Consejo de la Unión Europea

Bruselas, 14 de septiembre de 2018
(OR. en)

12129/18

Expediente interinstitucional: 2018/0331 (COD)

CT 144
ENFOPOL 450
COTER 114
JAI 881
CYBER 193
TELECOM 288
FREMP 142
AUDIO 64
DROIPEN 127
COHOM 107
CODEC 1468

PROPUESTA

De:	secretario general de la Comisión Europea, firmado por D. Jordi AYET PUIGARNAU, director
Fecha de recepción:	12 de septiembre de 2018
A:	D. Jeppe TRANHOLM-MIKKELSEN, secretario general del Consejo de la Unión Europea
N.° doc. Ción.:	COM(2018) 640 final
Asunto:	Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO para la prevención de la difusión de contenidos terroristas en línea *Contribución de la Comisión Europea a la reunión de los dirigentes de Salzburgo los días 19 y 20 de septiembre de 2018*

Adjunto se remite a las Delegaciones el documento – COM(2018) 640 final.

Adj.: COM(2018) 640 final

COMISIÓN
EUROPEA

Bruselas, 12.9.2018
COM(2018) 640 final

2018/0331 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

para la prevención de la difusión de contenidos terroristas en línea

Contribución de la Comisión Europea a la reunión de los dirigentes de Salzburgo los días 19 y 20 de septiembre de 2018

{SEC(2018) 397 final} - {SWD(2018) 408 final} - {SWD(2018) 409 final}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

1.1. Razones y objetivos de la propuesta

La ubicuidad de Internet permite a sus usuarios comunicarse, trabajar, socializar y crear, obtener y compartir información y contenidos con cientos de millones de personas en todo el mundo. Las plataformas de Internet generan beneficios importantes para el bienestar económico y social de los usuarios en la Unión y fuera de ella. No obstante, la capacidad de alcanzar a un público tan amplio a un mínimo coste también atrae a delincuentes que pretenden hacer un uso indebido de Internet con fines ilícitos. Los recientes ataques terroristas en el territorio de la UE han mostrado cómo los terroristas utilizan Internet de forma indebida para reclutar a seguidores y prepararlos, para planear y facilitar actividades terroristas, para glorificar sus atrocidades y para animar a otros a seguir ese ejemplo e insuflar el miedo en la opinión pública.

Los contenidos terroristas compartidos en línea con esos fines se difunden a través de prestadores de servicios de alojamiento de datos que permiten subir contenidos de terceros. Esos contenidos se han revelado como esenciales para la radicalización y para incentivar acciones por parte de los llamados «lobos solitarios», como las producidas en varios ataques terroristas recientes en Europa. Dichos contenidos no solo tienen repercusiones negativas importantes para las personas y la sociedad en general, sino que también reducen la confianza de los usuarios en Internet y menoscaban los modelos de negocio y la reputación de las empresas afectadas. Los terroristas no solo han hecho un uso indebido de grandes plataformas de redes sociales, sino también, de modo creciente, de prestadores de servicios de menor tamaño que ofrecen diferentes tipos de servicios de alojamiento de datos a escala mundial. Este uso indebido de Internet resalta la particular responsabilidad social que concierne a las plataformas de Internet en lo que respecta a la protección de sus usuarios frente a la exposición a contenidos terroristas y los graves riesgos de seguridad que esos contenidos entrañan para la sociedad en su conjunto.

Los prestadores de servicios de alojamiento de datos, en respuesta a los llamamientos de las autoridades públicas, han puesto en funcionamiento ciertas medidas para luchar contra los contenidos terroristas en sus servicios. Se han conseguido avances a través de marcos y asociaciones voluntarios, entre ellos el Foro de la UE sobre Internet, puesto en marcha en diciembre de 2015 como parte de la Agenda Europea de Seguridad. El Foro de la UE sobre Internet ha fomentado la cooperación voluntaria entre los Estados miembros y los prestadores de servicios de alojamiento de datos, así como medidas tendentes a reducir la accesibilidad de los contenidos terroristas en línea y a habilitar a la sociedad civil para aumentar el volumen de discursos alternativos eficaces en línea. Esta labor ha contribuido al aumento de la cooperación, la mejora de las respuestas que las empresas dan a los requerimientos provenientes de las autoridades nacionales y de la Unidad de Notificación de Contenidos de Internet de Europol, la toma de medidas proactivas de naturaleza voluntaria destinadas a mejorar la detección automática de contenidos terroristas, la mejora de la cooperación en el sector, incluido el desarrollo de la «base de datos de almohadillas» para evitar que se puedan subir contenidos terroristas conocidos a plataformas conexas, y la mejora de la transparencia de las iniciativas. Si bien la cooperación en el marco del Foro de la UE sobre Internet debe continuar en el futuro, los acuerdos voluntarios han mostrado sus limitaciones. En primer lugar, no todos los prestadores de servicios de alojamiento de datos afectados han participado en el Foro, y en segundo lugar, la escala y el ritmo de los avances entre los prestadores de

servicios de alojamiento de datos, considerados conjuntamente, no son suficientes para dar una respuesta adecuada a este problema.

Dadas estas limitaciones, es claramente necesaria una acción reforzada de la Unión Europea contra los contenidos terroristas en línea. El 1 de marzo de 2018, la Comisión adoptó una Recomendación sobre medidas para combatir eficazmente los contenidos ilícitos en línea, basada en la Comunicación de la Comisión de septiembre[1] y en la labor realizada en el marco del Foro de la UE sobre Internet. La Recomendación contiene un capítulo específicamente dedicado a determinar una serie de medidas para detener eficazmente tanto la subida a la red como el intercambio de propaganda terrorista en línea, como mejoras en el proceso de requerimiento, un plazo de una hora para dar respuesta a los requerimientos, una detección más proactiva, una retirada efectiva y unas garantías suficientes para evaluar los contenidos terroristas adecuadamente[2].

