Capítulo 8

Órdenes europeas de retirada de contenidos terroristas en línea. [Análisis del nuevo instrumento introducido por el reglamento (UE) 2021/784][1]

Coral Arangüena Fanego

Catedrática de Derecho Procesal
Universidad de Valladolid

I. INTRODUCCIÓN. LA NECESIDAD DE COMBATIR LA DIFUSIÓN EN LÍNEA DE CONTENIDOS TERRORISTAS

Los actos terroristas constituyen una de las violaciones más graves de los valores universales de la dignidad humana, la libertad, la igualdad y la solidaridad, y el disfrute de los derechos humanos y de las libertades fundamentales, en los que se basa la Unión Europea. También representan uno de los ataques más graves contra la democracia y el Estado de Derecho, principios que son comunes a los Estados miembros y en los que se fundamenta la Unión. Se trata de una realidad que describe con estas precisas palabras el Considerando 2 de la Directiva (UE) 2017/541, relativa a la lucha contra el terrorismo[2].

1. Trabajo realizado en el marco del proyecto de investigación "Proceso Penal y Unión Europea. Aná-lisis y propuestas. PID2020-116848GB-I00" (Plan nacional I+D+i. Ministerio de Ciencia e Innovación).

2. 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).

Las medidas que pueden adoptarse para combatirlo, muy variadas y cada vez más sofisticadas[3], gravitan sobre el delicado equilibrio que se ha de mantener entre dos intereses cruciales que ha de salvaguardar todo Estado democrático de Derecho: de un lado, la política de seguridad pública, encaminada a lograr la mejor prevención y represión de las conductas delictivas y, de otro, el debido respeto de los derechos y libertades de los ciudadanos[4]. En estas páginas nos ocuparemos de una de las más recientes que han comenzado a funcionar en la Unión Europea: las órdenes de retirada de contenidos terroristas en línea, introducidas por el Reglamento (UE) 2021/784, de 29 de abril de 2021, que ha entrado en vigor el 7 de junio de 2022[5].

La justificación de la creación de este nuevo mecanismo reside en la necesidad de atajar la propagación del mensaje terrorista, dada la facilidad con que se difunde en las redes. Advierte Velasco Núñez del crecimiento exponencial en los últimos años y en todo tipo de terrorismo de la elección de Internet como medio no sólo de informarse de objetivos, sino de reclutar acólitos y de planear ataques, habiéndose acuñado el término de la "yihad mediática" para el más mortífero que, desde diversos frentes y con carácter transnacional, sirve para la activación de métodos violentos[6]. Y añade Bustos Gisbert que el carácter global y descentralizado de Internet, sin un centro único de control, polifacético en las distintas formas de comunicación que permite, y donde reina la espontaneidad y el anonimato, han facilitado que Internet no sea sólo el reino del pluralismo (que lo es); sino que sea también el reino del radicalismo más brutal, agresivo e irrespetuoso de los más mínimos valores de convivencia. Un caldo

3. *Vid.* SANZ HERMIDA, A. "Garantismo y seguridad en el Estado de Derecho en la lucha (preventiva) contra la delincuencia organizada", en Garrido Carrillo (director), *Retos en la lucha contra la delincuencia organizada* (F. J. Garrido Carrillo, director), Aranzadi 2021, pp. 23-47.
4. ARNÁIZ SERRANO, A., "La articulación del derecho de defensa en la adopción de medidas cautelares de naturaleza personal en los delitos de terrorismo en el ordenamiento jurídico español", *Estudios Penales y Criminológicos*, vol. XXXVI (2016), pp. 493-494.
5. Reglamento (UE) 2021/7884 del Parlamento Europeo y del Consejo, de 29 de abril de 2021 sobre la lucha contra la difusión de contenidos terroristas en línea (DO L 172/79, de 17.5.2021).
6. VELASCO NÚÑEZ, E. *Delincuencia informática* (con Sanchís Crespo, C.), Tirant lo Blanch, Valencia, 2019, p. 27. Sobre Internet como facilitador de los procesos de radicalización y difusión del terrorismo *vid*., asimismo, MIRO LLINARES, F., "La detección del discurso radical en Internet. Aproximación, encuadre y propuesta de mejora de los análisis de Big Data desde un enfoque de Smart Data criminológico", en Alonso Rimo, A., Cuerda Arnau, M.L. y Fernández Hernández, A., *Terrorismo, sistema penal y derechos fundamentales*, Ed. Tirant lo Blanch, Valencia, 2018, pp. 626 a 632, especialmente.

de cultivo perfecto para las organizaciones terroristas[7] que han sabido explotar una vez más con versatilidad las herramientas disponibles en cada época[8].

Los contenidos terroristas compartidos en línea con fines de reclutar a seguidores y prepararlos, para planear y facilitar actividades terroristas, para glorificar sus atrocidades y para animar a otros a seguir ese ejemplo e insuflar el miedo en la opinión pública se difunden a través de prestadores de servicios de alojamiento de datos que permiten subir contenidos de terceros. Esos contenidos se han revelado como esenciales para la radicalización y para incentivar acciones por parte de los llamados «lobos solitarios», como las producidas en varios ataques terroristas recientes en Europa. Dichos contenidos no solo tienen repercusiones negativas importantes para las personas y la sociedad en general, sino que también reducen la confianza de los usuarios en Internet y menoscaban los modelos de negocio y la reputación de las empresas afectadas[9].

El Reglamento constituye el punto de llegada de un camino emprendido en 2015 por la Unión Europea[10] para combatir la difusión de los contenidos terroristas en línea con la creación del Foro de Internet de la Unión Europea[11] y de la Unidad de Notificación de Contenidos de Internet de Europol en el seno del Centro Europeo de Lucha contra el Terrorismo[12]. De un marco de cooperación voluntaria entre Estados miembros

7. BUSTOS GISBERT, R., "Libertad de expresión y control de la Red", en *Terrorismo y Derecho bajo la estela del 11 de septiembre* (Revenga Sánchez, editor), Tirant lo Blanch, Valencia, 2014, p. 166.
8. Así lo indica MONTES NOBLEJAS, D., "A vueltas con el terrorismo e internet: hacia una definición de ciberterrorismo", *Revista de Derecho UNED*, núm. 27, 2021, pp. 719 y 710.
9. Exposición de Motivos de la inicial *Propuesta de Reglamento del Parlamento Europeo y del Consejo para la prevención de la difusión de contenidos terroristas en línea*, COM (2018) 640 final, de 12.9.2018.
10. La página del Consejo de la Unión Europea ofrece una visión panorámica de la cronología seguida en esta materia en la UE (https:// https://www.consilium.europa.eu/es/policies/fight-against-terrorism/history-fight-against-terrorism/).
11. Foro que reúne cada año a representantes de los gobiernos de los Estados miembros, Europol y empresas de tecnología para coordinarse y combatir el contenido terrorista y el discurso del odio. Este Foro ha promovido la creación de una base de más de 200.00 hashes que sirve para evitar que los vídeos o fotografías ya etiquetados como contenido terrorista puedan volver a compartirse. *Vid*. Comisión Europea, *EU Internet Forum: Bringing together governments, Europol and technology companies to counter terrorist content and hate speech online,* Press release, Brussels, 3.12.2015, disponible en https:// https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6243. Última consulta, 30.09.2022.
12. European Union Referral Unit, (EU IRU) creada en julio de 2015 con el objetivo de detectar los contenidos extremistas terroristas y violentos en línea, frenar las

y prestadores de servicios de alojamiento de datos inaugurado en 2017 con la Comunicación de la Comisión "Hacia una mayor responsabilización de las plataformas en línea"[13], reforzado por la posterior Recomendación (UE) 2018/334 sobre "medidas para combatir eficazmente los contenidos ilícitos en línea"[14] y, por tanto, *soft law* se ha pasado a otro más riguroso (*hard law*) por medio de una norma de máximo nivel (Reglamento) de alcance general, obligatoria en todos sus elementos y directamente aplicable.

Solución legislativa justificada en la necesidad de establecer un marco jurídico claro y armonizado que evite el uso indebido de los servicios de alojamiento de datos para la difusión de contenidos terroristas en línea, con el fin de garantizar el correcto funcionamiento del mercado único digital y, al mismo tiempo, velar por la confianza y la seguridad. El Reglamento es directamente aplicable, ofrece claridad y mayor seguridad jurídica, y evita las interpretaciones divergentes en los Estados miembros y otros problemas de transposición que plantean otras normas europeas, como la Directiva, instrumento que se había empleado con anterioridad pero que en este ámbito (el de la lucha contra los contenidos terroristas en línea) no había dado los resultados esperados[15].

