Diario Oficial de la Unión Europea

C 135

Edición en lengua española

Comunicaciones e informaciones

64.º año

16 de abril de 2021

Sumario

ES

([1]) Texto pertinente a efectos del EEE.

III

(Actos preparatorios)

CONSEJO

POSICIÓN (UE) n.º 6/2021 DEL CONSEJO EN PRIMERA LECTURA

con vistas a la adopción de un Reglamento del Parlamento Europeo y del Consejo sobre la lucha contra la difusión de contenidos terroristas en línea

Adoptada por el Consejo el 16 de marzo de 2021

(Texto pertinente a efectos del EEE)

(2021/C 135/01)

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 ([1]),

De conformidad con el procedimiento legislativo ordinario ([2]),

Considerando lo siguiente:

(1) El presente Reglamento tiene por objetivo garantizar el correcto funcionamiento del mercado único digital en una sociedad abierta y democrática, mediante la lucha contra el uso indebido de los servicios de alojamiento de datos con fines terroristas y contribuyendo a la seguridad pública en toda la Unión. El funcionamiento del mercado único digital debe mejorarse mediante el refuerzo de la seguridad jurídica para los prestadores de servicios de alojamiento de datos y la confianza de los usuarios en el entorno en línea así como el fortalecimiento de las garantías de la libertad de expresión, incluidas la libertad de recibir y comunicar información e ideas en una sociedad abierta y democrática y la libertad y el pluralismo de los medios de comunicación.

(2) Las medidas reguladoras para luchar contra la difusión de contenidos terroristas en línea deben complementarse con las estrategias de lucha contra el terrorismo de los Estados miembros, entre las que se incluyen el refuerzo de la alfabetización mediática y el pensamiento crítico, la elaboración de discursos alternativos contrarios y otras iniciativas para reducir la incidencia de los contenidos terroristas en línea y la vulnerabilidad ante dichos contenidos, así como la inversión en trabajo social, las iniciativas de desradicalización y la colaboración con las comunidades afectadas para prevenir de forma sostenible la radicalización en la sociedad.

(3) Hacer frente a los contenidos terroristas en línea, que forma parte de un problema más amplio de difusión de contenidos ilícitos en línea, requiere una combinación de medidas legislativas, no legislativas y voluntarias basadas en la colaboración entre autoridades y prestadores de servicios de alojamiento de datos, con pleno respeto de los derechos fundamentales.

([1]) DO C 110 de 22.3.2019, p. 67.

([2]) Posición del Parlamento Europeo de 17 de abril de 2019 (pendiente de publicación en el Diario Oficial) y posición del Consejo en primera lectura de 16 de marzo de 2021. Posición del Parlamento Europeo de … (pendiente de publicación en el Diario Oficial).

(4) Los prestadores de servicios de alojamiento de datos activos en línea 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 los servicios de los prestadores de servicios de alojamiento de datos para llevar a cabo actividades ilícitas en línea. Es particularmente preocupante el uso indebido de dichos servicios por parte de grupos terroristas y sus seguidores para difundir contenidos terroristas en línea, con el fin de propagar su mensaje, de radicalizar y reclutar seguidores y de facilitar y dirigir actividades terroristas.

(5) Aunque no se trate del único factor, la presencia de contenidos terroristas en línea ha demostrado ser un catalizador para la radicalización de individuos que puede conducir a la comisión de actos terroristas y, por tanto, tiene graves consecuencias negativas para los usuarios, los ciudadanos y la sociedad en general, así como para los prestadores de servicios en línea que alojan esos contenidos, dado que menoscaba la confianza de sus usuarios y daña sus modelos de negocio. En vista de su papel esencial y de los medios y capacidades tecnológicos asociados a los servicios que prestan, los prestadores de servicios de alojamiento de datos tienen la responsabilidad social particular de proteger sus servicios del uso indebido por parte de los terroristas y a ayudar a luchar contra la difusión de contenidos terroristas a través de sus servicios en línea, teniendo en cuenta la importancia fundamental de la libertad de expresión, incluida la libertad de recibir y comunicar información e ideas en una sociedad abierta y democrática.

(6) La labor a escala de la Unión destinada 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. Es necesario complementar dicha labor con un marco legislativo claro para seguir reduciendo la accesibilidad de los contenidos terroristas en línea y luchar adecuadamente contra un problema que evoluciona con rapidez. El marco legislativo pretende basarse en esfuerzos voluntarios, reforzados por la Recomendación (UE) 2018/334 de la Comisión ([3]), y responde a los llamamientos del Parlamento Europeo para reforzar las medidas de lucha contra los contenidos ilícitos y nocivos en línea conforme al marco horizontal establecido por la Directiva 2000/31/CE del Parlamento Europeo y del Consejo ([4]), y del Consejo Europeo para mejorar la detección y la retirada de los contenidos en línea que incitan a actos terroristas.

(7) El presente Reglamento no debe afectar a la aplicación de la Directiva 2000/31/CE. En particular, las medidas tomadas por un prestador de servicios de alojamiento de datos en cumplimiento del presente Reglamento, incluidas cualesquiera medidas específicas, no deben suponer, por sí mismas, que ese prestador de servicios de alojamiento de datos deje de beneficiarse de la exención de responsabilidad que le concede esa Directiva. Además, el presente Reglamento no afecta a los poderes de las autoridades y los órganos jurisdiccionales nacionales de establecer la responsabilidad de los prestadores de servicios de alojamiento de datos si no se cumplen las condiciones establecidas en dicha Directiva para la exención de responsabilidad

(8) En caso de conflicto entre el presente Reglamento y la Directiva 2010/13/UE ([5]) en relación con las disposiciones que regulan los servicios de comunicación audiovisual tal como se definen en el artículo 1, apartado 1, letra a), de dicha Directiva, debe prevalecer la Directiva 2010/13/UE. Esto debe dejar invariables las obligaciones derivadas del presente Reglamento, en particular respecto a los prestadores de servicios de plataformas de distribución de vídeos.

(9) El presente Reglamento debe establecer las normas para luchar contra el uso indebido de los servicios de alojamiento de datos para la difusión de contenidos terroristas en línea, con el fin de garantizar el correcto funcionamiento del mercado interior. Dichas normas deben respetar plenamente los derechos fundamentales protegidos en la Unión, en particular los garantizados por la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»).

([3]) 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).

([4]) 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).

([5]) Directiva 2010/13/UE del Parlamento Europeo y del Consejo, de 10 de marzo de 2010, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual) (DO L 95 de 15.4.2010, p. 1).

(10) El presente Reglamento tiene el propósito de contribuir a la protección de la seguridad pública estableciendo al mismo tiempo garantías adecuadas y sólidas para velar por la protección de los derechos fundamentales, incluido el derecho al respeto de la vida privada, a la protección de los datos de carácter personal; a la libertad de expresión, incluido el derecho a recibir y transmitir información; el derecho a la libertad de empresa y a la tutela judicial. Además, se prohíbe toda discriminación. Las autoridades competentes y los prestadores de servicios de alojamiento de datos deben adoptar solamente las 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, y a la libertad y el pluralismo de los medios de comunicación, que constituyen los pilares esenciales de una sociedad democrática y pluralista y que son valores en los que se fundamenta la Unión. Las medidas que afecten a la libertad de expresión y de información deben ser muy específicas, para luchar contra la difusión de contenidos terroristas en línea respetando, al mismo tiempo, el 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 en la distribución y recepción de hechos, opiniones e ideas, de conformidad con la ley. Las medidas efectivas en línea de lucha contra los contenidos terroristas en línea y la protección de la libertad de expresión y de información no son objetivos incompatibles, sino que son objetivos complementarios que se refuerzan mutuamente.

(11) Con el fin de aportar claridad sobre las acciones que tanto los prestadores de servicios en línea como las autoridades competentes deben emprender para luchar contra la difusión de contenidos terroristas en línea, el presente Reglamento debe establecer una definición de «contenidos terroristas» a efectos preventivos que esté en consonancia con las definiciones de delitos pertinentes de la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo ([6]). Dada la necesidad de luchar contra la propaganda terrorista en línea más nociva, dicha definición debe incluir el material que incite o induzca a otro a cometer delitos de terrorismo o a contribuir a su comisión, que induzca a otro a participar en las actividades de un grupo terrorista, o que haga apología de actividades terroristas, también mediante la difusión de material que describa un ataque terrorista. La definición debe incluir material que proporcione instrucciones sobre la fabricación o el uso de explosivos, armas de fuego u otras armas o sustancias nocivas o peligrosas, así como de sustancias químicas, biológicas, radiológicas y nucleares (QBRN), o sobre otros métodos específicos o técnicas, entre ellas la selección de objetivos, con el objeto de cometer o contribuir a cometer delitos de terrorismo. Dicho material incluye texto, imágenes, grabaciones de sonido y vídeos, así como transmisiones en directo de delitos de terrorismo que conllevan el riesgo de que se puedan cometer otros delitos similares. Al evaluar si el material constituye contenido terrorista 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 con respecto a la seguridad y la integridad de las personas. El hecho de que el material haya sido producido por una persona, grupo o entidad incluidos en la lista de la Unión de personas, grupos o entidades implicados en actos terroristas y sujetos a medidas restrictivas, le sea atribuible o se haya difundido en su nombre, debe constituir un factor importante en esa evaluación.

(12) El material difundido con fines educativos, periodísticos, artísticos o de investigación, o con fines de sensibilización contra actividades terroristas no debe considerarse contenido terrorista. Al determinar si el material proporcionado por un proveedor de contenidos constituye «contenidos terroristas» con arreglo al presente Reglamento, se debe tener en cuenta, concretamente, el derecho a la libertad de expresión y de información, incluida la libertad y el pluralismo de los medios de comunicación, y la libertad de las artes y las ciencias. Especialmente en los casos en que el proveedor de contenidos asuma una responsabilidad editorial, cualquier decisión relativa a la retirada de material difundido debe tener en cuenta las normas periodísticas, establecidas por la reglamentación de prensa o de los medios de comunicación, de conformidad con el Derecho de la Unión, incluida la Carta. Además, la expresión de puntos de vista radicales, polémicos o controvertidos en el debate público sobre cuestiones políticas sensibles no debe considerarse contenido terrorista.

(13) Con objeto de luchar de manera eficaz contra la difusión de contenidos terroristas en línea y de asegurar al mismo tiempo el respeto de la vida privada de las personas, el presente Reglamento debe ser aplicable a los prestadores de servicios de la sociedad de la información que almacenen y difundan entre el público información y material proporcionados por un usuario del servicio a petición de este, independientemente de que el almacenamiento y la difusión al público de tal información y material sea de naturaleza meramente técnica, automática y pasiva. El concepto de «almacenamiento» se debe entender como la conservación de datos en la memoria de un servidor físico o virtual. Por lo tanto, deben quedar fuera del ámbito de aplicación del presente Reglamento los prestadores de servicios de «mera transmisión» o «almacenamiento temporal», así como de otros servicios proporcionados en otros niveles de la infraestructura de internet, que no conllevan almacenamiento, como los registros y los registradores, los proveedores

([6]) 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).

de sistemas de nombres de dominio (DNS, por sus siglas en inglés *«domain name systems»*), los servicios de pago o los servicios de protección contra ataques de denegación de servicio distribuido (DDoS, por sus siglas en inglés *«distributed denial of service»*).

(14) El concepto de «difusión entre el público» debe suponer poner la información a disposición de un número potencialmente ilimitado de personas, a saber, facilitar el acceso a la información a los usuarios en general sin exigir intervención ulterior del proveedor de contenidos, independientemente de que dichas personas accedan realmente a dicha información. En consecuencia, cuando el acceso a la información exija un registro o una admisión a un grupo de usuarios, debe considerarse que existe difusión entre el público solo cuando el registro o la admisión de los usuarios que intenten acceder a la información se produzca de modo automático sin que un ser humano decida o seleccione a quién otorgar acceso. Los servicios de comunicaciones interpersonales, tal como se definen en el artículo 2, punto 5, de la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo ([7]), como el correo electrónico o los servicios de mensajería privada, deben quedar fuera del ámbito de aplicación del presente Reglamento. Se considerará que la información se almacena y difunde entre el público a los efectos del presente Reglamento tan solo cuando dichas actividades se lleven a cabo previa solicitud directa del proveedor de contenidos. Por consiguiente, los prestadores de servicios tales como de infraestructura en la nube, que se proporcionan previa solicitud de partes distintas de los proveedores de contenidos y solo benefician en modo indirecto a estos últimos, no deben entrar en el ámbito de aplicación del presente Reglamento. El presente Reglamento debe abarcar, por ejemplo, los proveedores de medios sociales, 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 dichos servicios se emplean para poner la información almacenada a disposición del público previa solicitud directa del proveedor de contenidos. Cuando un prestador de servicios de alojamiento de datos preste varios servicios, el presente Reglamento se debe aplicar solamente a aquellos servicios que entren dentro de su ámbito de aplicación.