La necesidad de reforzar la actuación en relación con los contenidos terroristas en línea también se ha reflejado en llamamientos de los Estados miembros de la UE, algunos de los cuales ya han legislado al respecto o han anunciado su intención de hacerlo. Después de una serie de ataques terroristas en la UE, y ante la constatación de que los contenidos terroristas en línea siguen siendo fácilmente accesibles, el Consejo Europeo de 22 y 23 de junio de 2017 instó al sector a desarrollar «nuevas tecnologías y herramientas para mejorar la detección automática de contenidos y eliminar aquellos que inciten a perpetrar actos de terrorismo. Esto deberá completarse, en caso necesario, con las correspondientes medidas legislativas a escala de la UE». El Consejo Europeo de 28 de junio de 2018 acogió positivamente «la intención de la Comisión de presentar una propuesta legislativa para mejorar la detección y la retirada de contenidos que inciten al odio y a la comisión de actos terroristas». Además, el Parlamento Europeo, en su resolución sobre plataformas en línea y el mercado único digital de 15 de junio de 2017, instó a las plataformas correspondientes a «a que refuercen las medidas para luchar contra los contenidos ilegales y nocivos en línea» e hizo un llamamiento a la Comisión para que presentase propuestas que abordaran esas cuestiones.

La presente propuesta de la Comisión aborda esos problemas y da respuesta a los llamamientos de los Estados miembros y del Parlamento Europeo, buscando establecer un marco jurídico claro y armonizado que evite 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 único digital y, al mismo tiempo, velar por la confianza y la seguridad. El presente Reglamento pretende aportar claridad en lo relativo a la responsabilidad de los prestadores de servicios de alojamiento de datos en la toma de todas las medidas adecuadas, razonables y proporcionadas que sean necesarias para garantizar la seguridad de sus servicios y detectar y retirar de forma rápida y eficaz los contenidos terroristas en línea, teniendo en cuenta la importancia capital de la libertad de expresión y de información en una sociedad abierta y democrática. Asimismo, introduce una serie de garantías necesarias con objeto de velar por el pleno respeto de los derechos fundamentales, como la libertad de expresión y de información en una sociedad democrática, además de la posibilidad de acceder a recursos judiciales garantizada por el derecho a la tutela judicial efectiva consagrada en el artículo 19 del TUE y el artículo 47 de la Carta de los Derechos Fundamentales de la UE.

---

1 Comunicación sobre la lucha contra el contenido ilícito en línea [COM(2017) 555 final].

2 Recomendación de la Comisión, de 1 de marzo de 2018, sobre medidas para combatir eficazmente los contenidos ilícitos en línea [C(2018) 1177 final].

Mediante el establecimiento de una serie de deberes mínimos de diligencia para los prestadores de servicios de alojamiento de datos, incluidas algunas normas y obligaciones específicas, así como de obligaciones para los Estados miembros, la presente propuesta busca aumentar la eficacia de las medidas actuales en la detección, la identificación y la retirada de contenidos terroristas en línea sin restringir los derechos fundamentales, como la libertad de expresión y de información. Dicho marco jurídico armonizado facilitará la prestación de servicios en línea en el mercado único digital, garantizará unas condiciones equitativas para todos los prestadores de servicios de alojamiento de datos que prestan sus servicios en la Unión Europea y creará un marco jurídico sólido para la detección y la retirada de contenidos terroristas acompañado de garantías adecuadas de protección de los derechos fundamentales. En particular, las obligaciones de transparencia incrementarán la confianza entre los ciudadanos, en particular los usuarios de Internet, y mejorarán la responsabilidad y la transparencia en la actuación de las empresas, en particular con respecto a las autoridades públicas. La propuesta también establece obligaciones de puesta en marcha de mecanismos de reparación y reclamación que garanticen que los usuarios puedan impugnar la retirada de sus contenidos. Las obligaciones impuestas a los Estados miembros contribuirán a esos objetivos y mejorarán la capacidad de las autoridades pertinentes de tomar las medidas adecuadas contra los contenidos terroristas en línea y luchar contra la delincuencia. Cuando los prestadores de servicios de alojamiento de datos no cumplan lo dispuesto en el Reglamento, los Estados miembros podrán imponer sanciones.

1.2. Coherencia con las disposiciones vigentes de la UE en el ámbito político en cuestión

La presente propuesta es coherente con el acervo relacionado con el mercado único digital, en particular la Directiva sobre el comercio electrónico. En particular, las medidas tomadas por un prestador de servicios de alojamiento de datos en cumplimiento del presente Reglamento, incluidas las medidas proactivas, no deben suponer, por sí mismas, que ese prestador de servicios deje de beneficiarse de la exención de responsabilidad que le concede, si se cumplen ciertas condiciones, el artículo 14 de la Directiva sobre el comercio electrónico. La decisión de las autoridades nacionales de imponer medidas proactivas proporcionadas y específicas no debe, en principio, conllevar la imposición a los Estados miembros de una obligación general de supervisión en el sentido del artículo 15, apartado 1, de la Directiva 2000/31/CE. No obstante, dados los riesgos particularmente graves asociados a la difusión de contenidos terroristas, las decisiones basadas en el presente Reglamento pueden, de forma particular, suponer una excepción a ese principio en el marco de la UE. Antes de adoptar esas decisiones, la autoridad competente debe establecer un justo equilibrio entre las necesidades de seguridad pública y los intereses y derechos fundamentales afectados, en particular la libertad de expresión y de información, la libertad de empresa y la protección de datos de carácter personal y de la intimidad. Los deberes de diligencia de los prestadores de servicios de alojamiento de datos deben reflejar y respetar ese equilibrio, expresado en la Directiva sobre el comercio electrónico.

La propuesta es también coherente con la Directiva (UE) 2017/541 relativa a la lucha contra el terrorismo, cuyo fin es armonizar las normativas nacionales de tipificación de los delitos de terrorismo, y se ajusta a ella estrechamente. El artículo 21 de la Directiva relativa a la lucha contra el terrorismo exige que los Estados miembros tomen medidas que aseguren la retirada rápida de los contenidos en línea, limitada a aquellos que constituyan provocación pública y dejándoles libertad para elegir las medidas. El presente Reglamento, dada su naturaleza preventiva, no solo se refiere al material que incite al terrorismo sino también al material destinado a fines de reclutamiento o formación, lo que se corresponde con otros delitos relacionados con las actividades terroristas también cubiertos por la Directiva (UE) 2017/541.

El presente Reglamento impone directamente a los prestadores de servicios de alojamiento de datos deberes de diligencia en relación con la retirada de contenidos terroristas, y armoniza los procedimientos de órdenes de retirada con objeto de reducir la accesibilidad a los contenidos terroristas en línea.

