Revista Española de Derecho Europeo
88 | Octubre – Diciembre 2023
pp. 109-142
Madrid, 2023
DOI:10.37417/REDE/num88_2023_1976

ISSN: 1579-6302
Recibido: 16/10/2023 | Aceptado: 15/11/2023

LA RETIRADA DE CONTENIDOS ILÍCITOS CONSTITUTIVOS DE DELITO EN EL REGLAMENTO 2022/2065 RELATIVO A UN MERCADO ÚNICO DE SERVICIOS DIGITALES

THE REMOVAL OF UNLAWFUL CONTENT CONSTITUTING A CRIMINAL OFFENCE IN THE DIGITAL SERVICES MARKET REGULATION 2022/2065

Antonio Evaristo Gudín Rodríguez-Magariños*

RESUMEN: Se aborda en el presente estudio el contenido y alcance de las nuevas herramientas que el Reglamento (UE) 2022/2065, de mercado único de servicios digitales, pone a disposición de las autoridades estatales para luchar contra la delincuencia. El examen de los precedentes que han dado lugar al texto finalmente aprobado pone de manifiesto la existencia de un elemento de orden público no perfectamente definido que resulta determinante a la hora de definir el contenido y alcance de las nuevas herramientas que el reglamento pone a disposición de las autoridades estatales. La razón última de esta regulación subyace en el carácter condicional o dependiente de la difusión de la información. La información, como manifestación del derecho a la libertad de expresión, es inocua a la acción por gubernativa. Por el contrario, la difusión de información fuera del marco previsto por el emisor puede acarrear consecuencias imprevistas que requieran la intervención de los mercados por las autoridades estatales.

PALABRAS CLAVE: Reglamento (UE) 2022/2065, prestación de servicios digitales, supresión de contenidos ilícitos, ciberdelitos, jurisdicción internacional.

* Letrado del Servicio Común de Ejecutorias de la Audiencia Nacional. Doctor en Derecho. antgudin@valdepenas.uned.es. ORCID ID: 0009-0000-9283-4288

ABSTRACT: This study addresses the content and scope of the new tools that Regulation (EU) 2022/2065 on the digital services market puts at the disposal of state authorities to fight crime. An examination of the precedents that led to the text finally adopted reveals the existence of a not perfectly defined public policy feature that is decisive in defining the content and scope of the new tools that the regulation makes available to state authorities. The ultimate reason for this regulation lies in the conditional or dependent nature of the dissemination of information. Information, as a manifestation of the right to freedom of expression, is harmless to the action of the law. On the contrary, the dissemination of information outside the framework envisaged by the issuer may lead

KEYWORDS: Regulation 2022/2065, digital services, illegal content removal, cybercrime, jurisdiction.

1. LA SUPRESIÓN DE CONTENIDOS ILÍCITOS EN LOS MERCADOS DIGITALES.

La difusión de contenidos ilícitos en la red está suponiendo un reto para la aplicación del principio de legalidad. La rápida difusión de determinados contenidos y el carácter etéreo de la información obrante en la red da lugar a que la respuesta estatal llegue muchas veces demasiado tarde. Este hecho ha creado un espacio de inseguridad jurídica en los mercados digitales, que

el legislador ha pretendido corregir estableciendo mecanismos que permitan neutralizar este tipo de información ilícita. La situación descrita resulta si cabe más grave en el ámbito penal en el que los criminales se valen de la fugacidad de los contenidos digitales para poder escapar a la acción de las autoridades encargadas de la investigación del delito.

Los perjuicios de toda índole que se derivan de estos hechos suscitaron la cuestión de cuál sea el alcance de la responsabilidad de las empresas prestadoras de servicios digitales por el hecho de dar difusión a este tipo de información. La regla general, que se ha mantenido hasta la fecha, es que la condición de meros intermediarios del flujo de los contenidos digitales cuyo contenido les era desconocido les exoneraba de responsabilidad[1]. Sin embargo, esto no resultaba tan claro cuando la transmisión afectaba a grandes volúmenes de información[2]. La difusión de información cuando se lleva a cabo fuera del marco prestablecido donde fue emitida puede dar lugar a efectos colaterales que van más allá de la intención del transmisor. Es por tal razón que la jurisprudencia, primeramente, en materia de protección de datos y luego en diversos ámbitos, ha establecido especiales cargas de diligencia para los prestadores de servicios digitales que relativizan la regla de exoneración en estos supuestos[3].

Así se venían aplicando normas sectoriales para tipos de contenidos especialmente nocivos, en el que se delegaba en las empresas de prestación de servicios la facultad de retirar aquellos que pudieran resultar especialmente

---

[1] Véase en este sentido, las sentencias resolviendo la pretensión de requerimiento general e indiferenciado a compañías que gestionan archivos P2P en orden a la identificación de archivos sobre los que el solicitante alegue ser titular de derechos de propiedad intelectual, pretensión ejercitada por la sociedad de autores belga y desestimada por el Tribunal de Justicia de la Unión Europea en los casos SSTJUE 24/11/2011 ECLI:EU:C:2011:771 C-70/10, Scarlet Extended SA, caso c. SABAM 16/02/2012, C-360/10 ECLI:EU:C:2012:85, caso SABAM c Netiog NV.-

[2] Según Teruel Lozano es a partir de 2016 como consecuencia de la sentencia del TEDH en el caso Delfi c. Estonia cuando se produce en Europa un gran cambio en la comprensión de la responsabilidad de las plataformas digitales. En dicha sentencia se concluyó que no violaba el Convenio un Estado miembro que hiciese responsable a los portales de Internet «si no toman medidas para eliminar comentarios claramente ilegales sin retraso, incluso sin previo aviso de la presunta víctima o de tercero». Teruel Lozano, G. «Libertad de expresión, censura y pluralismo en las redes sociales: algoritmos y el nuevo paradigma regulatorio europeo», en la obra colectiva Derecho Público de la inteligencia artificial, coord. Balaguer Callejón, F. y Cotino Hueso, L., Fundación Giménez Abad: Zaragoza (2023): 198.