(15) A menudo los contenidos terroristas se difunden entre el público a través de servicios suministrados por prestadores de servicios de alojamiento de datos establecidos en terceros países. Con objeto de proteger a los usuarios en la Unión y asegurar que se aplican los mismos requisitos a todos los prestadores de servicios de alojamiento de datos con actividad en el mercado único digital, el presente Reglamento debe aplicarse a todos los proveedores de los servicios pertinentes prestados en la Unión, independientemente de su país de establecimiento. Debe considerarse que un prestador de servicios de alojamiento de datos ofrece dichos servicios en la Unión si dicho prestador permite a las personas físicas o jurídicas que se encuentren en uno o más Estados miembros utilizar sus servicios y si tiene una conexión sustancial con dichos Estados miembros.

(16) Debe considerarse que existe una conexión sustancial con la Unión cuando el prestador de servicios de alojamiento de datos tiene un establecimiento en la Unión, cuando existe un número significativo de usuarios de sus servicios en uno o más Estados miembros, o cuando sus actividades se orientan hacia uno o más Estados miembros. La orientación de las actividades hacia uno o más Estados miembros debe determinarse en función de todas las circunstancias pertinentes, incluidos factores como el uso de una lengua o una moneda utilizada generalmente en el Estado miembro de que se trate, o la posibilidad de encargar bienes o servicios de ese Estado miembro. Dicha orientación 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 una lengua comúnmente utilizada en el Estado miembro de que se trate, o de una gestión de las relaciones con los clientes que incluya por ejemplo la prestación de servicios a los clientes en una lengua comúnmente utilizada en tal Estado miembro. También se presumirá que existe una conexión sustancial cuando el prestador de servicios dirija sus actividades hacia uno o más Estados miembros, como establece el artículo 17, apartado 1, letra c), del Reglamento (UE) n.º 1215/2012 del Parlamento Europeo y del Consejo ([8]). La mera accesibilidad del sitio web de un prestador de servicios de alojamiento de datos, de una dirección de correo electrónico u otros datos de contacto en uno o más Estados miembros no debe ser, por sí sola, una condición suficiente para constituir una conexión sustancial. Además, 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 ([9]) no debe, por esa única razón, constituir una conexión sustancial con la Unión.

([7]) Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas (versión refundida) (DO L 321 de 17.12.2018, p. 36).

([8]) 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).

([9]) Reglamento (UE) 2018/302 del Parlamento Europeo y del Consejo, de 28 de febrero de 2018, sobre medidas destinadas a impedir el bloqueo geográfico injustificado y otras formas de discriminación por razón de la nacionalidad, del lugar de residencia o del lugar de establecimiento de los clientes en el mercado interior y por el que se modifican los Reglamentos (CE) n.º 2006/2004 y (UE) 2017/2394 y la Directiva 2009/22/CE (DO L 60I de 2.3.2018, p. 1).

(17) Deben armonizarse el procedimiento y las obligaciones resultantes de las órdenes de retirada que exijan a los prestadores de servicios de alojamiento de datos retirar o bloquear el acceso a los contenidos terroristas, previa evaluación por las autoridades competentes. Dada la velocidad con la que se difunden los contenidos terroristas por los servicios en línea, se debe imponer a los prestadores de servicios en línea la obligación de garantizar que se retiren los contenidos terroristas a que se refiere la orden de retirada, o que se bloquee el acceso a ellos en todos los Estados miembros, en el plazo de una hora desde la recepción de la orden de retirada. Excepto en situaciones de emergencia debidamente justificadas, la autoridad competente debe proporcionar al prestador de servicios de alojamiento información sobre los procedimientos y los plazos aplicables con al menos doce horas de antelación a la emisión de la primera orden de retirada a ese prestador. Los casos de emergencia debidamente justificados se producen cuando la retirada de los contenidos o el bloqueo del acceso a los contenidos terroristas transcurrida más de una hora desde la recepción de la orden de retirada produciría un daño grave, como por ejemplo situaciones de amenaza inminente para la vida o para la integridad física de una persona o cuando dichos contenidos muestren acontecimientos en curso que produzcan daños continuados para la vida o para la integridad física de una persona. La autoridad competente debe determinar si constituyen casos de emergencia y justificar debidamente su decisión en la orden de retirada. El prestador de servicios de alojamiento de datos debe informar lo antes posible a la autoridad competente que dictó la orden en caso de que no pueda acatar la orden de retirada en el plazo de una hora desde su recepción por motivos de fuerza mayor o imposibilidad de hecho, incluidos los motivos técnicos u operativos justificados, y cumplirá la orden de retirada tan pronto como se haya resuelto la situación.

(18) La orden de retirada debe incluir una motivación calificando el material que tiene que ser retirado o el acceso que debe ser bloqueado en tanto que contenido terrorista y proporcionar información suficiente para localizar dicho contenido, facilitando una dirección exacta URL y, cuando proceda, cualquier otra información adicional, por ejemplo una captura de pantalla del contenido en cuestión. No obstante, la motivación debe permitir al prestador de servicios de alojamiento de datos y, en última instancia, al proveedor de contenidos, ejercer de forma efectiva su derecho a la tutela judicial. Los motivos aducidos no deben implicar la divulgación de información sensible que pudiera poner en riesgo las investigaciones en curso.

(19) Las autoridades competentes deben presentar la orden de retirada directamente al punto de contacto designado o establecido por el prestador de servicios de alojamiento de datos a los efectos del presente Reglamento por cualquier medio electrónico capaz de producir un registro escrito en unas condiciones que permitan al prestador de servicios de alojamiento de datos determinar la autenticidad de la orden, incluida la exactitud de su fecha y hora de envío y recepción, como correos electrónicos o plataformas seguros u otros canales seguros, incluidos aquellos dispuestos por el prestador de servicios de alojamiento de datos, de conformidad con el Derecho de la Unión sobre la protección de los datos de carácter personal. Tal requisito debe poder cumplirse, en particular, mediante el uso de servicios cualificados de entrega electrónica certificada, tal y como establece el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo ([10]). Cuando el prestador de servicios de alojamiento de datos tenga su establecimiento principal en un Estado miembro distinto de la autoridad competente que dictó la orden, o su representante legal resida o está establecido en él, se debe presentar simultáneamente a la autoridad competente de dicho Estado miembro una copia de la orden de retirada.

(20) Debe ser posible para la autoridad competente del Estado miembro en el que el prestador de servicios de alojamiento de datos tenga su establecimiento principal o en el que su representante legal resida o esté establecido, examinar la orden de retirada dictada por las autoridades competentes de otro Estado miembro para determinar si infringe grave o manifiestamente el presente Reglamento o los derechos fundamentales garantizados en la Carta. Tanto el proveedor de contenidos como el prestador de servicios de alojamiento de datos deben tener derecho a solicitar dicho examen por parte de la autoridad competente 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. Cuando se presente dicha solicitud, la autoridad competente debe adoptar una decisión sobre si la orden de retirada contiene o no tal infracción. Si la decisión constata tal infracción, la orden de retirada debe dejar de tener efectos jurídicos. El examen debe llevarse a cabo rápidamente para garantizar que los contenidos retirados o cuyo acceso ha sido bloqueado por error se restablezcan lo antes posible.

([10]) 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 el que se deroga la Directiva 1999/93/CE (DO L 257 de 28.8.2014, p. 73).

(21) Los prestadores de servicios de alojamiento de datos expuestos a contenidos terroristas deben incluir en sus términos y condiciones, en caso de que las tengan, disposiciones destinadas a luchar contra el uso indebido de sus servicios para la difusión entre el público de contenidos terroristas en línea. Deben aplicarlas de manera resuelta, transparente, proporcionada y no discriminatoria.

(22) Dadas la magnitud del problema y la rapidez necesaria para detectar y retirar eficazmente los contenidos terroristas, la adopción de medidas específicas eficaces y proporcionadas 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 expuestos a contenidos terroristas deben tomar medidas específicas, teniendo en cuenta los riesgos y el nivel de exposición a los contenidos terroristas, así como los efectos sobre los derechos de terceros, y el interés público a la información. Los prestadores de servicios de alojamiento de datos deben determinar qué medida específica adecuada, eficaz y proporcionada debe emplearse para identificar y retirar los contenidos terroristas. Las medidas específicas pueden incluir medidas o capacidades técnicas u operativas adecuadas, como personal o medios técnicos para identificar y retirar o desactivar con prontitud el acceso a los contenidos terroristas, mecanismos para que los usuarios denuncien o señalen los supuestos contenidos terroristas, u otras medidas que el prestador de servicios de alojamiento de datos considere adecuadas y eficaces para hacer frente a la disponibilidad de contenidos terroristas en sus servicios.

(23) Al tomar medidas específicas, los prestadores de servicios de alojamiento de datos deben garantizar que se respeta el derecho de los usuarios a la libertad de expresión y de información, así como la libertad y el pluralismo de los medios de comunicación protegidos por la Carta. 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, cuando proceda, incluidas la supervisión y las verificaciones por personas para evitar que cualquier decisión no intencionada o errónea dé lugar a la retirada o el bloqueo de acceso de contenidos que no sean terroristas.

(24) El prestador de servicios de alojamiento de datos debe presentar a la autoridad competente informes sobre las medidas específicas tomadas, con el fin de permitirle establecer 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 la capacidad necesaria para la supervisión y verificación por personas. En su examen de la eficacia y la proporcionalidad de las medidas, las autoridades competentes deben tener en cuenta parámetros adecuados, entre ellos el número de órdenes de retirada dirigidas al prestador de servicios de alojamiento de datos, el tamaño y capacidad económica del servicios de alojamiento de datos y los efectos de sus servicios en la difusión de contenidos terroristas, por ejemplo sobre la base del número de usuarios en la Unión, así como las garantías establecidas para hacer frente al uso indebido de sus servicios para la difusión de contenidos terroristas en línea.

(25) En el caso de que la autoridad competente considere que las medidas específicas tomadas son insuficientes para hacer frente a los riesgos, dicha autoridad debe poder exigir la adopción de medidas específicas adicionales adecuadas, eficaces y proporcionadas. La exigencia de aplicar dichas medidas específicas adicionales no debe conllevar una exigencia general de supervisión o de iniciar búsquedas activas de hechos en el sentido del artículo 15, apartado 1, de la Directiva 2000/31/CE ni una exigencia de utilizar instrumentos automatizados. No obstante, debe ser posible para los prestadores de servicios de alojamiento de datos utilizar instrumentos automatizados si lo consideran adecuado y necesario para hacer frente con eficacia al uso indebido de sus servicios para la difusión de contenidos terroristas.

(26) 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 plazo necesario. Es preciso ampliar la exigencia de conservación a los datos conexos en la medida en que, de no hacerse así, cualquiera de esos datos pudiera perderse como consecuencia de la retirada de los contenidos terroristas correspondiente. Los datos conexos pueden consistir en datos tales como datos de los abonados, en particular datos correspondientes a la identidad del proveedor de contenidos, o en datos de acceso, incluidos datos sobre la fecha y hora de uso por parte del proveedor de contenidos y 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.

(27) La obligación de conservar los contenidos para procedimientos de control administrativos o judiciales es necesaria y se justifica por la necesidad de garantizar la existencia de recursos eficaces para el proveedor de contenidos cuyo contenido en línea haya sido retirado o cuyo acceso haya sido bloqueado, así como para garantizar el restablecimiento de dichos contenidos, en función del resultado de dichos procedimientos. La obligación de conservar el material a efectos de investigación o enjuiciamiento es necesaria y se justifica por el valor que este material podría tener a efectos de interrumpir o evitar las actividades terroristas. Por tanto, la conservación de los contenidos terroristas retirados con fines de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo debe ser también considerada como justificada. Los contenidos terroristas y los datos conexos deben almacenarse únicamente durante el plazo necesario que permita a las autoridades policiales comprobar su

contenido y decidir si sería necesario para esos fines. Con fines de prevención, detección, investigación y enjuiciamiento de delitos terroristas, la conservación de datos exigida se debe limitar a los datos que puedan tener un vínculo con los delitos de terrorismo y que, por lo tanto, puedan ser de utilidad para el enjuiciamiento de los delitos de terrorismo o para evitar graves riesgos para la seguridad pública. Si los prestadores de servicios de alojamiento de datos retiran el material o bloquean el acceso a él, en particular a través de sus propias medidas específicas, deben informar sin demora a las autoridades competentes sobre los contenidos cuya información conlleve una amenaza inminente para la vida o a una sospecha de delito de terrorismo.

