



Consejo de la
Unión Europea

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

6717/18

CYBER 39
TELECOM 51
CT 31
FREMP 22
JAI 181
AUDIO 10
DROIPEN 26
COHOM 34

NOTA DE TRANSMISIÓN

De:	secretario general de la Comisión Europea, firmado por D. Jordi AYET PUIGARNAU, director
Fecha de recepción:	7 de marzo de 2018
A:	D. Jeppe TRANHOLM-MIKKELSEN, secretario general del Consejo de la Unión Europea
N.º doc. Ción.:	C(2018) 1177 final
Asunto:	RECOMENDACIÓN DE LA COMISIÓN de 1.3.2018 sobre medidas para combatir eficazmente los contenidos ilícitos en línea

Adjunto se remite a las Delegaciones el documento – C(2018) 1177 final.

Adj.: C(2018) 1177 final

Bruselas, 1.3.2018
C(2018) 1177 final

RECOMENDACIÓN DE LA COMISIÓN

de 1.3.2018

sobre medidas para combatir eficazmente los contenidos ilícitos en línea

RECOMENDACIÓN DE LA COMISIÓN

de 1.3.2018

sobre medidas para combatir eficazmente los contenidos ilícitos en línea

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 292,

Considerando lo siguiente:

- (1) Internet y los prestadores de servicios a través de internet contribuyen significativamente a la innovación, el crecimiento económico y la creación de empleo en la Unión. Muchos de esos prestadores desempeñan un papel esencial en la economía digital al conectar a las empresas con los ciudadanos y facilitar el debate público y la distribución y asimilación de información objetiva, opiniones e ideas. Sin embargo, sus servicios son en algunos casos objeto de abusos por terceros que pretenden realizar actividades ilícitas en línea, por ejemplo la difusión de información relativa a terrorismo, abusos sexuales a menores, incitación al odio o infracciones de la legislación sobre protección de los consumidores, lo que puede socavar la confianza de sus usuarios y dañar sus modelos de negocio. En algunos casos, estos prestadores de servicios podrían incluso beneficiarse de tales actividades, por ejemplo al poner disponer de contenidos protegidos por derechos de autor sin la autorización de los titulares de tales derechos.
- (2) La presencia en línea de contenidos ilícitos tiene consecuencias negativas graves para los usuarios, otras empresas y ciudadanos afectados y la sociedad en general. Habida cuenta de su papel central y de los medios técnicos y las capacidades asociados a los servicios que ofrecen, los prestadores de servicios en línea tienen unas responsabilidades sociales particulares a efectos de contribuir a la lucha contra los contenidos ilícitos difundidos a través del uso de sus servicios.
- (3) Dado que una rápida retirada o el bloqueo del acceso a los contenidos ilícitos es a menudo esencial para limitar su difusión y los consiguientes perjuicios, esas responsabilidades implican, entre otras cosas, que los prestadores de servicios afectados deben poder tomar decisiones rápidas por lo que se refiere a las posibles medidas a adoptar con respecto a los contenidos ilícitos en línea. Dichas responsabilidades también implican que deben instaurarse garantías eficaces y adecuadas, en particular con el fin de garantizar que actúan de modo diligente y proporcionado, y de impedir la supresión no intencionada de contenidos lícitos.
- (4) Muchos prestadores de servicios en línea han reconocido estas responsabilidades y adoptado medidas al respecto. A nivel colectivo, se han hecho progresos importantes gracias a acuerdos voluntarios de distinto tipo, incluido el del Foro de Internet de la UE sobre contenido terrorista en línea, el Código de conducta de la UE relativo a la lucha contra la incitación ilegal al odio en internet y el Memorando de acuerdo sobre la venta de mercancías falsificadas. Sin embargo, a pesar de estos compromisos y de los avances realizados, los contenidos ilícitos en línea siguen suponiendo un problema grave en la Unión.

- (5) Preocupado por una serie de ataques terroristas en la UE y por la proliferación de propaganda terrorista en línea, el Consejo Europeo de los días 22 y 23 de junio de 2017 declaró que «espera que el sector ... desarrolle nuevas tecnologías y herramientas para mejorar la detección automática de contenidos y eliminar aquellos que inciten a perpetrar actos de terrorismo». El Parlamento Europeo, en su Resolución de 15 de junio de 2017, instó a las plataformas en línea a «reforzar las medidas para luchar contra los contenidos ilícitos y nocivos». El llamamiento a las empresas para que adopten una actitud más activa en la defensa de sus usuarios frente a los contenidos terroristas ha sido reiterado por los Ministros de los Estados miembros en el Foro de Internet de la UE. Por lo que se refiere a los derechos de propiedad intelectual, en sus Conclusiones de 4 de diciembre de 2014 sobre el respeto de dichos derechos, el Consejo invitó a la Comisión a considerar el uso de los instrumentos disponibles para identificar a los infractores de tales derechos y el papel de los intermediarios en la asistencia a la lucha contra las vulneraciones de los mismos.
- (6) El 28 de septiembre de 2017, la Comisión adoptó una Comunicación con orientaciones sobre la responsabilidad de los prestadores de servicios en línea en relación con los contenidos ilícitos en línea¹, en la que explicaba que evaluaría si eran necesarias medidas complementarias, entre otras cosas mediante el seguimiento de los avances logrados gracias a los acuerdos voluntarios. La presente Recomendación da continuación a dicha Comunicación y refleja el nivel de ambición que en ella se establece, materializándola y teniendo en cuenta al mismo tiempo los importantes progresos realizados mediante estos acuerdos voluntarios y basándose en ellos.
- (7) La presente Recomendación reconoce que se deben tener debidamente en cuenta las peculiaridades de la lucha contra los distintos tipos de contenidos ilícitos en línea y las respuestas específicas que pudieran ser necesarias, incluso mediante medidas legislativas específicas. Por ejemplo, reconociendo la necesidad de tales medidas legislativas específicas y a la vista de la evolución de las realidades del mercado, el 25 de mayo de 2016 la Comisión adoptó una propuesta de modificación de la Directiva 2010/13/UE, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual, a la vista de evolución de las realidades del mercado². El 14 de septiembre de 2016, la Comisión adoptó asimismo una propuesta de Directiva sobre los derechos de autor en el mercado único digital³, que establece la obligación de que determinados prestadores de servicios adopten, en cooperación con los titulares de derechos, medidas para asegurar el correcto funcionamiento de los acuerdos celebrados con los titulares de derechos para el uso de sus obras u otras prestaciones o para impedir la disponibilidad en sus servicios de obras u otras prestaciones identificadas por los titulares de los derechos mediante la cooperación con dichos prestadores. La presente Recomendación no afecta a tales medidas y propuestas legislativas.
- (8) La Directiva 2000/31/CE del Parlamento Europeo y del Consejo⁴ establece, bajo ciertas condiciones, exenciones de responsabilidad para determinados prestadores de servicios en línea, incluidos los prestadores de servicios de «alojamiento», en el

¹ COM(2017) 555 final, de 28 de septiembre de 2017.