El Reglamento complementa las normas que establece la futura Directiva de servicios de comunicación audiovisual, en la medida en que su ámbito de aplicación personal y material es más amplio. El Reglamento no solo abarca las plataformas de distribución de vídeos, sino todos los diferentes tipos de prestadores de servicios de alojamiento de datos. Además, no solo se refiere a vídeos sino también a imágenes y texto. Por otra parte, el presente Reglamento va más allá que la Directiva en términos de provisiones sustantivas, al armonizar las normas sobre las solicitudes de retirada de contenidos terroristas y las medidas proactivas.

La propuesta de Reglamento se basa en la Recomendación de la Comisión[3] sobre los contenidos ilícitos de marzo de 2018. La Recomendación sigue vigente, y todos aquellos que desempeñan un papel en la reducción de la accesibilidad de los contenidos ilícitos, incluidos los contenidos terroristas, deben seguir ajustando su labor a las medidas determinadas en la Recomendación.

1.3. Resumen de la propuesta de Reglamento

El ámbito de aplicación personal de la propuesta engloba a los prestadores de servicios de alojamiento de datos que ofrecen sus servicios dentro de la Unión, independientemente de su lugar de establecimiento o de su tamaño. La legislación propuesta introduce una serie de medidas destinadas a evitar el uso indebido de los servicios de alojamiento de datos para la difusión de los contenidos terroristas en línea, con el fin de garantizar el correcto funcionamiento del mercado único digital, al tiempo que se garantizan la confianza y la seguridad. La definición de contenidos terroristas ilícitos, que está en consonancia con la definición de delitos de terrorismo establecida en la Directiva (UE) 2017/541, es la de información utilizada para incitar a la comisión de delitos de terrorismo y hacer apología de dichos delitos, animando a contribuir a estos y facilitando instrucciones para cometerlos, así como promoviendo la participación en grupos terroristas.

Para garantizar la retirada de los contenidos terroristas ilícitos, el Reglamento introduce una orden de retirada que puede ser emitida como decisión administrativa o judicial por parte de una autoridad competente de un Estado miembro. En esos casos, el prestador de servicios de alojamiento de datos está obligado a retirar el contenido o bloquear el acceso a él en el plazo de una hora. Además, el Reglamento armoniza los requisitos mínimos para que los requerimientos enviados por las autoridades competentes de los Estados miembros y por los organismos de la Unión (como Europol) a los prestadores de servicios de alojamiento de datos sean evaluados conforme a sus respectivos términos y condiciones. Finalmente, el Reglamento exige que los proveedores de servicios de alojamiento de datos, cuando proceda, tomen medidas proactivas proporcionadas al nivel de riesgo y retiren el material terrorista de sus servicios, mediante la utilización de instrumentos de detección automatizada, entre otros medios.

Las medidas concebidas para reducir los contenidos terroristas en línea están acompañadas por una serie de garantías clave que buscan garantizar la plena protección de los derechos fundamentales. Como parte de las medidas de protección de los contenidos que no sean terroristas frente a una retirada errónea, la propuesta establece obligaciones de poner en

[3] Recomendación de la Comisión, de 1 de marzo de 2018, sobre medidas para combatir eficazmente los contenidos ilícitos en línea [C(2018) 1177 final].

marcha mecanismos de reparación y reclamación para garantizar que los usuarios puedan impugnar la retirada de sus contenidos. Además, el Reglamento introduce obligaciones en relación con la transparencia de las medidas tomadas contra los contenidos terroristas por los prestadores de servicios de alojamiento de datos, garantizando así la rendición de cuentas frente a los usuarios, los ciudadanos y las autoridades públicas.

El Reglamento también obliga a los Estados miembros a garantizar que sus autoridades competentes tengan la capacidad necesaria para intervenir contra los contenidos terroristas en línea. Además, los Estados miembros están obligados a informarse mutuamente y a cooperar entre sí, y pueden hacer uso de los canales establecidos por Europol para garantizar la coordinación en lo tocante a las órdenes de retirada y los requerimientos. El Reglamento también impone a los prestadores de servicios de alojamiento de datos las obligaciones de informar con mayor detalle sobre las medidas tomadas y de informar a las autoridades policiales cuando detecten contenidos que entrañen un riesgo para la vida o la seguridad. Finalmente, se obliga a los prestadores de servicios de alojamiento de datos a conservar los contenidos que retiren, lo cual sirve como garantía contra la retirada errónea y asegura que no se pierdan posibles pruebas a efectos de la prevención, la detección, la investigación y el enjuiciamiento de delitos de terrorismo.

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

2.1. Base jurídica

La base jurídica es el artículo 114 del Tratado de Funcionamiento de la Unión Europea, que permite la adopción de medidas que garanticen el funcionamiento del mercado interior.

El artículo 114 es la base jurídica adecuada para armonizar las condiciones en las que los prestadores de servicios de alojamiento de datos prestan dichos servicios a nivel internacional en el mercado único digital y para abordar las diferencias entre las disposiciones de los Estados miembros que, de otro modo, podrían obstaculizar el funcionamiento del mercado interior. Además, evita que surjan futuros obstáculos a la actividad económica derivados de posibles diferencias en el desarrollo de las normativas nacionales.

El artículo 114 del TFUE puede también servir para imponer obligaciones a los prestadores de servicios establecidos fuera del territorio de la UE cuando la prestación de sus servicios afecte al mercado interior, dado que ello es necesario para el objetivo perseguido en relación con el mercado interior.

2.2. Elección del instrumento

El artículo 114 del TFUE ofrece al legislador de la Unión la posibilidad de adoptar reglamentos y directivas.

Dado que la propuesta se refiere a obligaciones impuestas a prestadores de servicios que habitualmente ofrecen sus servicios en más de un Estado miembro, las divergencias en la aplicación de sus disposiciones podrían dificultar la prestación de servicios por parte de los prestadores que ejercen su actividad en múltiples Estados miembros. Un reglamento permite que la misma obligación sea impuesta de manera uniforme en toda la Unión, sea directamente aplicable, aporte claridad y una mayor seguridad jurídica y evite una transposición divergente en los Estados miembros. Por estas razones, se considera que un reglamento es la forma más apropiada para el presente instrumento.