[3] Hasta el presente, como afirma Teruel Lozano, «la normativa europea ha sido muy parca al respecto en buena medida de forma deliberada habida cuenta de que su objeto es lograr la mayor celeridad en la retirada de estos contenidos. De ahí que la mayoría de las garantías que se preen sean a "a posteriori" con los mecanismos de reclamación previstos, los instrumentos de revisión de las decisiones automatizadas y el deber de conservar los contenidos», Teruel Lozano, G. «Una lectura garantista de las nuevas tendencias en la lucha europea contra la difusión de mensajes terroristas en Internet», Revista de derecho constitucional europeo, núm. 34 (2020): 6.

perjudiciales. La Directiva de abuso sexual infantil (2011) fue la primera en exigir a los Estados miembros que garantizasen que los intermediarios de los sitios web que contengan o distribuyan pornografía infantil retirasen esos contenidos[4]. Lo mismo estaba ocurriendo en materia de lucha contra el terrorismo[5], discurso del odio[6], protección de la propiedad intelectual y derecho de marcas[7]. Como consecuencia de estas acciones, la Estrategia para el Mercado Único Digital adoptada en mayo de 2015 por la Comisión Europea había identificado el fomento de la equidad y la responsabilidad de las plataformas en línea como un ámbito en el que era necesario seguir actuando para garantizar un entorno digital justo, abierto y seguro a cuyo efecto se imponían especiales obligaciones a las empresas prestadoras de servicios digitales[8]. Sin embargo, después de que la Comisión Von der Leyen anunciara que propondría una nueva ley para modular la responsabilidad de las plataformas en línea[9], el Parlamento Europeo consideró que las exenciones deberían seguir aplicándose a las plataformas digitales que no tengan conocimiento real de las actividades o informaciones ilegales transmitidas[10].

El Reglamento (UE) 2021/784 de lucha contra el terrorismo, como veremos, supuso un cambio transcendental al habilitar a las autoridades estatales, y en concreto a las autoridades gubernativas, para que procediesen a la retirada de contenidos digitales que puedan comprometer la seguridad pública, subrogándose de alguna manera en la posición de los prestadores

---

[4] Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo. «DOUE» núm. 335, de 17 de diciembre de 2011.

[5] Decisión Marco 2005/671/JHA [2017] OJ L 88/6, art 21.

[6] Véase entre estas iniciativas la referente a la exclusión de contenidos relativos al discurso del odio. The EU Code of conduct on countering illegal hate speech online *https://commission.europa.eu/document/download/551c44da-baae-4692-9e7d-52d20c04e0e2_en*.

[7] Directiva 2001/29/EC [2019] OJ L 130/92.

[8] La Comisión inició la investigación en el sector del comercio electrónico en mayo de 2015 en el contexto de su estrategia para el mercado único digital, resultado del cual dio lugar al informe de la Comisión Europea « Informe preliminar sobre la investigación en el sector del comercio electrónico (15 de septiembre de 2016)», estos trabajos concluyeron a comunicación de la Comisión «la revisión intermedia de la aplicación de la Estrategia para el Mercado Único Digital Un mercado único digital conectado para todos» SWD (2017) 155 final.

Véase: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0228*.

[9] Informe de la Comisión Europea "A union that strives for more; the fist 100 days" https://neighbourhood-enlargement.ec.europa.eu/news/union-strives-more-first-100-days-2020-03-06_en, citado por Buiten, M.C. «Digital Service Ac: form Intermediary Liability to Plattform Regulation», Journal of Intellectual Property Informacion, Technology and E-Commerce, (dic. 2021): 364.

[10] Véase, «Report on the Digital Services Act and fundamental rights issues posed», octubre 2020, Committee on Civil Liberties, Justice and Home Affairs, Kris Peeters. https://www.europarl.europa.eu/doceo/document/A-9-2020-0172_EN.html.

de servicio[11]. Debe recordarse que la habilitación de los prestadores de servicios para supervisar determinados contenidos resultaba una consecuencia del marco contractual de las condiciones generales de prestación de servicio que condicionaba el uso de los servicios digitales contratado. Como apunta Arangüena Fanego, de un instrumento de cumplimiento «voluntario» se pasa a las «órdenes de retirada» cuya denominación ya pone de manifiesto su grado de vinculación al ser de obligatorio e inmediato cumplimiento por su destinatario[12]. El hecho es que, al autorizarse a la autoridad gubernativa para que pudiese retirar los contenidos ilícitos, se ha venido a reconocer la preexistencia de un orden público cuyo contenido y alcance resultaba, cuando menos, bastante discutible.

El Reglamento (UE) 2022/2065 de mercado de servicios digitales, en adelante RMSD, que entrará en vigor el 17 de febrero de 2024 ha hecho extensiva estas facultades a cualquier clase de contenido ilícito, no necesariamente constitutivo de delito. Junto a estas previsiones, se establece el marco en el que dichos servicios pueden prestarse[13], fijando de una parte especiales obligaciones de diligencia por parte de las empresas que suministran servicios de internet, y de otra, habilitando mecanismos excepcionales para suprimir contenidos ilícitos cuyo concreto contenido y alcance se difiere a las legislaciones nacionales[14].

Hasta el momento presente la legislación procesal se ha ocupado extensamente de las limitaciones que representa la intervención de las comunicaciones confidenciales, dando por hecho la posibilidad de acceder a contenidos en abierto. El hecho es que la rapidez de la extensión y la fugacidad de los

---

[11] Según Arangüena Fanego, citando a Galán Muñoz, afirma que se ha llegado a hablar, 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, Galán Muñoz, A. «Redes sociales discurso terrorista y Derecho penal, entre la prevención, la libertades fundamentales y ¿los negocios?» en la obra colectiva Galán Muñoz A. y Gómez Rivero C. (dir.), *La represión y persecución penal del discurso terrorista*, (Valencia 2022), p. 293; Cf.. Arangüena Fanego, C., «Nuevos pasos contra el terrorismo en la UE: Reglamento (UE) 2021/784». Revista de Estudios Europeos, núm. extraordinario monográfico 1 (2023): 79.

