COMISIÓN
EUROPEA

Bruselas, 14.2.2024
COM(2024) 64 final

INFORME DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

relativo al Reglamento (UE) 2021/784 sobre la lucha contra la difusión de contenidos terroristas en línea

{SWD(2024) 36 final}

1. RESUMEN

El Reglamento (UE) 2021/784 sobre la lucha contra la difusión de contenidos terroristas en línea establece el marco jurídico a escala europea para que los Estados miembros protejan a los ciudadanos de la exposición a material terrorista en línea. El Reglamento tiene por objetivo garantizar el correcto funcionamiento del mercado único digital mediante la lucha contra el uso indebido de los servicios de alojamiento de datos para la difusión entre el público de contenidos terroristas en línea. Con él se aspira a evitar que los terroristas se valgan de internet para propagar sus mensajes con el fin de intimidar, radicalizar, reclutar y facilitar ataques terroristas. Esto es especialmente pertinente en el contexto actual de conflicto e inestabilidad, que repercute en la seguridad de Europa. La guerra de agresión de Rusia contra Ucrania y el ataque terrorista perpetrado por Hamás contra Israel el 7 de octubre de 2023 dieron pie a un aumento de la difusión de contenidos terroristas en línea.

El marco regulador para hacer frente a los contenidos ilícitos en línea se reforzó aún más con la entrada en vigor de la Ley de Servicios Digitales el 16 de noviembre de 2022. La Ley de Servicios Digitales regula las obligaciones de los servicios digitales que actúan como intermediarios en su función de conectar a los consumidores con contenidos, servicios y bienes, protegiendo así mejor a los usuarios en línea y contribuyendo a un entorno en línea más seguro.

El Reglamento sobre la lucha contra la difusión de contenidos terroristas en línea entró en vigor el 7 de junio de 2022. De conformidad con el artículo 22 del Reglamento, la Comisión presentará un informe al Parlamento Europeo y al Consejo sobre la aplicación del Reglamento (en lo sucesivo, «Informe de aplicación»).

El presente Informe de aplicación se basa en la evaluación de la información facilitada por los Estados miembros, Europol y los prestadores de servicios de alojamiento de datos de conformidad con las obligaciones previstas en el Reglamento. Sobre la base de dicha evaluación, las principales conclusiones relativas a la aplicación del Reglamento pueden resumirse como sigue:

- A partir del 31 de diciembre de 2023, **veintitrés Estados miembros** han designado una o varias autoridades con la facultad de emitir órdenes de retirada con arreglo a lo dispuesto en el Reglamento[1]. La lista de autoridades de los Estados miembros está disponible en el sitio web de la Comisión y se actualiza periódicamente[2].

- A 31 de diciembre de 2023, la Comisión había recibido información sobre al menos 349 **órdenes de retirada de contenidos terroristas** dictadas por las autoridades competentes de seis Estados miembros (España, Rumanía, Francia, Alemania, Chequia y Austria) que, en la mayoría de los casos, condujeron a que los prestadores de servicios de alojamiento de datos respondieran rápidamente adoptando medidas para retirar o bloquear el acceso a los contenidos terroristas. Esto demuestra que las herramientas proporcionadas por el

[1] En el registro en línea, creado por la Comisión de conformidad con el artículo 12, apartado 4, del Reglamento, figuran las autoridades competentes a que se refiere el artículo 12, apartado 1, y el punto de contacto designado o establecido con arreglo al artículo 12, apartado 2, para cada una de ellas. Se actualiza regularmente a raíz de las notificaciones recibidas de los Estados miembros. Lista de autoridades nacionales competentes y puntos de contacto (europa.eu).
[2] Lista de autoridades nacionales competentes y puntos de contacto.

Reglamento ya empiezan a utilizarse y logran garantizar la rápida retirada de los contenidos terroristas por parte de los prestadores de servicios de alojamiento de datos, de conformidad con el artículo 3, apartado 3. Según la información recibida por la Comisión, estas órdenes de retirada no han sido impugnadas.

- **Existe una buena coordinación** entre las autoridades competentes de los Estados miembros y Europol, en particular la Unidad de Notificación de Contenidos de Internet (UNCI) de Europol, en la aplicación del Reglamento, especialmente en el tratamiento de las órdenes de retirada.
- La herramienta de Europol «**PERCI**»[3] entró en funcionamiento el 3 de julio de 2023. Algunos Estados miembros la han utilizado satisfactoriamente para transmitir tanto órdenes de retirada como requerimientos[4]. Las autoridades competentes españolas, alemanas, austríacas, francesas y checas se valieron de la herramienta para transmitir órdenes de retirada. En total, se tramitaron al menos 14 615 requerimientos en PERCI entre su puesta en marcha el 3 de julio y el 31 de diciembre de 2023.
- Si bien el Reglamento no contiene ninguna medida concreta sobre los requerimientos, según la información recibida por la Comisión, también se ha producido un **aumento de la capacidad de respuesta a los requerimientos** por parte de los prestadores de servicios de alojamiento de datos desde el inicio de la aplicación del Reglamento.
- Atendiendo a la información que obra en poder de la Comisión, a 31 de diciembre de 2023 no se había determinado que ningún prestador de servicios de alojamiento de datos estuviera expuesto a contenidos terroristas, tal como se define en el artículo 5, apartado 4, del Reglamento. Esta determinación es un requisito previo para la aplicación de las medidas específicas descritas en dicho artículo. No obstante, según los informes de transparencia presentados por los prestadores de servicios de alojamiento de datos, estos han adoptado medidas para **luchar contra el uso indebido de sus servicios** para la difusión de contenidos terroristas, en particular mediante la adopción de términos y condiciones específicos y la aplicación de otras disposiciones y medidas para limitar la difusión de contenidos terroristas.
- Los prestadores de servicios de alojamiento de datos también han adoptado medidas para la notificación de **amenazas inminentes para la vida**, de conformidad con el artículo 14, apartado 5, del Reglamento.