Dado que la norma europea contiene obligaciones impuestas a prestadores de servicios que habitualmente ofrecen sus servicios en más de un Estado miembro, las divergencias en la aplicación de sus disposiciones podrían dificultar la prestación de servicios por parte de los prestadores que ejercen su actividad en múltiples Estados miembros.

De aquí se explica que la base jurídica que lo sostiene sea el art. 114 del Tratado de Funcionamiento de la Unión Europea, que permite la

---

campañas de reclutamiento y enaltecimiento de actos violentos y asesorar a los Estados miembros sobre este tema. Unidad supervisada por el COSI cuyo mandato incluye notificar el contenido terrorista y extremista violento detectado a los proveedores de servicios en línea para que lo eliminen. *Vid*. al respecto, ESTÉVEZ MENDOZA, L., "Análisis de la efectividad e los mecanismos de lucha contra el terrorismo en la sociedad europea", en Garrido Carrillo, F. (dir.) y Faggiani, V. (coord.), *Lucha contra la criminalidad organizada y cooperación judicial en la UE: Instrumentos, límites y perspectivas en la era digital,* Thomson Reuters-Aranzadi, Cizur Menor, 2022, pp. 248 y 249.

13. COM (2017) 555 final.
14. DO L 63/50, de 6 de marzo de 2018.
15. Nos referimos a la Directiva (UE) 2017/541, ya citada (nota 2) que por primera vez estableció la obligación de los Estados miembros de adoptar medidas (legislativas, no legislativas o judiciales) para garantizar la rápida detección y eliminación de contenidos radicales, concretamente de aquellos que provoquen a la comisión de un delito de terrorismo, o su bloqueo (art. 21 y Considerando 22). Sobre este punto véase MIRO LLINARES, F., "La detección del discurso radical en Internet…", *op. cit*., pp. 629-631.

adopción de medidas que garanticen el funcionamiento del mercado interior y no ninguna de las disposiciones del Título V relativas al Espacio de Libertad, Seguridad y Justicia, por más que el fin de esta norma también sea el reforzamiento seguridad pública en la UE recurriendo para ello a la armonización de las condiciones de prestación de servicios transfronterizos por parte de los prestadores de servicios de alojamientos de datos.

II. ELEMENTOS BÁSICOS: ÁMBITO DE APLICACIÓN Y AUTORIDADES COMPETENTES

Como es tradicional en la legislación UE se establece en el Reglamento una serie de definiciones relevantes para determinar, entre otros extremos, el ámbito de aplicación subjetivo, objetivo y territorial (o geográfico) de la norma. Y se deja, según veremos, a la elección de los Estados miembros la designación de la autoridad o autoridades competentes para aplicar los instrumentos y soluciones en ella previstos.

Y pese a que no se trata de un instrumento de reconocimiento mutuo (recordemos, de nuevo, su base jurídica) toma de los instrumentos de reconocimiento mutuo propios del Espacio de Libertad, Seguridad y Justicia el empleo de formularios (plantillas) estandarizados y multilingües para facilitar la aplicación del que constituye su mecanismo estrella: la orden de retirada de contenidos terroristas en línea (en su caso, según veremos, con carácter transfronterizo).

1. ÁMBITO DE APLICACIÓN SUBJETIVO O PERSONAL

El ámbito de aplicación personal o subjetivo engloba a los prestadores de servicios de alojamiento de datos (PSAD, en adelante) que ofrecen sus servicios dentro de la Unión, independientemente de su lugar de establecimiento o de su tamaño[16]. A ellos les dirige el Reglamento una serie de obligaciones a las que después nos referiremos.

16. Algo que no ha escapado a la crítica puesto que dirigir de manera indiferenciada las órdenes de retirada a pequeños proveedores puede resultar desproporcionado porque les requerirá disponer de un mecanismo que pueda funcionar todos los días a todas las horas (24/7). *Vid*., en este sentido GASCÓN MARCÉN, A., "La responsabilidad de los intermediarios de Internet en la Unión Europea: iniciativas recientes y perspectivas de futuro", en Castelló Pastor, J.J. (director), *Desafíos jurídicos ante la integración digital: aspectos europeos e internacionales*, Aranzadi, Cizur Menor, 2021, p. 143 y, de la misma autora, "El nuevo Reglamento europeo para la prevención de contenidos terroristas en línea", en Fernández Cabrera, M. y Fernández Díaz, C.R. (directoras),

Quién sea PSAD viene definido por el art. 2.1 del Reglamento con remisión a la Directiva 2000/31/CE sobre el comercio electrónico[17] como cualquier persona física o jurídica que suministre servicios de la sociedad de la información dentro de la UE con independencia de su lugar de establecimiento (dentro o fuera de la UE) o de su tamaño, consistentes en el almacenamiento de información facilitada por el proveedor de contenidos a petición de éste.

El almacenamiento se entiende como "conservación de datos en la memoria de un servidor físico o virtual", según aclara el Considerando 13. De ahí que el Reglamento no resulte aplicable a otros intermediarios como los prestadores de servicios de mera transmisión o almacenamiento temporal (v.gr los proveedores de acceso a Internet), los proveedores de sistemas de nombres de dominio, los servicios de pago o los servicios de protección contra ataques de denegación de servicio distribuido, en la medida en que no implican el almacenamiento de contenidos.

La finalidad específica de luchar contra la difusión entre el público de contenidos terroristas lleva implícita que la información sea puesta a disposición de un número potencialmente ilimitado de personas, lo que conlleva la exclusión de los servicios de comunicaciones interpersonales como el correo electrónico, servicios de mensajería privada o servicios que requieren un registro o admisión previa para acceder a la información (Considerando 14). Caen en cambio dentro de esta categoría[18] los proveedores de medios sociales, los servicios de distribución de video, imágenes y audio, los servicios de intercambio de archivos y otros servicios en la nube, en la medida en que dichos servicios se emplean para poner la información almacenada a disposición del público previa solicitud directa del proveedor de contenidos[19].

Retos del Estado de Derecho en materia de inmigración y terrorismo, Ed. Iustel, Madrid, 2022, p. 532.

17. Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) (DO L 178 de 17.7.2000).

18. *Vid*. sobre este punto STJ de 3 de octubre de 2019 en el caso *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, C-18/18, EU:C:2019:821, donde entre otros extremos se analiza la consideración de *Facebook Ireland Limited* como prestador de servicios de alojamiento de datos en el sentido del artículo 14 de la Directiva 2000/31.*Vid*., asimismo, MORENO BLESA, L., "La retirada de contenidos ilícitos por los prestadores de servicios en línea", *Thémis-Revista de Derecho*, n.º 79, enero-junio 2021, pp. 73-86.

19. Por Proveedor de contenidos el Reglamento entiende cualquier usuario que ha proporcionado información que esté o haya estado almacenada y difundida entre el público por un PSAD (art. 2.2.º)

2. ÁMBITO DE APLICACIÓN OBJETIVO

El ámbito objetivo viene determinado básicamente por los "contenidos terroristas" en línea, que habrán de ser retirados en la forma que después veremos. Se trata de una categoría "porosa"[20] que debe delimitarse adecuadamente en la medida en que es la que se va a emplear para justificar que los contenidos calificados como tales van a ser expulsados del espacio público y, por ende, excluidos del ámbito de protección de las libertades de expresión e información amparadas por el art. 11 de la CDFUE[21].

La definición de "contenidos terroristas ilícitos" (art. 2.7 del Reglamento), que está en consonancia con la definición de delitos de terrorismo establecida en el art. 3.1 de la Directiva (UE) 2017/541, a la que remite el art. 2.6 del Reglamento, es la de material o información utilizada para incitar a la comisión de delitos de terrorismo y hacer apología de dichos delitos, inducir a una persona o grupo a cometerlos o contribuir a su comisión o a participar en las actividades de un grupo terrorista, proporcionar instrucciones sobre fabricación o uso de instrumentos y métodos para cometerlos.

Se trata de una definición que en la versión inicial de la Propuesta fue objeto de severas críticas por su amplitud[22]. Acertadamente, fue corregida y formulada de un modo más adecuado tomando como modelo precisamente el de la Directiva (UE) 2017/541. No obstante, subsiste en el precepto reformado una previsión final que sigue siendo excesivamente ambigua. La que considera también "contenido terrorista" el material que "constituya una amenaza de comisión de los delitos de terrorismo"[23].