[12] Arangüena Fanego, C., «Nuevos pasos contra el terrorismo en la UE: Reglamento (UE) 2021/784». Revista de Estudios Europeos, núm. extraordinario monográfico 1 (2023): 79.

[13] Sobre los pasos pendientes para su entrada en vigor véase https://digital-strategy.ec.europa.eu/es/policies/digital-services-act-package.

[14] La entrada en vigor de este Reglamento quedará, sin embargo, en gran parte condicionada por la entrada en vigor del Reglamento (UE) 2022/1925) sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales) que entrará en vigor el 2 de mayo de 2023, y que condicionará en gran medida la gestión de los servicios de mensajería, (véase sobre este particular Tapia Hermida, A. J. «Los veinte principios básicos de la Digitalización Mercantil Europea, Diario La Ley, núm. 10251 (2023).

contenidos digitales es un aspecto que hoy por hoy se presenta como especialmente idóneo para la comisión del delito. La posibilidad de actuación a prevención se muestra como una quimera y las actividades delictivas se extienden de una forma imparable, como una mancha de aceite, sin posibilidad de intervención efectiva por parte de los tribunales de justicia. La acción preventiva por medio de las órdenes de actuación y retención de datos que se prevén en el RMSD se muestra como la única forma de intervenir este tipo de contenidos, pero al hacerlo así, entra en conflicto no tanto con el derecho a la confidencialidad de las comunicaciones, como con el derecho mismo a recibir y transmitir información.

Al tiempo de escribir estas líneas, la falta de un desarrollo normativo por parte del Estado español de estas nuevas herramientas nos impide hacer un juicio en profundidad sobre el alcance de la reforma en el ámbito de la investigación penal. El hecho es que el precedente habido en el Reglamento 2021/784, en materia de contenidos terroristas, nos pone en la pista del alcance de estas nuevas herramientas, lo que hace necesario abordar cuales pueden ser sus límites en este ámbito[15].

2. LA RETIRADA DE CONTENIDOS ILÍCITOS POR LAS EMPRESAS DE PRESTACIÓN DE SERVICIOS DIGITALES EN LA LEGISLACIÓN DE PROTECCIÓN DE DATOS.

La información difundida de forma indiscriminada a un número indeterminado de destinatarios puede producir efectos inicialmente no pretendi-

[15] El texto finalmente aprobado resultado de un larguísimo proceso legislativo ha sido criticado por no haber abordado todas las cuestiones que se encontraban pendientes en una materia por lo demás bastante polémica. En concreto, entre estas ausencias, la principal de ellas según Savin se encontraba en la ausencia de previsiones con relación al sector de las telecomunicaciones, los servicios digitales y el mundo de los medios audiovisuales. Las propuestas se limitaron a operar con la división establecida en la legislación precedente, sin cuestionarla. Una alternativa al régimen actual podría haber sido una regulación basada en los servicios, que incluyera todos los servicios bajo un mismo instrumento legislativo y mantuviera una previsión separada para los servicios de telecomunicaciones. En segundo lugar, no se aborda con el suficiente detalle los problemas relacionados con la privacidad, se omiten las cuestiones del tratamiento de datos a gran escala, la dependencia de los datos y la exclusividad de los datos (algunos de los cuales son comunes la legislación sobre competencia y al derecho de marcas). Por último, apenas se reconoce el avance de la realidad mediada por la Inteligencia Artíficial. Al final, sin embargo, el éxito de la ley dependerá no tanto de su capacidad para aportar una solución a todas las cuestiones, ya que esto puede corregirse con legislación posterior, como de su poder para encontrar el equilibrio adecuado entre los diversos intereses afectados. Savin, A., «The EU Digital Services Act: Towards a More Responsible Internet» (February 16, 2021), CBS LAW Research Paper, núm. 21-04, disponible en *https://ssrn.com/abstract=3786792*, (consultado: 09/10/2022): 16.

dos[16]. Como hemos señalado en otros foros, la STJUE de 13 de mayo de 2014, en el caso Google c. Costeja, C-131/12[17], puso por primera vez de manifiesto las consecuencias de la difusión indiscriminada de la información fuera del marco al que inicialmente estaba destinada[18]. Para corregir estos excesos fijó correctamente el alcance del derecho a la supresión de datos como el derecho que el individuo tiene a evitar que, a través del tratamiento automatizado de los datos, se pueda dar difusión a ciertos hechos o circunstancias, que, de no intervenir los motores de búsqueda, no serían generalmente conocidos[19]. Pero lo más relevante, y que luego en el Reglamento General de Protección de Datos ha constituido el eje de la normativa en materia del derecho al olvido, son las responsabilidades que les fueron impuestas a los prestadores de servicios de internet por el hecho de difundir de forma automatizada datos de carácter personal. El artículo 17 estableció que los prestadores de servicios digitales estarían obligados, teniendo en cuenta la tecnología disponible y el coste de su aplicación, a la adopción de medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de aquellos[20].

De este modo la tutela de los intereses de los titulares de los datos personales queda en buena medida delegada en los operadores en línea quienes están llamados a corregir las disfunciones del sistema[21]. Su ejercicio, en todo caso, no tiene carácter absoluto, quedando supeditado a la interpretación de su al-

---

[16] Véase también en este sentido De Miguel Asensio, P.A., «Reglamento (UE) de Servicios Digitales», La Ley Unión Europea, núm. 109 (diciembre 2022): 3.

[17] ECLI:EU:C:2014:317.

[18] Gudín Rodríguez-Magariños, A. E. «Derecho al Recuerdo: examen comparado de la normativa de preservación de datos en los Estados Unidos y en la Unión Europea» Revista Jurídica de Castilla y León», núm. 55, (2021): 72.