Por lo que se refiere a los **prestadores de servicios de alojamiento de datos más pequeños**, la Comisión puso en marcha en 2021 una convocatoria de propuestas para ayudarlos a aplicar el Reglamento. La Comisión adjudicó en 2022 tres proyectos (véase la sección 4.8) que comenzaron

[3] PERCI (Plateforme Européenne de Retraits des Contenus illégaux sur Internet) es una plataforma para la retirada de contenidos ilícitos en línea desarrollada y administrada por Europol. Contribuye a la aplicación del Reglamento proporcionando una solución técnica para el tratamiento de requerimientos y órdenes de retirada dirigidos a los prestadores de servicios de alojamiento de datos, entre otras funcionalidades.

[4] Los requerimientos constituyen un mecanismo para alertar a los prestadores de servicios de alojamiento de datos para que tomen voluntariamente en consideración la compatibilidad de un contenido dado con sus términos y condiciones. El Reglamento (considerando 40) afirma que los requerimientos han demostrado ser eficaces y deben seguir estando disponibles junto con las órdenes de retirada.

sus trabajos en 2023 y que ya han dado algunos resultados en la prestación de apoyo a las pequeñas empresas para que cumplan el Reglamento.

La Comisión incoó procedimientos de infracción contra veintidós Estados miembros por no haber designado autoridades competentes con arreglo al artículo 12, apartado 1, del Reglamento y por incumplimiento de las obligaciones que les incumben en virtud del artículo 12, apartados 2 y 3, y del artículo 18, apartado 1, mediante el envío de **cartas de emplazamiento** el 26 de enero de 2023[5]. Tras el inicio de estos procedimientos de infracción, aumentó el número de Estados miembros que notificaron las autoridades competentes responsables de tramitar las órdenes de retirada, tal como se refleja en la información publicada en el registro en línea[6]. Además, once de los expedientes de infracción abiertos en enero de 2023 se habían archivado a 21 de diciembre de 2023[7].

Sobre la base de la información remitida por los Estados miembros y Europol y facilitada por los prestadores de servicios de alojamiento de datos, la Comisión consideró que la aplicación del Reglamento ha tenido un **efecto positivo** a la hora de limitar la difusión de contenidos terroristas en línea.

2. CONTEXTO

El Reglamento empezó a aplicarse el 7 de junio de 2022. Tiene por objetivo garantizar el correcto funcionamiento del mercado único digital mediante la lucha contra el uso indebido de los servicios de alojamiento de datos para la difusión entre el público de contenidos terroristas en línea. Proporciona a los Estados miembros herramientas específicas, en forma de órdenes de retirada, para hacer frente a la difusión de contenidos terroristas en línea y les permite solicitar a los prestadores de servicios de alojamiento de datos de todos los tamaños que adopten medidas específicas para proteger sus servicios de la explotación de los mismos por parte de agentes terroristas cuando estén expuestos a contenidos terroristas.

Además, con la entrada en vigor de la Ley de Servicios Digitales el 16 de noviembre de 2022, el panorama normativo se amplía mediante legislación horizontal con un amplio ámbito de aplicación destinado a garantizar un espacio digital más seguro para los consumidores, medidas eficaces para luchar contra los contenidos ilícitos y unas condiciones de servicio más transparentes. La Ley de Servicios Digitales dota a la Comisión de amplias competencias de supervisión, investigación y ejecución para adoptar medidas dirigidas a las plataformas en línea y los motores de búsqueda de muy gran tamaño. Estas medidas incluyen solicitudes de información e investigaciones sobre las medidas de moderación de contenidos de las empresas con la posibilidad de imponer multas.

La Ley de Servicios Digitales permite hacer frente a todas las formas de contenidos ilícitos, lo que permite a la Comisión cuestionar a las plataformas que faciliten datos para demostrar que están cumpliendo sus propios compromisos en materia de eliminación de contenidos. Mientras que el

[5] Véase el comunicado de prensa: Contenidos terroristas en línea (europa.eu).
[6] Lista de autoridades nacionales competentes y puntos de contacto (europa.eu). El registro en línea contiene información sobre las autoridades de veintitrés Estados miembros competentes para dictar órdenes de retirada de conformidad con el artículo 12, apartado 1, letra a).
[7] Finlandia, Malta, Chequia, Dinamarca, Rumanía, Suecia, Letonia, España, Lituania, Austria y Eslovaquia.

Reglamento sobre contenidos terroristas en línea proporciona una herramienta aún más potente para esta forma específica de contenidos ilícitos, con la obligación legal de retirar contenidos en el plazo de una hora desde la recepción de una orden de retirada y mecanismos de sanción eficaces.

Como ha puesto de relieve Europol en los informes sobre la situación y las tendencias del terrorismo en Europa (informes TE-SAT)[8] publicados en los últimos años, los terroristas utilizan ampliamente internet para propagar sus mensajes con el fin de intimidar, radicalizar, reclutar y facilitar ataques terroristas. Si bien las medidas voluntarias y las recomendaciones no vinculantes sirvieron para reducir la disponibilidad de contenidos terroristas en línea, las limitaciones, en particular el escaso número de prestadores de servicios de alojamiento de datos que adoptan mecanismos voluntarios[9], así como la fragmentación de las normas de procedimiento entre los distintos Estados miembros, limitaron la eficacia y la eficiencia de la cooperación entre los Estados miembros y los prestadores de servicios de alojamiento de datos, e hicieron necesario establecer medidas reguladoras[10]. Por lo tanto, la aplicación efectiva del Reglamento es fundamental para atajar la difusión de contenidos terroristas en línea. La Comisión ha apoyado proactivamente a las autoridades nacionales competentes en este proceso.