² COM(2016) 287 final, de 25 de mayo de 2016.

³ COM(2016) 593 final, de 14 de septiembre de 2016.

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, DO L 178 de 17.7.2000, p. 1.

sentido de su artículo 14. Para beneficiarse de la limitación de responsabilidad, los prestadores de servicios de alojamiento deben actuar con prontitud para retirar o bloquear el acceso a la información ilegal que almacenen en cuanto tengan conocimiento efectivo de ello y, en materia de reclamaciones por daños y perjuicios, conocimiento de hechos o circunstancias a partir de los cuales sea patente la actividad o información ilícita. Pueden obtener dicho conocimiento efectivo, entre otras cosas, a través de notificaciones que se les remitan. Como tal, la Directiva 2000/31/CE constituye la base para el desarrollo de procedimientos destinados a suprimir y desactivar el acceso a información ilícita y también establece la posibilidad de que los Estados miembros exijan que los prestadores de servicios afectados apliquen la diligencia debida respecto de los contenidos ilícitos que pudieran almacenar.

- (9) A la hora de adoptar medidas en relación con los contenidos ilícitos en línea, los Estados miembros deben respetar el principio del país de origen establecido en la Directiva 2000/31/CE. Por consiguiente, no pueden, por razones inherentes al ámbito coordinado, tal como se especifica en dicha Directiva, restringir la libre prestación de servicios de la sociedad de la información por prestadores establecidos en otro Estado miembro, sin perjuicio, no obstante, de la posibilidad de excepciones en determinadas condiciones establecidas en dicha Directiva.
- (10) Además, varios otros actos de Derecho de la Unión establecen un marco jurídico en relación con determinados tipos de contenidos ilícitos disponibles y que se difunden en línea. En particular, la Directiva 2011/93/UE del Parlamento Europeo y del Consejo⁵ requiere que los Estados miembros adopten medidas para eliminar páginas web que contengan o difundan pornografía infantil, y les ofrece la posibilidad de bloquear el acceso a ellas, siempre que se respeten determinadas garantías. La Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo⁶, que deberá transponerse al Derecho nacional a más tardar el 8 de septiembre de 2018, contiene disposiciones similares respecto de los contenidos en línea que constituyan una provocación pública a la comisión de un delito de terrorismo; también establece normas mínimas relativas a la definición de los delitos de terrorismo y los relacionados con grupos terroristas y actividades terroristas. Con arreglo a la Directiva 2004/48/CE del Parlamento Europeo y del Consejo, relativa al respeto de los derechos de propiedad intelectual⁷, las autoridades judiciales competentes podrán dictar mandamientos judiciales contra los intermediarios cuyos servicios sean utilizados por un tercero para infringir un derecho de propiedad intelectual.
- (11) En este contexto, además de las medidas voluntarias tomadas por algunos prestadores de servicios en línea, determinados Estados miembros han adoptado normas sobre los mecanismos de «notificación y acción» desde la adopción de la Directiva 2000/31/CE. Otros Estados miembros prevén adoptar tales normas. Estos mecanismos suelen buscar facilitar la notificación, al prestador de servicios de alojamiento de datos, de contenidos que la parte notificante considere ilícitos (en lo sucesivo denominada «notificación»), con objeto de que el proveedor pueda decidir si está o no de acuerdo con dicha evaluación y si desea retirar o bloquear el acceso a dichos contenidos (en lo

⁵ Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo, DO L 335 de 17.12.2011, p. 1.

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.

⁷ Directiva 2004/48/CE del Parlamento Europeo y del Consejo, de 29 de abril de 2004, relativa al respeto de los derechos de propiedad intelectual, DO L 157 de 30.4.2004, p. 45.

sucesivo denominada «acción»). Cada vez hay más diferencias entre estas normas nacionales. En consecuencia, los prestadores de servicios pueden estar sujetos a una serie de requisitos jurídicos que son diferentes en cuanto a su fondo y alcance.

- (12) En interés del mercado interior y de la eficacia de la lucha contra los contenidos ilícitos en línea, y a fin de salvaguardar el enfoque equilibrado que la Directiva 2000/31/CE pretende garantizar, es necesario establecer ciertos principios fundamentales que deben guiar la acción de los Estados miembros y de los prestadores de servicios afectados.
- (13) Estos principios deben establecerse y aplicarse en el pleno respeto de los derechos fundamentales protegidos en el ordenamiento jurídico de la Unión y, en particular, de los garantizados en la Carta de los Derechos Fundamentales de la Unión Europea. Los contenidos ilícitos en línea deben abordarse mediante salvaguardias adecuadas y sólidas para garantizar la protección de los derechos fundamentales en línea de todas las partes interesadas. Estos derechos incluyen, en función del caso, la libertad de expresión, que incluye la de recibir y divulgar información; el derecho al respeto de la vida privada y a la protección de los datos personales; así como el derecho a una tutela judicial efectiva de los usuarios de los servicios en cuestión. También pueden incluir la libertad de empresa, comprendida la libertad contractual, la de albergar servicios de alojamiento de datos, así como los derechos de los menores y la protección del derecho de propiedad, incluida la propiedad intelectual, la dignidad humana y la no discriminación de determinadas partes afectadas. En particular, las decisiones adoptadas por los prestadores de servicios de alojamiento de retirar o bloquear el acceso a los contenidos que almacenan debe tener debidamente en cuenta los derechos fundamentales y los intereses legítimos de sus usuarios, así como el papel central que los prestadores suelen desempeñar para facilitar el debate público y la distribución y la recepción de hechos, opiniones e ideas de conformidad con la ley.
- (14) De acuerdo con el enfoque horizontal subyacente a la exención de responsabilidad prevista en el artículo 14 de la Directiva 2000/31/CE, la presente Recomendación debe aplicarse a todo tipo de contenidos que no sean conformes con el Derecho de la Unión o con la legislación de los Estados miembros, con independencia de la naturaleza o el objeto preciso de dichas legislaciones. Basta con tener en cuenta las legislaciones de los Estados miembros que se vean afectados por la prestación del servicio de que se trata, en particular las de los Estados miembros en cuyo territorio esté establecido el prestador de servicios de alojamiento de datos o del país en el que se prestan los servicios. Además, al aplicar la presente Recomendación, deben tenerse debidamente en cuenta el tipo y la gravedad del perjuicio potencial causado por los contenidos ilícitos, que pueden estar estrechamente relacionados con la rapidez de cualquier acción emprendida, y lo que cabría razonablemente esperar de los prestadores de servicios de alojamiento, teniendo en cuenta, en su caso, el estado de desarrollo y la posible utilización de tecnologías. También han de tenerse debidamente en cuenta las diferencias que pudieran existir entre los diversos tipos de contenidos ilícitos y las medidas que han de adoptarse para luchar contra ellos.
- (15) Los prestadores de servicios de alojamiento desempeñan un papel especialmente importante en la lucha contra los contenidos ilícitos en línea, ya que almacenan información facilitada por los usuarios y a petición de estos, y dan acceso a ella a otros usuarios, a menudo a gran escala. Así pues, la presente Recomendación se refiere fundamentalmente a las actividades y responsabilidades de esos proveedores. No obstante, en su caso, las recomendaciones podrán también aplicarse, *mutatis mutandis*, en relación con otros prestadores de servicios en línea. Dado que el objetivo de la