---

20. En feliz expresión de TERUEL LOZANO, G. M., "Una lectura garantista de las nuevas tendencias en la lucha europea contrala difusión de mensajes terroristas en internet", *ReDC* núm. 34 Julio-Diciembre 2020, disponible en https://www.ugr.es/~redce/REDCE34/articulos/05_TERUEL.htm.
21. Véase la interesante propuesta de BUSTOS GISBERT para establecer una serie de criterios útiles para valorar, en cada caso concreto si un determinado contenido colgado en la Red incurre en alguno de los comportamientos delictivos descritos (BUSTOS GISBERT, R., "Libertad de expresión …", *op. cit.* apartado 4 –Criterios orientadores para la solución del conflicto entre libertad de expresión y lucha contra el terrorismo en la Red–, pp. 170-172).
22. C.fr., entre otros, las críticas de BARATA, J., *New EU Proposal on the Prevention of Terrorist Content Online: An Important Mutation of the E-Commerce Intermediaries' Regime*, Centre for Internet and Society, 2018, pp. 4 y 5, disponible (última consulta 27.09.2022) en: https://cyberlaw.stanford.edu/sites/default/files/publication/files/2018.10.11.Comment.Terrorism.pdf; TERUEL LOZANO, G. M., "Una lectura garantista…", *op. cit*.
23. Sobre los delitos de ciberterrorismo *vid*. VELASCO NÚÑEZ, E. *Delincuencia informática…*, *op. cit*. pp. 238-251.

Los Considerandos 11 y 12 aclaran y concretan el sentido del precepto examinado al precisar, el primero de ellos, que al evaluar si el material constituye contenido terrorista en el sentido del Reglamento, las autoridades competentes y los prestadores de servicios de alojamiento de datos deben tener en cuenta factores como la naturaleza y la literalidad de las declaraciones, el contexto en el que se realizaron y su potencial de conllevar consecuencias nocivas con respecto a la seguridad y la integridad de las personas. Y, asimismo, y a modo de prevención o salvaguardia para evitar confundir una actuación o publicación en el ejercicio de la libertad de prensa y de información con "difusión de contenidos terroristas" indica el Considerando 12 que el material difundido con fines educativos, periodísticos, artísticos o de investigación, o con fines de sensibilización contra actividades terroristas no debe considerarse contenido terrorista. Como tampoco lo son la expresión de puntos de vista radicales, polémicos o controvertidos en el debate público sobre cuestiones políticas sensibles. Al determinar si el material proporcionado por un proveedor de contenidos constituye «contenidos terroristas» con arreglo al Reglamento y, especialmente en los casos en que el proveedor de contenidos asuma una responsabilidad editorial, cualquier decisión relativa a la retirada de material difundido debe tener en cuenta las normas periodísticas, establecidas por la reglamentación de prensa o de los medios de comunicación, de conformidad con el Derecho de la Unión, incluida la Carta.

3. ÁMBITO DE APLICACIÓN ESPACIAL O GEOGRÁFICO

Las obligaciones impuestas por el Reglamento alcanzan a todos los prestadores de servicios de alojamiento de datos establecidos en la UE y en terceros países, en la medida en que ofrezcan sus servicios en la Unión.

La justificación de esta eficacia "extraterritorial" del Reglamento en cuanto también resulta aplicable a los prestadores de servicios de alojamiento de datos establecidos fuera de la Unión pero que ofrecen servicios dentro de ella es clara, dado que se busca garantizar que todas las empresas con actividad en el mercado único digital cumplan los mismos requisitos, independientemente de su país de establecimiento y habida cuenta de que una proporción significativa de los PSAD expuestos a contenidos terroristas en sus servicios están establecidos en terceros países. Resulta por ello una solución plenamente razonable y coherente con el fundamento y los objetivos del Reglamento[24].

24. En este sentido, DE MIGUEL ASENSIO, P. A., "Servicios de alojamiento de datos y medidas contra la difusión de contenidos terroristas en línea: el Reglamento (UE) 2021/784", *La Ley Unión Europea* n.º 93, 1 de junio de 2021 y, asimismo, "Reglamento

La determinación de si un PSAD ofrece dichos servicios en la Unión requiere evaluar si el prestador permite a las personas físicas o jurídicas que se encuentren en uno o más Estados miembros[25] utilizar sus servicios y si tiene una "conexión sustancial" con dichos Estados miembros. Conexión sustancial que se entiende concurrente cuando el PSAD tiene algún establecimiento –en sentido amplio– en la Unión y que, en otro caso, requiere para poder apreciarla estar fundada en "criterios objetivos específicos" que el Reglamento no establece de modo taxativo. aunque a título de ejemplo indica algunos en el art. 2.5 (tener un número significativo de usuarios de sus servicios en un Estado miembro u orientar sus actividades hacia uno o más Estados miembros[26]).

4. AUTORIDADES COMPETENTES

Cada Estado miembro designará la autoridad o autoridades competentes para ocuparse de los distintos cometidos ligados a la aplicación del Reglamento.

En primer lugar, para dictar órdenes de retirada de conformidad con el art. 3, y designación en su seno de un punto de contacto para tramitar las aclaraciones o peticiones de información derivadas de la emisión de la orden.

En segundo lugar, para examinar las órdenes de retirada dictadas por la autoridad competente de otro Estado miembro (las órdenes transfronterizas del art. 4).

En tercer lugar, para supervisar la aplicación de las medidas específicas (proactivas y/o preventivas) adoptadas por los PSAD de conformidad con el art. 5.

En cuarto y último lugar, para imponer sanciones a los PSAD que incumplan las obligaciones del Reglamento, de conformidad con el art. 18.

(UE) 2021/784 sobre la lucha contra la difusión de contenidos terroristas en línea: segunda parte", disponible en https://pedrodemiguelasensio.blogspot.com (entrada de 21 de mayo de 2021).

25. Imprecisa expresión a juicio de P. A. DE MIGUEL ASENSIO (*op. et locs.cits*) sin que en el articulado se concrete si lo determinante es la nacionalidad, la residencia o simplemente que se encuentren en la UE, si bien el Considerando 15 aclara que lo determinante a estos efectos es que el PSAD permita a las personas que se encuentran en uno o más Estados miembros utilizar sus servicios.

26. Lo cual puede deducirse, por ejemplo, del uso de una determinada lengua o empleo de una moneda propia de un Estado miembro. *Cfr.* Considerandos 5 y 16 del Reglamento (UE) 2021/784.

Si bien el art. 13 no indica el tipo de autoridad que debe ocuparse de tales cometidos, sí exige que actúen con garantía de independencia, objetividad y pleno respeto a los derechos fundamentales[27]. El Considerando 35 aclara que es facultad de cada Estado miembro decidir el número de autoridades que debe designar y si son de carácter administrativo, policial o judicial, sin perjuicio de que además puedan encomendarse tales funciones a un organismo ya existente.

De la consulta al Registro de autoridades hecho público por la Comisión en cumplimiento del art. 12.4 del Reglamento[28] se advierte una mayoritaria inclinación por autoridades policiales. Inclinación también seguida por España que ha designado como autoridad competente para emitir órdenes de retirada, examinar las de carácter transfronterizo y supervisar las medidas específicas al Centro de Inteligencia contra el Terrorismo y la Delincuencia Organizada (CITCO) dependiente de la Secretaría de Estado de Seguridad del Ministerio del Interior[29], encomendando la imposición de sanciones por infracciones leves y graves al Secretario de Estado de Seguridad y, por infracciones muy graves, al Ministro del Interior.

Sin perjuicio de que, según se acaba de indicar, el Reglamento deja en este punto total libertad a los Estados miembros, la solución ha sido muy criticada, especialmente en lo que se refiere a que no se reserve a autoridades judiciales la emisión de las órdenes de retirada y su intervención, según veremos, pueda limitarse al recurso que eventualmente se interponga frente a ellas (es decir, a un control *ex post*)[30].

27. *Cfr.* art. 13.2: Los Estados miembros garantizarán que sus autoridades competentes lleven a cabo sus funciones en virtud del presente Reglamento de forma objetiva y no discriminatoria, al tiempo que respetan plenamente los derechos fundamentales. Las autoridades competentes no solicitarán ni aceptarán instrucciones de ningún otro organismo en relación con la ejecución de sus funciones en virtud del artículo 12, apartado 1.

28. Disponible en https://ec.europa.eu/home-affairs/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online/list-national-competent-authority-authorities-and-contact-points_en#austria.

29. Indicando como punto de contacto el propio Centro de Inteligencia contra el Terrorismo y la Delincuencia Organizada (CITCO), Secretaría de Estado de Seguridad del Ministerio del Interior por medio del correo electrónico iru@interior.es con copia a: citco@interior.es.