De conformidad con el artículo 22 del Reglamento, la Comisión tenía la obligación de presentar un informe sobre la aplicación del Reglamento («Informe de ejecución») al Parlamento Europeo y al Consejo a más tardar el 7 de junio de 2023, sobre la base de la información facilitada por los Estados miembros, que a su vez se basó parcialmente en la información facilitada por los prestadores de servicios de alojamiento de datos (artículo 21). El retraso en la presentación del Informe de ejecución se debe, por una parte, a la transmisión tardía a la Comisión de información clave por parte de los Estados miembros y los prestadores de servicios de alojamiento de datos. Por otra parte, se consideró importante reflejar en el informe de aplicación el uso de PERCI, que entró en funcionamiento el 3 de julio de 2023 y se ha utilizado desde entonces para la tramitación de órdenes de retirada de conformidad con el Reglamento.

El presente informe de aplicación solo pretende ofrecer una visión general basada en hechos de los aspectos pertinentes relacionados con la aplicación del Reglamento. No contiene ninguna interpretación del Reglamento y no se pronuncia sobre las interpretaciones u otras medidas adoptadas en aplicación del Reglamento.

De conformidad con el artículo 21, apartado 2, del Reglamento, la Comisión debía elaborar, a más tardar en la misma fecha (7 de junio de 2023), un programa detallado para el seguimiento de las consecuciones, los resultados y las repercusiones del Reglamento. Más concretamente, está previsto que el programa de seguimiento establezca 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. Dicho programa se establece en el documento de trabajo de

[8] Informes TE-SAT de Europol de 2023 https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_TE-SAT_2023.pdf y de 2022 https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf.

[9] Comisión Europea (2018), *Impact Assessment accompanying the Proposal for a Regulation on preventing the dissemination of terrorist content online* [«Evaluación de impacto que acompaña a la propuesta de Reglamento para la prevención de la difusión de contenidos terroristas en línea», documento en inglés] [SWD(2018) 408 final], consultada el 4.5.2023 en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:408:FIN

[10] Ibidem.

los servicios de la Comisión adjunto. Especifica las medidas 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 las repercusiones del Reglamento y realizar una evaluación del mismo con arreglo a su artículo 23.

3. OBJETIVO Y METODOLOGÍA DEL INFORME

El objetivo del presente informe es evaluar la aplicación del Reglamento y su repercusión hasta la fecha a la hora de limitar la difusión de contenidos terroristas en línea. Esto incluye las medidas adoptadas por los Estados miembros y los prestadores de servicios de alojamiento de datos, como modificaciones de sus términos y condiciones de servicio y directrices comunitarias, así como su cumplimiento y capacidad de respuesta a las órdenes de retirada.

Con este fin, la Comisión recabó información de los Estados miembros, la Unidad de Notificación de Contenidos de Internet (UNCI) de Europol y los prestadores de servicios de alojamiento de datos, en particular la información recogida en los informes de transparencia y seguimiento con arreglo a los artículos 7, 8 y 21 del Reglamento. Se recibió información con arreglo a los artículos 8 y 21 de dieciocho Estados miembros. La información sobre las medidas adoptadas por los prestadores de servicios de alojamiento de datos se recopiló a través de sus informes anuales de transparencia y de Europol, así como mediante la comunicación voluntaria directa con los servicios de la Comisión. El presente Informe de aplicación incluye la información recibida por la Comisión hasta el 31 de diciembre de 2023.

Obligaciones de seguimiento y transparencia (artículos 21, 7 y 8)

Para la elaboración del informe de aplicación, de conformidad con el artículo 21, apartado 1, del Reglamento, los Estados miembros están obligados a recabar información de sus autoridades competentes y de los prestadores de servicios de alojamiento de datos que estén bajo su jurisdicción información y a enviarla a la Comisión a más tardar el 31 de marzo de cada año. Esto incluye información sobre las medidas que hayan adoptado de conformidad con el Reglamento en el año civil anterior. El artículo 21, apartado 1, menciona al tipo de información que los Estados miembros deben recabar sobre las medidas adoptadas para cumplir el Reglamento, como, por ejemplo, información detallada sobre las órdenes de retirada o el número de solicitudes de acceso a contenidos conservados para permitir investigaciones, procedimientos de denuncia y procedimientos de control administrativos o judiciales.

De conformidad con el artículo 7, apartado 1, del Reglamento, los prestadores de servicios de alojamiento de datos han de establecer claramente en sus términos y condiciones su política destinada a luchar contra la difusión de contenidos terroristas, incluida, en su caso, una explicación significativo del funcionamiento de las medidas específicas.

Además, con arreglo al artículo 7, apartado 2, del Reglamento, 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 Reglamento en un año natural determinado deberá publicar un informe de transparencia sobre las medidas de ese año. Dicho informe debe publicarse antes del 1 de marzo del año siguiente.

El artículo 7, apartado 3, del Reglamento establece la información mínima que estos informes de transparencia deben incluir, como las medidas adoptadas para la detección de contenidos terroristas y el bloqueo del acceso a estos, el número de elementos retirados o restablecidos y el resultado de las reclamaciones.

De acuerdo con lo dispuesto en el artículo 8 del Reglamento, las autoridades competentes designadas por los Estados miembros han de publicar informes anuales de transparencia sobre las actividades realizadas con arreglo al Reglamento. El artículo 8, apartado 1, hace referencia a la información mínima que deben incluir estos informes[11].