presente Recomendación es abordar los riesgos relacionados con los contenidos ilícitos en línea que afectan a los consumidores en la Unión, la misma se refiere a las actividades de los prestadores de servicios de alojamiento de datos, con independencia de que estén establecidos en la Unión o en un tercer país, siempre que dirijan sus actividades a consumidores residentes en la Unión.

- (16) Los mecanismos para presentar notificaciones a los prestadores de servicios de alojamiento de datos sobre contenidos que se consideran ilícitos son un medio importante para combatir los contenidos ilícitos en línea. Estos mecanismos deben facilitar la notificación por todas las personas o entidades que deseen hacerlo. Por lo tanto, estos mecanismos deben ser de fácil acceso y utilización para todos los usuarios. No obstante, los prestadores de servicios de alojamiento deben seguir siendo flexibles, por ejemplo, en relación con el formato de la notificación o la tecnología utilizados, a fin de permitir soluciones eficientes y de evitar cargas desproporcionadas a dichos proveedores.
- (17) De conformidad con la jurisprudencia del Tribunal de Justicia relativa al artículo 14 de la Directiva 2000/31/CE, la notificación debe ser suficientemente precisa y estar debidamente fundamentada, de modo que el prestador de servicios de alojamiento de datos que la reciba pueda tomar una decisión con conocimiento de causa y diligente por lo que se refiere al efecto que debe darse a la notificación. Por tanto, debe garantizarse, en la medida de lo posible, que dicha norma se cumpla. Sin embargo, que una determinada notificación dé lugar a un nivel de conocimiento o conciencia en el sentido del artículo 14 de esa Directiva debe apreciarse a la luz de las peculiaridades de cada asunto, teniendo en cuenta que el conocimiento efectivo puede también obtenerse de otras formas distintas a las notificaciones.
- (18) Disponer de los datos de quien efectúa la notificación no suele ser necesario para que el prestador de servicios de alojamiento de datos pueda tomar una decisión informada y diligente sobre el curso que se debe dar a la notificación recibida. Obligar a facilitar los datos de contacto como requisito previo para la presentación de una notificación supondría un obstáculo a la notificación. No obstante, la inclusión de los datos de contacto es necesaria para que el prestador de servicios de alojamiento pueda responder. Por tanto, facilitar sus datos de contacto debería ser una posibilidad para el remitente de la notificación, sin que esto sea obligatorio.
- (19) A fin de aumentar la transparencia y la exactitud de los mecanismos de notificación y acción para permitir la reparación en caso necesario, los prestadores de servicios de alojamiento deben, cuando posean los datos de contacto de los notificadores o los proveedores de contenidos, informar oportuna y adecuadamente a los interesados de las medidas adoptadas en el contexto de dichos mecanismos, en particular por lo que se refiere a sus decisiones sobre la retirada o el bloqueo del acceso a dicho contenido. La información que debe facilitarse debe ser proporcionada, en el sentido de que debe corresponder a las alegaciones formuladas por los interesados en sus notificaciones o contranotificaciones y permitir, al mismo tiempo, soluciones adecuadas y diferenciadas, sin provocar una carga excesiva para los prestadores.
- (20) Con el fin de garantizar la transparencia y la equidad, y evitar la retirada no intencionada de contenidos lícitos, los proveedores de contenidos deben, en principio, ser informados de la decisión de retirar o bloquear el acceso a los contenidos almacenados, siempre que así lo soliciten, y deberá ofrecérseles la posibilidad de impugnar la decisión a través de una contranotificación, con vistas a la anulación general de esa decisión en su caso, independientemente de si esta decisión se adoptó

sobre la base de una notificación o un requerimiento o en virtud de medidas activas adoptadas por el prestador de servicios de alojamiento de datos.

- (21) No obstante, considerando la naturaleza de los contenidos de que se trata, el objetivo de tal procedimiento de contranotificación y la carga adicional que supone para los prestadores de servicios de alojamiento de datos, no existe ninguna justificación para recomendar facilitar la información sobre esa decisión y la posibilidad de impugnarla cuando sea manifiesto que los contenidos en cuestión son ilícitos y se refieren a delitos graves que supongan un peligro para la vida o la seguridad de las personas, tales como los previstos en la Directiva (UE) 2017/541 y en la Directiva 2011/93/UE. Además, en determinados casos, razones de orden público y de seguridad pública y, en particular, motivos relacionados con la prevención, la investigación, la detección y el enjuiciamiento de delitos, pueden justificar no facilitar directamente esa información al prestador de contenidos afectado. Por lo tanto, los prestadores de servicios de alojamiento de datos no deben hacerlo cuando una autoridad competente haya presentado una solicitud al respecto basada en motivos de orden público y de seguridad pública, siempre que dicha autoridad lo haya requerido a la luz de estos motivos. En la medida en que esto supone una restricción del derecho a ser informado, en relación con el tratamiento de datos personales, deben respetarse las condiciones pertinentes establecidas en el Reglamento (UE) 2016/679.
- (22) Los mecanismos de notificación y acción no deben afectar en modo alguno a los derechos de las partes interesadas a entablar acciones judiciales, de conformidad con la legislación aplicable, con respecto a cualquier contenido que se considere ilícito o a cualquier medida adoptada a este respecto por los prestadores de servicios de alojamiento. Los mecanismos de resolución extrajudicial de litigios que se planteen en este contexto pueden ser un complemento importante de los procedimientos judiciales, sobre todo si permiten una resolución rápida, asequible y eficaz del litigio. Por lo tanto, deben favorecerse los acuerdos extrajudiciales siempre que los correspondientes mecanismos cumplan determinadas normas, especialmente en términos de equidad procesal, que el acceso de las partes a los tribunales no se vea afectado y que no se cometan abusos.
- (23) A fin de evaluar mejor la eficacia de los mecanismos de notificación y otras actividades de los prestadores de servicios de alojamiento de datos en lo que se refiere a los contenidos considerados ilegales y de garantizar la rendición de cuentas, debe existir transparencia ante la opinión pública. Así pues, los prestadores de servicios de alojamiento de datos deben publicar periódicamente informes sobre estos mecanismos y otras actividades, suficientemente exhaustivos y detallados para permitir una adecuada visión de la situación. Asimismo, deben aclarar previamente, en sus condiciones de servicio, sus políticas de retirada o bloqueo del acceso a los contenidos que almacenan, incluidos los ilícitos.
- (24) Además de los mecanismos de notificación y acción, la adopción voluntaria de medidas activas, proporcionadas y específicas por los prestadores de servicios de alojamiento, en particular utilizando medios automatizados en determinados casos, también puede constituir un elemento importante en la lucha contra los contenidos ilícitos en línea, sin perjuicio de lo dispuesto en el artículo 15, apartado 1, de la Directiva 2000/31/CE. En relación con dichas medidas activas, debe tenerse en cuenta la situación de los prestadores de servicios de alojamiento de datos que, debido a su tamaño o a la escala a la que operan disponen de escasos recursos y conocimientos técnicos, y de la necesidad de garantías efectivas y adecuadas que acompañen a tales medidas.