30. Véase, por ejemplo, TERUEL LOZANO, G. M. "Una lectura garantista…", *op. cit.*; RODRÍGUEZ RÍOS, S. F. " Una mirada al Reglamento (UE) 2021/784 como nuevo instrumento en la lucha contra la difusión del terrorismo en internet " en Pereira Puigvert, S. y Ordoñez Ponz, F. (directores), *Investigación y proceso penal en el siglo XXI: Nuevas tecnologías y protección de datos*, Thomson Reuters Aranzadi, Cizur Menor, 2021, p. 355. Algún autor, ante el texto de la inicial Propuesta de Reglamento ya daba por supuesto que en España debían ser autoridades judiciales las encargadas de la emisión de las órdenes atribuyendo expresamente este cometido a los Juzgados

III. ACTUACIONES PARA COMBATIR LA DIFUSIÓN. LAS OBLIGACIONES A CARGO DE LOS PROVEEDORES

El Reglamento incorpora una serie de obligaciones a los PSAD, en relación con contenidos terroristas, ya de carácter coercitivo, ya de carácter preventivo y/o proactivo, ya de carácter operativo.

Las de carácter coercitivo consisten básicamente en el cumplimiento de forma inmediata de la orden de retirada o bloqueo de contenidos que se les dirija, con la obligación adicional de su conservación por plazo determinado y el deber de designar un punto de contacto para su recepción y rápido tratamiento (art. 3 y 15)[31]. Téngase en cuenta que, según veremos a continuación, la ejecución de la orden de retirada ha de llevarse a cabo en el plazo de una hora.

El incumplimiento sistemático o persistente puede ser objeto de sanciones económicas de hasta el 4% del volumen de negocios mundial del prestador de servicios de alojamiento de datos en el ejercicio precedente (art. 18). Son los Estados miembros los encargados de establecer el régimen de sanciones (eficaces, proporcionadas y disuasorias)[32] aplicables a las infracciones del Reglamento[33], además de determinar –según hemos visto– la autoridad encargada de imponerlas.

Las de carácter preventivo/proactivo son, a su vez, de dos tipos.

Centrales de Instrucción de la Audiencia Nacional (así GIL GARCÍA, F. S., "Nueva Propuesta de Reglamento del Parlamento Europeo y del Consejo para la prevención de la difusión de contenidos terroristas en línea", en *FODERTICS 8.0: Estudios sobre tecnologías disruptivas y justicia* (Bueno de Mata, F. director), Ed. Comares, Granada, 2020, pp. 348 y 349).

31. El punto de contacto del PSAD debe consistir en cualquier medio específico, interno o externalizado, que permita la presentación electrónica de órdenes de retirada así como en los medios técnicos y personales que permitan su rápido tratamiento. El punto de contacto del prestador de servicios de alojamiento de datos no tiene que estar situado en la Unión y el PSAD es libre de utilizar un punto de contacto ya existente, siempre que este sea capaz de cumplir las funciones encomendadas en virtud del presente Reglamento. Con vistas a garantizar que los contenidos terroristas se retiren o que el acceso a ellos se bloquee en el plazo de una hora desde la recepción de una orden de retirada, los prestadores de servicios de alojamiento de datos deben garantizar que el punto de contacto está disponible ininterrumpidamente [Considerando 42 del Reglamento (UE) 2021/784].
32. Aunque el Reglamento (UE) no detalla las sanciones a imponer, sí determina en el art. 18.2 una serie de extremos que los Estados miembros deberán tener en cuenta para graduarlas correctamente, cuestión en la que incide, igualmente su Considerando 45.
33. En España tales sanciones son impuestas por la Secretaría de Estado de Interior para las leves y graves, y por el Ministro del Interior para las muy graves. Sanciones frente a las cuales puede interponerse recurso contencioso-administrativo ante la Sala de lo Contencioso de la Audiencia Nacional (art. 11 de la LJCA) cuya resolución es recurrible en casación ante la Sala Tercera del Tribunal Supremo.

Por una parte, las que podríamos denominar como "generales" consistentes en el deber de informar a las autoridades competentes (o al punto de contacto del Estado miembro de la Unión en que tengan su establecimiento principal o su representante legal) y a Europol cuando detecten contenidos terroristas que conlleven una amenaza inminente para la vida (art. 14.5).

Por otra, las que el Reglamento califica de "específicas" y que implican la adopción por los PSAD "expuestos a contenidos terroristas" de medidas específicas para impedir el alojamiento y difusión de contenidos terroristas.

Ser un PSDA "expuesto" es condición que se adquiere por decisión de la autoridad competente del Estado miembro del establecimiento principal del prestador o en el que su representante legal resida y que, una vez recibida, obliga a implementar medidas en un plazo máximo de tres meses.

La decisión indicada debe basarse en factores objetivos, si bien el art. 5.4 del Reglamento se limita a mencionar a modo de ejemplo el que se trate de un prestador que en los doce meses anteriores haya recibido dos o más órdenes de retirada.

En cuanto a las medidas a adoptar, a elección del PSAD, pueden ser cualquiera de las enumeradas en el art. 5.2 del Reglamento para luchar contra el uso indebido de sus servicios, entre las que se encuentra la adopción de medios técnicos apropiados para identificar y retirar los contenidos o bloquearlos con rapidez, lo que apunta a la posibilidad de emplear filtros automáticos[34], no siempre eficaces y adecuados atendida la dificultad de discernir en atención a su contexto la verdadera intencionalidad de un mensaje[35]. Se trata de seleccionar, en cada caso, aquéllas que sean

34. Filtros automáticos que pueden ser de dos tipos. Los que funcionan con hashes y comparan el contenido subido con una base de datos de contenidos que ya han sido clasificado como terrorista. O los que buscan detectar contenido a través de programas de inteligencia artificial como, por ejemplo, de procesamiento del lenguaje natural. Sobre estos filtros y los problemas que plantean *vid*. GASCÓN MARCÉN, A., "El nuevo Reglamento europeo…", *op. cit*., pp. 537 y 538; MIRO LLINARES, F. "La detección de discurso radical en Internet…", *op. cit*., pp. 632-636 y, del mismo autor, "Predictive policing: utopia or dystopia? On attitudes towards the use of big data algorithms for law enforcement", en *IDP: Revista de Internet, Derecho y Política*, n.º 30.

35. Como indica SÁNCHEZ RUBIO, no contamos con Inteligencia Artificial capaz de emular el pensamiento humano, sino que encontramos ciertas limitaciones. La IA sigue siendo como un niño pequeño superdotado al que entrenas para hacer tareas pequeñas pero que no tiene la sabiduría, el juicio o el sentido común de una persona con experiencia ["Los informes de inteligencia en la prevención del discurso del terrorismo", en Galán Muñoz, A. y Gómez Rivero, C. (directores), *La represión y persecución penal del discurso terrorista*, Ed. Tirant lo Blanch, Valencia, 2022, p. 793. *Vid*.,

eficaces, selectivas y proporcionadas atendida la gravedad del nivel de exposición de los servicios de PSAD a los contenidos terroristas, así como sus capacidades técnicas y solidez financiera y teniendo muy en cuenta los derechos fundamentales de los usuarios evitando una obligación general de supervisión[36] que pueda llegar a convertir a los PSAD en una suerte de "censores de la Red con potestades semi-públicas"[37].

El cese en tal condición ("expuesto") se produce por decisión de la autoridad competente adoptada de oficio o a petición del PSAD (art. 5 apartados 4.º a 7.º). Mientras eso sucede el PSAD está sometido a una cierta monitorización para comprobar su adecuación a la conducta debida tras el cumplimiento correcto de las medidas específicas empleadas.

Las obligaciones que podrían calificarse como de tipo operativo, en cuanto dirigidas a posibilitar la aplicación del Reglamento consisten, más allá de las de transparencia que aparecen recogidas en el art. 7[38] y en el ya citado nombramiento de un punto de contacto para recibir y tramitar las órdenes, en establecer un mecanismo eficaz y accesible para permitir que los proveedores de contenidos retirados o bloqueados reclamen y soliciten su restablecimiento (art. 10). Además, y para los PSAD que no tengan su establecimiento principal en la UE, en la obligación adicional de designar un representante legal en la Unión que deberá residir o estar establecido en un Estado miembro, a efectos de la recepción, el cumplimiento y la ejecución de órdenes de retirada y otras decisiones dictadas por las autoridades competentes (art. 17).

IV. ESPECIAL CONSIDERACIÓN DE LAS ÓRDENES DE RETIRADA DE CONTENIDOS TERRORISTAS EN LÍNEA

Sin duda, el instrumento estrella que introduce el Reglamento (UE) 2021/784 para la lucha contra la difusión por internet de contenidos

asimismo, pp. 734-741 sobre las distintas herramientas de IA para detectar contenidos terroristas].

36. El riesgo de censura privada se neutraliza con el mantenimiento de la exención de responsabilidad que prevé la Directiva 2000/31/CE (Comercio electrónico) ya citada (nota 17).
37. En expresión de TERUEL LOZANO, G. M., "Una lectura garantista…", *op. cit.* que expresa su temor al respecto y su preocupación también desde la perspectiva de la garantía de la libertad de expresión y del pluralismo.
38. Obligaciones recogidas en el art. 7 exigiendo que los PSAD detallen claramente en sus términos y condiciones su política destinada a luchar contra los contenidos terroristas en línea y en la publicación de un informe anual de transparencia cuando se trate de un PSAD que haya adoptado medidas en ese ámbito o al que se haya exigido su adopción en virtud del Reglamento.

terroristas lo constituyen las denominadas órdenes de retirada o de bloqueo que dan un significativo paso adelante sobre los "requerimientos" existentes hasta la fecha.