[19] Señala Rodríguez Lainz, como dentro de la difícil convivencia entre la Directiva 2002/58/CE y el Reglamento (UE) 2016/679, regida por la compleja norma de remisión del art. 95 del Reglamento General de protección de datos, la Directiva (UE) 2016/680 representaría un argumento adicional en favor del tratamiento de estos datos conservados por motivos comerciales para fines de investigación en la lucha contra la delincuencia grave. Tal deber de cesión de datos, que ya encontraría por basamento jurídico el propio mandato del art. 15.1 de la Directiva 2002/58/CE, no comportaría, por otra parte, en modo alguno una carga adicional a los proveedores. Rodríguez Lainz, J. L. «La evolución de la jurisprudencia del Tribunal de Justicia de la Unión Europea en materia de conservación indiscriminada de datos de comunicaciones electrónicas en la STJUE del Caso G.D. y Comissioner an Garda Síochána» Diario La Ley, núm. 10058, Sección Tribuna (28 de abril de 2022).

[20] Kuner, C., «The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges» en la obra colectiva Burkhard Hess & Cristina M. Mariottini (Coord.) *Protecting Privacy in Private International and Procedural Law and by Data Protection* (Ashgate/Nomos, 2015): 19.

[21] Véase en este sentido, Lee, quien equipara la función de los responsables de los grandes motores de búsqueda al de las agencias estatales con poderes regulación, decisión y ejecución semejante al de aquellas, véase Lee, E. «Recognizing Rights in

cance y de los medios disponibles por los responsables de tratamiento. Estos podrían rechazar la solicitud de supresión de datos además de en el caso de cumplimiento de una obligación legal que requiera el tratamiento de datos, en los supuestos de cumplimiento de una misión realizada en interés público o de ejercicio de poderes públicos conferidos al responsable del tratamiento (art. 17.2 RGPD)[22].

La intervención de las empresas en los mercados digitales es consecuencia del marco contractual establecido entre estas y los usuarios, en el que, si bien la definición de su contenido es enteramente libre, no lo es tanto el alcance de la difusión de los contenidos digitales. La difusión de estos contenidos está condicionada por los deberes de cumplimiento normativo al que están sometidas a su vez las empresas prestadoras de servicios digitales. Esta relación de sujeción especial de los prestadores de servicios digitales explica que se les habilite para limitar la difusión de los contenidos digitales. Se dota así de facultades de policía, que como veremos son limitadas al carecer de iniciativa para la pesquisa y monitorización de las redes, pero que les permite intervenir a instancia de los afectados para corregir abusos[23].

A partir de estos postulados el legislador europeo se ocupó especialmente de engrosar dichas facultades en atención a principios de orden público a la que dichas compañías estaban especialmente afectas. Véase en este sentido, la Resolución del Parlamento Europeo, de 15 de junio de 2017, sobre las plataformas en línea y el mercado único digital 2016/2276(INI) que constituye como veremos el precedente directo de la normativa de supervisión de contenidos ilícitos. Posteriormente, la Comunicación de la Comisión sobre la lucha contra el contenido ilícito en línea de 28 de septiembre de 2017 COM(2017) 555, y muy en particular su Recomendación de 1 de marzo de 2018, sobre medidas para combatir eficazmente los contenidos ilícitos en línea COM(2018)1177 refuerzan esta idea de sujeción a un orden público como requisito para actuar en el mercado.

Todas estas normas constituyeron hitos muy destacados que marcaron el camino a seguir en los años siguientes. Los últimos pasos en este proceso se encuentran dirigidos al reconocimiento a la autoridad competente de la facultad de dictar órdenes para la supresión de los contenidos ilícitos, primero con relación a los contenidos terroristas en el Reglamento (UE) 2021/784, y posteriormente respecto de cualquier otro contenido en el Reglamento (UE)

Real Time: The role of Google in the European Right to be forgotten», University of California, Davis Law Review, Vol. 49., (2016): 1017 a 1095.

[22] Véase en este sentido STJUE de 6 de octubre de 2020 en el caso Quadrature du Net, asunto 512/18, cdos. 193 a 212, STJUE de 24 de noviembre de 2011, Scarlet Extended, C70/10, EU:C:2011:771, cdos. 40; de 16 de febrero de 2012, SABAM, C360/10, EU:C:2012:85, cdo. 34; de 15 de septiembre de 2016, Mc Fadden, C484/14, EU:C:2016:689, cdo. 55, y de 7 de agosto de 2018, SNB-REACT, C521/17, EU:C:2018:639, cdo. 42.

[23] De Miguel Asensio, P. «Aplicación del derecho a la supresión de enlaces por buscadores». https://pedrodemiguelasensio.blogspot.com/2020/01/aplicacion-del-derecho-la-supresion-de.htm. Consulta 8/10/2023.

2022/2065 que es objeto del presente estudio. Las órdenes de actuación e información de contenidos digitales que en dicha normativa se contemplan suponen un salto cualitativo cuyo alcance y eficacia exige cuando menos una revisión crítica[24].

3. LA LUCHA CONTRA LA DIFUSIÓN DE CONTENIDOS TERRORISTAS EN LÍNEA, EL REGLAMENTO (UE) 2021/784.

El Reglamento (UE) 2021/784, de lucha contra la difusión de contenidos terroristas, supuso un punto y aparte en la acción de las autoridades estatales para limitar la difusión de contenidos obrantes en el mercado digital que puedan promover el terrorismo. Hasta entonces la acción supervisora se limitaba al control de las normas de cumplimiento del marco contractual de la prestación de servicios digitales. El Reglamento, como decimos, dio un paso más adelante en orden a la intervención de las autoridades en el mercado digital, habilitando directamente la retirada de contenidos ilícitos, en este caso, vinculados al mensaje terrorista.

A este objeto se articula en su artículo 13 la posibilidad de emisión ordenes de retirada de datos que incluso pueden tener carácter transfronterizo. Tal como hemos apuntado anteriormente, de un instrumento de cumplimiento normativo se pasa directamente a órdenes de carácter marcadamente compulsivo[25], en las que el proveedor no tiene obligación, ni posibilidad alguna de valorar la orden, ni de decidir si la misma es correcta, sólo ha de cumplirla[26].