(28) 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 procedimiento de control administrativo o judicial y permitir el acceso de las autoridades policiales a los datos necesarios para la investigación y el enjuiciamiento de los delitos de terrorismo. Sin embargo, a petición de la autoridad o del órgano jurisdiccional competente, se debe poder prorrogar este plazo por el tiempo que sea necesario en caso de que se inicien dichos procedimientos y no se completen en el plazo de seis meses. La duración del plazo de conservación debe ser suficiente para permitir a las autoridades policiales conservar el material necesario en relación con las investigaciones y el enjuiciamiento, garantizando el equilibrio con los derechos fundamentales.

(29) El presente Reglamento no debe afectar 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, tal y como se regulan en el Derecho de la Unión o en el Derecho nacional.

(30) 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 que hayan adoptado medidas o a los que se les haya exigido la adopción de medidas con arreglo al presente Reglamento en un año natural determinado deben publicar informes anuales de transparencia que contengan información sobre la actuación relacionada con la identificación y retirada de contenidos terroristas.

(31) Las autoridades competentes deben publicar informes anuales de transparencia que incluyan información sobre el número de órdenes de retirada, el número de casos en que una orden no fue ejecutada y el número de decisiones relativas a medidas específicas, el número de asuntos sometidos a procedimientos de control administrativos o judiciales y el número de decisiones que impongan sanciones.

(32) El derecho a una tutela judicial efectiva está garantizado en el artículo 19 del Tratado de la Unión Europea (TUE) y en el artículo 47 de la Carta. 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 debe incluir, 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 o cualquier decisión que resulte del examen de las órdenes de retirada con arreglo al presente Reglamento ante un órgano jurisdiccional del Estado miembro cuya autoridad competente haya dictado la orden de retirada o haya tomado respectivamente la decisión así como la posibilidad de que los prestadores de servicios de alojamiento de datos impugnen una decisión relativa a sanciones o medidas específicas ante un órgano jurisdiccional del Estado miembro cuya autoridad competente tomó dicha decisión.

(33) Los procedimientos de reclamación constituyen una garantía necesaria contra la retirada o bloqueo de acceso erróneos de contenidos en línea cuando dichos contenidos están 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 un contenido cuando se haya retirado o cuyo acceso se haya bloqueado por error no debe afectar a la posibilidad que tiene el prestador de servicios de alojamiento de hacer cumplir sus términos y condiciones.

(34) La tutela judicial efectiva en virtud del artículo 19 del TUE y del artículo 47 de la Carta exige que los proveedores de contenidos puedan cerciorarse de los motivos por los que los contenidos que suministran 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 para impugnar la retirada o bloqueo. Dependiendo de las circunstancias, los prestadores de servicios de alojamiento de datos deben poder sustituir contenidos que han sido retirados o cuyo acceso ha sido bloqueado por un mensaje que indique que los contenidos han sido retirados o cuyo acceso ha sido bloqueado de conformidad con el presente Reglamento. Si así se solicita por los proveedores de contenidos, debe facilitarse información adicional sobre los motivos de la retirada o del bloqueo, así como los recursos para la retirada o bloqueo. Si las autoridades competentes deciden que, por razones de seguridad pública y en particular en el contexto de una investigación, es inadecuado o contraproducente notificar directamente al proveedor de contenidos la retirada o bloqueo, deben informar en consecuencia al prestador de servicios de alojamiento de datos.

(35) A efectos del presente Reglamento, los Estados miembros deben designar a las autoridades competentes. Ello no debe necesariamente implicar la creación de una nueva autoridad, y deben poder encomendarse las funciones establecidas en el presente Reglamento a un organismo ya existente. El presente Reglamento debe requerir la designación de autoridades competentes para dictar órdenes de retirada, examinar órdenes de retirada, supervisar medidas específicas e imponer sanciones, mientras que debe ser posible para todo Estado miembro decidir el número de autoridad competente que debe designarse y si son administrativa, policial o judicial. Los Estados miembros deben garantizar que las autoridades competentes desempeñen sus funciones de forma objetiva y no discriminatoria y no soliciten ni acepten instrucciones de ningún otro organismo en relación con el ejercicio de las funciones con arreglo al presente Reglamento. Esto no debe impedir su supervisión de conformidad con el Derecho constitucional nacional. Los Estados miembros deben comunicar las autoridades competentes designadas con arreglo al presente Reglamento a la Comisión, que debe publicar en línea un registro en el que figuren las autoridades competentes. Dicho registro en línea debe ser fácilmente accesible, a fin de facilitar la rápida verificación de la autenticidad de las órdenes de retirada por parte de los prestadores de servicios de alojamiento de datos.

(36) Con objeto de evitar la duplicación del trabajo y posibles interferencias con las investigaciones, y para minimizar la carga de los prestadores de servicios afectados, las autoridades competentes deben intercambiar información, coordinarse y cooperar entre sí y, cuando proceda, con Europol, antes de dictar órdenes de retirada. A la hora de decidir la emisión de una orden de retirada, la autoridad competente debe tener debidamente en cuenta toda notificación de injerencia en una investigación (prevención de conflictos). Cuando una autoridad competente sea informada por la autoridad competente de otro Estado miembro de una orden de retirada existente, no debe dictar una orden relativa al mismo asunto. Al aplicar las disposiciones del presente Reglamento, Europol puede proporcionar apoyo conforme a su mandato actual y al marco jurídico vigente.

(37) Con objeto de garantizar una aplicación eficaz y suficientemente coherente de las medidas específicas adoptadas por los prestadores de servicios de alojamiento de datos, las autoridades competentes deben coordinarse y cooperar entre sí en relación con las conversaciones que mantengan con los prestadores de servicios de alojamiento de datos en lo que se refiere a las órdenes de retirada y la determinación, la aplicación y el examen de las medidas específicas. Dicha coordinación y cooperación también son necesarias en relación con las demás medidas de aplicación del presente Reglamento, incluidas las relativas a la adopción de normas relativas a sanciones y a su imposición. La Comisión debe facilitar esta coordinación y cooperación.

(38) 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 de las conversaciones posteriores entre el prestador de servicios de alojamiento de datos y las autoridades competentes de otros Estados miembros. A esos efectos, los Estados miembros deben garantizar unos canales y mecanismos de comunicación adecuados y seguros que permitan compartir la información pertinente a su debido tiempo.

(39) Con el fin de facilitar los intercambios rápidos entre las autoridades competentes y entre estas y los prestadores de servicios de alojamiento de datos, y de impedir la duplicación del trabajo, se debe animar a los Estados miembros a utilizar los instrumentos específicos desarrollados por Europol, como la actual Aplicación de Gestión de los Requerimientos de Internet, o los que la han sucedido.

(40) Los requerimientos por parte de los Estados miembros y de Europol han demostrado ser un medio eficaz y rápido de aumentar la concienciación de los prestadores de servicios de alojamiento de datos respecto de contenidos específicos accesibles a través de sus servicios y de capacitarlos para actuar con rapidez. Estos requerimientos, que constituyen un 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 voluntariamente en consideración la compatibilidad de ese contenido con sus términos y condiciones, debe seguir estando disponible junto a las órdenes de retirada. La decisión final sobre la retirada o no de los contenidos por su incompatibilidad con sus términos y condiciones sigue correspondiendo al prestador de servicios de alojamiento de datos. El presente Reglamento no debe afectar al mandato de Europol establecido en el Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo ([11]). Por consiguiente, ninguna disposición del presente Reglamento debe interpretarse como impedimento para que los Estados miembros y Europol utilicen requerimientos como instrumento para hacer frente a los contenidos terroristas en línea.

(41) Dadas las consecuencias particularmente graves de determinados contenidos terroristas en línea, los prestadores de servicios de alojamiento de datos deben informar con celeridad a las autoridades oportunas del Estado miembro pertinente, o a las autoridades competentes del Estado miembro en que estén establecidos o tengan un representante legal, de los contenidos terroristas que impliquen una amenaza inminente para la vida o a una sospecha de delito de terrorismo. Para garantizar la proporcionalidad, esta obligación se debe limitar a los delitos de terrorismo definidos en el artículo 3, apartado 1 de la Directiva (UE) 2017/541. Dicha obligación de informar no debe implicar para los prestadores de servicios de alojamiento de datos una obligación de búsqueda activa de indicios de tal amenaza inminente para la vida o sospecha de delito de terrorismo. Se debe entender que el Estado miembro pertinente es el Estado miembro que tenga jurisdicción para investigar y enjuiciar los delitos de terrorismo, 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 deben remitir la información a Europol, que puede dar el oportuno curso al asunto con arreglo a su mandato, incluido el remitir dicha información a las autoridades nacionales correspondientes. Las autoridades competentes de los Estados miembros deben poder usar esa información para adoptar medidas de investigación disponibles con arreglo al Derecho de la Unión o del Estado miembro.

(42) Los prestadores de servicios de alojamiento de datosdeben designar o establecer puntos de contacto para facilitar el tratamiento rápido de las órdenes de retirada. El punto de contacto sólo debe servir para funciones operativas. El punto de contacto debe consistir en cualquier medio específico, interno o externalizado, que permita la presentación electrónica de órdenes de retirada, así como en los medios técnicos o personales que permitan el tratamiento rápido de estas. No es necesario que el punto de contacto esté situado en la Unión. El prestador de servicios de alojamiento de datos debe ser libre de utilizar un punto de contacto ya existente a efectos del presente Reglamento, siempre que el punto de contacto pueda desempeñar las funciones establecidas en el 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 puntos de contacto de los prestadores de servicios de alojamiento de datos expuestos a contenidos terroristas deben ser accesibles en cualquier momento. La información sobre el punto de contacto debe incluir información sobre la lengua en que se puede dirigir a él. 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 las instituciones de la Unión en la que se puedan consultar sus términos y condiciones.

(43) A falta de la exigencia general de que los prestadores de servicios de alojamiento de datos garanticen 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 su representante legal resida o esté establecido. Esto debe entenderse sin perjuicio de las normas de competencia establecidas a los efectos de las órdenes de retirada y las decisiones que resulten del examen de las órdenes de retirada con arreglo al presente Reglamento. 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 jurisdicción sobre ellos y en consecuencia, poder imponer sanciones, siempre que se respete el principio de *ne bis in idem*.

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

(44) Los 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 establecidas en el presente Reglamento. Debe ser posible para ellos recurrir a un representante legal ya designado a otros efectos, siempre que este pueda desempeñar las funciones previstas en el presente Reglamento. El representante legal debe tener la capacidad de actuar en representación del prestador de servicios de alojamiento de datos.

(45) Las sanciones son necesarias para garantizar el cumplimiento efectivo del presente Reglamento por los prestadores de servicios de alojamiento de datos. Los Estados miembros deben adoptar normas sobre sanciones, que pueden ser de carácter administrativo o penal, así como, cuando proceda, directrices para la imposición de multas. El incumplimiento en casos concretos puede ser sancionado, con respeto de los principios de *ne bis in idem* y de proporcionalidad, y con la garantía de que esas sanciones tienen en cuenta la inobservancia sistemática. Las sanciones pueden adoptar diferentes formas, entre ellas la de advertencia formal en caso de infracciones leves o la de sanción pecuniaria en relación con infracciones más graves o sistemáticas. Deben imponerse sanciones particularmente rigurosas en los casos en que el prestador de servicios de alojamiento de datos incumpla de forma sistemática o reiterada la obligación de retirada de los contenidos terroristas, o de bloqueo del acceso a ellos, en el plazo de una hora desde la recepción de una orden de retirada. Para garantizar la seguridad jurídica, el presente Reglamento debe establecer qué infracciones son sancionables y las circunstancias que son pertinentes para determinar el tipo y nivel de tales sanciones. Al determinar si se deben imponer o no sanciones económicas, deben tenerse debidamente en cuenta los recursos económicos del prestador de servicios de alojamiento de datos. Asimismo, la autoridad competente debe tener en cuenta si el prestador de servicios de alojamiento de datos es una empresa emergente o una micro empresa, pequeña o mediana empresa tal que definidas en la Recomendación 2003/361/CE de la Comisión ([12]). También se deben tener en cuenta otras circunstancias adicionales, por ejemplo, si la conducta del prestador de servicios de alojamiento de datos ha sido objetivamente imprudente o reprobable o si la infracción se ha cometido por negligencia o intencionadamente. Los Estados miembros deben garantizar que las sanciones impuestas por infracción del presente Reglamento no incentiven la retirada de material que no sea terrorista.

