la orden de retirada;
 - d) la marca de fecha y hora de la emisión;
 - e) información sobre los recursos disponibles para el prestador de servicios de alojamiento de datos y el proveedor de contenidos;
 - f) cuando sea pertinente, 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.
4. A petición del prestador de servicios de alojamiento de datos o del proveedor de contenidos, la autoridad competente facilitará una motivación [...] **complementaria en la que se explique por qué los contenidos se consideran contenidos terroristas**, 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.
5. Las autoridades competentes dirigirán 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 transmitirán 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.
6. **Sin demora indebida**, [...] los prestadores de servicios de alojamiento de datos acusarán recibo e informarán [...] 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.

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, 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.
8. Si el prestador de servicios de alojamiento de datos no puede cumplir la orden de retirada por contener esta errores manifiestos o no contener 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.
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 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.

Artículo 4 bis

Procedimiento de consulta para órdenes de retirada

1. *La autoridad emisora remitirá una copia de la orden de retirada 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 lo transmita 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 emisora.*
3. *La autoridad emisora tendrá en cuenta dichas circunstancias y, cuando proceda, retirará o adaptará la orden de retirada.*

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 suficiente [...] **sobre** los motivos por los que los contenidos se consideran contenidos terroristas, **y facilitará** 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.
6. El prestador de servicios de alojamiento de datos informará, **sin demora indebida**, [...] 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.

Artículo 6
Medidas proactivas

1. Los proveedores de servicios de alojamiento de datos tomarán, [...] **en función del riesgo y del nivel de exposición a los contenidos terroristas**, medidas proactivas para proteger sus servicios frente a la difusión de contenidos terroristas. Las medidas serán eficaces y proporcionadas, teniendo en cuenta el riesgo y el nivel de exposición a contenidos terroristas, los derechos fundamentales de los usuarios y la importancia capital de la libertad de expresión y de información en una sociedad abierta y democrática.

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) [...] **abordar de modo eficaz la posibilidad de** que vuelvan a **aparecer** [...] 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.

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.
4. Cuando no pueda alcanzarse un acuerdo en el plazo de tres meses desde la solicitud a que se refiere el apartado 3, la autoridad competente a que se refiere el artículo 17, apartado 1, letra c), podrá emitir una decisión que imponga medidas proactivas adicionales específicas que sean necesarias y proporcionadas. La decisión tendrá en cuenta, en particular, 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 de información. ***La autoridad competente a que se refiere el artículo 17, apartado 1, letra c), tendrá discrecionalidad para decidir sobre la naturaleza y el ámbito de aplicación de las medidas proactivas, de conformidad con el objetivo del presente Reglamento.*** Dicha decisión 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).
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 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.

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 a tenor de los artículos 4, 5 y 6 y los datos conexos retirados como consecuencia de la retirada de los contenidos terroristas, [...] que sean necesarios para:
 - a) procedimientos de revisión administrativa o judicial;
 - b) la prevención, la detección, la investigación o el enjuiciamiento de delitos de terrorismo.
2. Los contenidos terroristas y los datos conexos a que se refiere el apartado 1 se conservarán durante seis meses. Los contenidos terroristas se conservarán, a solicitud de la autoridad o del órgano jurisdiccional competente, durante un plazo más largo cuando sea necesario para procedimientos de revisión administrativa o judicial, en el sentido del apartado 1, letra a), que se encuentren en curso.
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

1. Los prestadores de servicios de alojamiento de datos establecerán en sus términos y condiciones su política destinada a evitar la difusión de contenidos terroristas, incluida, cuando proceda, una explicación sustanciosa del funcionamiento de las medidas proactivas, entre ellas el uso de instrumentos automatizados.
2. Los prestadores de servicios de alojamiento de datos, [...] **expuestos a contenidos terroristas**, publicarán informes anuales de transparencia sobre las actuaciones llevadas a cabo contra la difusión de contenidos terroristas.
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;
 - b) información sobre las medidas del prestador de servicios de alojamiento de datos destinadas a **abordar de modo eficaz la posibilidad de** [...] que vuelvan a [...] **aparecer** contenidos que hayan sido retirados o cuyo acceso haya sido bloqueado previamente por considerarse que se trataba de contenidos terroristas;
 - c) número de elementos de contenido terrorista retirados o cuyo acceso haya sido bloqueado como consecuencia de órdenes de retirada, requerimientos o medidas proactivas, respectivamente;
 - d) resumen y resultados de los procedimientos de reclamación.

Artículo 9

Garantías en relación con el uso y la aplicación de medidas proactivas

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.

2. Dichas garantías consistirán, en particular, en la supervisión y verificaciones por personas, cuando proceda y, en cualquier caso, cuando se precise una evaluación detallada del contexto pertinente para determinar si los contenidos deben considerarse contenidos terroristas o no.

Artículo 10

Mecanismos de reclamación

1. Los prestadores de servicios de alojamiento de datos establecerán mecanismos eficaces y accesibles que permitan 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 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.
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.