El Reglamento no determinaba que tipo de autoridad resultaría competente para la expedición de las órdenes. En el apartado 35 de la exposición de

---

[24] Así con referencia a la propuesta de Reglamento sobre lucha contra la difusión de contenidos terroristas, lo que luego sería el Reglamento (UE) 2021/784, Teruel Lozano, señalaba «*es deseable que las órdenes de retirada contenidos en línea sean decididas por una autoridad judicial, en lugar de administrativa o policial, a través de un procedimiento más garantista; y debería contemplarse con las las posibilidades de recurso judicial cuando se bloquee el acceso o se retire un contenido, incluso en los casos en los que la decisión haya sido adoptada por un operador privado. Adicionalmente se ha propuesto que los poderes públicos velen porque las plataformas y a los proveedores de servicios respeten la neutralidad en internet y salvaguarden su pluralismo, y no sólo se preocupen por colaborar con ellas para eliminar contenidos ilícitos*». Teruel Lozano, G. «Una lectura garantista de las nuevas tendencias en la lucha europea contra la difusión de mensajes terroristas en Internet», *Revista de Derecho Constitucional Europeo*, núm. 34, (2020): 14.

[25] Arangüena Fanego, C. «Nuevos pasos contra el terrorismo en la UE: Reglamento (UE) 2021/784 y las órdenes de retirada de contenidos terroristas en línea». Revista de Estudios Europeos, núm. Extra 1, 2023, Ejemplar dedicado a: Consolidación del Espacio Europeo de Libertad, Seguridad y Justicia en materia penal (2023): 79.

[26] Galán Muñoz, A. «Redes sociales discurso terrorista y Derecho Penal. Entre la prevención, las libertades fundamentales y los ¿los negocios?» en la obra colectiva *La represión y persecución penal del discurso terrorista*, editorial Tirant Lo Blanc, Valencia, (2022): 293.

motivos se señalaba que correspondía a los Estados miembros decidir el número de autoridades competentes que deban designarse, y si son administrativas, policiales o judiciales, si bien en todo caso las autoridades competentes desempeñan sus funciones de forma objetiva y no discriminatoria, a cuyo efecto se les prohíbe que acepten instrucciones de ningún otro organismo en relación con el ejercicio de las funciones que el reglamento les confiere.

La referencia a una autoridad independiente, que ejercite sus funciones, sin estar vinculada a las instrucciones de otro organismo, hizo pensar a muchos en una remisión a las previsiones contenidas en el artículo 51 del RGPD respecto a las autoridades de control independiente. En este sentido, y con referencia a la propuesta de Reglamento, Gil García entre otros autores daba por sobrentendido, que esta autoridad independiente tendría que ser una autoridad judicial, postulando en concreto que la emisión de este tipo órdenes debería de corresponder a los juzgados centrales de instrucción[27]. En esta misma línea, se pronuncia Teruel Lozano, quien, como luego veremos, se muestra especialmente crítico por estimar que dicha asignación pueda entrar en conflicto con la proscripción constitucional de censura previa[28].

El hecho es que la mayoría de los países se han inclinado por confiar estos cometidos a las autoridades policiales adscritas al Ministerio del Interior. Tal es el caso de Alemania, Bulgaria, Croacia, Chipre, Chequia, Dinamarca, Eslovaquia, Estonia, Finlandia, Francia, Irlanda, Lituania, Letonia, Luxemburgo y Suecia. En el caso de Bélgica, se optó por la Fiscalía y en el de Holanda por el Ministerio de Justicia, Austria y Rumania por su parte confiaron estas funciones una agencia estatal encargada de la regulación de las comunicaciones audiovisuales, siendo Malta el único país que ha confiado estos cometidos a los tribunales de justicia, concretamente a la sección criminal del Tribunal de Justicia de aquel país[29]. En lo que se refiere a España, el órgano designado es el Centro de Inteligencia contra el terrorismo y la Delincuencia Organizada (CITCO), organismo dependiente del Ministerio del Interior, adscrito a la Secretaria General de Seguridad, al que corresponde la recepción, integración y análisis de la información estratégica disponible en la lucha contra todo tipo de delincuencia organizada o grave, terrorismo y radicalismo violento, el diseño de estrategias específicas contra estas amenazas y su financiación. Le corresponde en particular el establecimiento de criterios de actuación y

---

[27] 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 la obra colectiva» Estudios sobre tecnologías disruptivas y justicia: FODERTICS 8.0: estudios sobre tecnologías disruptivas y justicia / coord. por Irene González Pulido; Federico Bueno de Mata (dir.), Lorenzo Mateo Bujosa Vadell (pr.), 2020,): 348 y 349.

[28] Teruel Lozano, G. «Una lectura garantista de las nuevas tendencias en la lucha europea contra la difusión de mensajes terroristas en Internet», *Revista de Derecho Constitucional Europeo*, núm. 34 (2020): 4.

[29] *https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online/list-national-competent-authority-authorities-and-contact-points_en.*

coordinación operativa de los órganos u organismos actuantes en los supuestos de concurrencia en las investigaciones sobre los mismos delitos, a cuyo efecto la coordinación con los juzgados centrales y con el servicio de ejecutorias de la Audiencia Nacional está siendo decisiva en orden a neutralizar las acciones terroristas[30].

La justificación de la creación de este nuevo mecanismo, como apunta Arangüena Fanego, reside en la necesidad de atajar la propagación del mensaje terrorista, dada la facilidad con que se difunde en las redes y el crecimiento exponencial no sólo de adoctrinamiento, sino también de fijación de objetivos y de planeamiento de ataques terroristas[31]. La difusión de estos contenidos al amparo del anonimato que proporcionan los medios digitales constituye un riesgo para la población que sólo puede ser conjurado mediante el cese de la difusión de los contenidos terroristas. Como consecuencia de ello, el Reglamento 2021/784 (UE) impone nuevas obligaciones a los prestadores de servicios de alojamiento de datos que actúan en la Unión Europea, entre las que se encuentra la de cumplir en menos de una hora con la orden de retirada o bloqueo de los contenidos terroristas ordenada por la autoridad competente de un Estado miembro.