A 31 de diciembre de 2023, dieciocho Estados miembros habían enviado información a la Comisión sobre las medidas adoptadas de conformidad con el Reglamento, mientras que veintitrés Estados miembros habían designado una autoridad o autoridades con la facultad de dictar órdenes de retirada con arreglo a lo dispuesto en el Reglamento.

4. PUNTOS ESPECÍFICOS DE LA EVALUACIÓN

4.1. ÓRDENES DE RETIRADA (artículo 3)

En total, a 31 de diciembre de 2023, la Comisión había sido informada de, al menos, 349 órdenes de retirada remitidas a Telegram, Meta, Justpaste.it, TikTok, DATA ROOM S.R.L., FLOKINET S.R.L., Archive.org, Soundcloud, X, Jumpshare.com, Krakenfiles.com, Top4Top.net y Catbox por las autoridades competentes de España, Rumanía, Francia, Alemania, Austria y Chequia.

La autoridad competente española (Centro de Inteligencia contra el Terrorismo y el Crimen Organizado, CITCO) ha enviado sesenta y dos órdenes de retirada, mientras que la autoridad competente rumana (Autoritatea Națională pentru Administrare și Reglementare în Comunicații, ANCOM) envió dos órdenes de retirada y la autoridad competente francesa (Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, OCLCTIC) envió veintiséis órdenes de retirada. Desde el atentado terrorista perpetrado por Hamás contra Israel, la autoridad alemana competente (Bundeskriminalamt, BKA) ha enviado 249 órdenes de retirada.

La autoridad competente española ha transmitido sesenta y dos órdenes de retirada: dieciocho antes de la puesta en marcha de PERCI y cuarenta y cuatro a través de PERCI Proporcionó una descripción detallada de la transmisión de las primeras órdenes de retirada dictadas y del curso dado a estas, algo muy importante para comprender mejor las implicaciones y efectos del Reglamento.

Las dos primeras órdenes de retirada fueron dictadas por la autoridad competente española el 24 de abril de 2023[12] en relación con dos contenidos terroristas, uno vinculado al terrorismo de derechas y otro al yihadismo. El contenido que fue objeto de la primera orden de retirada era un documento PDF publicado en Telegram con acceso ilimitado, que abogaba por la violencia

[11] Véase el texto del Reglamento (UE) 2021/784, artículo 8, apartado 1: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32021R0784.

[12] Ministerio del Interior | El CITCO culmina la retirada de Internet de dos contenidos que alentaban al terrorismo

terrorista y hacía apología de los ataques terroristas de derechas. El contenido terrorista objeto de la segunda orden de retirada era un vídeo cargado en Internet Archive con imágenes de yihadistas de la organización terrorista conocida como Estado Islámico en situación de combate. Los dos contenidos se retiraron de ambas plataformas en menos de una hora, en cumplimiento de lo dispuesto en el artículo 3, apartado 3, del Reglamento. En la evaluación facilitada por la autoridad competente española se explicó que se había optado por una orden de retirada en lugar de un requerimiento por dos razones principales: cumplimiento de los requisitos del Reglamento sobre órdenes de retirada y emergencia. A continuación, la autoridad competente española envió nuevas órdenes de retirada.

Las autoridades españolas destacaron los retos relacionados con el uso de un formulario web por parte de un prestador de servicios de alojamiento de datos (Meta) para recibir órdenes de retirada en lugar de proporcionar un punto de contacto directo. Este formulario web también dio lugar a problemas de comunicación con la autoridad competente del Estado miembro en el que está situado el establecimiento principal del prestador de servicios de alojamiento de datos.

La autoridad competente francesa dictó su primera orden de retirada el 13 de julio de 2023 dirigida a una plataforma para compartir texto e imágenes (Justpaste.it), que retiró los contenidos terroristas en el plazo de una hora. El contenido perseguido era propaganda de Al Qaeda, más concretamente de su órgano de prensa Rikan Ka Mimber, procedente de su sucursal india Al Qaeda del Subcontinente Indio. La retirada completa del contenido se confirmó en la plataforma PERCI de Europol.

La autoridad alemana competente dictó seis, dieciséis y cinco órdenes de retirada el 16, el 18 y el 24 de octubre de 2023, respectivamente, contra propaganda de Hamás y de la Yihad Islámica Palestina. El acceso a los contenidos fue bloqueado en la UE de conformidad con el artículo 3, apartado 3, del Reglamento. La autoridad alemana competente había remitido en primer lugar requerimientos y, posteriormente, había dictado órdenes de retirada, ya que no se dio curso a dichos requerimientos. Tras el ataque de Hamás el 7 de octubre de 2023, la autoridad alemana competente ha enviado 249 órdenes de retirada, principalmente a Telegram[13].

La autoridad checa competente y la autoridad austriaca competente dictaron 2 y 8 órdenes de retirada a X y Telegram, respectivamente.

Por lo que se refiere al uso de un formulario web para recibir las órdenes de retirada por parte de un prestador de servicios de alojamiento de datos, las autoridades españolas indicaron dos cuestiones: 1) en el contexto del artículo 3, apartado 2, del Reglamento, un formulario web no permite a las autoridades competentes de los Estados miembros enviar al prestador de servicios de alojamiento de datos información sobre los procedimientos y plazos aplicables antes de dictar la primera orden de retirada; 2) en el contexto del artículo 4, apartado 1, un formulario web no permite remitir al mismo tiempo 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 y al representante legal del prestador de servicios de alojamiento de datos.

[13] Según la información que obra en poder de la Comisión.