2.3. Subsidiariedad

Teniendo en cuenta la dimensión transfronteriza de los problemas abordados, las medidas incluidas en la propuesta deben adoptarse a escala de la Unión con el fin de alcanzar los objetivos. Internet es, por su propia naturaleza, transfronterizo, y el contenido alojado en un Estado miembro es accesible, normalmente, desde cualquier otro Estado miembro.

Está surgiendo un marco fragmentario de normas nacionales destinadas a combatir los contenidos terroristas en línea, y los riesgos están aumentando. Esto impondría a las empresas la carga de tener que cumplir normativas divergentes y crearía condiciones desiguales para las empresas y resquicios en materia de seguridad.

La actuación de la UE, por tanto, refuerza la seguridad jurídica e incrementa la eficacia de las acciones de los prestadores de servicios de alojamiento de datos frente a los contenidos terroristas en línea. Esto debe permitir que más empresas, incluidas empresas establecidas fuera de la Unión Europea, tomen medidas, lo cual reforzaría la integridad del mercado único digital.

Con ello se justifica la necesidad de la actuación de la UE, como anunciaron las Conclusiones del Consejo Europeo de junio de 2018 que invitaban a la Comisión a presentar una propuesta legislativa en este ámbito.

2.4. Proporcionalidad

La propuesta establece normas destinadas a que los prestadores de servicios de alojamiento de datos apliquen medidas para retirar con celeridad los contenidos terroristas de sus servicios. Sus características principales limitan la propuesta a lo necesario para alcanzar sus objetivos.

La propuesta tiene en cuenta la carga que supone para los prestadores de servicios en línea y contiene garantías, incluida la protección de la libertad de expresión y de información y de otros derechos fundamentales. El plazo de una hora para la retirada solamente se aplica a las órdenes de retirada, para aquellos contenidos cuya ilicitud han determinado las autoridades competentes mediante una decisión que puede revisarse judicialmente. Para los requerimientos, existe la obligación de establecer medidas que faciliten una evaluación con celeridad de los contenidos terroristas, sin imponer, no obstante, la obligación de retirada ni plazos absolutos. La decisión final sigue siendo voluntaria para el prestador de servicios de alojamiento de datos. La carga de evaluar los contenidos que pesa sobre las empresas se alivia por el hecho de que las autoridades competentes de los Estados miembros y los organismos de la Unión facilitan explicaciones sobre las razones por las que los contenidos pueden considerarse contenidos terroristas. Los proveedores de servicios de alojamiento de datos pueden, cuando proceda, tomar medidas proactivas para proteger sus servicios frente a la difusión de contenidos terroristas. Las obligaciones específicas relacionadas con las medidas proactivas están limitadas a los prestadores de servicios de alojamiento de datos expuestos a contenidos terroristas, como evidencia la recepción de una orden de retirada que se ha convertido en definitiva, y deben estar proporcionadas al nivel de riesgo y a los recursos de la empresa. La conservación de los contenidos retirados y los datos conexos se limita al período de tiempo proporcionado a efectos de permitir procedimientos de revisión judicial o administrativa y de la prevención, la detección, la investigación y el enjuiciamiento de los delitos de terrorismo.

3. RESULTADOS DE LAS EVALUACIONES EX POST, DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

3.1. Consultas con las partes interesadas

En la preparación de la presente propuesta legislativa, la Comisión ha consultado a todas las partes interesadas pertinentes para entender sus puntos de vista y las posibles alternativas. La Comisión llevó a cabo una consulta pública abierta sobre medidas para mejorar la eficacia al hacer frente a los contenidos ilícitos, en la que recibió 8 961 respuestas, de las que 8 749 fueron de particulares, 172 de organizaciones, 10 de administraciones públicas y 30 de otras categorías. En paralelo, se realizó una encuesta del Eurobarómetro sobre los contenidos ilícitos en línea, con una muestra aleatoria de 33 500 residentes de la UE. La Comisión también consultó a las autoridades de los Estados miembros y a los proveedores de servicios de alojamiento de datos, durante mayo y junio de 2018, respecto de medidas específicas para combatir los contenidos terroristas en línea.

En líneas generales, la mayor parte de las partes interesadas expresaron que los contenidos terroristas en línea son un grave problema social que afecta a los usuarios de Internet y a los modelos de negocio de los prestadores de servicios de alojamiento de datos. Más generalmente, el 65 % de los participantes en la encuesta del Eurobarómetro[4] consideraron que Internet no es seguro para sus usuarios y el 90 % de los participantes consideraron importante limitar la propagación de los contenidos ilícitos en línea. Las consultas con los Estados miembros revelaron que, si bien los acuerdos voluntarios están produciendo resultados, muchos de ellos ven necesaria la imposición de obligaciones vinculantes en relación con los contenidos terroristas, percepción ya expresada en las Conclusiones del Consejo Europeo de junio de 2018. Aunque, en general, los prestadores de servicios de alojamiento de datos estaban a favor de una continuación de las medidas voluntarias, señalaron los posibles efectos negativos de la fragmentación normativa que estaba surgiendo en la Unión.

Muchas partes interesadas también destacaron la necesidad de garantizar que cualquier medida normativa para la retirada de contenidos, en particular las medidas proactivas y los plazos estrictos, se equilibrase con las garantías de los derechos fundamentales, principalmente la libertad de palabra. Las partes interesadas señalaron una serie de medidas necesarias relacionadas con la transparencia, la rendición de cuentas y la necesidad de una revisión por personas al utilizar instrumentos automatizados.

3.2. Evaluación de impacto

El Comité de Control Reglamentario emitió un dictamen favorable con reservas sobre la evaluación de impacto y presentó varias sugerencias de mejora[5]. A raíz de ese dictamen, se modificó la evaluación de impacto para abordar las principales observaciones del Comité, poniendo el foco específicamente sobre los contenidos terroristas, enfatizando al mismo tiempo las implicaciones sobre el funcionamiento del mercado único digital y analizando en mayor profundidad las repercusiones sobre los derechos fundamentales y el funcionamiento de las garantías propuestas en las opciones.

En caso de no tomarse medidas adicionales, es previsible que las acciones voluntarias del escenario de partida continuaran y tuvieran ciertas repercusiones en la reducción de los

[4] Eurobarómetro 469, Contenidos ilícitos en línea, junio de 2018.