- (25) En especial, puede ser apropiado adoptar tales medidas activas cuando ya se haya establecido el carácter ilícito de los contenidos o cuando el tipo de contenidos sea tal que la contextualización no resulte esencial. Puede depender también de la naturaleza, escala y finalidad de las medidas previstas, el tipo de contenidos de que se trate, si los contenidos ha sido notificados por cuerpos de seguridad o Europol y de si se han adoptado medidas al respecto por haber sido considerado ilícito. En lo tocante, en particular, al material relacionado con abusos sexuales a menores, los prestadores de servicios de alojamiento de datos deben adoptar medidas activas para detectar e impedir la difusión de dicho material, con arreglo a los compromisos alcanzados en el contexto de la Alianza Mundial contra el abuso sexual de menores en línea.
- (26) En este contexto, en su Comunicación de 28 de septiembre de 2017 sobre la lucha contra los contenidos ilícitos en línea, la Comisión expuso su opinión de que adoptar medidas activas de carácter voluntario no conduce automáticamente a que un prestador de servicios de alojamiento de datos afectado pierda el beneficio de la exención de responsabilidad prevista en el artículo 14 de la Directiva 2000/31/CE.
- (27) Es esencial que todas las medidas para combatir los contenidos ilícitos en línea estén sujetas a unas garantías adecuadas y efectivas que velen por que los prestadores de servicios de alojamiento actúen con diligencia y de forma proporcionada al establecer y aplicar sus políticas en materia de los contenidos que almacenan, incluidos los ilícitos, a fin de garantizar, en particular, que los usuarios puedan recibir y difundir libremente información en línea, de conformidad con la legislación aplicable. Además de las garantías establecidas en la legislación aplicable, por ejemplo en relación con la protección de los datos personales, deben establecerse y aplicarse garantías particulares, en especial la vigilancia y la comprobación realizadas por personas, cuando proceda, en relación con el uso de medios automatizados, a fin de evitar decisiones no intencionadas y erróneas.
- (28) Debe garantizarse una cooperación fluida, efectiva y adecuada entre las autoridades competentes y los prestadores de servicios de alojamiento a la hora de luchar contra los contenidos ilícitos en línea. Esta cooperación podría beneficiarse de la asistencia de Europol en su caso, por ejemplo para combatir el terrorismo y los abusos sexuales y la explotación sexual de menores, la pornografía infantil y la captación de menores. Con objeto de facilitar esta cooperación, los Estados miembros y los prestadores de servicios de alojamiento de datos deben designar puntos de contacto y establecer procedimientos para el tratamiento de las notificaciones presentadas por dichas autoridades de forma prioritaria y con un nivel adecuado de confianza en cuanto a su exactitud, teniendo en cuenta los conocimientos especiales y las responsabilidades de dichas autoridades. A fin de abordar con eficacia determinados delitos especialmente graves, tales como los previstos en la Directiva (UE) 2017/541 y en la Directiva 2011/93/UE, que puedan llegar a conocimiento de los prestadores de servicios de alojamiento de datos en el ejercicio de su actividad, debe invitarse a los Estados miembros a que hagan uso de la posibilidad establecida en el artículo 15, apartado 2, de la Directiva 2000/31/CE, de establecer obligaciones legales de notificación, de conformidad con la legislación aplicable, en concreto el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo⁸.

⁸ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), DO L 119 de 4.5.2016, p. 1.