1. NATURALEZA DE LAS ÓRDENES

Se trata de decisiones vinculantes de carácter unilateral por las que la autoridad emisora competente de un Estado miembro obliga a un prestador de servicios en la UE y que en su caso puede estar establecido o representado en otro Estado miembro diferente, a la retirada de contenidos terroristas.

Adviértase, en primer lugar, la relevancia de este nuevo instrumento que ha aparecido en el escenario europeo para combatir la difusión de los contenidos terroristas. Se ha pasado, en este punto, de los "requerimientos" previstos en la ya citada Recomendación (UE) 2018/334 de la Comisión[39] para una retirada en cierto modo "voluntaria" y también en el texto de la inicial Propuesta de Reglamento[40], a las "órdenes de retirada" de obligatorio e inmediato cumplimiento por su destinatario. Se ha hablado, por ello, de un sistema de mera "notificación-acción", donde el proveedor no tiene obligación ni posibilidad alguna de valorar la orden, ni de decidir si la misma es correcta o no; solo ha de cumplirla[41].

Como característica significativa de estas órdenes cabe señalar que, a diferencia de los instrumentos de reconocimiento mutuo, el destinatario de la orden de retirada es directamente el PSAD establecido o representado en la UE bien en el propio Estado de la autoridad emisora de la orden, bien en otro diverso, pero no una autoridad de ese Estado. Es decir, la orden vinculante se dirige al proveedor de servicios (a su representante

39. Véase §§ 32-35 de la Recomendación (UE) 2018/334.

40. *Cfr.* Art. 5 de la Propuesta de Reglamento [COM (2018) 640 final]. Aunque dicho artículo se ha suprimido y no se ha llevado al articulado del Reglamento, el Considerando 40 aclara que el instrumento del requerimiento sigue estando a disposición de los Estados miembros. Con todo, y pese a su en apariencia menor relevancia, no escaparon a la crítica. En este sentido BARATA, J., (*New EU Proposal.., op. cit*.) indicaba que podrían convertirse en un mecanismo para delegar en entidades privadas la responsabilidad de decidir y hacer cumplir medidas que, de otro modo, tendrían que ser adoptadas por organismo públicos con la oportunidad adecuada de revisión judicial.

41. Así GALÁN MUÑOZ, A., "Redes sociales, discurso terrorista y Derecho Penal. Entre la prevención, las libertades fundamentales y ¿los negocios?", en Galán Muñoz, A. y Gómez Rivero, C. (directores), *La represión y persecución penal del discurso terrorista*, Ed. Tirant lo Blanch, Valencia, 2022, p. 293.

legal designado en la UE) quien deberá cumplirla sin necesidad de la intervención o supervisión directa y/o inmediata de ninguna autoridad del Estado de ejecución (más allá de lo que luego se dirá con referencia a las denominadas "órdenes transfronterizas").

Se trata del primer modelo que se implanta en la UE basado en una cooperación directa entre autoridades (policiales, administrativas o judiciales) y proveedores de servicios que encuentra su justificación en razones de eficacia y de celeridad en la respuesta. Adelanta así las soluciones previstas en la Propuesta de Reglamento (UE) sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal[42], por más que se trate de instrumentos totalmente diversos.

A la hora de su dictado se ha de tener presente que, en la medida que estas decisiones pueden suponer una injerencia en las libertades de expresión y de información, las mismas habrán de ser adoptadas en un proceso legalmente establecido en tutela de ciertos derechos o bienes constitucionales –como ocurre en este supuesto– y, en todo caso, deberán superar un estricto test sobre su proporcionalidad y necesidad según ha afirmado tanto el TEDH[43] como el Tribunal de Justicia UE[44].

2. REQUISITOS PARA SU EMISIÓN

Entre los que podemos considerar como de tipo objetivo, se requiere que la orden de retirada se proyecte sobre contenidos terroristas según

42. Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal, COM (2018) 225 final, de 17.4.2018.

43. Véase STEDH de 18 de diciembre de 2012, *Yildirim contra Tuquía*, en relación a la orden preventiva de bloqueo dictada por las autoridades turcas de una página web considerada ofensiva y, asimismo, STEDH de 1 de diciembre de 2015, caso *Cengiz y otros contra Turquía* y STEDH de 23 de junio de 2020, *Vladimir Kharitonov contra Rusia*. Consúltese con carácter general sobre la jurisprudencia del TEDH sobre esta materia, BUSTOS GISBERT, R., "Los derechos de libre comunicación en una sociedad democrática", en *La Europa de los Derechos. El Convenio Europeo de Derechos Humanos* (García Roca, J. y Santolaya, P. coordinadores), Centro de Estudios Políticos y Constitucionales, 3.ª ed., Madrid, 2014, pp. 473-509.

44. *Vid*. STJ de 13 de marzo de 2019, P*olonia contra Parlamento Europeo y Consejo*, C-128/17, EU:C:2019:194, § 94; STJ de 3 de octubre de 2019, *Glawischnig-Piesczek*, C-18/18, EU:C:2019:821, §§ 33-48; STJ (GS) de 16 de julio de 2020, *Facebook Ireland y Schrems*, C-311/18, EU:C:2020:559, § 176; STJ (GS) de 17 de diciembre de 2020, *Centraal Israëlitisch Consistorie van België y otros*, C-336/19, EU:C:2020:1031, § 64; STJ (GS) de 26 de abril de 2022, *Polonia contra Parlamento Europeo y Consejo*, C-401/19, EU:C:2022:297, §§ 65-67.

se definen en art. 2.7 ya examinado del Reglamento; esto es, material que incite o induzca a cometer un delito de terrorismo [art. 3 de la Directiva (UE) 2017/541] o constituya una amenaza de comisión de tales delitos, o a participar en las actividades de un grupo terrorista o proporcione instrucción sobre la fabricación de explosivos o armas. La inclusión en alguna de las categorías citadas y la exclusión en ellas del material difundido con fines educativos, periodísticos, artísticos o de investigación exige una ponderación de las circunstancias del caso concreto atendidos los derechos a la libertad de información, expresión, libertad de artes y las ciencias. Y requiere, además, que en la orden se motive expresamente la razón por la que ese contenido finalmente es considerado terrorista y, en consecuencia, debe ser retirado [art. 3.4.b)] con la finalidad de permitir al PSAD y, en última instancia, al proveedor de contenidos, ejercer de forma efectiva su derecho a la tutela judicial efectiva en vía de recurso.

En lo referido a los requisitos subjetivos, la orden ha de ser dictada por la autoridad competente (judicial, policial o administrativa) del Estado miembro [art. 12.1.a) y 13] dirigida –art. 3.5– al establecimiento principal del prestador de servicios en la UE (y, concretamente, a su punto de contacto) o bien al representante legal designado en la UE de conformidad con el art. 17.

3. PROCEDIMIENTO

En los casos que podríamos considerar generales u ordinarios, en que la orden de retirada se dirige a un PSAD con establecimiento principal o representante legal en el Estado miembro emisor de la orden, se establece un procedimiento en el que las actuaciones a realizar se reparten entre la autoridad que emite la orden y el PSAD que la recibe.

3.1. Actuaciones a realizar por la autoridad competente que dicta la orden

Salvo supuestos de urgencia, debe facilitar al destinatario la información sobre los procedimientos y plazos aplicables con, al menos, doce horas de antelación a su dictado si es la primera vez que le dirige una orden.

Deberá emitir la orden empleando la plantilla o formulario que aparece en el Anexo I con el contenido del art. 3.4; a saber: identificación de la autoridad que la dicta y que autentifica la orden; motivación suficientemente detallada referida al carácter terrorista de los contenidos a retirar/

bloquear con indicación del supuesto en que se encuadran de entre los enumerados en el art. 2.7; URL que permita la identificación de los contenidos terroristas; datos temporales; información sobre vías de recurso y sus plazos para el PSAD y para el proveedor de contenidos; en su caso, decisión de que no se facilite información por el PSAD al proveedor de contenidos sobre la retirada/bloqueo por concurrir razones de seguridad pública (como la prevención, investigación, detección y enjuiciamiento de delitos de terrorismo)[45].

Obsérvese que una correcta intelección de lo previsto en el art. 2.7 indica que la autoridad competente de emisión debe valorar debidamente si el contenido on line ha de ser calificado como "terrorista" y plasmar en la plantilla su motivación en tal sentido, una vez llevado a cabo el necesario testde proporcionalidad de los derechos en juego.