[5] Enlace al dictamen del Comité de Control Reglamentario en RegDoc.

contenidos terroristas en línea. Sin embargo, es improbable que todos los prestadores de servicios de alojamiento de datos expuestos a esos contenidos tomaran medidas voluntarias, y es previsible que surgiera una mayor fragmentación jurídica que introdujera nuevas barreras a la prestación transfronteriza de servicios. Se estudiaron tres opciones principales además del escenario de partida, con niveles crecientes de eficacia en lo que se refiere a abordar los objetivos establecidos en la evaluación de impacto y la meta general de reducir los contenidos terroristas en línea.

El ámbito de aplicación de estas obligaciones en las tres opciones abarcaba a todos los prestadores de servicios de alojamiento de datos (ámbito de aplicación personal) establecidos en la UE y en terceros países, en la medida en que ofrezcan sus servicios en la Unión (ámbito de aplicación geográfico). Dada la naturaleza del problema y la necesidad de evitar el abuso de las plataformas más pequeñas, no se preveían exenciones para las pymes en ninguna de las opciones. Todas las opciones exigían que los prestadores de servicios de alojamiento de datos tengan un representante legal en la UE, incluidas las empresas establecidas fuera de ella, para garantizar el cumplimiento de las normas de la Unión. En todas las opciones, se preveía que los Estados miembros desarrollasen mecanismos sancionadores.

Todas las opciones incluían la creación de un nuevo sistema armonizado de órdenes legales de retirada en relación con los contenidos terroristas en línea, emitidas por las autoridades nacionales a los prestadores de servicios de alojamiento de datos, y la exigencia de retirar esos contenidos en el plazo de una hora. Estas órdenes no requerirían necesariamente una evaluación por parte de los prestadores de servicios de alojamiento de datos, y estarían sujetas a recurso judicial.

Las garantías son una característica común de las tres opciones, en particular los procedimientos de reclamación y unas vías de reparación eficaces, incluido el recurso judicial, así como otras disposiciones para evitar la retirada errónea de contenidos que no sean terroristas garantizando a la vez el respeto de los derechos fundamentales. Además, todas las opciones incluyen obligaciones de información en forma de transparencia pública y de presentación de informes a los Estados miembros y la Comisión, así como a las autoridades en caso de presunto delito. Por otra parte, se prevén obligaciones de cooperación entre autoridades nacionales, prestadores de servicios de alojamiento de datos y, cuando sea pertinente, Europol.

Las principales diferencias entre las tres opciones están relacionadas con el alcance de la definición de contenidos terroristas, el nivel de armonización de los requerimientos, el alcance de las medidas proactivas, las obligaciones de coordinación entre los Estados miembros y los requisitos de conservación de datos. La opción 1 limitaría el ámbito de aplicación material a los contenidos difundidos para incitar directamente a la comisión de un acto terrorista, siguiendo una definición restrictiva, mientras que las opciones 2 y 3 adoptarían un enfoque más amplio, que incluiría también el material relativo al reclutamiento y la formación. En cuanto a las medidas proactivas, en la opción 1 los prestadores de servicios de alojamiento de datos expuestos a contenidos terroristas tendrían que llevar a cabo una evaluación de riesgos, pero las medidas proactivas para evitar los riesgos seguirían siendo voluntarias. La opción 2 exigiría que los prestadores de servicios de alojamiento de datos prepararan un plan de acción, que podría incluir el uso de instrumentos automatizados para evitar que vuelvan a subirse contenidos ya retirados. La opción 3 incluye medidas proactivas más amplias, que exigen que los proveedores de servicios expuestos a contenidos terroristas también detecten material nuevo. En todas las opciones, los requisitos relativos a las medidas proactivas serían proporcionados al nivel de exposición a material terrorista, así como a la capacidad económica del prestador de servicios. En lo que respecta a los requerimientos, la opción 1 no

armonizaría el enfoque relativo a los requerimientos, mientras que la opción 2 lo haría solo para Europol y la opción 3 incluiría, adicionalmente, los requerimientos de los Estados miembros. En las opciones 2 y 3, los Estados miembros estarían obligados a informarse mutuamente, a coordinarse y a cooperar entre sí, y en la opción 3 también tendrían que garantizar que sus autoridades competentes tengan la capacidad de detectar y notificar contenidos terroristas. Finalmente, la opción 3 también incluye la exigencia de conservar los datos como garantía en casos de retirada errónea y como medio de facilitar las investigaciones penales.

En todas las opciones legislativas se prevé que las disposiciones legales vayan acompañadas por una serie de medidas de apoyo, en particular para facilitar la cooperación entre las autoridades nacionales y de estas con Europol, así como la cooperación con los prestadores de servicios de alojamiento de datos, y de apoyo en materia de investigación, desarrollo e innovación para el desarrollo y la adopción de soluciones tecnológicas. También podrían utilizarse instrumentos adicionales de apoyo y de concienciación para pymes tras la adopción del instrumento legal.

La evaluación de impacto concluyó que se exigen una serie de medidas para alcanzar el objetivo de la acción. La definición amplia de contenidos terroristas, que tiene en cuenta el material más nocivo, resultaría preferible a una definición restrictiva de contenidos (opción 1). Limitar las obligaciones proactivas a evitar que vuelvan a subirse contenidos terroristas (opción 2) tendría un menor impacto que establecer obligaciones relativas a la detección de nuevos contenidos terroristas (opción 3). Las disposiciones sobre requerimientos deben incluir los requerimientos tanto de Europol como de los Estados miembros (opción 3) y no estar limitadas únicamente a los requerimientos de Europol (opción 2), dado que los requerimientos de los Estados miembros son una importante contribución que forma parte del esfuerzo general de reducción de la accesibilidad a los contenidos terroristas en línea. Estas medidas tendrían que ser implementadas de forma complementaria a las medidas comunes a todas las opciones, incluidas unas garantías sólidas frente a la retirada errónea de contenidos.

3.3. Derechos fundamentales

La propaganda en línea de los terroristas busca incitar a las personas a llevar a cabo ataques terroristas, incluso facilitándoles instrucciones detalladas sobre la forma de infligir el máximo daño. Habitualmente, después de ese tipo de atrocidades se publica más propaganda, en la que se hace apología de esos actos y se anima a otros a seguir el ejemplo. El presente Reglamento contribuye a la protección de la seguridad pública mediante la reducción de la accesibilidad de los contenidos terroristas que promueven y fomentan la vulneración de los derechos fundamentales.