(46) El uso de plantillas normalizadas facilita la cooperación y el intercambio de información entre las autoridades competentes y los prestadores de servicios de alojamiento de datos, 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 mayor nivel de calidad del proceso. Del mismo modo, las plantillas de información deben permitir un intercambio de información normalizado, lo cual reviste especial importancia cuando los prestadores de servicios de alojamiento de datos no pueden cumplir las exigencias que les imponen una orden de retirada. Los canales de envío autenticado pueden garantizar la autenticidad de la orden de retirada, incluida la precisión de la fecha y la hora de envío y de recepción de la orden.

(47) A 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 los poderes para adoptar actos con arreglo al artículo 290 del Tratado de Funcionamiento de la Unión Europea, por lo que respecta a la modificación de los anexos 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 ([13]). En particular, a fin de garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo reciben toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus expertos tienen acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados.

(48) Los Estados miembros deben recabar información relativa a la aplicación del presente Reglamento. Los Estados miembros deben poder utilizar los informes de transparencia de los prestadores de servicios de alojamiento de datos y complementarlos, cuando sea necesario, con información más pormenorizada, como sus informes de transparencia propios en virtud del presente Reglamento. Debe elaborarse un programa detallado para el seguimiento de las realizaciones, los resultados y las repercusiones del presente Reglamento, con objeto de servir de base a una evaluación de la aplicación del presente Reglamento.

([12]) Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas (DO L 124 de 20.5.2003, p. 36).

([13]) DO L 123 de 12.5.2016, p. 1.

(49) Fundamentándose en los hallazgos y conclusiones del informe de aplicación y en el resultado de la actividad de seguimiento, la Comisión debe llevar a cabo una evaluación del presente Reglamento en el plazo de tres años a partir de la fecha de su entrada en vigor. La evaluación debe basarse en los criterios de eficiencia, necesidad, eficacia, proporcionalidad, pertinencia, coherencia y valor añadido de la Unión. Debe evaluar el funcionamiento de las diferentes medidas operativas y técnicas previstas en el presente Reglamento, incluidas la eficacia de las medidas de refuerzo de la detección, la identificación y la retirada de contenidos terroristas en línea, la eficacia de los mecanismos de salvaguardia y las repercusiones sobre los derechos fundamentales que puedan resultar afectados, como la libertad de expresión y de información, incluida la libertad y el pluralismo de los medios de comunicación, la libertad de empresa, el derecho a la vida privada y la protección de los datos de carácter personal. La Comisión debe también evaluar la repercusión sobre los intereses de terceros que puedan resultar afectados.

(50) Dado que el objetivo del presente Reglamento, a saber, garantizar el correcto funcionamiento del mercado único digital luchando contra la difusión de contenidos terroristas en línea, no puede ser alcanzado de manera suficiente por los Estados miembros, sino que, debido a las dimensiones y efectos de la acción, puede lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del TUE. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho 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 luchar contra el uso indebido de los servicios de alojamiento de datos para la difusión entre el público de contenidos terroristas en línea, en particular:

a) sobre los deberes razonables y proporcionados de diligencia que deben aplicar los prestadores de servicios de alojamiento de datos para luchar contra la difusión entre el público de contenidos terroristas a través de sus servicios y garantizar, cuando sea necesario, la retirada o el bloqueo de acceso rápidos a dichos contenidos;

b) las medidas que deben tomar los Estados miembros, de conformidad al Derecho de la Unión y a reserva de las salvaguardias adecuadas para proteger los derechos fundamentales, en particular la libertad de expresión e información en una sociedad abierta y democrática, con el fin de:

   i) detectar y permitir la retirada rápida de los contenidos terroristas por parte de los prestadores de servicios de alojamiento, y

   ii) facilitar la cooperación entre las autoridades competentes de los Estados miembros, los prestadores de servicios de alojamiento de datos y, cuando proceda, Europol.

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, en la medida en que difundan información entre el público.

3. No se considerará contenido terrorista el material difundido entre el público con fines educativos, periodísticos, artísticos o de investigación, o destinados a evitar el terrorismo o combatirlo, incluido el material que sea la expresión de opiniones polémicas o controvertidas en el transcurso del debate público. Una evaluación determinará la verdadera finalidad de dicha difusión y si el material se difunde entre el público para dichos fines.

4. El presente Reglamento no tendrá el efecto de modificar la obligación de respetar los derechos, libertades y principios a que se refiere el artículo 6 del TUE y se aplicará sin perjuicio de los principios fundamentales relativos a la libertad de expresión e información, incluidos la libertad y el pluralismo de los medios de comunicación.

5. El presente Reglamento se entiende sin perjuicio de las Directivas 2000/31/CE y 2010/13/CE. En lo que respecta a los servicios de comunicación audiovisual, tal como se definen en el artículo 1, apartado 1, letra a), de la Directiva 2010/13/UE, prevalecerá la Directiva 2010/13/UE.

Artículo 2

Definiciones

A los efectos del presente Reglamento, se entenderá por:

1) «prestador de servicios de alojamiento de datos»: un prestador de servicios a que se refiere el artículo 1, letra b), de la Directiva (UE) 2000/31/CE del Parlamento Europeo y del Consejo ([14]) consistentes en el almacenamiento de información facilitada por el proveedor de contenidos a petición de este;

2) «proveedor de contenidos»: un usuario que ha suministrado información que esté o haya estado almacenada y difundida entre el público por un prestador de servicios de alojamiento de datos;

3) «difusión entre el público»: la puesta a disposición de información, a petición de un proveedor de contenidos, a un número potencialmente ilimitado de personas;

4) «ofrecer servicios en la Unión»: permitir a las personas físicas o jurídicas de uno o más Estados miembros usar los servicios de un prestador de servicios de alojamiento de datos que tenga una conexión sustancial con ese Estado miembro o esos Estados miembros;

5) «conexión sustancial»: la conexión de un prestador de servicios de alojamiento de datos con uno o más Estados miembros debido a su establecimiento en la Unión, o por criterios objetivos específicos, tales como:

   a) tener un número de usuarios significativo en uno o más Estados miembros; o

   b) la orientación de sus actividades hacia uno o más Estados miembros.

6) «delitos de terrorismo»: los delitos definidos en el artículo 3 de la Directiva (UE) 2017/541;

7) «contenidos terroristas»: uno o más de los siguientes tipos de material, en particular material que:

   a) incite a la comisión de uno de los delitos a que se refiere el artículo 3, apartado 1, letras a) a i), de la Directiva (UE) 2017/541, cuando tal material preconice directa o indirectamente a través por ejemplo de la apología de actos terroristas, la comisión de delitos de terrorismo, generando con ello un riesgo de que se puedan cometer uno o varios de dichos delitos;

   b) induzca a una persona o grupo de personas a cometer o contribuir a la comisión de los delitos a que se refiere el artículo 3, apartado 1, letras a) a i), de la Directiva (UE) 2017/541;

   c) induzca a una persona o grupo de personas a participar en las actividades de un grupo terrorista en el sentido del artículo 4, letra b) de la Directiva (UE) 2017/541;

   d) proporcione instrucción sobre la fabricación o el uso de explosivos, armas de fuego u otras armas o sustancias nocivas o peligrosas, o sobre otros métodos o técnicas específicos cuyo fin sea la comisión o la contribución a la comisión de cualquiera de los delitos de terrorismo a que se refiere el artículo 3, apartado 1, letras a) a i), de la Directiva (UE) 2017/541;

   e) constituya una amenaza de comisión de los delitos a que se refiere el artículo 3, apartado 1, letras a) a i), de la Directiva (UE) 2017/541;

([14]) Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (DO L 241 de 17.9.2015, p. 1).

8) «términos y condiciones»: todos los términos, condiciones y cláusulas, independientemente de su nombre o forma, que rigen la relación contractual entre un prestador de servicios de alojamiento de datos y sus usuarios;

9) «establecimiento principal»: la sede central o el domicilio social del prestador de servicios de alojamiento de datos en que se ejercen las principales funciones financieras y el control operativo.

Sección II

Medidas para luchar contra la difusión de contenidos terroristas en línea

Artículo 3

Órdenes de retirada

1. La autoridad competente de todo Estado miembro estará facultada para dictar una orden de retirada por la que se exija a cualquier prestador de servicios de alojamiento de datos la retirada de los contenidos terroristas o el bloqueo del acceso a ellos en todos los Estados miembros.

2. Si una autoridad competente pertinente no ha dictado previamente una orden de retirada dirigida a un prestador de servicios de alojamiento de datos, facilitará a dicho prestador de servicios de alojamiento de datos información sobre los procedimientos y plazos aplicables al menos doce horas antes de dictar la orden de retirada.

El primer párrafo no será de aplicación en casos de emergencia debidamente justificados.

3. Los prestadores de servicios de alojamiento de datos retirarán los contenidos terroristas o bloquearán el acceso a ellos en todos los Estados miembros tan pronto como sea posible y, en cualquier caso, en el plazo de una hora desde la recepción de la orden de retirada.

4. Las autoridades competentes dictarán órdenes de retirada utilizando la plantilla establecida en el anexo I. Las órdenes de retirada contendrán los elementos siguientes:

a) detalles de la identificación de la autoridad competente que dicte la orden de retirada y la autenticación de la orden de retirada por esa autoridad competente;

b) una motivación suficientemente detallada que explique por qué los contenidos se consideran contenidos terroristas y una referencia a los tipos de material correspondientes a que se refiere el artículo 2, punto 7;

c) un localizador uniforme de recursos («URL», por sus siglas en inglés «uniform resource locator») exacto y, cuando sea necesario, información adicional que permita la identificación de los contenidos terroristas;

d) una referencia al presente Reglamento como base jurídica de la orden de retirada;

e) la marca de fecha y hora, así como la firma electrónica de la autoridad competente que dictó la orden de retirada;

f) información fácilmente comprensible sobre las vías de recurso disponibles para el prestador de servicios de alojamiento de datos y para el proveedor de contenidos, incluida sobre los recursos ante la autoridad competente y ante los órganos jurisdiccionales, así como sobre los correspondientes plazos de recurso;

g) cuando sea necesario y proporcionado, la decisión de no divulgar información sobre la retirada de contenidos terroristas, o el bloqueo del acceso a ellos, de conformidad con el artículo 11, apartado 3.

5. La autoridad competente dirigirá las órdenes de retirada al establecimiento principal del prestador de servicios de alojamiento de datos o a su representante legal designado de conformidad con el artículo 17.

Dicha autoridad competente transmitirá la orden de retirada al punto de contacto a que se refiere el artículo 15, apartado 1, 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 informarán sin demora indebida a la autoridad competente, mediante la plantilla establecida en el anexo II, de la retirada de los contenidos terroristas o del bloqueo del acceso a ellos en todos los Estados miembros, indicando en particular la hora de dicha retirada o bloqueo.

7. Si el prestador de servicios de alojamiento de datos no puede cumplir con la orden de retirada por causa de fuerza mayor o de imposibilidad de hecho no atribuible a él, incluidas razones técnicas u operativas objetivamente justificables, informará sin demora indebida a la autoridad competente que dictó la orden de retirada basada en dichos motivos, mediante la plantilla establecida en el anexo III.

El plazo indicado en el apartado 3 comenzará a correr desde el momento en que dejen de concurrir los motivos a que se refiere el primer párrafo del presente apartado.

8. Si el prestador de servicios de alojamiento de datos no puede cumplir la orden de retirada porque esta contiene errores manifiestos o no contiene información suficiente para su ejecución, informará sin demora indebida a la autoridad competente que dictó la orden de retirada y pedirá las aclaraciones necesarias mediante la plantilla establecida en el anexo III.

El plazo indicado en el apartado 3 comenzará a correr desde el momento en que el prestador de servicios de alojamiento reciba las aclaraciones necesarias.

9. La orden de retirada pasará a ser definitiva cuando expire el plazo de recurso si no se ha interpuesto ningún recurso de conformidad con el Derecho nacional o cuando se haya confirmado a raíz de un recurso.

Cuando la orden de retirada pase a ser definitiva, la autoridad competente que la haya dictado informará de tal hecho a la autoridad competente 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, a que se refiere el artículo 12, apartado 1, letra c).

Artículo 4

Procedimiento para las órdenes de retirada transfronterizas

1. A reserva de lo dispuesto en el artículo 3, cuando el prestador de servicios de alojamiento de datos no tenga su establecimiento principal o su representante legal en el Estado miembro de la autoridad competente que dictó la orden de retirada, dicha autoridad remitirá al mismo tiempo una copia de dicha orden de retirada a la autoridad competente 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.