La plantilla una vez cumplimentada en la lengua oficial del Estado miembro en el que el PSAD tiene su establecimiento principal o en el que reside o está establecido su representante legal (art. 15.2) y firmada electrónicamente por la autoridad competente será transmitida al punto de contacto del PSAD (art. 15.1) por medios electrónicos (art. 3.5.II) y una copia de ella se remitirá a Europol, al objeto de la debida cooperación y coordinación[46] reclamada por el Reglamento que evite duplicidades de trabajo, y para facilitar la futura emisión de su informe anual (art. 14.1 y 14.6).

3.2. Actuaciones a realizar por el PSAD que recibe la orden

Como regla general el PSAD recibida la orden retirará los materiales o bloqueará el acceso a ellos en el plazo de una hora tras la recepción de la orden y lo comunicará a la autoridad emisora mediante la plantilla que aparece en el Anexo II, que incluye la precisión de la hora en que ha tenido lugar.

Se trata de un plazo extraordinariamente breve, justificado en la necesidad de actuar con la máxima celeridad para atajar la difusión de la información, aunque criticado porque se aplica a todos los PSAD

45. El art. 11.3, que prevé esta reserva, fija un `plazo máximo de seis semanas, aunque admite una prórroga por otras seis semanas cuando dicha reserva siga estando justificada

46. *Vid*. al respecto "Europol explica cómo combate la difusión de contenidos terroristas en internet", información publicada en Escudo Digital el 28 de noviembre de 2021 disponible en https://www.escudodigital.com/ciberseguridad/europol-bases-combatir-contenidos-terroristas-internet_50273_102.html.

independientemente de su tamaño, lo cual puede resultar desproporcionado al requerir disponer de un mecanismo que pueda funcionar todos los días y a todas horas (24/7)[47]. Máxime atendidas las importantes sanciones que se anudan a un incumplimiento de las órdenes y que, conforme indica el art. 8, en caso de incumplimiento sistemático y persistente su importe puede llegar al 4% del volumen de negocios anual del PSAD en el ejercicio precedente.

A la vista de lo indicado en el art. 3 y el contenido de la propia plantilla de los Anexos II (Sección B) y III (Sección B) parece dejarse en manos de los PSAD decidir por cuál de las dos opciones (retirada de contenidos o bloqueo del acceso a ellos) se inclinan, apartándose en este punto de la solución apuntada por la Directiva (UE) 2017/541, relativa a la lucha contra el terrorismo, en la que se confería un carácter prioritario a la retirada y subsidiario, al bloqueo[48].

Como indica De Miguel Asensio, se trata de dos opciones con implicaciones diversas en la medida en que la retirada supone, en principio, que los contenidos dejen de estar accesibles a través de los servicios de ese prestador en cualquier lugar del mundo, mientras que el bloqueo se limita a imposibilitar el acceso a los mismos desde el territorio de la UE. Y si bien a la luz de la jurisprudencia del Tribunal de Justicia los mandamientos de retirada de contenidos ilícitos de Internet con alcance mundial resultan típicamente excepcionales, cuando se trata de contenidos terroristas puede estar justificada su imposición[49].

Salvo que medie prohibición de la autoridad emisora en la orden, el PSAD informará al proveedor de contenidos de los motivos de la retirada y del derecho a recurrir la orden, o bien le entregará copia de la orden en la que constan tales extremos (art. 11).

Además, deberá conservar de manera adecuada los contenidos retirados o bloqueados y datos conexos a efectos de los eventuales recursos que puedan interponerse frente a la orden (por el propio prestador o por el proveedor de

47. Así GASCÓN MARCÉN, A., "El nuevo Reglamento…", *op. cit*., p. 532.

48. Atendido su Considerando 22 en el que podía leerse que (la cursiva es nuestra): Los Estados miembros deben esforzarse al máximo por cooperar con terceros países al objeto de *garantizar la eliminación* de contenidos en línea que constituyan una provocación pública a la comisión de un delito de terrorismo desde los servidores ubicados en su territorio. *No obstante, cuando no sea factible la eliminación* de estos contenidos en origen, *también* pueden ponerse en marcha *mecanismos que bloqueen el acceso* a los mismos desde el territorio de la Unión…" Y añadía a continuación en su Considerando 23 que "la eliminación de contenidos en línea que constituyan una provocación pública a la comisión de un delito de terrorismo *o, cuando esto no sea posible*, el bloqueo del acceso…".

49. DE MIGUEL ASENSIO, P. A. "Servicios de alojamiento de datos…", *op. cit*. p. 4.

contenidos)[50], tramitación de denuncias de los proveedores de contenidos al amparo del art. 10 y, lo que es más relevante, prevención, detección, investigación o enjuiciamiento de delitos de terrorismo. Sin perjuicio de que el plazo de conservación debe limitarse al estrictamente necesario en cada caso en atención a los fines perseguidos, se fija el de seis meses como máximo por estimarse que garantiza la proporcionalidad debida al objeto de dejar el tiempo suficiente para iniciar el procedimiento de control administrativo o judicial y permitir a las autoridades policiales o judiciales el acceso a los datos necesarios para la investigación y enjuiciamiento de delitos de terrorismo. No obstante, a petición de la autoridad emisora o del órgano jurisdiccional competente, podrá prorrogarse por el plazo adicional imprescindible para los procedimientos de control administrativos y/o judiciales[51].

De esta solución general que pasa, según hemos visto, por dar cumplimiento inmediato a la orden de retirada se exceptúa únicamente el caso de que medie una imposibilidad de cumplirla por fuerza mayor, por existir razones técnicas u operativas o por contener errores manifiestos. Extremos estos que, en cualquier caso, no permiten una "valoración" del acierto o no de la orden en cuanto al fondo; esto es, si los contenidos son o no terroristas. Simplemente suspender temporalmente su acatamiento en espera de que se corrijan los defectos advertidos. En tales supuestos el PSAD deberá informar de inmediato a la autoridad emisora mediante el empleo de la plantilla recogida en el Anexo III, dando cuenta de los motivos concurrentes que imposibilitan el cumplimiento.

Si se subsanan los defectos o se proporciona la información complementaria necesaria, se ejecutará la orden en el plazo de una hora tras la recepción de las aclaraciones o desaparición de los impedimentos.

3.3. Actuaciones complementarias posteriores

Una vez que la orden sea firme (esto es, cuando expire el plazo para recurrir o, interpuesto recurso, una vez resuelto y confirmada la orden), la autoridad que la emitió deberá informar a la autoridad competente de supervisión (en caso de no ser ella misma) para futuras medidas específicas a cargo del PSAD (art. 3.9.II).

Además, tanto la autoridad emisora como el propio prestador de servicios deberán presentar los informes de transparencia anuales a que resultan obligados en virtud de los arts. 8.2, 7.2-3, respectivamente, del Reglamento.

50. Ante los órganos jurisdiccionales del Estado miembro que la dictó y conforme al procedimiento establecido por su legislación (art. 9).

51. *Cfr.* art. 6 y Considerandos 26 a 28 del Reglamento (UE) 2021/784.

4. ESPECIALIDADES EN LAS ÓRDENES DE RETIRADA TRANSFRONTERIZA

Bajo esta denominación –órdenes transfronterizas– regula el art. 4 del Reglamento una serie de disposiciones aplicables a las órdenes adoptadas por la autoridad competente de un Estado miembro distinto de aquel en el que el prestador destinatario de la medida tenga su establecimiento principal o en el que resida o esté establecido su representante legal.

En estos casos el procedimiento expuesto anteriormente se complica al entrar en juego otra autoridad (la del Estado miembro en el que el PSAD destinatario tiene su establecimiento principal o reside su representante legal) que debe ser informada del dictado de la orden tras lo cual, ya sea de oficio, ya a petición del PSAD o del proveedor de contenidos, examina la adecuación de la orden al Reglamento y puede vetarla.

Se trata de una solución acertada, adoptada para hacer frente a las críticas que había suscitado el texto de la inicial Propuesta de Reglamento con respecto a la posibilidad de que las órdenes pudieran dirigirse directamente a un intermediario situado en otro Estado miembro sin pasar por la autoridad de ese Estado[52]; es decir, sin que su carácter transfronterizo tuviera la más mínima relevancia[53]. El riesgo siempre latente de que este tipo de mecanismos pueda ser utilizado en otras jurisdicciones por gobiernos autoritarios para fomentar la censura, sobre todo si se hace una

52. *Vid*. en este sentido la Carta a los eurodiputados para impedir la aprobación del Reglamento, firmada por sesenta organizaciones de Derechos Humanos y de periodistas (ACCESS NOW, INTERNATIONAL & OTHERS, *Join letter to members of the European Parliament*, 2021, accesible en https://edri.org/wp-content/uploads/2021/04/MEP_TERREG_Letter_EN_78.pdf).