La propuesta podría afectar a una serie de derechos fundamentales:

(a) Derechos del proveedor de los contenidos: derecho a la libertad de expresión; derecho a la protección de los datos de carácter personal; derecho al respeto de la vida privada y familiar, principio de no discriminación y derecho a la tutela judicial efectiva.

(b) Derechos del prestador de servicios: derecho a la libertad de empresa; derecho a la tutela judicial efectiva.

(c) Derechos de los ciudadanos: derecho a la libertad de expresión y de información.

Teniendo en cuenta el acervo pertinente, se incluyen en la propuesta de Reglamento garantías adecuadas y sólidas para velar por la protección de los derechos de esas personas.

Un primer elemento en ese contexto es que el Reglamento establece una definición de contenidos terroristas en línea concordante con la definición de delitos de terrorismo de la Directiva (UE) 2017/541. La definición es aplicable en relación con las órdenes de retirada y los requerimientos, así como con las medidas proactivas. La definición también garantiza que solo se retiren los contenidos ilícitos que se correspondan con la definición a escala de la Unión de los delitos relacionados. Por otro lado, el Reglamento incluye deberes generales de diligencia para los prestadores de servicios de alojamiento de datos, que deben actuar 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 terroristas.

Más concretamente, el Reglamento se ha concebido para garantizar la proporcionalidad de las medidas tomadas con respecto a los derechos fundamentales. En lo que respecta a las órdenes de retirada, la evaluación de los contenidos (incluidos los controles legales, cuando sea necesario) por una autoridad competente justifica el plazo de retirada de una hora para esta medida. Además, las disposiciones del presente Reglamento relacionadas con los requerimientos se limitan a aquellos enviados por las autoridades competentes y los organismos de la Unión en los que se facilitan explicaciones sobre las razones por las que los contenidos pueden considerarse contenidos terroristas. Aunque la responsabilidad de retirar los contenidos señalados en un requerimiento sigue correspondiendo al prestador de servicios de alojamiento de datos, esta decisión se ve facilitada por la evaluación antes mencionada.

En lo que respecta a las medidas proactivas, la responsabilidad de detectar, evaluar y retirar contenidos sigue correspondiendo a los prestadores de servicios de alojamiento de datos, a los que se exige poner en funcionamiento garantías para velar por que los contenidos no se retiren erróneamente, incluso mediante una revisión por personas, en particular si se exige una mayor contextualización. Por otra parte, a diferencia de lo que sucede en el escenario de partida, en el que las empresas más afectadas crean instrumentos automatizados sin supervisión pública, tanto la concepción como la aplicación de las medidas estarían sujetas a la presentación de informes a los organismos competentes de los Estados miembros. Esta obligación reduce los riesgos de retiradas erróneas tanto para las empresas que crean nuevos instrumentos como para aquellos que ya los estén usando. Además, se exige a los prestadores de servicios de alojamiento de datos que faciliten a los proveedores de contenidos mecanismos de reclamación fáciles de usar para impugnar la decisión de retirar sus contenidos, y que publiquen informes de transparencia destinados al público en general.

Finalmente, para el caso de que cualesquiera contenidos o datos conexos fueran retirados erróneamente a pesar de estas garantías, se exige a los prestadores de servicios de alojamiento de datos que los conserven durante un período de seis meses para poder restablecerlos, de forma que se garantice la eficacia de los procedimientos de reclamación y revisión con vistas a proteger la libertad de expresión y de información. Al mismo tiempo, la conservación también es útil a efectos de hacer cumplir la ley. Los prestadores de servicios de alojamiento de datos tienen que poner en funcionamiento garantías técnicas y organizativas para velar por que los datos no se usen para otros fines.

Las medidas propuestas, en particular aquellas relativas a las órdenes de retirada, los requerimientos, las medidas proactivas y la conservación de datos, no solo deben proteger a los usuarios de Internet contra los contenidos terroristas, sino también contribuir a proteger el derecho a la vida de los ciudadanos mediante la reducción de la accesibilidad de los contenidos terroristas en línea.

4. REPERCUSIONES PRESUPUESTARIAS

La propuesta legislativa de Reglamento no tiene repercusiones en el presupuesto de la Unión.

5. OTROS ELEMENTOS

5.1. Planes de ejecución y modalidades de seguimiento, evaluación e información

La Comisión elaborará, en el plazo de [un año desde la fecha de aplicación del presente Reglamento] 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 medidas que deben adoptar la Comisión y los Estados miembros al recopilar y analizar los datos y otras pruebas necesarias con el fin de seguir los avances y evaluar el presente Reglamento.

En virtud del programa de seguimiento elaborado, en el plazo de dos años desde la entrada en vigor del presente Reglamento, la Comisión presentará un informe sobre su aplicación, que se fundamentará en los informes de transparencia publicados por las empresas y en la información facilitada por los Estados miembros. La Comisión llevará a cabo una evaluación cuando hayan transcurrido como mínimo cuatro años desde la fecha de entrada en vigor del Reglamento.

Teniendo en cuenta las conclusiones extraídas de la evaluación, incluida la posible persistencia de ciertas lagunas o vulnerabilidades, y los adelantos tecnológicos, la Comisión valorará la necesidad de ampliar el ámbito de aplicación del Reglamento. En caso necesario, la Comisión presentará propuestas para adaptar el presente Reglamento.

La Comisión apoyará la aplicación, el seguimiento y la evaluación del Reglamento mediante un grupo de expertos de la Comisión. El grupo también facilitará la cooperación entre los prestadores de servicios de alojamiento de datos, las autoridades policiales y Europol; fomentará los intercambios y las prácticas para detectar y retirar los contenidos terroristas, aportará conocimientos especializados sobre la evolución de los métodos de actuación de los terroristas en línea y proporcionará asesoramiento y directrices, cuando proceda, que faciliten la aplicación de las disposiciones.