4. LA SUPRESIÓN DE CONTENIDOS ILÍCITOS EN EL REGLAMENTO 2022/2065 DE REGULACIÓN DEL MERCADO DE SERVICIOS DIGITALES.

El Reglamento 2022/2065 sigue la línea marcada por el de 2021 haciendo extensivas las facultades que las autoridades estatales venían ejercitando en el marco de prevención de contenidos terroristas a cualesquiera otros contenidos ilícitos. Con todo, el Reglamento no define qué contenidos en línea son ilícitos, ni cual pueda ser el alcance de la ilicitud que permita habilitar tan extraordinarios medios, limitándose a remitirse a lo dispuesto en el Derecho de la Unión o de un Estado miembro en el entendimiento que lo es toda información que vulnere el Derecho de la Unión o de un Estado miembro-art. 3.h) del RMSD[32]. Estos no tienen por qué ser necesariamente constitutivos de

[30] Dicho organismo constituía ya punto nacional de contacto con la EU Internet Referral Unit de Europol, agencia que ha desarrollado una herramienta denominada PERCI, que facilita el contacto entre las autoridades competentes nacionales y los prestadores de servicios de internet.

[31] Arangüena Fanego, C. «Nuevos pasos contra el terrorismo en la UE: Reglamento (UE) 2021/1784 y la orden de retirada de contenidos terroristas en línea». *Revista de Estudios Europeos*, n.º Extraordinario monográfico 1 (2023): 68.

[32] Para De Miguel Asensio resultaría más acertado referirse al Derecho que resulte aplicable, como hace el cdo. art. 12, pues no cabe descartar que, en particular en los litigios en materia civil y mercantil, pueda ser el de un tercer Estado. De Miguel Asensio, P. «Obligaciones de diligencia y responsabilidad de los intermediarios: El Reglamento (UE) de Servicios Digitales». *La Ley Unión Europea*, núm. 109, diciembre (2022): 6.

delito u otras infracciones graves, de hecho, se prevé que puedan aplicarse respecto de abusos en materia de condiciones generales de contratación, en materia de propiedad intelectual, derecho de marca o derecho al olvido. El objeto del reglamento es dotar a las autoridades estatales de un instrumento adecuado y seguro para combatir la presencia de estos contenidos que pueden poner en cuestión la aplicación del principio de legalidad en los mercados digitales.

Ese carácter instrumental es coherente con la constatación de que puede resultar imposible obtener el reconocimiento y ejecución de las resoluciones, en especial fuera de la UE. La problemática que se plantea respecto del uso de esta herramienta para la investigación del delito viene dada, por una parte, por los condicionantes exigidos por la presunción de inocencia, que impide su empleo con carácter prospectivo y general. De otra, una vez que se ha concretado el alcance que pueda llegar a tener la vulneración de la norma infringida, se hará preciso delimitar hasta qué punto pueda quedar afectado el derecho al entorno digital por el empleo de estos recursos por las autoridades gubernativas[33].

5. OBLIGACIONES DE DILIGENCIA DEBIDA.

La nueva regulación contenida en el Reglamento de Servicios Digitales, si bien, parte de la exención de responsabilidad de las prestaciones de servicio intermediarios, condiciona dicha exención al cumplimiento de las normas de diligencia que la propia ley previene, normas de diligencia que van a ser distintas según se trate de servicios de mera transmisión, memoria cache, alojamiento de datos o si vienen referidos a grandes plataformas de prestación de servicios digitales[34].

---

[33] Si se ha admitido, como veremos, la exclusión de contenidos substancialmente similares a los que ya hayan sido declarados ilegales, respecto de los que si se permite hacer extensiva la declaración de ilicitud (STJUE 3/10/2019, asunto C-18/18, caso Facebook; actualmente, se contemplaría en los arts. 4.3, 5.2 y 6.4 RMSD).

[34] Hasta entonces el alcance de la responsabilidad de las plataformas de servicios digitales en Internet había sido una cuestión polémica. La Comisión Europea, como parte de la Estrategia para el Mercado Único Digital adoptada en 2015, había declarado la necesidad de definir la responsabilidad de las plataformas en línea como un ámbito en el que resultaba imprescindible seguir actuando para garantizar un entorno digital justo, abierto y seguro. Después de que la Comisión Von der Leyen anunciara que propondría una nueva ley para modernizar estas materias el Parlamento Europeo mantuvo que los principios clave del régimen de responsabilidad siguen estando justificados, pero al mismo tiempo pedía más equidad, transparencia y responsabilidad en relación con la moderación de los contenidos digitales, garantizando el respeto de los derechos fundamentales y en su caso mediante una reparación independiente. Para ello, el Parlamento propuso un procedimiento detallado de notificación y retirada para combatir los contenidos ilegales, así como normas exhaustivas para la publicidad en línea y permitir el desarrollo y uso de contratos inteligentes. el desarrollo y la utilización de contratos inteligentes. El Consejo Europeo subrayó que las normas armonizadas sobre responsabilidades y rendición de cuentas para los servicios digitales

De este modo, se incluyen en su Capítulo II diversas reglas adicionales que pretenden complementar las normas preexistentes en materia de responsabilidad, al tiempo que establece en su Capítulo III un conjunto muy elaborado de obligaciones de «diligencia debida» adaptadas a diversas categorías de prestadores de servicios intermediarios en aquellos supuestos que el intermediario de servicios digitales actúa con la diligencia que le es exigible. El incumplimiento de la obligación de diligencia puede incluso determinar la obligación de indemnizar a los usuarios por los daños sufridos como consecuencia del incumplimiento de las obligaciones impuestas. La colaboración con las autoridades estatales que se encuentra implícita en el deber de diligencia exige también a las empresas que actúan en el mercado digital que procedan a la designación de un punto de contacto con las autoridades competentes por cada Estado miembro, así como la designación por cada uno de ellos de un coordinador de servicios digitales responsable de todo lo relativo a la aplicación del nuevo Reglamento. A todos ellos se les atribuyen competencia de investigación, ejecución y sanción (art. 51) y ante los que los usuarios de los servicios pueden presentar reclamaciones (art. 53).