53. El acierto de esta solución se manifiesta asimismo en el hecho que probablemente este modelo también se extienda a las órdenes de entrega de pruebas electrónicas (Reglamento e-evidence) ya que el Parlamento Europeo ha insistido en que se notifique al Estado en que esté localizado el intermediario. *Cfr. Informe sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal*, de 11.12.2020, Doc. A9-0256/2020 PE642.987v02-00 LIB (Comisión de Libertades Civiles, Justicia y Asuntos de Interior. Ponente: Birgit Sippel). Sobre la Propuesta de Reglamento y análisis del Informe del Comité LIBE *vid*. CHRISTAKIS, T. "Lost in notification? Protective logic as compared to efficiency in the European Parliament's e-evidence Draft Report", en *Cross-Border Data Forum* posted 7.01.2020, disponible en https://www.crossborderdataforum.org/lost-in-notification-protective-logic-as-compared-to-efficiency-in-the-european-parliaments-e-evidence-draft-report/ (último acceso 30.09.2022) y DE HOYOS SANCHO, M., "Reflexiones acerca de la propuesta de Reglamento UE sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal", en *Revista General de Derecho Procesal* 58 (2022).

definición muy amplia de lo que son contenidos terroristas[54], aconsejaba crear salvaguardas para los derechos en juego dando entrada a la autoridad del Estado miembro del establecimiento del PSAD para que pudiera objetar la aplicación de la orden.

Veámoslo con algo más de detalle.

4.1. Actuaciones a realizar por la autoridad competente que dicta la orden

Con esta regulación se exige que la autoridad competente que dicta la orden, una vez cumplido con el trámite establecido en el art. 3 (información previa y dictado de la orden mediante el formulario del Anexo I con remisión al PSAD), envíe copia de la orden a la autoridad competente del Estado miembro en el que el PSAD destinatario tiene su establecimiento principal o resida su representante legal.

4.2. Actuaciones a realizar por el PSAD que recibe la orden

El PSAD, una vez recibida la orden debe cumplir con la retirada o bloqueo en el plazo de una hora, comunicándolo a la autoridad emisora mediante la plantilla correspondiente (Anexo II), informando de la retirada al proveedor de contenidos, y adoptando las cautelas necesarias para un eventual restablecimiento de contenidos o reactivación del acceso.

Pero, además, dentro del plazo de cuarenta y ocho horas desde la recepción de la orden puede remitir una solicitud motivada a la autoridad competente del Estado miembro en el que tiene su establecimiento o representante legal para que examine su regularidad.

4.3. Actuaciones de la autoridad competente del Estado miembro en el que el PSAD destinatario tiene su establecimiento principal o su representante legal

A esta autoridad se le confiere llevar a cabo el examen de la conformidad de la orden con las exigencias del Reglamento y de la Carta de Derechos Fundamentales de la UE, algo que puede realizar de oficio en el plazo de setenta y dos horas tras la recepción de la copia o que estará

54. *Vid*. GASCÓN MARCÉN, A., "El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea", *Cuadernos de Derecho Transnacional* (octubre 2021), Vol. 13, N.º 2, pp. 219-220.

obligado a realizar si media instancia del prestador de servicios o del proveedor de contenidos, en el plazo de setenta y dos horas tras recibir dicha solicitud.

De advertir que concurre alguna de dichas irregularidades ha de informar a la autoridad emisora de su intención de dictar una decisión contraria y de los motivos para hacerlo. Tras ello, y dentro de los plazos indicados emitirá una decisión motivada con comunicación a la autoridad que dictó la orden, a Europol y, en su caso, a los solicitantes. Si declara la existencia de una infracción en la orden, esto impedirá que despliegue efectos jurídicos y, por tanto, el PSAD deberá restablecer los contenidos retirados o el acceso a ellos[55].

En consecuencia, y como advierte De Miguel, prima el criterio de la autoridad del Estado miembro en el que el prestador destinatario de la medida tenga su establecimiento principal o en el que resida o esté establecido su representante legal, sin tener en cuenta a qué Estado o Estados miembros van dirigidos los contenidos en cuestión. El art. 4 no contempla que la disparidad de criterios al interpretar el Reglamento se resuelva de modo que el prestador de servicios de alojamiento deba bloquear el acceso a los contenidos únicamente desde el territorio del Estado miembro cuya autoridad competente ha considerado que constituyen contenidos terroristas; ni siquiera, según parece, aunque se trate de contenidos que puedan ser considerados como dirigidos específicamente a ese Estado miembro[56].

4.4. Eventuales actuaciones posteriores

También en el caso de estas órdenes transfronterizas queda abierta la vía de recurso por los PSAD y por los proveedores de contenidos. Ahora bien, teniendo en cuenta que en estas órdenes transfronterizas lo normal es que, ya sea de oficio, ya a instancia del prestador de servicios o del proveedor de contenidos, medie una decisión de la autoridad competente del Estado miembro en el que el PSAD destinatario tiene su establecimiento principal o su representante legal, se prevé que la impugnación de tal decisión "confirmatoria" de la orden de retirada se tramite precisamente

55. El art. 4 precisa en su apartado 7 que ese restablecimiento inmediato se impone "sin perjuicio de la posibilidad por parte del prestador de hacer cumplir sus términos y condiciones de conformidad con el Derecho de la Unión y el Derecho nacional". Se trata de una previsión que facilita que el prestador no restablezca esos materiales en caso de que considere que infringen sus condiciones y su retirada es conforme a Derecho.

56. DE MIGUEL ASENSIO, P. A. "Servicios de alojamiento de datos…", *op. cit*. p. 5.

ante los órganos jurisdiccionales del Estado miembro de la autoridad competente que dictó dicha decisión y no ante los de aquél que emitió la orden (art. 9.1 en relación con art. 4.4).

V. ALGUNAS REFLEXIONES FINALES

Expuesto el contenido fundamental del Reglamento (UE) 2021/784, podemos destacar ante todo su carácter innovador en el ámbito a que afecta (que no es otro que la lucha contra el terrorismo) y los avances innegables que de cara a aportar claridad, uniformidad y seguridad jurídica proporciona una norma de este tipo –Reglamento– frente a la Directiva, siempre prestada a transposiciones algo divergentes en los Estados miembros.

Pese a ello, y en nuestra opinión, la norma adolece de poca concreción y detalle en algunos aspectos (v.gr. coordinación con las autoridades competentes de otros Estados miembros y con Europol[57]) y deja excesivamente abiertos y/o a elección de los Estados miembros otros (v.gr. la naturaleza de las autoridades llamadas a intervenir en la tramitación de las órdenes) probablemente en una calculada visión de que se trataba de extremos que, en otro caso, podrían generar un mayor rechazo a la rápida aprobación del instrumento.

Y es que otra cuestión que merece la pena destacar es la rápida aprobación y puesta en marcha de este Reglamento (a diferencia de otras normas presentadas por las mismas fechas[58]), puesto que han transcurrido menos de cuatro años desde la presentación de la Propuesta por la Comisión,

57. No se olvide que entre las funciones de Europol el art. 4 de su Reglamento, en el apartado 1 incluye la de: "m) respaldar las acciones de los Estados miembros para prevenir y combatir las formas de delincuencia enumeradas en el anexo I que hayan sido facilitadas, fomentadas o cometidas a través de internet, incluyendo las siguientes actuaciones: i) ayudar a las autoridades competentes de los Estados miembros, a petición de estas, a responder a ciberataques de presunto origen delictivo, ii) cooperar con las autoridades competentes de los Estados miembros en relación con las órdenes de retirada, de conformidad con el artículo 14 del Reglamento (UE) 2021/784, y iii) notificar contenidos en línea a los proveedores de servicios en línea de que se trate para que examinen de manera voluntaria la compatibilidad de esos contenidos con sus propias condiciones contractuales". [art. 4.1.m) conforme nueva redacción dada por el Reglamento (UE) 2022/991 del Parlamento Europeo y del Consejo, de 8 de junio de 2022 por el que se modifica el Reglamento (UE) 2016/794 en lo que se refiere a la cooperación de Europol con entidades privadas, el tratamiento de datos personales por Europol en apoyo de investigaciones penales y el papel de Europol en materia de investigación e innovación].

58. Y aun previamente, como, por ejemplo, la Propuesta de Reglamento del Parlamento europeo y del Consejo sobre las órdenes europeas de entrega y conservación de

hasta la entrada en vigor el pasado 7 de junio de 2022 de la norma europea. Aunque toca una materia sensible que afecta a derechos garantizados por la CDFUE, la incidencia en el ámbito de la seguridad colectiva y el interés con que la Propuesta fue acogida y seguida por el Consejo[59] han hecho que fuera aprobada en un tiempo *record*.