2. Cuando un prestador de servicios de alojamiento de datos reciba una orden de retirada a tenor del presente artículo, adoptará las medidas requeridas en el artículo 3 así como las medidas necesarias para poder restablecer los contenidos en cuestión o reactivar el acceso a los mismos, de conformidad con el apartado 7 del presente artículo.

3. La autoridad competente del Estado miembro en el que el prestador de servicios de alojamiento de datos tenga su establecimiento principal o su representante legal resida o esté establecido podrá, en el plazo de 72 horas a partir de la recepción de la copia de la orden de retirada de conformidad con el apartado 1, examinar la orden de retirada para determinar si infringe o no gravemente o de forma manifiesta el presente Reglamento o los derechos y libertades fundamentales garantizados por la Carta

En caso de que considere que existe infracción, adoptará, en el mismo plazo, una decisión motivada a tal efecto.

4. Los prestadores de servicios de alojamiento de datos y los proveedores de contenidos tendrán derecho a presentar, en un plazo de 48 horas a partir, bien de la recepción de la orden de retirada, o de la información con arreglo al artículo 11, apartado 2, respectivamente, una solicitud motivada a la autoridad competente del Estado miembro en el que el prestador de servicios de alojamiento de datos tenga su establecimiento principal o su representante legal resida o esté establecido para examinar la orden de retirada a que se refiere el apartado 3, párrafo primero, del presente artículo.

En un plazo de 72 horas a partir de la recepción de la solicitud, la autoridad competente adoptará, tras el examen de la orden de retirada, una decisión motivada en la que exponga sus conclusiones sobre la existencia de una infracción.

5. Antes de adoptar una decisión en virtud del apartado 3, párrafo segundo, o una decisión que constate la existencia de una infracción en virtud del apartado 4, párrafo segundo, la autoridad competente informará a la autoridad competente que dictó la orden de retirada de su intención de adoptar la decisión y de los motivos de su decisión.

6. Cuando la autoridad competente del Estado miembro en el que el prestador de servicios de alojamiento de datos tenga su establecimiento principal o su representante legal resida o esté establecido adopte una decisión motivada de conformidad con los apartados 3 y 4 del presente artículo, comunicará sin demora dicha decisión a la autoridad competente que dictó la orden de retirada, al prestador de servicios de alojamiento de datos, al proveedor de contenidos que haya solicitado el examen de conformidad con el apartado 4 del presente artículo y, de conformidad con el artículo 14, a Europol. Si la decisión constata una infracción con arreglo al apartado 3 o 4 del presente artículo, la orden de retirada dejará de tener efectos jurídicos.

7. Tras recibir una decisión que constate una infracción comunicada de conformidad con el apartado 6, el prestador de servicios de alojamiento de datos de que se trate restablecerá inmediatamente los contenidos o el acceso a ellos, sin perjuicio de la posibilidad de hacer cumplir sus términos y condiciones de conformidad con el Derecho de la Unión y el Derecho nacional.

Artículo 5

Medidas específicas

1. Cuando corresponda, un prestador de servicios de alojamiento de datos expuestos a contenidos terroristas de los referidos en el apartado 4 incluirá en sus términos y condiciones disposiciones destinadas a luchar contra el uso indebido de sus servicios para la difusión de contenidos terroristas, y las aplicará.

Lo hará de manera diligente, proporcionada y no discriminatoria, con la debida consideración en toda circunstancia a los derechos fundamentales de los usuarios y teniendo en cuenta, en particular, la importancia capital de la libertad de expresión e información en una sociedad abierta y democrática, procurando evitar la retirada de contenidos que no sean terroristas.

2. Un prestador de servicios de alojamiento de datos expuesto a contenidos terroristas de los referidos en el apartado 4 tomará medidas específicas para proteger sus servicios contra la difusión entre el público de contenidos terroristas.

Corresponderá al prestador de servicios de alojamiento de datos la decisión sobre la elección de las medidas específicas. Dichas medidas podrán incluir una o varias de las siguientes:

a) medidas o capacidades técnicas y operativas adecuadas, tales como una dotación de personal o medios técnicos apropiados para identificar y retirar los contenidos terroristas o bloquear el acceso a ellos rápidamente;

b) mecanismos de fácil uso y acceso para que los usuarios informen o alerten al prestador de servicios de alojamiento de datos de presuntos contenidos terroristas;

c) cualquier otro mecanismo para aumentar la concienciación respecto de los contenidos terroristas en sus servicios, como los mecanismos de moderación de los usuarios;

d) cualquier otra medida que el prestador de servicios de alojamiento de datos considere apropiada para luchar contra la disponibilidad de contenidos terroristas en sus servicios.

3. Las medidas específicas cumplirán todos los requisitos siguientes:

a) serán eficaces para mitigar el nivel de exposición de los servicios del prestador de servicios de alojamiento de datos a los contenidos terroristas;

b) serán selectivas y proporcionadas, teniendo en cuenta, en particular, la gravedad del nivel de exposición de los servicios del prestador de servicios de alojamiento de datos a contenidos terroristas, así como las capacidades técnicas y operativas, la solidez financiera, el número de usuarios de los servicios del prestador de servicios de alojamiento de datos y el volumen de contenidos que facilitan;

c) se aplicarán teniendo plenamente en cuenta los derechos e intereses legítimos de los usuarios, en particular los derechos fundamentales de los usuarios relativos a la libertad de expresión e información, al respeto de la vida privada y a la protección de los datos de carácter personal;

d) se aplicarán de manera diligente y no discriminatoria.

Cuando las medidas específicas impliquen el recurso a medidas técnicas, se facilitarán garantías eficaces y adecuadas para velar por la precisión y evitar la supresión de material que no constituya contenidos terroristas, en particular mediante la supervisión y verificación humanas.

4. Un prestador de servicios de alojamiento de datos está expuesto a contenidos terroristas cuando la autoridad competente del Estado miembro de su establecimiento principal o en el que su representante legal resida o esté establecido haya

a) adoptado una decisión basada en factores objetivos, como que el prestador de servicios de alojamiento de datos haya recibido dos o más órdenes firmes de retirada en los doce meses anteriores, de que lo considera expuesto a contenidos terroristas, y

b) notificado al prestador de servicios de alojamiento de datos la decisión a que se refiere la letra a).

5. Tras recibir la decisión a que se refiere el apartado 4 o, en su caso, el apartado 6, el prestador de servicios de alojamiento de datos informará a la autoridad competente de las medidas específicas que haya adoptado y que tiene intención de adoptar para cumplir los apartados 2 y 3. Lo hará en un plazo de tres meses a partir de la recepción de la decisión y anualmente con posterioridad. Esta obligación cesará una vez que la autoridad competente decida, a raíz de una solicitud con arreglo al apartado 7, que el prestador de servicios de alojamiento de datos ha dejado de estar expuesto a contenidos terroristas.

6. Cuando, en función de los informes a que se refiere el apartado 5, y en su caso, cualesquiera otros factores objetivos, la autoridad competente considere que las medidas específicas no cumplen los apartados 2 y 3, transmitirá una decisión al prestador de servicios de alojamiento de datos en la que le exigirá que tome las medidas necesarias para garantizar que se cumplen los apartados 2 y 3.

El prestador de servicios de alojamiento de datos podrá elegir el tipo de medidas específicas a adoptar.

7. Todo prestador de servicios de alojamiento de datos podrá, en cualquier momento, solicitar a la autoridad competente la revisión y, cuando proceda, la modificación o la revocación de las decisiones a que se refieren los apartados 4 o 6.

En el plazo de tres meses a partir de la recepción de esa solicitud, la autoridad competente adoptará una decisión motivada sobre la solicitud basada en factores objetivos e informará de ella al prestador de servicios de alojamiento de datos.

8. Toda exigencia de adopción de medidas específicas se entenderá sin perjuicio de lo dispuesto en el artículo 15, apartado 1, de la Directiva 2000/31/CE y no conllevará una obligación general de los prestadores de servicios de alojamiento de datos de supervisar la información que transmitan o almacenen, ni una obligación general de buscar activamente hechos o circunstancias que indiquen una actividad ilegal.

Toda exigencia de adopción de medidas específicas no incluirá la obligación de que el prestador de servicios de alojamiento de datos utilice herramientas automatizadas.

Artículo 6

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 a los cuales se haya bloqueado el acceso como consecuencia de una orden de retirada o de medidas específicas en virtud de los artículos 3 o 5 así como cualesquiera datos conexos retirados como consecuencia de la retirada de dichos contenidos terroristas que sean necesarios para:

a) los procedimientos de control administrativos o judiciales o y la tramitación de denuncias en virtud del artículo 10 contra una decisión de retirada de los contenidos terroristas y los datos conexos o de bloqueo del acceso a ellos; o

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 a partir de la retirada a o el bloqueo. Los contenidos terroristas se conservarán, a solicitud de la autoridad o del órgano jurisdiccional competente, durante un periodo especificado adicional solo si es necesario, y solo durante el tiempo que sea necesario, para los procedimientos de control administrativos o judiciales contemplados en el 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 con arreglo al apartado 1 estén sujetos a garantías técnicas y organizativas adecuadas.

Estas garantías técnicas y organizativas asegurarán que el acceso a los contenidos terroristas y a los datos conexos conservados, así como el tratamiento de dichos contenidos y datos, solo se realicen para los fines a que se refiere el apartado 1, y asegurarán 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 7

Obligaciones de transparencia para los prestadores de servicios de alojamiento de datos

1. Los prestadores de servicios de alojamiento de datos establecerán claramente en sus términos y condiciones su política destinada a luchar contra la difusión de contenidos terroristas, incluida, en su caso, una explicación sustanciosa del funcionamiento de las medidas específicas, entre ellas, cuando proceda, el uso de herramientas automatizadas.

2. Un prestador de servicios de alojamiento de datos que haya adoptado medidas destinadas a luchar contra la difusión de contenidos terroristas o al que se haya exigido adoptar medidas a ese respecto en virtud del presente Reglamento en un año natural determinado publicará un informe de transparencia sobre las medidas de ese año. Publicará dicho informe antes del 1 de marzo del año siguiente.

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 identificación y retirada, o del bloqueo a su acceso, de contenidos terroristas;

b) información sobre las medidas del prestador de servicios de alojamiento de datos destinadas a luchar contra la reaparición en línea de material que haya sido retirado o al que se haya bloqueado el acceso previamente por considerarse que se trataba de contenidos terroristas, en particular cuando se hayan utilizado herramientas automatizadas;

c) número de elementos de contenido terrorista retirados o a los cuales se haya bloqueado el acceso como consecuencia de órdenes de retirada o medidas específicas, y número de órdenes de retirada en las que no se hayan retirado los contenidos o los accesos no hayan sido bloqueados en virtud del artículo 3, apartado 7, párrafo primero, y apartado 8, párrafo primero, junto con los motivos para ello;

d) número y resultado de las reclamaciones tramitadas por el prestador de servicios de alojamiento de datos de conformidad con el artículo 10,

e) número y resultado de los procedimientos de control administrativos o judiciales iniciados por el prestador de servicios de alojamiento de datos,

f) número de casos en los que se exigió al prestador de servicios de alojamiento de datos que restableciera los contenidos o el acceso a ellos como resultado de los procedimientos de control administrativos o judiciales,

g) número de casos en que el prestador de servicios de alojamiento de datos restableció los contenidos, o el acceso a ellos, a raíz de una reclamación por parte del proveedor de contenidos.

Artículo 8

Informes de transparencia de las autoridades competentes

1. Las autoridades competentes publicarán informes anuales de transparencia sobre las actividades realizadas con arreglo al presente Reglamento. Dichos informes incluirán como mínimo la siguiente información relativa al año natural correspondiente:

a) el número de órdenes de retirada dictadas en virtud del artículo 3, con indicación del número de órdenes de retirada a la que se aplica el artículo 4, apartado 1, el número de órdenes de retirada examinadas con arreglo al artículo 4, e información sobre la ejecución de dichas órdenes de retirada por los prestadores de servicios de alojamiento de datos afectados, incluido el número de casos en los que se retiraron contenidos terroristas o se bloqueó el acceso a ellos y el número de casos en que dichos contenidos no fueron retirados ni el acceso a ellos bloqueado;

b) el número de decisiones tomadas de conformidad con el artículo 5, apartados 4, 6 o 7, y la información sobre la ejecución de dichas decisiones por los prestadores de servicios de alojamiento de datos, con una descripción de las medidas específicas;

c) el número de casos en los que las órdenes de retirada y las decisiones adoptadas de conformidad con el artículo 5, apartados 4 y 6, estuvieran sujetas a procedimientos de control administrativos o judiciales e información sobre el resultado de los procedimientos correspondientes;

d) el número de decisiones por las que se impusieron sanciones en virtud del artículo 18, y una descripción del tipo de sanción aplicada.