- (29) Además de las autoridades competentes, determinadas personas o entidades, incluidas las organizaciones no gubernamentales y las asociaciones comerciales, también podrían tener una experiencia concreta y desear asumir voluntariamente determinadas responsabilidades relacionadas con la lucha contra los contenidos ilícitos en línea. A la luz de su valor añadido y del a veces alto número de notificaciones afectadas, debe fomentarse la cooperación entre tales notificantes fiables y los prestadores de servicios de alojamiento, en particular tratando prioritariamente las notificaciones que presenten y con un nivel adecuado de confianza en cuanto a su exactitud. No obstante, de conformidad con su estatuto particular, esa cooperación solo debe estar abierta a los individuos y entidades que respeten los valores en que se fundamenta la Unión, tal como se establece en el artículo 2 del Tratado de la Unión Europea, y que reúnan determinadas condiciones adecuadas, que, por otro lado, deben ser claras y objetivas y estar a disposición del público.
- (30) La lucha contra los contenidos ilícitos en línea requiere un planteamiento general puesto que a menudo estos contenidos migran fácilmente de un prestador de servicios de alojamiento de datos a otro y tienden a explotar los eslabones más débiles de la cadena. En consecuencia, resulta esencial una cooperación consistente, en particular, en la puesta en común con carácter voluntario de experiencias, mejores prácticas y soluciones tecnológicas. Esta cooperación es especialmente importante por lo que respecta a los prestadores de servicios de alojamiento de datos que por su tamaño o la escala en la que operan, disponen de escasos recursos y conocimientos técnicos.
- (31) El terrorismo implica el uso ilegal e indiscriminado de la violencia y la intimidación contra los ciudadanos. Los terroristas dependen cada vez más de internet para difundir propaganda terrorista y a menudo utilizan métodos sofisticados para garantizar una rápida y amplia difusión. Aunque se han realizado progresos, especialmente en el contexto del Foro de Internet de la UE, sigue siendo urgente dar una respuesta más rápida y eficaz a los contenidos terroristas en línea, además de necesario que los prestadores de servicios de alojamiento que participan en el Foro de Internet de la UE cumplan plenamente sus compromisos relativos a una información eficaz y exhaustiva.
- (32) Habida cuenta de las particularidades vinculadas a la lucha contra los contenidos terroristas en línea, las recomendaciones relativas a la lucha contra los contenidos ilícitos en general deberían completarse con determinadas recomendaciones específicas sobre la lucha contra los contenidos terroristas en línea, aprovechando y consolidando los esfuerzos emprendidos en el marco del Foro de Internet de la UE.
- (33) Considerando la especial gravedad de los riesgos asociados con los contenidos terroristas y el papel central de los prestadores de servicios de alojamiento en la difusión de dicho contenido, los prestadores deben adoptar todas las medidas razonables para vetar esos contenidos terroristas y, si es posible, evitar alojarlo, condicionadas a la posibilidad de fijar y respetar sus condiciones de servicio y a la necesidad de garantías adecuadas y eficaces, y sin perjuicio de lo dispuesto en el artículo 14 de la Directiva 2000/31/CE.
- (34) En particular, estas medidas deben consistir en cooperar con las autoridades competentes y Europol en relación con los requerimientos, que son un medio concreto de notificación a los prestadores de servicios de alojamiento adaptado a las particularidades de la lucha contra los contenidos terroristas. Al presentar requerimientos, las autoridades competentes y Europol deben poder solicitar la retirada o el bloqueo del acceso a los contenidos que consideren de naturaleza

terrorista bien por referencia a la legislación aplicable o a las condiciones de servicio del prestador de servicios de alojamiento de datos de que se trate. Estos mecanismos de requerimiento deben añadirse a los mecanismos existentes para presentar notificaciones, incluidos los notificantes fiables, que pueden utilizarse también para notificar contenidos que se considere que tienen naturaleza terrorista.

- (35) Habida cuenta de que los contenidos de naturaleza terrorista suelen provocar más daños durante la primera hora de su aparición en línea y de los conocimientos específicos y las responsabilidades de las autoridades competentes y de Europol, los requerimientos deben ser evaluados y, en su caso, conducir a la adopción de medidas en un plazo de una hora, como norma general.
- (36) Las medidas contra los contenidos terroristas deben consistir también en medidas activas, proporcionadas y específicas, recurriendo, entre otras vías, a medios automatizados, con el fin de detectar, identificar y retirar o bloquear el acceso a dichos contenidos terroristas y de garantizar que los contenidos terroristas no reaparezcan, sin perjuicio de lo dispuesto en el artículo 15, apartado 1, de la Directiva 2000/31/CE. A este respecto, ha de tenerse en cuenta la necesidad de garantías adecuadas y efectivas que acompañen a tales medidas, en particular las recomendadas en el capítulo II de la presente Recomendación.
- (37) La cooperación, tanto entre los prestadores de servicios de alojamiento como entre estos y las autoridades competentes, reviste la máxima importancia a la hora de luchar contra los contenidos terroristas en línea. En especial, los instrumentos tecnológicos que permiten la detección automatizada de contenido, tales como la base de datos de resúmenes criptográficos, pueden ayudar a alcanzar el objetivo de evitar la diseminación de contenidos entre diferentes servicios de alojamiento. Debe promoverse esta cooperación y el desarrollo, explotación y puesta en común de dichos instrumentos tecnológicos, haciendo uso de la experiencia de Europol cuando proceda. Los esfuerzos de cooperación son especialmente importantes para permitir que los prestadores de servicios de alojamiento que, debido a su tamaño o a la escala a la que operan, disponen de escasos recursos y conocimientos técnicos, respondan de forma eficaz y urgente a los requerimientos y tomen medidas activas, según lo recomendado.
- (38) El mayor número posible de prestadores de servicios de alojamiento de datos deben unirse a los esfuerzos de cooperación y todos los prestadores participantes deben ayudar a optimizar y maximizar el uso de dichos instrumentos. La celebración de acuerdos de trabajo entre todas las partes pertinentes, incluido, en su caso, Europol, también debe fomentarse, dado que dichos acuerdos pueden ayudar a garantizar un enfoque coherente y efectivo y permitir el intercambio de experiencias y conocimientos.
- (39) Con el fin de garantizar el respeto del derecho fundamental a la protección de las personas físicas en relación con el tratamiento de datos personales, así como la libre circulación de los datos de carácter personal, el tratamiento de dichos datos en el contexto de todas las medidas adoptadas para cumplir la presente Recomendación debe ser plenamente conforme con las normas en materia de protección de datos, en particular el Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo⁹, y debe ser controlado por las autoridades de supervisión competentes.

⁹ Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las

- (40) La presente Recomendación respeta los derechos fundamentales y observa los principios reconocidos, en particular, por la Carta de los Derechos Fundamentales de la Unión Europea. En especial, la presente Recomendación tiene por objeto garantizar el pleno respeto de los artículos 1, 7, 8, 10, 11, 16, 17, 21, 24 y 47 de la misma.
- (41) La Comisión tiene la intención de supervisar minuciosamente las medidas adoptadas en respuesta a la presente Recomendación. Así pues, los Estados miembros y los prestadores de servicios de alojamiento deben estar preparados para entregar a la Comisión, siempre que esta lo solicite, toda la información pertinente que pueda esperarse razonablemente que ofrezcan para permitir dicho control. Sobre la base de la información así obtenida y del resto de la información disponible, incluida la relativa a los diversos acuerdos voluntarios, la Comisión evaluará los efectos habida cuenta de la presente Recomendación y determinará si son necesarias otras medidas adicionales, incluida la presentación de propuestas de actos jurídicamente vinculantes del Derecho de la Unión. Dadas las particularidades y la urgencia de luchar contra los contenidos terroristas en línea, dicho seguimiento y evaluación deben efectuarse sobre la base de información detallada y con especial celeridad, en un plazo de tres meses a partir de la fecha de publicación de la presente Recomendación, mientras que para otros contenidos ilícitos es conveniente hacerlo seis meses después de dicha publicación.