Los PSAD, se convierten en los protagonistas esenciales para la detección y eliminación del discurso terrorista en Internet, bien sea porque por iniciativa voluntaria asumen dicha responsabilidad social, bien sea porque el Estado les impone nuevas obligaciones y, por tanto, les restringe su libertad de prestación de servicios de una forma sin precedentes[60]. Y los instrumentos previstos en el Reglamento para luchar contra la difusión de los contenidos terroristas en línea se revelan adecuados y eficaces; en especial, las órdenes de retirada[61], sin duda el instrumento estrella de la norma europea.

Sin perjuicio de las bondades de la nueva regulación, su eficacia no está exenta de problemas puesto que la calificación de un contenido en línea como "terrorista" presenta perfiles complejos que difícilmente pueden acreditarse mediante simples decisiones algorítmicas[62] toda vez que

---

pruebas electrónicas a efectos de enjuiciamiento penal [COM (2018), 225 final], presentada por la Comisión europea el 14 de abril de 2018.

59. *Vid*. Conclusiones del Consejo Europeo de 10 y 11 de diciembre de 2020 (EUCO 22/20, Bruselas, 1.12.2020).

60. En este sentido y ya antes de la aprobación de este Reglamento lo afirmaba MIRO LLINARES, "La detección del discurso radical en Internet…", *op. cit*., pp. 630 y 631.

61. Como indica BUENO DE MATA, la función del Derecho no es solo la de resolver los conflictos, sino que tiene una labor principal anterior en la prevención de los mismos. Se necesitan así instrumentos enfocados a inteligencia, es decir, saber prever lo que puede ocurrir y frenar los ataques antes de que se ejecuten [BUENO DE MATA, F., "Análisis de las medidas de cooperación judicial internacional para la obtención transfronteriza de pruebas en materia de cibercrimen", en *La Transformación digital de la cooperación jurídica penal internacional* (Fontestad Portalés, L., directora), Thomson Reuters Aranzadi, Cizur Menor, 2021, p. 29]. En este sentido y en nuestra opinión las órdenes de retirada de contenidos terroristas en línea son un buen ejemplo de este tipo de instrumentos, de finalidad claramente preventiva, para hacer frente a la amenaza terrorista.

62. Como advierte MIRO LLINARES ("La detección del discurso radical…", *op. cit.*, pp. 644 y 645), resulta esencial continuar con las estrategias de detección y retirada de los contenidos radicales y de propaganda extremista y terrorista en el ciberespacio, pero ello exige el uso de herramientas y técnicas que vayan más allá de la informática y tengan en cuenta el conocimiento criminológico y jurídico para la detección de los auténticos contenidos con capacidad de radicalización. La prevención del discurso radical online por medio de la detección, bloqueo y retirada de contenidos se encuentra en un estado muy embrionario y sólo superará tal fase cuando incorpore los hallazgos y métodos de detección de contenidos comunicativos radicales que puede aportar la criminología y el derecho y seamos capaces

tal concepto en su origen ha sido formulado para ser determinado judicialmente tras un procedimiento contradictorio en el que se pruebe la concurrencia de los elementos objetivos y subjetivos del delito objeto de la acusación[63]. A esto se añade el dato, muy relevante, de que las autoridades que emiten las órdenes de retirada no tienen por qué ser judiciales al dejarse a los Estados miembros libertad para optar por autoridades de este tipo o bien de tipo administrativo o policial, inclinándose mayoritariamente por estas últimas tal y como revela la consulta al Registro *on line* de la Comisión.

Y, a este respecto, suscita dudas si la eficacia, la celeridad y aún la seguridad de esta solución y que la intervención de los órganos jurisdiccionales se limite a un control *ex post* casan bien con el respeto a los derechos afectados (básicamente libertad de expresión y de comunicación). Dudas que, por ejemplo, ya ha despejado el Consejo constitucional francés avalando la solución que permite la norma (y que en Francia ha determinado que se confiera a autoridades administrativas la emisión de las órdenes) en sentencia de 3 de agosto de 2022. En ella ha considerado constitucional la previsión indicada atendidas, de una parte, las prevenciones establecidas en el Reglamento para evitar que el contenido difundido al público con fines educativos, periodísticos, artísticos o de investigación, pueda ser considerado "contenido terrorista"; de otra, la exigencia de que para acordar la retirada la autoridad administrativa competente deba incluir no sólo una referencia al tipo de contenido de que se trate, sino también una motivación suficientemente detallada que explique las razones por las que se considera de carácter terrorista; y, por último, la posibilidad de recurso ante los órganos jurisdiccionales en vía contencioso-administrativa[64].

---

de traducirlos al lenguaje de las ciencias de la computación. Sólo así, generando sinergias para el desarrollo de algoritmos capaces de discriminar si un determinado mensaje es radical o neutral, o identificando los patrones situacionales que definen el entorno donde se ha publicado dicho mensaje, podremos estar seguros de que estamos identificando aquello que realmente queremos evitar, y siempre bajo el respeto a los derechos fundamentales y, aquí en especial, a la libertad de expresión

63. Así lo indica SCHEININ, M.: The EU Regulation on Terrorist Content: An Emperor without Clothes, VerfBlog, entrada del 2019/1/30, disponible en https://verfassungsblog.de/the-eu-regulation-on-terrorist-content-an-emperor-without-clothes/, DOI: 10.17176/20190211-214620-0. Como indica el autor citado, lo que realmente ocurrió (actus reus) importa, pero también importa la intención con la que se cometió el acto (mens rea). Por lo tanto, copiar y pegar incluso exactamente la misma redacción en una normativa que permita a los algoritmos o a los analistas humanos retirar material de Internet no puede basarse en los mismos criterios, ya que sólo pueden aplicarse mediante la presentación de pruebas reales sobre la intención y el contexto.

64. Sentencia 2022-841 DC disponible en Rol N.º 843-2022.

Finalmente, debemos advertir, como problema añadido, el de la fragmentación en la regulación europea sobre la lucha contra los contenidos ilícitos *on line*. No deja de entrañar una cierta complejidad para los operadores jurídicos y aún para las empresas que operan en el sector de las comunicaciones y que deben cooperar en las actuaciones frente a la difusión de contenidos ilícitos la multiplicidad de normas aplicables a una misma materia. Más allá de las normas europeas sobre terrorismo, adoptadas en el marco del ELSJ y, por tanto, con base en el título V del TFUE[65], confluyen varias normas sobre servicios digitales adoptadas con base en el art. 114 TFUE que prevén la retirada de contenidos ilícitos. Y es que al Reglamento (UE) 2021/784 que hemos analizado en estas páginas se ha sumado recientemente el Reglamento (UE) 2022/2065 de servicios digitales[66] (conocido como Ley de servicios digitales o por su acrónimo DSA del inglés Digital Services Act)[67] en cuyo articulado se prevé también una orden de retirada de contenidos ilícitos[68]. Cierto es que dicha norma una vez resulte aplicable (con carácter general, a partir del 17 de noviembre de 2024)[69] actuará como *lex generalis* y el Reglamento (UE) 2021/784 lo hará como *lex specialis*[70]. Pero con independencia de esta solución queda la duda de si no hubiera sido más conveniente que el nuevo Reglamento incorporara en su seno las normas del Reglamento (UE) 2021/784 en aras de ese esfuerzo de consolidación y de clarificación que recomienda la propia UE para aligerar el entramado normativo[71] y que, sin embargo, omite sistemáticamente.

65. En el momento actual contamos con una Propuesta sobre el intercambio de información digital en casos de terrorismo y Propuesta por la que se crea una plataforma de colaboración para los ECIS presentadas por la Comisión el 2 y el 8 de diciembre de 2021, respectivamente (Documentos 9259/22 y 14684/21).
66. Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales), DO L 277, de 27 de octubre de 2022.
67. *Vid*., CUATRECASAS, "Puntos clave de la Propuesta de Digital Services Act: nuevas obligaciones para intermediarios y plataformas en línea", *Legal Flash de propiedad intelectual y Derecho Digital*, 21 de enero de 2021.
68. "Orden de actuación contra contenidos ilícitos", regulada en el art. 9 del Reglamento (UE) 2022/2065 al que se añade, en el art. 10, una "Orden de entrega de información".
69. *Cfr.* art. 93 del Reglamento de Servicios Digitales.
70. *Cfr.* art. 2.4 y Considerandos 10 y 44.II del Reglamento (UE) 2022/2065.
71. *Vid*. PASCUA MATEO, F., "La técnica normativa en el sistema jurídico comunitario", en *Cuadernos de Derecho Público*, n.º 28, 2006, pp. 125-169.