4.2 ÓRDENES DE RETIRADA TRANSFRONTERIZAS (artículo 4)

Por lo que respecta a las dos primeras órdenes de retirada dictadas en abril de 2023, la autoridad competente española no pudo enviar copias a la autoridad del Estado miembro en el que el prestador de servicios de alojamiento de datos tenía su establecimiento principal o su representante legal, ya que ninguno de los dos prestadores de servicios de alojamiento de datos tenía en aquel momento su establecimiento principal o un representante legal en la UE. Para las órdenes de retirada posteriores, la autoridad competente española remitió copias a la autoridad competente del Estado miembro en el que el prestador de servicios de alojamiento de datos tenía su establecimiento principal o había designado a su representante legal.

Los Estados miembros señalaron que la transmisión de órdenes de retirada a los prestadores de servicios de alojamiento de datos establecidos en terceros países que aún no habían cumplido su obligación de designar una representación legal en la UE suponía un reto. En este contexto, la Comisión prestó su apoyo a los Estados miembros para garantizar que los prestadores de servicios de alojamiento de datos cumplan su obligación de designar un representante legal en la UE y de proporcionar un punto de contacto (artículo 15, apartado 1, del Reglamento), como una dirección de correo electrónico, para garantizar una actuación inmediata. Además, la Comisión ha recordado a los prestadores de servicios de alojamiento de datos sus obligaciones en distintos foros, incluido el Foro de la UE sobre Internet.

Según la información de que dispone la Comisión, hasta la fecha ninguna autoridad competente del Estado miembro en el que el prestador de servicios de alojamiento de datos tenga su establecimiento principal ha examinado una orden de retirada con arreglo al artículo 4 del Reglamento para determinar si infringe o no gravemente o de forma manifiesta el Reglamento o los derechos y libertades fundamentales, ya que todavía no se ha presentado ninguna solicitud motivada de examen. En consecuencia, hasta la fecha, ninguna autoridad ha constatado que una orden de retirada haya infringido el Reglamento o los derechos fundamentales de esa manera.

Ningún prestador de servicios de alojamiento de datos ha restablecido hasta la fecha los contenidos (ni ha reactivado el acceso a ellos) que hubieran sido objeto de una orden de retirada en virtud del examen de conformidad con el artículo 4 del Reglamento, ya que dicho examen y las solicitudes de restablecimiento aún no han tenido lugar. Por lo tanto, no se dispone de información sobre cuánto tiempo se tarda normalmente en restablecer los contenidos o reactivar el acceso a ellos, ni sobre las «medidas necesarias» adoptadas por los prestadores de servicios de alojamiento de datos para restablecer el contenido o reactivar el acceso a los contenidos.

4.3. TUTELA JUDICIAL (artículo 9)

Según la información de que dispone la Comisión, los prestadores de servicios de alojamiento de datos no han impugnado hasta la fecha las órdenes de retirada o las decisiones de retirada con arreglo al artículo 5, apartado 4, ante los órganos jurisdiccionales pertinentes. No obstante, un prestador de servicios de alojamiento de datos alegó la imposibilidad de ejecutar una orden de retirada.

De acuerdo con la información facilitada por los Estados miembros[14], al menos doce Estados miembros disponen de «procedimientos efectivos» para que los prestadores de servicios de alojamiento de datos y los proveedores de contenidos puedan impugnar una orden de retirada dictada o una decisión adoptada con arreglo al artículo 4, apartado 4, o al artículo 5, apartados 4, 6 o 7, ante los órganos jurisdiccionales de la autoridad competente de dichos Estados miembros (artículo 9, apartados 1 y 2). En los Estados miembros en los que existen esta clase de procedimientos, se trata principalmente de demandas. Sin embargo, no es posible determinar si estos procedimientos son «efectivos» o específicos del Reglamento con los datos actuales aportados por los Estados miembros, ya que hasta la fecha no se ha impugnado ninguna decisión.

4.4. MEDIDAS ESPECÍFICAS Y TRANSPARENCIA ASOCIADA (artículos 5 y 7)

Según la información disponible, hasta la fecha ningún prestador de servicios de alojamiento de datos ha sido considerado expuesto a contenidos terroristas en el sentido del artículo 5, apartado 4, del Reglamento. En consecuencia, el requisito de adoptar las medidas específicas establecidas en dicho artículo (aún) no se aplica a ningún prestador de servicios de alojamiento de datos.

No obstante, cabe señalar que, según los informes de transparencia presentados por los prestadores de servicios de alojamiento de datos, varios de ellos han adoptado medidas para luchar contra el uso indebido de sus servicios para la difusión de contenidos terroristas, en particular la adopción de términos y condiciones específicos y la aplicación de otras disposiciones y medidas para limitar la difusión de contenidos terroristas. Como se ha señalado anteriormente, de conformidad con el artículo 7, los prestadores de servicios de alojamiento de datos deben garantizar la transparencia a este respecto no solo mediante la presentación de informes de transparencia, sino también mediante la inclusión de información clara en sus términos y condiciones.

4.5. AMENAZA INMINENTE PARA LA VIDA (artículo 14, apartado 5)

De conformidad con el artículo 14, apartado 5, del Reglamento, 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 no sea posible identificar a los Estados miembros afectados, el prestador de servicios de alojamiento de datos transmitirá la información a Europol para que se le dé el curso adecuado.

A 31 de diciembre de 2023, la Comisión había sido informada de nueve casos en los que la Unidad de Notificación de Contenidos de Internet de la UE de Europol había recibido información sobre contenidos terroristas que conllevan una amenaza inminente para la vida. Dado que el artículo 14, apartado 5, del Reglamento no establece la obligación de informar a Europol en todos los supuestos, el número de notificaciones podría ser mayor. El único Estado miembro que facilitó información sobre la aplicación del artículo 14, apartado 5, fue España. El 18 de abril de 2023, las autoridades españolas recibieron una comunicación de Amazon sobre un supuesto contenido

[14] Cabe señalar que la información facilitada no es necesariamente completa. Sería necesario realizar más evaluaciones para obtener una visión completa y totalmente actualizada de la manera en que los Estados miembros han dado cumplimiento al requisito de garantizar la disponibilidad de procedimientos de recurso eficaces.

terrorista que conllevaba una amenaza inminente para la vida en la plataforma de videojuegos Twitch. Se determinó que el contenido no reunía las condiciones aplicables a los contenidos terroristas que conllevan una amenaza inminente para la vida en el sentido del Reglamento.