2. Los informes de transparencia anuales a que se refiere el apartado 1 no incluirán información que pueda causar perjuicio a las actividades en curso en materia de prevención, detección, investigación o enjuiciamiento de delitos de terrorismo o a los intereses de la seguridad nacional.

Artículo 9

Tutela judicial

1. Los prestadores de servicios de alojamiento de datos que hayan recibido una orden de retirada dictada en virtud del artículo 3, apartado 1, o una decisión adoptada en virtud del artículo 4, apartado 4, o del artículo 5, apartados 4, 6 o 7, tendrán derecho a una tutela judicial efectiva. Dicho derecho incluirá el de impugnar dicha orden de retirada ante los órganos jurisdiccionales del Estado miembro de la autoridad competente que dictó la orden de retirada y el de impugnar la decisión adoptada con arreglo al artículo 4, apartado 4, o al artículo 5, apartados 4, 6 o 7, ante los órganos jurisdiccionales del Estado miembro de la autoridad competente que adoptó la decisión.

2. Los proveedores de contenidos cuyos contenidos hayan sido retirados o a los cuales se haya bloqueado el acceso como consecuencia de una orden de retirada tendrán derecho a una tutela judicial efectiva. Dicho derecho incluirá el de impugnar la orden de retirada dictada en virtud del artículo 3, apartado 1, ante los órganos jurisdiccionales del Estado miembro de la autoridad competente que dictó dicha orden de retirada y el de impugnar la decisión adoptada con arreglo al artículo 4, apartado 4, ante los órganos jurisdiccionales del Estado miembro de la autoridad competente que adoptó la decisión.

3. Los Estados miembros establecerán procedimientos efectivos para ejercer los derechos a que se refiere el presente artículo.

Artículo 10

Mecanismos de reclamación

1. Los prestadores de servicios de alojamiento de datos establecerán un mecanismo eficaz y accesible que permita a los proveedores de contenidos cuyos contenidos hayan sido retirados o a los cuales se haya bloqueado el acceso como consecuencia de medidas específicas con arreglo al artículo 5 presentar una reclamación relativa a la retirada o al bloqueo, en la que se solicite el restablecimiento de los contenidos o el acceso a ellos.

2. Los prestadores de servicios de alojamiento de datos deben examinar rápidamente todas las reclamaciones que reciban mediante el mecanismo a que se refiere el apartado 1 y restablecer los contenidos o el acceso a ellos sin demora indebida cuando la retirada o el bloqueo del acceso no estuviese justificado. Informarán al reclamante sobre el resultado de la reclamación en el plazo de dos semanas desde su recepción.

En caso de desestimación de la reclamación, los prestadores de servicios de alojamiento de datos proporcionarán una explicación de los motivos de su decisión al reclamante.

El restablecimiento de los contenidos, o del acceso a ellos, no impedirá la iniciación de procedimientos de control administrativos o judiciales para impugnar la decisión del prestador de servicios de alojamiento de datos o de la autoridad competente.

Artículo 11

Información a los proveedores de contenidos

1. Cuando un prestador de servicios de alojamiento de datos haya retirado contenidos terroristas o bloqueado el acceso a ellos, pondrá a disposición del proveedor de contenidos información sobre la retirada el bloqueo.

2. A petición del proveedor de contenidos, el prestador de servicios de alojamiento de datos informará al proveedor de contenidos de los motivos de la retirada o del bloqueo y de su derecho a recurrir la orden de retirada, o proporcionará al proveedor de contenidos una copia de la orden de retirada.

3. La obligación contemplada en los apartados 1 y 2 no será de aplicación cuando la autoridad competente que dicte la orden de retirada decida que es necesario y proporcionado que no se divulgue esa información por razones de seguridad pública, como la prevención, la investigación, la detección y el enjuiciamiento de los delitos de terrorismo, durante el tiempo necesario, sin que exceda las seis semanas a partir de dicha decisión. En esos casos, el prestador de servicios de alojamiento de datos no divulgará información alguna acerca de la retirada de contenidos terroristas o del bloqueo del acceso a ellos.

La autoridad competente podrá prorrogar este periodo por otras seis semanas, cuando dicha no divulgación siga estando justificada.

Sección IV

Autoridades competentes y cooperación

Artículo 12

Designación de las autoridades competentes

1. Cada Estado miembro designará la autoridad o autoridades competentes para:

a) dictar órdenes de retirada de conformidad al artículo 3;

b) examinar las órdenes de retirada de conformidad con el artículo 4;

c) supervisar la aplicación de las medidas específicas de conformidad al artículo 5;

d) imponer sanciones de conformidad al artículo 18.

2. Cada Estado miembro garantizará que se designe o establezca un punto de contacto en el seno de las autoridades competentes a que se refiere el apartado 1, letra a), para tramitar las solicitudes de aclaraciones e información en relación con las órdenes de retirada que haya dictado dicha autoridad competente.

Los Estados miembros velarán por que la información sobre el punto de contacto esté disponible para el público.

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

4. A más tardar el … [*doce meses después de la fecha de entrada en vigor del presente Reglamento*] la Comisión creará un registro en línea en el que figurarán las autoridades competentes a que se refiere el apartado 1 así como el punto de contacto designado o establecido con arreglo al apartado 2 para cada una de ellas. La Comisión publicará con regularidad sus eventuales modificaciones.

Artículo 13

Autoridades competentes

1. Los Estados miembros garantizarán que sus autoridades competentes tengan las facultades necesarias y los recursos suficientes para alcanzar los objetivos y cumplir las obligaciones que se derivan del presente Reglamento.

2. Los Estados miembros garantizarán que sus autoridades competentes lleven a cabo sus funciones en virtud del presente Reglamento de forma objetiva y no discriminatoria, al tiempo que respetan plenamente los derechos fundamentales. Las autoridades competentes no solicitarán ni aceptarán instrucciones de ningún otro organismo en relación con la ejecución de sus funciones en virtud del artículo 12, apartado 1.

El párrafo primero del apartado 1 no impedirá su supervisión de conformidad con el Derecho constitucional nacional.

Artículo 14

Cooperación entre los prestadores de servicios de alojamiento de datos, las autoridades competentes y Europol

1. Las autoridades competentes intercambiarán información, se coordinarán y cooperarán entre sí y, cuando proceda, con Europol, en relación con las órdenes de retirada, en particular para evitar la duplicación del trabajo, mejorar la coordinación y evitar interferencias con las investigaciones en diferentes Estados miembros.

2. Las autoridades competentes de los Estados miembros intercambiarán información con las autoridades competentes a que se refiere el artículo 12, apartado 1, letras c) y d), y se coordinarán y cooperarán con ellas en lo relativo a las medidas específicas tomadas con arreglo al artículo 5 y las sanciones impuestas en virtud del artículo 18. Los Estados miembros se asegurarán de que las autoridades competentes a que se refiere el artículo 12, apartado 1, letras c) y d), estén en posesión de toda la información necesaria.

3. A efectos del apartado 1, los Estados miembros dispondrán de canales o mecanismos de comunicación adecuados y seguros para velar por que la información necesaria se intercambie en tiempo oportuno.

4. Para la aplicación efectiva del presente Reglamento, así como para evitar la duplicación del trabajo, los Estados miembros y los prestadores de servicios de alojamiento de datos podrán hacer uso de herramientas específicas, incluidas las establecidas por Europol, para facilitar, en particular:

a) el tratamiento y la información en relación con las órdenes de retirada de conformidad con el artículo 3; y

b) la cooperación con vistas a la determinación y la aplicación de medidas específicas con arreglo al artículo 5.

5 Cuando los prestadores de servicios de alojamiento de datos tengan conocimiento de contenidos terroristas que conlleven una amenaza inminente para la vida, informarán rápidamente a las autoridades competentes para que se investiguen y enjuicien las infracciones penales en el Estado miembro o los Estados miembros de que se trate. Cuando sea imposible identificar el Estado miembro o los Estados miembros de que se trate, los prestadores de servicios de alojamiento de datos informarán, con arreglo al artículo 12, apartado 2, al punto de contacto del Estado miembro en el que tengan su establecimiento principal o en el que su representante legal resida o esté establecido, y transmitirán la información relativa a los contenidos terroristas a Europol para que se le dé el curso adecuado.

6 Se anima a las autoridades competentes a que envíen a Europol copias de las órdenes de retirada que permitan a Europol presentar un informe anual que incluya un análisis de los tipos de contenidos terroristas sujetos a órdenes de retirada o de bloqueo del acceso a ellos con arreglo al presente Reglamento.

Artículo 15

Puntos de contacto de prestadores de servicios de alojamiento de datos

1. Cada prestador de servicios de alojamiento de datos designará o establecerá un punto de contacto para la recepción de órdenes de retirada por medios electrónicos y su rápido tratamiento con arreglo a los artículos 3 y 4. El prestador de servicios de alojamiento garantizará que la información sobre el punto de contacto esté disponible para el público.

2. La información mencionada en el apartado 1 del presente artículo especificará las lenguas oficiales de las instituciones de la Unión, a las que se refiere el Reglamento 1/58 ([15]), en que sea posible dirigirse al punto de contacto y en que tendrán lugar las subsiguientes comunicaciones en relación con las órdenes de retirada en virtud del artículo 3. 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.

([15]) Reglamento n.º 1 por el que se fija el régimen lingüístico de la Comunidad Económica Europea (DO 17 de 6.10.1958, p. 385).

Sección V

Aplicación y ejecución

Artículo 16

Jurisdicción

1. La jurisdicción a efectos de los artículos 5, 18 y 21 corresponderá al Estado miembro del 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 la Unión se encuentra bajo la jurisdicción del Estado miembro en el que resida o esté establecido su representante legal.

2. Cuando un prestador de servicios de alojamiento de datos que no tenga su establecimiento principal en la Unión no designe un representante legal, la jurisdicción corresponderá a todos los Estados miembros.

3. Cuando la autoridad competente de un Estado miembro ejerza jurisdicción conforme al apartado 2, informará de ello a las autoridades competentes de todos los demás Estados miembros.

Artículo 17

Representante legal

1. Los prestadores de servicios de alojamiento de datos que no tengan su establecimiento principal 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, y las decisiones dictadas por las autoridades competentes.

2. Los prestadores de servicios de alojamiento de datos otorgarán a su representante legal los poderes y recursos necesarios para cumplir con dichas órdenes de retirada y decisiones y para cooperar con las autoridades competentes.

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.

3. El representante legal puede ser considerado responsable de las infracciones del presente Reglamento, sin perjuicio de cualquier responsabilidad del prestador de servicios de alojamiento de datos o de las acciones legales contra este.

4. El prestador de servicios de alojamiento de datos notificará la designación a la autoridad competente a que se refiere el artículo 12, apartado 1, del Estado miembro en el que resida o esté establecido su representante legal.

El prestador de servicios de alojamiento de datos pondrá la información sobre el representante legal a disposición del público.

Sección VI

Disposiciones finales

Artículo 18

Sanciones

1. Los Estados miembros establecerán el régimen de sanciones aplicable a las infracciones d del presente Reglamento cometidas por prestadores de servicios de alojamiento de datos y tomarán todas las medidas necesarias para garantizar su aplicación. Dichas sanciones se limitarán a las infracciones del artículo 3, apartados 3 y 6, el artículo 4, apartados 2 y 7, el artículo 5, apartados 1, 2, 3, 5 y 6, los artículos 6, 7, 10 y 11, el artículo 14, apartado 5, el artículo 15, apartado 1, y el artículo 17.

Las sanciones contempladas en el párrafo primero serán eficaces, proporcionadas y disuasorias. A más tardar el … [doce *meses después de 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.

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

a) la naturaleza, gravedad y duración de la infracción;

b) el carácter doloso o culposo de la infracción;

c) las infracciones previas del prestador de servicios de alojamiento de datos;

d) la solidez financiera del prestador de servicios de alojamiento de datos;

e) el nivel de cooperación con las autoridades competentes del prestador de servicios de alojamiento de datos;

f) la naturaleza y el tamaño del prestador de servicios de alojamiento de datos considerado responsable, en particular si es una microempresa o una pequeña o mediana empresa;

g) el grado de responsabilidad del prestador de servicios de alojamiento de datos considerado responsable, teniendo en cuenta las medidas técnicas y organizativas adoptadas por él para cumplir con el presente Reglamento.