HA ADOPTADO LA PRESENTE RECOMENDACIÓN:

CAPÍTULO I

FINALIDAD Y TERMINOLOGÍA

1. Se invita a los Estados miembros y a los prestadores de servicios de alojamiento de datos, en relación con los contenidos facilitados por proveedores de contenidos que almacenan a petición de dichos proveedores, a adoptar medidas eficaces, apropiadas y proporcionadas para combatir los contenidos ilícitos en línea, con arreglo a los principios establecidos en la presente Recomendación y de plena conformidad con la Carta de los Derechos Fundamentales de la Unión Europea, en particular, el derecho a la libertad de expresión y de información, y otras disposiciones aplicables del Derecho de la Unión, en particular por lo que respecta a la protección de los datos personales, la competencia y el comercio electrónico.
2. La presente Recomendación se basa, consolidándolos, en los avances registrados en el marco de acuerdos voluntarios entre prestadores de servicios de alojamiento y otros prestadores de servicios por lo que se refiere a diferentes tipos de contenidos ilícitos. En el ámbito del terrorismo, se basa, consolidándolos, en los avances logrados en el marco del Foro de Internet de la UE.
3. La presente Recomendación debe entenderse sin perjuicio de los derechos y obligaciones de los Estados miembros para adoptar medidas en relación con los contenidos ilícitos en línea, de acuerdo con el Derecho de la Unión, incluida la posibilidad de que las autoridades judiciales o administrativas de los Estados miembros, de conformidad con sus respectivos ordenamientos jurídicos, obliguen a los prestadores de servicios de alojamiento a retirar o bloquear el acceso a dichos contenidos ilícitos. La presente Recomendación se entiende asimismo sin perjuicio

autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de estos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, DO L 119 de 4.5.2016, p. 89.

de la posición de los prestadores de servicios de alojamiento de datos con arreglo a la Directiva 2000/31/CE y de la posibilidad que se les ofrece de establecer y hacer cumplir sus condiciones de prestación de servicios de conformidad con el Derecho de la Unión y la legislación de los Estados miembros.

4. A efectos de la presente Recomendación, se entenderá por:

- a) «prestador de servicios de alojamiento de datos»: prestador de servicios de la sociedad de la información consistentes en el almacenamiento de datos facilitados por el destinatario del servicio a petición del mismo, en el sentido del artículo 14 de la Directiva 2000/31/CE, con independencia de su lugar de establecimiento y que enfoca sus actividades a consumidores residentes en la Unión;
- b) «contenidos ilícitos»: cualquier información que no sea conforme con el Derecho de la Unión o la legislación del Estado miembro de que se trate;
- c) «usuario»: cualquier persona física o jurídica que sea el destinatario de los servicios prestados por un prestador de servicios de alojamiento de datos;
- d) «proveedor de contenidos»: usuario que ha enviado información que esté o haya sido almacenada a petición suya por un prestador de servicios de alojamiento de datos;
- e) «notificación»: comunicación dirigida a un prestador de servicios de alojamiento de datos por un notificante en relación con contenidos almacenados por dicho prestador que el notificante considere que constituyen contenidos ilícitos y con respecto al cual solicite al prestador su retirada o el bloqueo del acceso sobre una base voluntaria;
- f) «notificante»: persona física o jurídica que haya presentado una notificación a un prestador de servicios de alojamiento de datos;
- g) «comunicante fiable»: persona física o jurídica que un prestador de servicios de alojamiento de datos considere que posee competencias y responsabilidades particulares a efectos de la lucha contra los contenidos ilícitos en línea;
- h) «contenidos terroristas»: toda información cuya difusión puede ser tipificada como uno de los delitos contemplados en la Directiva (UE) 2017/541 o como un acto terrorista conforme a la legislación de un Estado miembro afectado, incluida la difusión de información relevante que haya sido elaborada por grupos terroristas o entidades incluidas en las listas pertinentes establecidas por la Unión o por las Naciones Unidas o que sea imputable a los mismos;
- i) «cuerpos de seguridad»: autoridades competentes designadas por los Estados miembros de conformidad con su legislación nacional para realizar tareas policiales, con fines de prevención, investigación, detección o enjuiciamiento de delitos en relación con contenidos ilícitos en línea;
- j) «autoridades competentes»: autoridades designadas por los Estados miembros de conformidad con su legislación nacional para realizar tareas de lucha contra los contenidos ilícitos en línea, incluidos los cuerpos de seguridad y las autoridades administrativas encargadas de hacer cumplir la legislación en determinados ámbitos, con independencia de la naturaleza o del objeto específico de esa legislación;

- k) «requerimiento»: comunicación dirigida a un prestador de servicios de alojamiento de datos presentada por la autoridad competente o por Europol en relación con contenidos almacenados por dicho prestador que la autoridad competente o Europol consideren que son contenidos terroristas y en la que se solicita a dicho prestador que retire o bloquee voluntariamente el acceso a ese contenido.

CAPÍTULO II

RECOMENDACIONES GENERALES SOBRE TODOS LOS TIPOS DE CONTENIDOS ILÍCITOS

Presentación y tramitación de notificaciones

5. Conviene prever mecanismos para la presentación de notificaciones. Dichos mecanismos deben ser fácilmente accesibles, de fácil utilización y permitir la presentación de notificaciones por medios electrónicos.
6. Estos mecanismos deben permitir y alentar la presentación de notificaciones que sean suficientemente precisas y estén debidamente fundamentadas para permitir que el prestador de servicios de alojamiento de datos que se trate adopte una decisión con conocimiento de causa y diligentemente por lo que respecta a los contenidos a los que se refiera la notificación, en particular si deben considerarse ilícitos o no y si es necesario retirarlos o bloquear el acceso a los mismos. Estos mecanismos deben tener unas características que faciliten la comunicación de notificaciones que expliquen las razones por las que el notificante considera que esos contenidos son ilícitos y una indicación clara de su localización.
7. Aunque no estará obligado a ello, el notificante debe tener la posibilidad de incluir sus datos de contacto en una notificación. Si decide hacerlo, debe garantizarse su anonimato frente al proveedor de contenidos.
8. Cuando los datos de contacto del notificante sean conocidos por el prestador de servicios de alojamiento de datos, el prestador debe enviarle al notificante una confirmación de la recepción de la notificación e informarle, sin demora injustificada y de forma proporcionada, de su decisión por lo que respecta al contenido al que se refiera la notificación.