4.6. COOPERACIÓN ENTRE LOS PRESTADORES DE SERVICIOS DE ALOJAMIENTO DE DATOS, LAS AUTORIDADES COMPETENTES Y EUROPOL (artículo 14)

Como ya se ha mencionado anteriormente, Europol ha desarrollado una plataforma denominada «PERCI» para apoyar la aplicación del Reglamento centralizando, coordinando y facilitando la **transmisión de órdenes de retirada y requerimientos** por parte de los Estados miembros a los prestadores de servicios de alojamiento de datos. La plataforma está operativa desde el 3 de julio de 2023. Antes de la plena implantación de PERCI, Europol había establecido mecanismos de contingencia para propiciar la transmisión manual de órdenes de retirada, la prevención de conflictos en relación con contenidos para evitar interferencias en las investigaciones en curso y la respuesta a crisis en situaciones de «amenaza inminente para la vida».

PERCI es un sistema único que permite la cooperación entre las autoridades competentes, los prestadores de servicios de alojamiento de datos y Europol, tal como se prevé en el artículo 14 del Reglamento, en lo que respecta a las cuestiones reguladas por el Reglamento. Más concretamente, PERCI:

- es una solución basada en la nube diseñada para garantizar la seguridad y la protección de datos en la nube;
- es una plataforma única para la comunicación y la coordinación colaborativas y en tiempo real, que apoya la rápida retirada de los contenidos terroristas;
- facilita el proceso de examen de las órdenes de retirada transfronterizas;
- refuerza la prevención de conflictos, aspecto importante para evitar que la autoridad competente de un Estado miembro envíe una orden de retirada dirigida contra contenidos sujetos a una investigación en curso en otro Estado miembro;
- permite que los prestadores de servicios de alojamiento de datos reciban las órdenes de retirada de manera unificada y normalizada desde un único canal.

De manera independiente, PERCI también permite la transmisión de requerimientos.

En la actualidad, aparte de su importancia en relación con los requerimientos (véase el considerando 40 del Reglamento), PERCI facilita la transmisión de órdenes de retirada (artículos 3 y 4), la coordinación y la presentación de informes de los Estados miembros (artículo 8), así como la prevención de conflictos en caso de colisión con investigaciones en curso sobre el contenido respecto del que se pretende dictar una orden de retirada (artículo 14). Se están introduciendo

mejoras en PERCI para incorporar tareas adicionales derivadas del Reglamento, como el examen de las órdenes de retirada transfronterizas (artículo 4)[15].

Los Estados miembros confirmaron que, de conformidad con el artículo 14 del Reglamento:

- las autoridades competentes intercambian información, se coordinan y cooperan con otras autoridades competentes;
- las autoridades competentes intercambian información, se coordinan y cooperan con Europol;
- existen mecanismos para mejorar la cooperación, evitando al mismo tiempo interferir con las investigaciones que se produzcan en otros Estados miembros;
- la mayoría de los Estados miembros consideran a PERCI como la herramienta predilecta para la transmisión de órdenes de retirada, ya que permite coordinar las actuaciones mediante la prevención de conflictos.

4.7. EFECTOS EN LOS REQUERIMIENTOS

Los requerimientos de contenidos terroristas son una herramienta voluntaria que ya se utilizaba antes de la adopción del Reglamento. Si bien el Reglamento no contiene normas particulares sobre los requerimientos, de conformidad con su considerando 40, nada en el Reglamento impide a los Estados miembros y a Europol utilizar los requerimientos como instrumento para luchar contra los contenidos terroristas en línea.

Desde su creación en 2015, la Unidad de Notificación de Contenidos de Internet de la UE de Europol ha participado activamente en la detección de contenidos terroristas en línea y en la remisión de alertas a los prestadores de servicios de alojamiento de datos, así como en el desarrollo de herramientas (por ejemplo, PERCI y anteriormente IRMA[16]) para facilitar la transmisión de los requerimientos.

Según la información facilitada a la Comisión, las autoridades de los Estados miembros siguen utilizando requerimientos con determinados prestadores de servicios de alojamiento de datos, aunque podrían considerar la posibilidad de dictar órdenes de retirada dirigidas a los prestadores

[15] En particular: - artículos 3 y 4: Transmisión de órdenes de retirada; — Artículo 3, apartados 6 a 8: observaciones de los prestadores de servicios de alojamiento de datos; — Artículo 4, apartado 3 a 7: sistema de examen; - artículo 7: presentación de informes; - Artículo 14, apartado 1: la eliminación de conflictos, la coordinación y la prevención de duplicaciones; Artículo 14, apartado 3: canales o mecanismos de comunicación adecuados y seguros; - artículo 14, apartado 4: uso de una herramienta específica establecida por Europol; -artículo 14, apartado 5: comunicación de «amenazas inminentes para la vida»; -considerando 40: transmisión de requerimientos.

[16] Europol desarrolló la aplicación para la gestión de la notificación de contenidos en internet (IRMA) en 2016 para favorecer la notificación (señalización) de contenidos ilícitos a los proveedores de servicios en línea. Inicialmente, se concedió acceso a IRMA al personal de Europol y a unidades especializadas de siete Estados miembros. IRMA fue sustituida por PERCI el 3 de julio de 2023.

de servicios de alojamiento de datos que no respondan a los requerimientos o por otras razones, como la urgencia de retirar el contenido.