Artículo 11

Información a los proveedores de contenidos

1. Cuando los prestadores de servicios de alojamiento de datos hayan retirado contenidos terroristas o bloqueado el acceso a ellos, pondrán a disposición del proveedor de contenidos información sobre la retirada de los contenidos terroristas o el bloqueo del acceso a ellos.
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.

3. La obligación fijada en los apartados 1 y 2 no será de aplicación cuando la autoridad competente decida 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 [...] **seis** semanas a partir de dicha decisión. ***Este periodo podrá prorrogarse por otras [...] seis semanas, en casos justificados.*** 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.

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.

Artículo 13

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

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 [...] **competentes**, 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.
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 para velar por que la información pertinente se comparta a su debido tiempo.

3. ***Para la aplicación efectiva del presente Reglamento así como para evitar la duplicación***, los Estados miembros y los prestadores de servicios de alojamiento de datos podrán elegir hacer uso de instrumentos específicos, incluidos [...] los establecidos por organismos de la Unión [...] ***competentes*** como Europol, para facilitar, en particular:
- 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;
 - c) la cooperación con vistas a la determinación y la aplicación de medidas proactivas de conformidad con el artículo 6.
4. Cuando los prestadores de servicios de alojamiento de datos tengan conocimiento de cualquier indicio de delitos de terrorismo informarán rápidamente a las autoridades competentes para investigar y enjuiciar las infracciones penales en el Estado miembro o Estados miembros [...] correspondientes [...]. ***Cuando sea imposible identificar al Estado miembro o Estados miembros correspondientes***, [...] los prestadores de servicios de alojamiento de datos [...] ***informarán, de conformidad con el artículo 14, apartado 2, al punto de contacto del Estado miembro en el que tengan su establecimiento principal o un representante legal, y transmitirán también*** esa información a Europol para que se le dé el curso adecuado.

Artículo 14

Puntos de contacto

1. Los prestadores de servicios de alojamiento de datos establecerán un punto de contacto que permita la recepción de órdenes de retirada y requerimientos por medios electrónicos y garantice su procesamiento rápido de conformidad con los artículos 4 y 5. Velarán por que esta información esté disponible al público.

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 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.
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.

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. ***Cualquier Estado miembro tendrá jurisdicción a los fines de los artículos 4 y 5, independientemente de dónde tenga el prestador de servicios su establecimiento principal o haya designado un representante legal.***
2. Cuando un prestador de servicios de alojamiento de datos no designe un representante legal, la jurisdicción corresponderá a todos los Estados miembros. ***Cuando un Estado miembro decida ejercer su jurisdicción informará de ello a todos los demás Estados miembros.***

[...] [...]

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, las solicitudes y las decisiones emitidos 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.
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, 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.
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 autoridad o autoridades competentes para:
 - a) emitir órdenes de retirada con arreglo al artículo 4;
 - 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;
 - c) supervisar la aplicación de las medidas proactivas con arreglo al artículo 6;
 - d) hacer cumplir las obligaciones que impone el presente Reglamento mediante sanciones con arreglo al artículo 18.

2. A más tardar [*doce*] meses después de la fecha de entrada en vigor del presente Reglamento], los Estados miembros notificarán a la Comisión *cuál es la autoridad o las autoridades competentes a que se refiere el apartado 1*. La Comisión publicará la notificación, y sus eventuales modificaciones, en el *Diario Oficial de la Unión Europea*.

Artículo 18

Sanciones

1. Los Estados miembros determinarán el régimen de sanciones aplicable a las infracciones 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:
 - a) el artículo 3, apartado 2 (términos y condiciones de los prestadores de servicios de alojamiento de datos);
 - b) el artículo 4, apartados 2 y 6 (aplicación de las órdenes de retirada e información sobre ellas);

- c) el artículo 5, apartados 5 y 6 (evaluación de los requerimientos e información sobre ellos);
 - d) el artículo 6, apartados 2 y 4 (informes sobre medidas proactivas y adopción de medidas tras una decisión que imponga medidas proactivas específicas);
 - e) el artículo 7 (conservación de datos);
 - f) el artículo 8 (transparencia);
 - g) el artículo 9 (garantías en relación con las medidas proactivas);
 - 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);
 - k) el artículo 14, apartado 1 (puntos de contacto);
 - l) el artículo 16 (designación de un representante legal).
2. Las sanciones que se impongan serán eficaces, proporcionadas y disuasorias. A más tardar *[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.
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 *o física* considerada responsable;

- d) la solidez financiera de la persona jurídica *o física* considerada responsable;
 - e) el nivel de cooperación del prestador de servicios de alojamiento de datos con las autoridades competentes.
4. Los Estados miembros garantizarán que el incumplimiento sistemático 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.

Artículo 19

Requisitos técnicos y modificaciones de las plantillas de órdenes de retirada

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 para los medios electrónicos que deben usar las autoridades competentes para la transmisión de las órdenes de retirada.
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 sobre la mejora de la legislación de 13 de abril de 2016.
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, 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 4 y 5;

- 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;
- 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 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. 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.

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 de [*doce* [...] meses después de su entrada en vigor].

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

Hecho en Bruselas, el

Por el Parlamento Europeo

El presidente

Por el Consejo

El presidente