3. Los Estados miembros garantizarán que el incumplimiento sistemático o persistente de las obligaciones contempladas en el artículo 3, apartado 3, sea objeto de sanciones económicas de hasta el 4 % del volumen de negocios mundial del prestador de servicios de alojamiento de datos en el ejercicio precedente.

Artículo 19

Requisitos técnicos y modificaciones de los anexos

1. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 20 con el fin de complementar el presente Reglamento con los requisitos técnicos necesarios 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 conformidad con el artículo 20 para modificar los anexos con el fin de abordar de forma efectiva la posible necesidad de mejoras en lo que concierne al contenido de las plantillas de orden de retirada y 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 mencionados en el artículo 19 se otorgarán a la Comisión por un período de tiempo indefinido a partir del … [*un año después de la entrada en vigor del presente Reglamento*].

3. La delegación de poderes mencionada en 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 ella. No afectará a la validez de los actos delegados que ya estén en vigor.

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

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 a partir de su notificación al Parlamento Europeo y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas 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 que estén bajo su jurisdicción información sobre las actuaciones que hayan emprendido de conformidad con el presente Reglamento en el año civil anterior, y la enviarán a la Comisión a más tardar el 31 de marzo de cada año. Dicha información incluirá los elementos siguientes:

a) el número de órdenes de retirada dictadas y el número de elementos de contenido terrorista que se hayan retirado o a los cuales se haya bloqueado el acceso, y la rapidez de la retirada o del bloqueo;

b) las medidas específicas tomadas con arreglo al artículo 5, incluido el número de elementos de contenido terrorista que se hayan retirado o a los cuales se haya bloqueado el acceso y la rapidez de la retirada o del bloqueo;

c) el número de solicitudes de acceso adoptadas por las autoridades competentes en relación con los contenidos conservados por los prestadores de servicios de alojamiento de datos con arreglo al artículo 6;

d) el número de procedimientos de control iniciados y las actuaciones emprendidas por los prestadores de servicios de alojamiento de datos con arreglo al artículo 10;

e) el número de procedimientos de control administrativos o judiciales iniciados y las decisiones tomadas por la autoridad competente de conformidad con el Derecho nacional.

2. A más tardar el … [*dos años después de la entrada en vigor del presente Reglamento*], la Comisión elaborará un programa detallado para el seguimiento de las consecuciones, 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 con arreglo al artículo 23.

Artículo 22

Informe de aplicación

A más tardar el … [*dos años después de la fecha de entrada en vigor del presente Reglamento*], la Comisión presentará un informe al Parlamento Europeo y al Consejo sobre la aplicación del presente Reglamento. Dicho informe incluirá 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 elaboración del informe.

Artículo 23

Evaluación

A más tardar el … [*tres años después de la entrada en vigor del presente Reglamento*], la Comisión llevará a cabo una evaluación del presente Reglamento y presentará un informe al Parlamento Europeo y al Consejo sobre su aplicación, que entre otros asuntos trate:

a) el funcionamiento y la eficacia de los mecanismos de salvaguardia, en particular los establecidos en el artículo 4, apartado 4, el artículo 6, apartado 3, y los artículos 7 a 11;

b) el impacto de su aplicación sobre los derechos fundamentales, en particular la libertad de expresión y de información, el respeto de la intimidad y la protección de los datos de carácter personal; y

c) la contribución del presente Reglamento a la protección de la seguridad pública.

En su caso, el informe irá acompañado de propuestas legislativas.

Los Estados miembros facilitarán a la Comisión la información necesaria para la elaboración del informe.

La Comisión evaluará asimismo la necesidad y la viabilidad de crear una plataforma europea sobre contenidos terroristas en línea para facilitar la comunicación y la cooperación en virtud del presente Reglamento.

Artículo 24

Entrada en vigor y aplicación

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 … [*doce meses después de la entrada en vigor del presente Reglamento*].

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

Hecho en …, el …

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente*
...	…

ANEXO I

ORDEN DE RETIRADA

(artículo 3 del Reglamento (UE) 2021/ … del Parlamento Europeo y del Consejo ([1]) ([*]))

De conformidad con el artículo 3 del Reglamento (UE) 2021/ … ([*]), (en lo sucesivo, «Reglamento») el destinatario de la orden de retirada retirará los contenidos terroristas o bloqueará el acceso a ellos en todos los Estados miembros tan pronto sea posible y, en cualquier caso, en el plazo de una hora desde la recepción de la orden de retirada.

De conformidad con el artículo 6 del Reglamento, los destinatarios deben conservar los contenidos que hayan sido retirados o a los que se haya bloqueado el acceso y los datos conexos durante seis meses, o durante un período más largo en caso de que así se lo soliciten las autoridades u órganos jurisdiccionales competentes.

De conformidad con el artículo 15, apartado 2, del Reglamento, la presente orden de retirada se envía en una de las lenguas designadas por el destinatario.

SECCIÓN A:

Estado miembro de la autoridad competente que dicta la orden:

……

Nota: se facilitan los datos de la autoridad competente que dicta la orden en las secciones E y F.

Destinatario y, cuando proceda, representante legal:

……

Punto de contacto:

……

Estado miembro en el que el prestador de servicios de alojamiento de datos tenga su establecimiento principal o en el que su representante legal resida o esté establecido:

……

Fecha y hora de emisión de la orden de retirada

……

Número de referencia de la orden de retirada:

……

([1]) Reglamento (UE) 2021/ … ([*]) del Parlamento Europeo y del Consejo sobre la lucha contra los contenidos terroristas en línea (OJ L …)

([*]) Número del Reglamento que figura en el documento ST 14308/20 [2018/0331 (COD)].

SECCIÓN B: contenidos terroristas que deben retirarse o a los cuales debe bloquearse el acceso en todos los Estados miembros lo antes posible y, en cualquier caso, en el plazo de una hora desde la recepción de la orden de retirada

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

……

Motivos por los que el material se considera contenido terrorista de conformidad con el artículo 2, punto 7, del Reglamento.

El material (marque la casilla o casillas pertinentes):

☐ incita a otros a cometer delitos de terrorismo al preconizar su comisión, a través por ejemplo de la apología de actos terroristas (artículo 2, punto 7, letra a), del Reglamento)

☐ induce a otros a cometer delitos de terrorismo o a contribuir a su comisión, (artículo 2, punto 7, letra b) del Reglamento)

☐ induce a otros a participar en las actividades de un grupo terrorista (artículo 2, punto 7, letra c), del Reglamento);

☐ proporciona instrucción sobre la fabricación o el uso de explosivos, armas de fuego u otras armas o sustancias nocivas o peligrosas, o sobre otros métodos o técnicas específicos cuyo fin sea la comisión o la contribución a la comisión de cualquiera de los delitos de terrorismo (artículo 2, punto 7, letra d), del Reglamento)

☐ constituye una amenaza de comisión de uno de los delitos de terrorismo (artículo 2, punto 7, letra e), del Reglamento).

Información adicional sobre los motivos por los que el material se considera contenido terrorista:

……

……

……

SECCIÓN C: información para el proveedor de contenidos

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

☐ por razones de seguridad pública, el destinatario debe abstenerse de informar al proveedor de contenidos de la retirada de, o bloqueo del acceso a, contenidos terroristas.

Si esta casilla no es pertinente, remítase a la sección G para los pormenores en cuanto a la posibilidad de impugnar la orden de retirada en el Estado miembro de la autoridad competente que la dictó, con arreglo al Derecho nacional (debe remitirse una copia de la orden de retirada al proveedor de contenidos, si así lo solicita);

SECCIÓN D: Información a la autoridad competente del Estado miembro en el que el prestador de servicios de alojamiento de datos tenga su establecimiento principal o en el que su representante legal resida o esté establecido

Márquese la casilla o las casillas correspondientes:

☐ el Estado en el que el prestador de servicios de alojamiento de datos tiene su establecimiento principal o en el que está su representante legal es diferente del Estado miembro de la autoridad competente que dicta la orden de retirada

☐ se envía una copia de la orden de retirada a la autoridad competente del Estado miembro en el que el prestador de servicios de alojamiento de datos tenga su establecimiento principal o en el que su representante legal resida o esté establecido

SECCIÓN E: Datos de la autoridad competente que dicta la orden de retirada

Tipo (marque la casilla correspondiente):

☐ juez, órgano jurisdiccional o juez de instrucción

☐ autoridad policial

☐ otra autoridad competente→ rellene también la Sección (F)

Datos de la autoridad competente que dicta la orden y/o de su representante que certifica que la orden de retirada es precisa y correcta:

Nombre de la autoridad competente que dicta la orden:

……

Nombre del representante y puesto que ocupa (cargo/grado):

……

Expediente n.º: ……

Dirección ……

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

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

Dirección de correo electrónico: ……

Fecha……

Sello oficial (en su caso) y firma ([2]): ……

([2]) La firma no es necesaria si la orden de retirada se envía a través de canales de transmisión autenticada que pueden garantizar la autenticidad de dicha orden.

SECCIÓN F: Datos de contacto para el seguimiento

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

……

Datos de contacto de la autoridad competente del Estado miembro donde el prestador de servicios de alojamiento de datos tiene su establecimiento principal o donde su representante legal reside o está establecido:

……

SECCIÓN G: Información sobre posibilidades de recurso

Información sobre el organismo u órgano jurisdiccional competente, los plazos y los procedimientos para impugnar la orden de retirada:

Organismo u órgano jurisdiccional competente ante el que es impugnable la orden de retirada:

……

Plazo para impugnar la orden de retirada:

[dias/meses a partir de]

……

Enlace a las disposiciones nacionales:

……

ANEXO II

FORMULARIO DE INFORMACIÓN TRAS LA RETIRADA DE CONTENIDOS TERRORISTAS O EL BLOQUEO DEL ACCESO A ELLOS

[artículo 3, apartado 6, del Reglamento (UE) 2021/ … del Parlamento Europeo y del Consejo ([1]) ([*])]

SECCIÓN A:

Destinatario de la orden de retirada:

……

Autoridad competente que dictó la orden de retirada:

……

Referencia de la autoridad competente que dictó la orden de retirada:

……

Referencia del destinatario:

……

Fecha y hora de recepción de la orden de retirada:

……

SECCIÓN B: Medidas adoptadas en cumplimiento de la orden de retirada

(Marque la casilla correspondiente):

☐ se han retirado los contenidos terroristas

☐ se ha bloqueado en todos los Estados miembros el acceso a los contenidos terroristas

Fecha y hora de la medida adoptada:

……

([1]) Reglamento (UE) 2021/ … ([*]) del Parlamento Europeo y del Consejo sobre la lucha contra los contenidos terroristas en línea (OJ L …).

([*]) Número del Reglamento que figura en el documento ST 14308/20 [2018/0331 (COD)].

SECCIÓN C: Datos del destinatario

Nombre del prestador de servicios de alojamiento de datos:

……

O

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

……

Estado miembro del establecimiento principal del prestador de servicios de alojamiento de datos:

……

O

Estado miembro de residencia o de establecimiento del representante legal del prestador de servicios de alojamiento de datos:

……

Nombre de la persona autorizada:

……

Dirección de correo electrónico del punto de contacto:

……

Fecha:

……

ANEXO III

INFORMACIÓN SOBRE LA IMPOSIBILIDAD DE EJECUTAR LA ORDEN DE RETIRADA

(artículo 3, apartados 7 y 8, del Reglamento (UE) 2021/ … del Parlamento Europeo y del Consejo ([1]) ([*]))

SECCIÓN A:

Destinatario de la orden de retirada:

……

Autoridad competente que dictó la orden de retirada:

……

Referencia de la autoridad competente que dictó la orden de retirada:

……

Referencia del destinatario:

……

Fecha y hora de recepción de la orden de retirada:

……

SECCIÓN B: No ejecución

1) La orden de retirada no puede ejecutarse en el plazo exigido, por el motivo o los motivos siguientes (marque la casilla o las casillas correspondientes):

☐ La orden de retirada no puede ejecutarse en el plazo exigido, por el motivo o los motivos siguientes (marque la casilla o las casillas correspondientes):

☐ la orden de retirada contiene errores manifiestos

☐ la orden de retirada no contiene suficiente información

2) Facilite información adicional sobre los motivos de la no ejecución:

……

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

……

([1]) Reglamento (UE) 2021/ … ([*]) del Parlamento Europeo y del Consejo sobre la lucha contra los contenidos terroristas en línea (OJ L …).

([*]) Número del Reglamento que figura en el documento ST 14308/20 [2018/0331 (COD)].