La aplicación del presente Reglamento podría facilitarse mediante una serie de medidas de apoyo. Entre estas medidas podría estar el desarrollo de una plataforma dentro de Europol que asista en la coordinación de los requerimientos y las órdenes de retirada. Las investigaciones financiadas por la UE sobre la evolución de los métodos de actuación de los terroristas mejoran el conocimiento de todas las partes interesadas pertinentes y aumentan su concienciación. Además, Horizonte 2020 apoya la investigación con el objetivo de desarrollar nuevas tecnologías, incluida la prevención automatizada de la subida de contenidos terroristas. Por otra parte, la Comisión va a seguir estudiando cómo apoyar a las autoridades competentes y a los prestadores de servicios de alojamiento de datos en la aplicación del presente Reglamento a través de los instrumentos financieros de la UE.

5.2. Explicación detallada de las disposiciones específicas de la propuesta

El artículo 1 establece el objeto e indica que el Reglamento establece normas para evitar el uso indebido de los servicios de alojamiento de datos para la difusión de contenidos terroristas en línea, incluidos deberes de diligencia para los prestadores de servicios de alojamiento de datos y medidas que deben adoptar los Estados miembros. Asimismo, establece el ámbito de aplicación geográfico, que abarca a los prestadores de servicios de alojamiento de datos que ofrecen servicios en la Unión, independientemente de su lugar de establecimiento.

El artículo 2 recoge las definiciones de los términos utilizados en la propuesta. También establece una definición de contenidos terroristas a efectos preventivos, basada en la Directiva sobre la lucha contra el terrorismo, que incluye el material y la información que incite 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.

El artículo 3 enumera los deberes de diligencia que los prestadores de servicios de alojamiento de datos deben aplicar al actuar en consonancia con el presente Reglamento y, en particular, con el debido respeto de los derechos fundamentales afectados. Prevé la inclusión de disposiciones adecuadas en los términos y condiciones de los prestadores de servicios de alojamiento de datos para garantizar su aplicación.

El artículo 4 exige que los Estados miembros faculten a las autoridades competentes para emitir órdenes de retirada e impone a los prestadores de servicios de alojamiento de datos la exigencia de retirar los contenidos en el plazo de una hora desde la recepción de una orden de retirada. Asimismo, fija los elementos mínimos que deben contener las órdenes de retirada y los procedimientos que deben seguir los prestadores de servicios de alojamiento de datos para informar a la autoridad emisora y para comunicarle la imposibilidad de cumplir una orden o la necesidad de aclaraciones. También exige que la autoridad emisora informe a la autoridad que supervise las medidas proactivas del Estado miembro al que corresponda la jurisdicción del prestador de servicios de alojamiento de datos.

El artículo 5 establece la exigencia de que los prestadores de servicios de alojamiento de datos pongan en marcha medidas para evaluar con celeridad los contenidos a que se refiera un requerimiento de una autoridad competente de un Estado miembro o de un organismo de la Unión, sin imponer, no obstante, la exigencia de retirar los contenidos objeto del requerimiento ni fijar plazos concretos para actuar. Además, fija los elementos mínimos que deben contener los requerimientos y los procedimientos que deben seguir los prestadores de servicios de alojamiento de datos para informar a la autoridad emisora y para solicitar aclaraciones a la autoridad que haya emitido el requerimiento.

El artículo 6 exige que los prestadores de servicios de alojamiento de datos tomen medidas proactivas eficaces y proporcionadas cuando proceda. Establece un procedimiento que garantiza que ciertos prestadores de servicios de alojamiento de datos (concretamente, aquellos que hayan recibido una orden de retirada que se haya convertido en definitiva) tomen medidas proactivas adicionales, cuando sea necesario, para atenuar los riesgos en consonancia con la exposición a contenidos terroristas en sus servicios. El prestador de servicios de alojamiento de datos debe cooperar con la autoridad competente en lo que respecta a las medidas necesarias exigidas y, en caso de no poder alcanzarse un acuerdo, la autoridad puede

imponer la adopción de medidas al prestador de servicios. El artículo también fija un procedimiento para la revisión de la decisión de la autoridad.

El artículo 7 exige que los prestadores de servicios de alojamiento de datos conserven los contenidos retirados y los datos conexos durante seis meses a efectos tanto de los procedimientos de revisión como de investigación. Este plazo puede ampliarse para permitir que la revisión se complete. El artículo también exige que los prestadores de servicios pongan en marcha garantías para velar por que los contenidos retirados y los datos conexos no puedan ser objeto de acceso ni de procesamiento para otros fines.

El artículo 8 obliga a los prestadores de servicios de alojamiento de datos a explicar sus políticas en lo que se refiere a la lucha contra los contenidos terroristas y a publicar informes anuales de transparencia sobre las acciones emprendidas a ese respecto.

El artículo 9 fija garantías específicas en relación con el uso y la aplicación de medidas proactivas al utilizar instrumentos automatizados, para garantizar que las decisiones sean adecuadas y estén bien fundadas.

El artículo 10 exige a los prestadores de servicios de alojamiento de datos que apliquen mecanismos de reclamación contra las retiradas, los requerimientos y las medidas proactivas y que examinen rápidamente todas las reclamaciones.

El artículo 11 establece la obligación de que los prestadores de servicios de alojamiento de datos faciliten información sobre la retirada al proveedor de contenidos, salvo que la autoridad competente exija que no se divulgue esa información por razones de seguridad pública.

El artículo 12 exige a los Estados miembros que garanticen que las autoridades competentes tienen la capacidad y los recursos suficientes para cumplir las responsabilidades que les impone el presente Reglamento.

El artículo 13 exige que los Estados miembros cooperen entre sí y, cuando proceda, con Europol para evitar las duplicidades y la interferencia con las investigaciones. El artículo también permite la posibilidad de que los Estados miembros y los prestadores de servicios de alojamiento de datos hagan uso de instrumentos específicos, incluidos los de Europol, para procesar órdenes de retirada y requerimientos e informar sobre ellos y para cooperar en relación con medidas proactivas. Además, exige a los Estados miembros que cuenten con canales de comunicación adecuados para garantizar el intercambio oportuno de información en lo que se refiere a la aplicación y el cumplimiento de las disposiciones del presente Reglamento. El artículo también obliga a los prestadores de servicios de alojamiento de datos a informar a las autoridades pertinentes cuando tengan noticia de cualquier indicio de delito de terrorismo en el sentido del artículo 3 de la Directiva (UE) 2017/541 sobre la lucha contra el terrorismo.

El artículo 14 prevé la creación de puntos de contacto tanto por los prestadores de servicios de alojamiento de datos como por los Estados miembros, con el fin de facilitar la comunicación entre ellos, en particular en lo relativo a los requerimientos y las órdenes de retirada.