6. FACULTADES DE LAS PLATAFORMAS DE PRESTACIÓN DE SERVICIOS EN ORDEN AL CUMPLIMIENTO DE LAS OBLIGACIONES DE DILIGENCIA.

Para llevar a efecto estos cometidos se dota a las plataformas de servicio en línea además de capacidad para la supresión de contenidos digitales, de facultades tanto para el cierre de cuentas, como de suspender o cesar la prestación de servicios respecto de las personas que muestren comportamientos abusivos. Se tratan, estas últimas, de facultades exorbitantes, en la medida que implican un juicio sobre la conducta de la persona y que están sujetas a formalidades especiales, tanto en lo que se refiere a su adopción, como a la notificación y recurso ante la jurisdicción ordinaria. Desde el punto de vista de nuestro ordenamiento jurídico penal una medida de esta índole sólo sería posible como una pena accesoria o una medida de peligrosidad amparada en la comisión de hechos constitutivos de delito[35].

Recientemente el Tribunal Supremo se ha pronunciado sobre este particular en la sentencia del pleno de la Sala Segunda del Tribunal Supremo 547/2022, de 2 de junio [ECLI:ES:TS:2022:2356], de la que fue ponente Mar-

---

deben garantizar un nivel adecuado de seguridad jurídica para los intermediarios de internet, véase *https://ec.europa.eu/commission/presscorner/detail/en/ip_20_403* accedido el 12 de mayo de 2021.

[35] Los magistrados disidentes quienes suscriben la posición contraria ponen de manifiesto el distinto alcance de la prohibición en la medida prevista en sentencia respecto de la contemplada en el artículo 48 del CP, en la medida que la pena impuesta se dirige a restringir la capacidad de comunicación; no su libertad deambulatoria, lo que exigiría cuando menos una previsión legal efecto.

chena Gómez, y que dio lugar a la presentación de votos particulares por parte de los magistrados Antonio del Moral y Javier Hernández García. En esta sentencia, que luego trataremos más detenidamente, se cuestionaba la posibilidad de hacer extensiva una pena accesoria de prohibición de concurrir a determinados lugares, al acceso de un youtuber a la conocida red social de elevación de videos digitales como consecuencia de la condena por un delito de aporofobia. Se afirma en la sentencia que «*la prohibición de acudir al lugar del delito, impuesta al amparo del art. 48 del CP, representa una de las distintas posibilidades que ofrece nuestro sistema para excluir el riesgo de nuevas ofensas, en el presente caso, a la dignidad de terceros. Pero no es, desde luego, la única*». Señalando como fórmulas alternativas la posibilidad de imposición de la pena de inhabilitación especial para el ejercicio de una profesión y oficio o incluso el comiso de la cuenta de *Youtube* del penado.

7. DILIGENCIA DEBIDA Y OBLIGACIONES DE CUMPLIMIENTO NORMATIVO EN ORDEN A LA AVERIGUACIÓN DEL DELITO.

Como hemos visto, las obligaciones de diligencia deben encuadrarse dentro del marco más amplio de las obligaciones de cumplimiento normativo que pueden exigir una actitud proactiva de las plataformas de servicios digitales. En este sentido, si bien la Directiva de Comercio Electrónico había declarado expresamente la inexistencia de una obligación general de monitorización o de búsqueda activa de hechos, principio que se ratifica en el RMSD, tal exoneración no excluye que las compañías de prestación de servicios digitales puedan llevar a efecto, en el marco de las obligaciones de cumplimiento normativo, la realización de investigaciones voluntarias por iniciativa propia.

En este sentido el art. 7 del RMSD inmediatamente antes de excluir la obligación de monitorización declara con una extraña técnica legislativa que no se considerará que los prestadores de servicios intermediarios no reúnen las condiciones para acogerse a las exenciones de responsabilidad a que se refieren los artículos 4, 5 y 6 por la sola razón de que realicen, de buena fe y de modo diligente, investigaciones por iniciativa propia de forma voluntaria, o adopten medidas con el fin de detectar, identificar y retirar contenidos ilícitos, o bloquear el acceso a estos, o adoptar las medidas necesarias para cumplir los requisitos del Derecho de la Unión y del Derecho nacional, incluidos los requisitos establecidos en el propio Reglamento[36].

[36] Y decimos que se trata de una extraña técnica legislativa en la medida que del tenor de la norma no se puede determinar con claridad a que razón responde estas facultades extravagantes de los prestadores de servicio, si obedece a una extensión de diligencia de las normas de cumplimiento o si es consecuencia accesoria de la habilitación conferida para la supresión de contenidos.

Tal posicionamiento se encuentra ajustado a la jurisprudencia que nace de la STJUE de 3 de octubre de 2019 en el caso Glawischnig-Piesczek, C-18/18, en la que se dispone la obligatoriedad de la eliminación de contenidos similares, cuando se cuenten con los elementos esenciales para poder determinar la ilicitud del contenido de una información alojada en las redes sociales (cdo. 45)[37]. En la indicada sentencia se planteó la posibilidad de adoptar tales medidas con carácter genérico, haciendo extensión de las facultades de supervisión a contenidos similares, pero no idénticos a los declarados ilícitos. El alto tribunal europeo declaró entonces, que habida cuenta que este tipo de redes sociales facilitan la transmisión rápida entre sus diferentes usuarios de datos e informaciones almacenadas por el prestador de servicios de alojamiento de datos, existe un riesgo real de que una información que ha sido declarada ilícita sea reproducida y compartida posteriormente por otros usuarios en la red.