Información a los proveedores de contenidos y contranotificaciones

9. Cuando un prestador de servicios de alojamiento de datos decida retirar o bloquear el acceso a cualquier contenido que almacene porque considere que se trata de un contenido ilícito, con independencia de los medios utilizados para detectar, identificar o retirar, o bloquear el acceso a dicho contenido, y cuando los datos de contacto del proveedor de contenidos sean conocidos por el prestador de servicios de alojamiento de datos, el proveedor deberá, sin demora indebida, ser informado de manera proporcionada de dicha decisión y de las razones para su adopción, así como de la posibilidad de impugnar dicha decisión con arreglo a los términos del punto 11.
10. No obstante, el punto 9 no se aplicará cuando sea manifiesto que los contenidos de que se trate son ilícitos y se refieren a delitos graves que supongan un peligro para la vida o la seguridad de las personas. Además, los prestadores de servicios de alojamiento de datos no deben facilitar la información a que se refiere dicho punto cuando (y en la medida en que) la autoridad competente así lo solicite por razones de

orden público y de seguridad pública, en particular, la prevención, la investigación, la detección y el enjuiciamiento de delitos.

11. Los proveedores de contenidos deben tener la posibilidad de oponerse a la decisión del prestador de servicios de alojamiento de datos mencionado en el punto 9 en un plazo razonable, mediante la presentación de una contranotificación a dicho prestador. El mecanismo de presentación de tal contranotificación deberá ser de fácil utilización y permitir la presentación por medios electrónicos.
12. Es preciso garantizar que el prestador de servicios de alojamiento de datos tenga en cuenta cualquier posible contranotificación que reciba. Cuando la contranotificación contenga razones para que el prestador considere que los contenidos a los que se refiere la contranotificación no han de considerarse ilícitos, debe revocar su decisión de retirar o bloquear el acceso a dicho contenido, sin dilaciones indebidas y sin perjuicio de su posibilidad de establecer y hacer cumplir sus condiciones de prestación de servicios de conformidad con el Derecho de la Unión y el Derecho de los Estados miembros.
13. El prestador de servicios de alojamiento de datos deberá informar al proveedor de contenido que haya presentado una contranotificación, así como al notificante de que se trate, sin demora injustificada y cuando conozca sus datos de contacto, de la decisión que haya tomado en relación con los contenidos afectados.

Solución extrajudicial de litigios

14. Se anima a los Estados miembros a facilitar, cuando proceda, la celebración de acuerdos extrajudiciales para resolver litigios relacionados con la retirada o el bloqueo de los contenidos ilícitos de que se trate. Los mecanismos de solución extrajudicial de litigios deben ser fácilmente accesibles, eficaces, transparentes e imparciales y garantizar que los acuerdos son justos y conformes a la legislación aplicable. Los intentos de resolver estos litigios fuera de los tribunales no deben afectar al acceso a los tribunales de las partes afectadas.
15. Cuando estén disponibles en el Estado miembro de que se trate, se anima a los prestadores de servicios de alojamiento a que permitan el uso de mecanismos extrajudiciales de resolución de litigios.

Transparencia

16. Se debe alentar a los prestadores de servicios de alojamiento de datos a que publiquen de forma clara, comprensible y suficientemente detallada su política con respecto a la retirada o el bloqueo de los contenidos que almacenan, en particular los considerados ilícitos.
17. Se debe alentar a los prestadores de servicios de alojamiento a publicar periódicamente, de preferencia al menos una vez al año, informes sobre su actividad en relación con la retirada y el bloqueo del contenido considerado ilegal. Estos informes incluirán, en particular, datos sobre la cantidad y el tipo de contenidos, el número de notificaciones y contranotificaciones recibidas y el tiempo necesario para la adopción de medidas.

Medidas activas

18. Los prestadores de servicios de alojamiento de datos deben ser invitados a tomar, en su caso, medidas activas, proporcionadas y específicas en relación con los contenidos ilícitos. Tales medidas podrían implicar la utilización de medios automatizados para la detección de contenidos ilícitos solo cuando se cuente con garantías apropiadas, proporcionadas y efectivas, en particular las garantías mencionadas en los puntos 19 y 20.

Garantías

19. Para evitar la retirada de contenidos lícitos, sin perjuicio de la posibilidad de que los prestadores de servicios de alojamiento establezca y aplique sus condiciones de prestación de servicios de conformidad con la normativa de la Unión y la legislación de los Estados miembros, deben existir salvaguardias eficaces y apropiadas para garantizar que los prestadores de servicios de alojamiento actúen con diligencia y de forma proporcionada respecto de los contenidos que almacenan, en particular al gestionar las notificaciones y contranotificaciones y al decidir sobre la posible retirada o el bloqueo de los contenidos considerados ilícitos.
20. Cuando el prestador de servicios de alojamiento de datos use medios automatizados para el almacenamiento del contenido, deberá contarse con salvaguardias eficaces y apropiadas para garantizar que las decisiones adoptadas en relación con esos contenidos, en particular las decisiones de retirar o bloquear el acceso a los contenidos considerados ilícitos, sean precisas y bien fundamentadas. Dichas garantías deben consistir, en particular, en la vigilancia y verificaciones por personas, cuando proceda y, en cualquier caso, cuando se precise una evaluación detallada del contexto pertinente para determinar si el contenido debe considerarse ilícito o no.

Protección frente a comportamientos abusivos

21. Deben adoptarse medidas efectivas y apropiadas para prevenir la presentación o la actuación en base a notificaciones o contranotificaciones que sean presentadas de mala fe y otras formas de comportamientos abusivos en relación con las medidas recomendadas en la presente Recomendación para luchar contra los contenidos ilícitos en línea.

Cooperación entre Estados miembros y prestadores de servicios de alojamiento

22. Los Estados miembros y los prestadores de servicios de alojamiento de datos deben designar puntos de contacto para las cuestiones relacionadas con los contenidos ilícitos en línea.
23. Deben establecerse procedimientos acelerados para tramitar las notificaciones presentadas por las autoridades competentes.
24. Se invita a los Estados miembros a establecer obligaciones legales a los efectos de que los prestadores de servicios de alojamiento informen rápidamente a los cuerpos de seguridad con vistas a la prevención, investigación, detección o enjuiciamiento de delitos, de las pruebas de presuntos delitos graves que supongan un peligro para la vida o la seguridad de las personas en el marco de sus actividades para retirar o bloquear el acceso a los contenidos ilícitos, con arreglo a los requisitos jurídicos aplicables, en particular por lo que respecta a la protección de los datos personales, incluido el Reglamento (UE) 2016/679.

Cooperación entre prestadores de servicios de alojamiento y notificantes fiables

25. Debe fomentarse la cooperación entre prestadores de servicios de alojamiento de datos y notificantes fiables. En particular, deben establecerse procedimientos acelerados para tramitar las notificaciones presentadas por notificantes fiables.
26. Se debe alentar a los prestadores de servicios de alojamiento de datos a que publiquen condiciones claras y objetivas para determinar qué personas o entidades consideran notificantes fiables.
27. Estas condiciones deben estar encaminadas a garantizar que los particulares o entidades afectados dispongan de los conocimientos especializados necesarios y desarrollen sus actividades en tanto que notificantes fiables de forma diligente y objetiva, basada en el respeto de los valores en que se fundamenta la Unión.