4.8. APOYO A LOS PRESTADORES DE SERVICIOS DE ALOJAMIENTO DE DATOS MÁS PEQUEÑOS PARA LA APLICACIÓN DEL REGLAMENTO

El Reglamento contiene diversas obligaciones para los prestadores de servicios de alojamiento de datos. Si bien los grandes prestadores de servicios de alojamiento de datos suelen contar con las capacidades técnicas, la capacidad de verificación humana y los conocimientos necesarios para aplicar el Reglamento, los pequeños pueden tener unos recursos financieros, técnicos y humanos, así como unos conocimientos especializados más limitados para ello. Al mismo tiempo, cada vez es más frecuente que los prestadores de servicios de alojamiento de datos más pequeños sean objeto de ataques por parte de agentes malintencionados para explotar sus servicios. Esta situación también podría atribuirse a la eficacia de los esfuerzos de moderación de contenidos desplegados por los grandes prestadores de servicios de alojamiento de datos. Aunque esta tendencia muestra el éxito de las medidas de moderación de contenidos, también pone de relieve la necesidad de ayudar a los prestadores de servicios de alojamiento de datos más pequeños a aumentar su capacidad y sus conocimientos para cumplir los requisitos del Reglamento.

Para responder a este reto, la Comisión puso en marcha una convocatoria de propuestas en el marco del Fondo de Seguridad Interior para apoyar a los prestadores de servicios de alojamiento de datos más pequeños a aplicar el Reglamento[17]. La Comisión seleccionó tres proyectos[18] a los que apoyará con un enfoque triple. En primer lugar, informando y sensibilizando sobre las normas y los requisitos del Reglamento, en segundo lugar, desarrollando, aplicando e implantando las herramientas y los marcos necesarios para luchar contra la difusión de contenidos terroristas en línea, y, en tercer lugar, compartiendo experiencias y mejores prácticas en toda la industria.

Los tres proyectos empezaron sus trabajos en 2023 y ya han logrado resultados valiosos. Por ejemplo, en su informe de cartografía, el proyecto FRISCO[19] constató que los micro y los pequeños prestadores de servicios de alojamiento de datos tienden a tener una sensibilización y un conocimiento muy limitados del Reglamento y subrayaba las posibles dificultades a las que podrían enfrentarse para responder a las órdenes de retirada en el plazo de una hora, ya que a menudo carecen de servicios 24/7. La falta de recursos es un reto, así como el establecimiento de

[17] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/isf/wp-call/2021-2022/call-fiche_isf-2021-ag-tco_en.pdf.

[18] 1) Marco basado en la IA para apoyar a los microprestadores (y pequeños prestadores) de servicios de alojamiento de datos en la denuncia y retirada de contenidos terroristas en línea (ALLIES), 2) Lucha contra los contenidos terroristas en línea (FRISCO) y 3) Tecnología contra el terrorismo en Europa (TATE). Enlace para más información: Portal de Financiación y Licitaciones (europa.eu).

[19] Realizado a lo largo de un período de seis meses concluido en mayo de 2023. El informe se basa en los comentarios de cuarenta y ocho prestadores europeos de servicios de alojamiento de datos, treinta y tres respuestas a través de nuestra encuesta en línea y quince a través de entrevistas. FRISCO, *D2.1: Mapping Report on needs and barriers for compliance Understanding small and micro hosting service providers' needs and awareness in relation to implementing the TCO Regulation requirements* [«D2.1: Informe de situación de las necesidades y obstáculos para el cumplimiento. Percepción de las necesidades y conocimientos de los microprestadores y pequeños prestadores de servicios de alojamiento de datos en relación con la aplicación de los requisitos del Reglamento sobre la lucha contra la difusión de contenidos terroristas en línea», documento en inglés], disponible en Deliverables | Frisco (friscoproject.eu)|

líneas de comunicación con las fuerzas y cuerpos de seguridad. Más de la mitad de los prestadores de servicios de alojamiento de datos encuestados por los contratistas no moderan los contenidos generados por los usuarios y declararon que nunca se encontraron con contenidos terroristas en sus plataformas. Es probable que estos prestadores de servicios de alojamiento de datos adopten medidas *ad hoc* si dichos contenidos aparecen en sus plataformas.

A través de estos tres proyectos, los pequeños prestadores de servicios de alojamiento de datos reciben apoyo en sus esfuerzos por cumplir las normas del Reglamento también mediante la creación de puntos de contacto y la aplicación de mecanismos para las reclamaciones de los usuarios.

Además, el artículo 3, apartado 2, del Reglamento, que exige el suministro oportuno de información sobre los procedimientos y plazos aplicables a los prestadores de servicios de alojamiento de datos que no hayan sido destinatarios de una orden de retirada dictada previamente, puede ser pertinente, en particular, para los prestadores de servicios de alojamiento de datos más pequeños.

4.9. GARANTÍAS DE LOS DERECHOS FUNDAMENTALES

El Reglamento incluye diversas garantías para reforzar la rendición de cuentas y la transparencia de las medidas adoptadas para la retirada de contenidos terroristas en línea. A este respecto, se hace referencia a lo expuesto anteriormente, en particular a la información facilitada sobre las vías de recurso, la notificación y el mecanismo especial para las órdenes de retirada transfronterizas.

Además, el artículo 23 del Reglamento exige que la Comisión informe sobre 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, en el contexto de la evaluación del Reglamento. Dichas garantías se refieren a los mecanismos de reclamación, recurso y sanción adoptados y aplicados contra el riesgo de retirada errónea de contenidos terroristas en línea para proteger a los proveedores de contenidos y a los prestadores de servicios de alojamiento de datos. Por lo tanto, la evaluación del funcionamiento y la eficacia de los mecanismos de salvaguardia formará parte de la evaluación con arreglo al artículo 23.