El artículo 15 establece la jurisdicción del Estado miembro a efectos de la supervisión de las medidas proactivas, la imposición de sanciones y las labores de seguimiento.

El artículo 16 exige que los prestadores de servicios de alojamiento de datos que no tengan un establecimiento en ningún Estado miembro, pero que ofrezcan servicios dentro de la Unión, designen un representante legal en la Unión.

El artículo 17 exige que los Estados miembros designen a las autoridades encargadas de la emisión de órdenes de retirada, de los requerimientos sobre contenidos terroristas, de la supervisión de la aplicación de las medidas proactivas y de hacer cumplir el Reglamento.

El artículo 18 establece que los Estados miembros deben fijar normas sobre sanciones por el incumplimiento y establece criterios que los Estados miembros deben tener en cuenta al determinar el tipo y el nivel de las sanciones. Dada la particular importancia de una retirada con celeridad de los contenidos terroristas señalados en una orden de retirada, deben establecerse normas específicas sobre sanciones económicas en caso de infracciones sistemáticas de esta exigencia.

El artículo 19 fija un procedimiento más rápido y más flexible para modificar las plantillas de las órdenes de retirada y los canales de envío autenticado mediante actos delegados.

El artículo 20 establece las condiciones en las que la Comisión tiene poderes para adoptar actos delegados que establezcan las modificaciones necesarias en las plantillas y los requisitos técnicos de las órdenes de retirada.

El artículo 21 obliga a los Estados miembros a recabar y comunicar información específica relacionada con la aplicación del Reglamento con el fin de asistir a la Comisión en el ejercicio de sus funciones de conformidad con el artículo 23. La Comisión elaborará un programa detallado para la supervisión de las realizaciones, los resultados y las repercusiones del Reglamento.

El artículo 22 establece que la Comisión debe presentar un informe sobre la aplicación del presente Reglamento dos años después de su entrada en vigor.

El artículo 23 establece que la Comisión debe presentar un informe sobre la evaluación del presente Reglamento cuando hayan transcurrido como mínimo tres años desde su entrada en vigor.

El artículo 24 dispone que la propuesta de Reglamento entre en vigor a los veinte días de su publicación en el Diario Oficial y que sea aplicable seis meses después de la fecha de su entrada en vigor. La proposición de ese plazo tiene en cuenta la necesidad de medidas de ejecución y, al mismo tiempo, reconoce la urgencia de la plena aplicación de las normas contenidas en la propuesta de Reglamento. El plazo de seis meses se ha fijado partiendo del supuesto de que las negociaciones se desarrollarán con rapidez.

2018/0331 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

para la prevención de la difusión de contenidos terroristas en línea

Contribución de la Comisión Europea a la reunión de los dirigentes de Salzburgo los días 19 y 20 de septiembre de 2018

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 Europeo[6],

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.

(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

[6] DO C [...] de [...], p. [...].

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 Comisión[7], 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.

(5) La aplicación del presente Reglamento no debe afectar a la aplicación del artículo 14 de la Directiva 2000/31/CE[8]. 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.

(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.

(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, que constituye uno de los pilares esenciales

[7] 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).

[8] 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).

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.

(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 Consejo[9]. Dada la necesidad de luchar contra la propaganda terrorista en línea más nociva, la definición debe incluir el material y la información que incite 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. 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 deben ser adecuadamente protegidos. Además, la expresión de puntos de vista radicales, polémicos o controvertidos en el debate público sobre cuestiones políticas sensibles no debe considerarse contenido terrorista.

(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, 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

[9] 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).

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, 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.

(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 Consejo[10]. 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[11] no puede, por esa única razón, considerarse como dirección u orientación de las actividades hacia un determinado territorio dentro de la Unión.

(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.

---

10 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).

11 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.° 2006/2004 y (UE) 2017/2394 y la Directiva 2009/22/CE (DO L 601 de 2.3.2018, p. 1).

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 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 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.

(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 Consejo[12].

(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[13].

---

12 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).

13 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

(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 nivel de exposición a los contenidos terroristas.

(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

---

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).

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, 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.

(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 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.

(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. 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.

(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 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 cuando emitan órdenes de retirada o envíen requerimientos 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.

(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.

(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, 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[14].

(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 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. 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*.

(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.

(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

[14] COM(2018) 225 final.

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, 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 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 legislación[15]. 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

[15] DO L 123 de 12.5.2016, p. 1.

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. 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.

(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.

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:

  (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;

(5) «contenidos terroristas» uno o más de los elementos de información siguientes:

  (a) los que inciten a la comisión de delitos de terrorismo o los defiendan, incluidos los que hagan apología de ellos, provocando con ello un peligro de comisión de dichos actos;

  (b) los que fomenten la contribución a delitos de terrorismo;

  (c) los que promuevan las actividades de un grupo terrorista, en particular fomentando la participación en un grupo terrorista o el apoyo al mismo, en el sentido del artículo 2, apartado 3, de la Directiva (UE) 2017/541;

  (d) los que instruyan 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 u el domicilio social en que se ejerzan las principales funciones financieras y el control operativo.

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 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 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 decisión 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;

   (b) una motivación que explique por qué los contenidos se consideran contenidos terroristas, al menos por referencia a las categorías de contenidos terroristas enumeradas en el artículo 2, apartado 5;

   (c) un localizador uniforme de recursos (URL) y, cuando sea necesario, información adicional que permita la identificación de los contenidos de que se trate;

   (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 para el prestador de servicios de alojamiento de datos y el proveedor de contenidos;

(g) 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 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.

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. 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.

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 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.

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.

Artículo 6
Medidas proactivas

1. Los proveedores de servicios de alojamiento de datos tomarán, cuando proceda, 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) 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.

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. 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 y 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 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 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;

   (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 [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.

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 pertinentes

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.

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. 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:

   (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 infracciones penales en el Estado miembro correspondiente o al punto de contacto del Estado miembro de conformidad con el artículo 14, 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, transmitir 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.

2. Cuando un prestador de servicios de alojamiento de datos no designe un representante legal, la jurisdicción corresponderá a todos los Estados miembros.

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.

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 [*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 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 [*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.

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.

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 del [seis 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	*Por el Consejo*
El Presidente	*El Presidente*