Cooperación entre prestadores de servicios de alojamiento de datos

28. En su caso, los prestadores de servicios de alojamiento de datos deben intercambiar experiencias, soluciones tecnológicas y mejores prácticas para combatir los contenidos ilícitos en línea, entre otros y en particular, con los prestadores de servicios de alojamiento que por su tamaño o la escala en la que operan, disponen de recursos y conocimientos técnicos limitados, también en el contexto de la cooperación permanente entre prestadores de servicios de alojamiento de datos a través de códigos de conducta, memorandos de acuerdo y otros acuerdos voluntarios.

CAPÍTULO III

RECOMENDACIONES ESPECÍFICAS EN RELACIÓN CON LOS CONTENIDOS TERRORISTAS

Aspectos generales

29. Las recomendaciones específicas en relación con los contenidos terroristas establecidas en el presente capítulo se aplicarán además de las recomendaciones generales recogidas en el capítulo II.
30. Los prestadores de servicios de alojamiento de datos deberán indicar expresamente en sus condiciones de servicio que no almacenarán contenidos terroristas.
31. Los prestadores de servicios de alojamiento de datos deberán adoptar medidas con el fin de no almacenar contenidos terroristas, en particular por lo que respecta a requerimientos, medidas activas y cooperación de conformidad con los puntos 32 a 40.

Presentación y tramitación de requerimientos

32. Los Estados miembros deben garantizar que sus autoridades competentes tengan la capacidad y los recursos suficientes para identificar y detectar eficazmente los contenidos terroristas y para presentar requerimientos ante los prestadores de servicios de alojamiento de datos en cuestión, en particular a través de internet y de las unidades de nacionales encargadas de los requerimientos, en cooperación con la Unidad de Notificación de Contenidos de Internet de la UE en el seno de Europol.
33. Deben preverse mecanismos que permitan la presentación de requerimientos y procedimientos acelerados para tramitarlos, en particular los presentados por las

unidades nacionales de notificación de contenidos de internet y la Unidad de Notificación de Contenidos de Internet de la UE en el seno de Europol.

34. Los prestadores de servicios de alojamiento de datos deben, sin demora indebida, enviar acuses de recibo de los requerimientos e informar a la autoridad competente o a Europol de sus decisiones respecto de los contenidos a los que se refieren los requerimientos, indicando, en su caso, si los contenidos han sido retirados o bloqueados, o los motivos para no retirarlos o bloquearlos.
35. Los prestadores de servicios de alojamiento de datos deben evaluar y, en su caso, retirar o bloquear el acceso a contenidos identificados en los requerimientos, por regla general en el plazo de una hora a partir del momento en que se haya recibido el requerimiento.

Medidas activas

36. Los prestadores de servicios de alojamiento de datos deben adoptar medidas activas, proporcionadas y específicas, entre otras cosas, mediante medios automatizados, con el fin de detectar, identificar y retirar o desactivar el acceso a los contenidos terroristas.
37. Los prestadores de servicios de alojamiento de datos deben adoptar medidas activas, proporcionadas y específicas, entre otras cosas mediante medios automatizados, a fin de impedir inmediatamente que los proveedores de contenidos presenten de nuevo contenidos que ya hayan sido retirados o bloqueados por haberse considerado contenidos de naturaleza terrorista.

Cooperación

38. Con el fin de evitar la difusión de contenidos terroristas entre diferentes servicios de alojamiento de datos, los prestadores de servicios de alojamiento de datos deben ser invitados a cooperar mediante la puesta en común y la optimización de instrumentos tecnológicos adecuados y proporcionados, incluidos los que permitan la detección automática de contenidos. Cuando sea posible desde el punto de vista tecnológico, deben capturarse todos los formatos de contenidos a través de los cuales se difunden los contenidos terroristas. Tal cooperación debe incluir, en particular, a los prestadores de servicios de alojamiento que, debido a su tamaño o a la escala a la que operan, disponen de escasos recursos y conocimientos técnicos.
39. Los prestadores de servicios de alojamiento de datos deben ser invitados a adoptar las medidas necesarias para el correcto funcionamiento y la mejora de los instrumentos mencionados en el punto 38, en particular facilitando identificadores relativos a todos los contenidos considerados contenidos terroristas y aprovechando plenamente las posibilidades de estos instrumentos.
40. Las autoridades competentes y los prestadores de servicios de alojamiento de datos deben celebrar acuerdos de trabajo, también con Europol, cuando proceda, sobre asuntos relativos a los contenidos terroristas en línea, entre otras cosas para reforzar la comprensión de las actividades terroristas en línea, mejorar los mecanismos de requerimiento, evitar una innecesaria duplicación de esfuerzos, y facilitar las solicitudes de los cuerpos de seguridad a efectos de las investigaciones penales en relación con el terrorismo.

CAPÍTULO IV

SUMINISTRO DE INFORMACIÓN

41. Los Estados miembros deberán comunicar a la Comisión, a intervalos regulares, de preferencia cada tres meses, un informe sobre los requerimientos presentados por sus autoridades competentes y las decisiones adoptadas por los prestadores de servicios de alojamiento a dichos requerimientos, así como sobre su cooperación con los prestadores en la lucha contra los contenidos terroristas.
42. A fin de permitir el control de los efectos de la presente Recomendación por lo que respecta a los contenidos terroristas en el plazo máximo de tres meses a partir de la fecha de su publicación, los prestadores de servicios de alojamiento deben presentar a la Comisión, previa solicitud de esta, toda la información pertinente que permita dicho control. Esta información podrá incluir, en particular, datos sobre la cantidad de contenidos retirados, o cuyo acceso se haya bloqueado, de conformidad con las requerimientos o notificaciones o con arreglo a la adopción de medidas activas y la utilización de medios automatizados. También puede incluir el número de requerimientos recibidos y el tiempo necesario para la adopción de medidas, así como la cantidad de contenidos que se haya impedido presentar o volver a presentar a través del uso de sistemas automatizados de detección de contenidos y otros instrumentos tecnológicos.
43. A fin de permitir el control de los efectos de la presente Recomendación en lo que respecta a contenidos ilícitos distintos de los contenidos terroristas, a más tardar seis meses después de la fecha de su publicación, los Estados miembros y los prestadores de servicios de alojamiento de datos deben presentar a la Comisión, a petición de esta, toda la información pertinente que permita dicho control.

Hecho en Bruselas, el 1.3.2018

Por la Comisión
Miembro de la Comisión