En este sentido, en el programa de seguimiento a que se refiere el artículo 21, apartado 2, del Reglamento, se establece un marco de indicadores para la evaluación de los efectos del Reglamento en los derechos fundamentales, que se incorporará a la evaluación del Reglamento.

El programa de seguimiento contribuirá a la valoración, que se llevará a cabo como parte de la evaluación, del funcionamiento y la eficacia de los mecanismos de salvaguardia aplicados en el contexto del Reglamento, y su impacto en los derechos fundamentales. Este ámbito de impacto refleja los dos ámbitos mencionados en el artículo 23 del Reglamento: a) el funcionamiento y la eficacia de los mecanismos de salvaguardia, en particular los previstos en el artículo 4, apartado 4, el artículo 6, apartados 3 y 7 a 11; y 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.

4.10. AUTORIDADES COMPETENTES (artículo 13)

De conformidad con el artículo 13 del Reglamento, los Estados miembros deben garantizar que sus autoridades competentes tengan las facultades necesarias y los recursos suficientes para alcanzar los objetivos y cumplir las obligaciones que se derivan del Reglamento. Algunos Estados miembros han adoptado las siguientes medidas para asegurarse de que las autoridades competentes dispongan de las facultades necesarias y de recursos suficientes:

- creación de nuevos órganos o direcciones;
- asignación de financiación adicional y personal de refuerzo; y
- elaboración de nuevos marcos legislativos.

5. CONCLUSIÓN

Es de suma importancia que se apliquen plenamente todas las herramientas y medidas a escala de la UE para hacer frente rápidamente a los contenidos ilícitos difundidos en línea. Este es el caso, en particular, a la vista de la magnitud de tales contenidos ilícitos, como ha demostrado recientemente la difusión de contenidos relacionados con el ataque perpetrado por Hamás contra Israel.

El Reglamento contribuye a aumentar la seguridad pública en toda la Unión para evitar que los prestadores de servicios de alojamiento de datos que operan en el mercado interior sean utilizados por terroristas para propagar sus mensajes con el fin de intimidar, radicalizar, reclutar y facilitar ataques terroristas.

A raíz de la incoación de procedimientos de infracción en enero de 2023, **se han logrado avances**. A 31 de diciembre de 2023, veintitrés Estados miembros habían designado autoridades competentes con arreglo al artículo 12, apartado 1, tal como se refleja en el registro en línea, lo que ha dado lugar a un uso más sistemático de las medidas y herramientas previstas en el Reglamento. Además, a 21 de diciembre de 2023, se habían archivado once de los veintidós expedientes de infracción abiertos en enero de 2023. La Comisión insta a los demás Estados miembros a que adopten las medidas necesarias para designar las autoridades competentes en virtud del artículo 12, apartado 1, y cumplir las obligaciones que les incumben con arreglo al artículo 12, apartados 2 y 3, y al artículo 18, apartado 1.

En general, los Estados miembros han informado de que la transmisión de las órdenes de retirada dirigidas a los prestadores de servicios de alojamiento de datos ha sido fluida gracias al apoyo de Europol. Atendiendo a la información recibida de los Estados miembros y de Europol, se han transmitido al menos 349 **órdenes de retirada de contenidos terroristas** desde que empezó a aplicarse el Reglamento. En diez casos, la retirada de los contenidos terroristas o el bloqueo del acceso a estos por parte de un prestador de servicios de alojamiento de datos no se produjeron en el plazo máximo de una hora establecido por el Reglamento.

Según la información enviada por los Estados miembros y Europol, a pesar de que el Reglamento no contiene ninguna norma a este respecto, desde la fecha de inicio de la aplicación del Reglamento se ha incrementado la capacidad de respuesta ante los requerimientos de contenidos terroristas.

Además, Europol recibió en nueve casos información de prestadores de servicios de alojamiento de datos sobre contenidos terroristas que conllevaban una amenaza inminente para la vida, de conformidad con el artículo 14, apartado 5.

Existen canales y procedimientos de comunicación más eficientes, especialmente desde la puesta en marcha de la plataforma PERCI el 3 de julio de 2023, lo que dio lugar a un enfoque más sistemático de la transmisión de órdenes de retirada, al tiempo que PERCI también se utiliza para transmitir un elevado número de requerimientos. Los Estados miembros y Europol expresaron la expectativa de que el despliegue de PERCI beneficiará el uso de estos instrumentos para luchar contra los contenidos terroristas en línea.

Por todo ello, la Comisión considera que, en general, el Reglamento ha tenido un **efecto positivo** a la hora de limitar la difusión de contenidos terroristas en línea. No obstante, en diez de 349 casos, el prestador de servicios de alojamiento de datos destinatario superó el plazo máximo de una hora establecido en el Reglamento para retirar los contenidos terroristas o bloquear el acceso a ellos.

La Comisión apoya proactivamente a los Estados miembros y a los prestadores de servicios de alojamiento de datos, en particular mediante talleres técnicos organizados antes y después de la fecha de inicio de la aplicación del Reglamento. El último tuvo lugar el 24 de noviembre de 2023. La Comisión también ofrece apoyo a los prestadores de servicios de alojamiento de datos más pequeños para garantizar la plena y rápida aplicación del Reglamento y ayudarles a hacer frente a los retos encontrados hasta la fecha.

La Comisión seguirá supervisando la ejecución y la aplicación del Reglamento. La Comisión seguirá de cerca los resultados de los instrumentos previstos en el Reglamento a través del programa de seguimiento, que se incorporará a la evaluación del Reglamento de conformidad con el artículo 23.