SECCIÓN C: Datos del prestador de servicios de alojamiento de datos o su representante legal

Nombre del prestador de servicios de alojamiento de datos:

……

O

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

……

Nombre de la persona autorizada:

……

Datos de contacto (dirección de correo electrónico):

……

Firma:

……

Fecha y hora:

……

Exposición de motivos del Consejo: Posición (UE) n.º 6/2021 del Consejo en primera lectura con vistas a la adopción de un Reglamento del Parlamento Europeo y del Consejo sobre la lucha contra la difusión de conteidos terroristas en línea

(2021/C 135/02)

I. INTRODUCCIÓN

1. El 12 de septiembre de 2018, la Comisión presentó al Consejo y al Parlamento Europeo la propuesta ([1]) mencionada de Reglamento para la prevención de la difusión de contenidos terroristas en línea. Su base jurídica es el artículo 114 (Aproximación de las legislaciones) del Tratado de Funcionamiento de la Unión Europea y la propuesta está sujeta al procedimiento legislativo ordinario.

2. Mediante carta de 24 de octubre de 2018, el Consejo consultó al Comité Económico y Social Europeo (CESE), que emitió su dictamen sobre la propuesta el 12 de diciembre de 2018 ([2]) durante su pleno de diciembre.

3. El 6 de diciembre de 2018, el Consejo acordó una orientación general ([3]) sobre los contenidos terroristas en línea que constituyó el mandato para las negociaciones con el Parlamento Europeo en el contexto del procedimiento legislativo ordinario.

4. El 12 de febrero de 2019, el Supervisor Europeo de Protección de Datos envió sus «observaciones formales» sobre el proyecto de Reglamento al Parlamento Europeo, a la Comisión y al Consejo ([4]). Ese mismo día, la Agencia de los Derechos Fundamentales de la Unión Europea emitió un dictamen sobre la propuesta ([5]) a raíz de una solicitud del Parlamento Europeo de 6 de febrero de 2019.

5. El 17 de abril de 2019, el Parlamento Europeo aprobó una posición en primera lectura ([6]) sobre la propuesta de la Comisión, con 155 enmiendas a dicha propuesta, por 308 votos a favor, 204 en contra y 70 abstenciones.

6. El Consejo y el Parlamento Europeo entablaron negociaciones en octubre de 2019 con vistas a llegar a un acuerdo temprano en segunda lectura. Las negociaciones concluyeron con éxito el 10 de diciembre de 2020 al alcanzar el Parlamento Europeo y el Consejo un acuerdo provisional sobre un texto transaccional.

7. El 16 de diciembre de 2020, el Coreper (2.ª parte) examinó y confirmó provisionalmente el texto transaccional definitivo en vista del acuerdo alcanzado con el Parlamento Europeo ([7]).

8. El 11 de enero de 2021, la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE) del Parlamento Europeo refrendó el acuerdo transaccional. El 13 de enero, el presidente de la Comisión LIBE remitió una carta al presidente del Coreper (2.ª parte) para informarle de que, en caso de que el Consejo transmitiera formalmente al Parlamento Europeo su posición en la forma presentada en el anexo de dicha carta, recomendaría al Pleno que la aprobase en segunda lectura sin enmiendas, a reserva de la revisión jurídico-lingüística ([8]).

([1]) Documentos 12129/18 + ADD 1-3.
([2]) DO C 110 de 22.3.2019, p. 67 (documento 15729/19).
([3]) Documento 15336/18.
([4]) Ref. 2018-0822 D2545 (documento WK 9232/2019).
([5]) Dictamen 2/2019 de la Agencia de los Derechos Fundamentales (documento WK 9235/2019).
([6]) Véase el documento 8663/19 [nota informativa del GIP.2 (Relaciones Interinstitucionales) al Coreper en la que se presenta el resultado de la primera lectura del Parlamento Europeo]; el mandato del Parlamento fue confirmado por el Pleno de los días 10 y 11 de octubre de 2019.
([7]) Documento 12906/20.
([8]) Documento 5634/21.

II. OBJETIVO

9. El Reglamento prevé un claro marco jurídico que establece las responsabilidades que incumben a los Estados miembros y a los prestadores de servicios de alojamiento de datos a la hora de combatir el uso indebido de dichos servicios para difundir contenidos terroristas en línea, garantizando el buen funcionamiento del mercado único digital y velando por la confianza en el entorno en línea y su seguridad. En concreto, pretende aportar claridad en cuanto a la responsabilidad de los prestadores de servicios de alojamiento de datos a la hora de garantizar la seguridad de sus servicios y de tratar, identificar y eliminar los contenidos terroristas en línea, o bloquear el acceso a dichos contenidos, de forma rápida y eficaz. Establece un nuevo y eficaz instrumento operativo para eliminar los contenidos terroristas, al permitir la emisión de órdenes de retirada que tienen un efecto transfronterizo. Tiene por objeto, además, mantener garantías para asegurar la protección de los derechos fundamentales, en particular la libertad de expresión e información en una sociedad abierta y democrática y la libertad de empresa. El Reglamento estipula que deben retirarse los contenidos terroristas en el plazo máximo de una hora desde la recepción de una orden de retirada y establece las responsabilidades de las plataformas en línea a la hora de garantizar que se retiren dichos contenidos. Además de las posibilidades de recurso judicial garantizadas por el derecho a la tutela judicial efectiva, el Reglamento introduce una serie de garantías y mecanismos de reclamación.

10. La autoridad o autoridades competentes de cualquier Estado miembro pueden emitir órdenes de retirada dirigidas a cualquier prestador de servicios de alojamiento de datos dentro de la Unión. La autoridad o autoridades competentes del Estado miembro en el que el prestador de servicios tenga su establecimiento principal tendrán el derecho —y, en caso de recibir una solicitud motivada de los prestadores de servicios de alojamiento de datos o los proveedores de contenidos, la obligación— de examinar la orden de retirada si se considera que esta infringe grave o manifiestamente el propio Reglamento o que vulnera los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea. Los Estados miembros deben adoptar el régimen de sanciones por incumplimiento de las obligaciones, teniendo en cuenta, entre otras cosas, la naturaleza de la infracción y el tamaño de la empresa en cuestión.

III. ANÁLISIS DE LA POSICIÓN DEL CONSEJO EN PRIMERA LECTURA

ASPECTOS GENERALES

11. El Parlamento Europeo y el Consejo entablaron negociaciones con el fin de alcanzar un acuerdo en segunda lectura sobre la base de una posición del Consejo en primera lectura que el Parlamento pudiera aprobar sin cambios. El texto de la posición del Consejo en primera lectura sobre el Reglamento para la prevención de la difusión de contenidos terroristas en línea refleja plenamente el acuerdo transaccional alcanzado entre los dos colegisladores, asistidos por la Comisión Europea.

SÍNTESIS DE LAS PRINCIPALES CUESTIONES

12. A petición del Parlamento Europeo, se cambió el título del Reglamento por el de «Reglamento sobre la lucha contra [...] la difusión de contenidos terroristas en línea».

13. La definición de «contenidos terroristas» es coherente con las definiciones de los delitos pertinentes recogidos en la Directiva relativa a la lucha contra el terrorismo ([9]). En cuanto al ámbito de aplicación, la posición del Consejo en primera lectura incluye el material difundido entre el público, es decir, a un número potencialmente ilimitado de personas. No debe considerarse contenido terrorista el material difundido con fines educativos, periodísticos, artísticos o de investigación, o con fines de sensibilización al objeto de prevenir o combatir el terrorismo, ni tampoco la expresión de puntos de vista polémicos o controvertidos en el debate público sobre cuestiones políticas sensibles. Se determinará con una evaluación la verdadera finalidad de la difusión. Asimismo, se ha especificado que el Reglamento no tendrá el efecto de modificar la obligación de respetar los derechos, libertades y principios a que se refiere el artículo 6 del TUE, y que se aplicará sin perjuicio de los principios fundamentales relativos a la libertad de expresión e información, incluidos la libertad y el pluralismo de los medios de comunicación.

([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).

14. Los prestadores de servicios de alojamiento de datos tomarán medidas adecuadas, razonables y proporcionadas a fin de atajar eficazmente el uso indebido de sus servicios para la difusión de contenidos terroristas en línea. Si los prestadores de servicios de alojamiento de datos están expuestos a contenidos terroristas, deberán adoptar medidas específicas para proteger sus servicios contra la difusión de tales contenidos. El texto acordado fusiona tres artículos [el artículo 3 (Deberes de diligencia), el artículo 6 (Medidas proactivas) y el artículo 9 (Garantías en relación con las medidas proactivas)] en un artículo titulado «Medidas específicas». La elección de estas medidas corresponde al prestador de servicios de alojamiento de datos. La posición del Consejo en primera lectura deja claro que el prestador de servicios de alojamiento de datos puede utilizar distintas medidas para combatir la difusión de contenidos terroristas, en particular medidas automatizadas, que se pueden adaptar a las capacidades del prestador de servicios de alojamiento de datos y a la naturaleza de los servicios que ofrece. En caso de que la autoridad competente considere que las medidas específicas tomadas son insuficientes para hacer frente a los riesgos, podrá exigir la adopción de medidas específicas adicionales adecuadas, eficaces y proporcionadas. No obstante, la exigencia de aplicar dichas medidas específicas adicionales no debe conllevar una exigencia general de supervisión o de iniciar búsquedas activas de hechos en el sentido del artículo 15, apartado 1, de la Directiva 2000/31/CE ([10]), ni una exigencia de utilizar instrumentos automatizados. Para garantizar la transparencia, los prestadores de servicios de alojamiento de datos deberán publicar informes anuales de transparencia sobre las medidas tomadas contra la difusión de contenidos terroristas.

15. Se ha reforzado el papel del Estado miembro de acogida en lo que respecta a las órdenes de retirada con efectos transfronterizos, mediante la introducción de un procedimiento de examen: la autoridad competente 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 podrá, *motu proprio*, examinar la orden de retirada dictada por las autoridades competentes de otro Estado miembro para determinar si infringe grave o manifiestamente el Reglamento o los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea. Ante una solicitud motivada de un prestador de servicios de alojamiento de datos o de un proveedor de contenidos, el Estado miembro de acogida está obligado a examinar si existe tal infracción.

16. Excepto en situaciones de emergencia debidamente justificadas, la autoridad competente debe enviar a los prestadores de servicios de alojamiento de datos a quienes no se haya dirigido con anterioridad una orden de retirada una notificación, con información sobre los procedimientos y plazos aplicables, al menos 12 horas antes emitir la orden de retirada, especialmente con vistas a aliviar la carga de las pequeñas y medianas empresas (pymes).

17. Se ha suprimido el artículo sobre los requerimientos —un mecanismo de notificación de contenidos terroristas a los prestadores de servicios de alojamiento de datos, para la evaluación voluntaria por estos en función de sus términos y condiciones—, pero un considerando aclara que los Estados miembros y Europol pueden seguir utilizando los requerimientos.

18. Los contenidos terroristas que hayan sido retirados o a los que se haya bloqueado el acceso como consecuencia de una orden de retirada o de medidas específicas deben conservarse durante seis meses a partir de la retirada o el bloqueo; este plazo puede prorrogarse tanto como sea necesario en el contexto de un procedimiento de revisión.

19. Los Estados miembros establecerán un régimen de sanciones aplicables a las infracciones de las disposiciones del Reglamento que cometan los prestadores de servicios de alojamiento de datos. Las sanciones podrían adoptar diferentes formas, entre ellas la de advertencia formal en caso de infracciones leves o la de sanción pecuniaria en relación con infracciones más graves. La posición del Consejo en primera lectura establece qué infracciones son sancionables y las circunstancias que son pertinentes para determinar el tipo y nivel de tales sanciones. Los prestadores de servicios de alojamiento de datos podrían ser objeto de sanciones de hasta el 4 % de su volumen de negocios mundial si incumplen de forma sistemática o reiterada la obligación de retirar los contenidos terroristas o de bloquear el acceso a ellos en el plazo de una hora.

IV. **CONCLUSIÓN**

20. La posición del Consejo refleja plenamente el acuerdo transaccional alcanzado en las negociaciones entre el Parlamento Europeo y el Consejo, con la ayuda de la Comisión. Este acuerdo transaccional queda ratificado en la carta del presidente de la Comisión LIBE del Parlamento Europeo al presidente del Coreper (2.ª parte) con fecha de 13 de enero de 2021.

([10]) 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).

ISSN 1977-0928 (edición electrónica)
ISSN 1725-244X (edición papel)

Oficina de Publicaciones
de la Unión Europea
L-2985 Luxemburgo
LUXEMBURGO

ES