En este sentido, si bien no existe una obligación general de supervisión o monitorización de las informaciones obrantes en las redes sociales (cdo. 37), una medida cautelar adoptada por la autoridad competente en el que se define los aspectos esenciales de un contenido ilícito debe habilitar su extensión a otros contenidos que transmiten esencialmente el mismo mensaje, aunque los términos utilizados o la combinación de estos difiera ligeramente de la información cuyo contenido ha sido declarado ilícito. De no poderse hace extensiva esta declaración de ilicitud a otros supuestos similares, tal como señala la sentencia comentada, «*los efectos de tal medida cautelar podrían eludirse fácilmente almacenando mensajes que apenas difieran de los mensajes declarados ilícitos con anterioridad, lo cual podría llevar a que el interesado tuviera que multiplicar los procedimientos al objeto de poner fin a los actos de los que es víctima*» (cdo. 41).

La resolución comentada fijó en el cdo. 25, los criterios para hacer extensiva la retirada de contenidos similares declarando que debe tratarse de una orden que contenga elementos concretos debidamente identificados por el autor de la medida cautelar, como el nombre de la persona víctima de la infracción constatada anteriormente, las circunstancias en las que se ha comprobado dicha infracción, así como un contenido similar al que se ha declarado ilícito. En cualquier caso, «*las diferencias en la formulación de ese contenido similar con respecto al contenido declarado ilícito no deben obligar al prestador de servicios de alojamiento de datos de que se trate a realizar una apreciación autónoma del referido contenido*», ni imponga una obligación excesiva impuesta al prestador de servicios de alojamiento de datos. La supervisión y la búsqueda que requieren este tipo de órdenes se limitan a los datos que contienen los elementos especificados en la medida cautelar acordada y su contenido difamatorio de naturaleza similar, pero no obliga al prestador de servicios de alojamiento de datos a realizar una apreciación autónoma, al poder este utilizar técnicas e instrumentos de búsqueda automatizados,

[37] STJUE de 3 de octubre de 2019, asunto *Eva Glawsching-Piesczek*, C-18/18, ECLI:EU:C:2019:821.

(véase también en este sentido la STJUE de 26 de abril de 2022 en el asunto *Polonia / Parlamento y Consejo*, C-401/19).

8. NIVEL DE DILIGENCIA DEBIDA EN ATENCIÓN AL GRADO DE TRATAMIENTO DE LA INFORMACIÓN.

Como hemos apuntado el RMSD establece un distinto nivel de exigencia según el grado de estabilidad de los datos en las plataformas de servicio digital. Siguiendo a Buiten cabría distinguir las siguientes categorías[38]:

— Servicios de mera intermediación (Intermediary Service), si la prestación de servicios digitales se limita a la transmisión automática de información.

— Plataformas de servicio (hosting service), si la información ha sido recibida en sus bases de datos al sólo objeto de canalizar la transmisión de información a tercero.

— Plataformas de almacenamiento (online plattforms), si han sido facilitados al objeto de que estos queden almacenados a petición del destinatario del servicio de forma indefinida.

— Grandes plataformas de prestación de servicios digitales a las que se imponen especiales deberes de diligencia en atención al volumen de información que es tratada (very large online plattforms, VLOPs).

Las dos primeras categorías, referidas a la mera transmisión y memoria cache, permanecen en lo sustancial inalteradas respecto de la Directiva de Comercio Electrónico 2000/31/CE (véase art. 21 y los arts. 4 y 5 del RSD con el cdo. art. 43 y los arts. 12 y 13 de la DCE). En el caso de los servicios de alojamiento, la novedad más importante a juicio de De Miguel Asensio es la inclusión de una previsión específica respecto de la responsabilidad en materia de protección en relación con la actividad de las plataformas en línea que permitan que los consumidores celebren contratos a distancia con comerciantes[39].

8.1. Prestación de servicios de mera intermediación (intermediary service)

Entre los supuestos de prestación de servicios digitales de mera transmisión se encontrarían los puntos de intercambio de internet, los puntos de acceso inalámbrico, las redes privadas virtuales, los servicios de DNS y traductores DNS, los registros de nombres de dominio de primer nivel, los registradores, las autoridades de certificación que expiden certificados

[38] Buiten, C.M. «The Digital Service Act from Intermediary Liability to platform regulation», 12, *JIPITEC* (2021): 367.

[39] De Miguel Asensio, P. «Obligaciones de diligencia y responsabilidad de los intermediarios: El Reglamento (UE) de Servicios Digitales». *La Ley Unión Europea*, núm. 109, (diciembre 2022): 6.

digitales, la transmisión de voz por internet y otros servicios de comunicación interpersonal. En estos casos, la exclusión de responsabilidad es total, siempre que no sea el emisor o destinatario de la información, y no seleccione o modifique la información contenida en la transmisión, circunstancia que por lo demás es inherente a su condición de mero transmisor. Buiten identifica la responsabilidad de estas empresas con una obligación general de diligencia debida (due diligence) en el marco de las obligaciones de cumplimiento normativo propio del sector de las comunicaciones, que está en la base de todo el sistema[40].

8.2. Plataformas de prestación de servicios intermediación digital (hosting service)

Supuestos de plataformas de prestación de servicios digitales (hosting service) serían los proxies inversos o los proxies de adaptación de contenidos (ver cdo. art. 29). La principal diferencia entre las plataformas de servicio digitales (hosting service) y las plataformas de almacenamiento se encuentra en que, mientras que en estas el tratamiento de la información se encuentra preordenada a su difusión, en el caso de las plataformas de alojamiento están orientadas a la conservación de los datos[41]. La exclusión de la responsabilidad en estos casos quedará condicionada, además de al hecho de no modificar la información, al cumplimiento de las previsiones siguientes: a que se cumplan las condiciones de acceso a la información, a que se cumplan las normas relativas a la actualización de la información conforme a las especificaciones técnicas propias del sector, a que no se interfiera en la utilización lícita de la tecnología y a que se actúe con prontitud para retirar la información que haya almacenado, o bloquear el acceso a ella, en cuanto tenga conocimiento efectivo del hecho de que una autoridad judicial o administrativa ha ordenado la retirada o el bloqueo de la fuente original de la información (art. 5.1 RMSD). La peculiaridad propia de este tipo de plataformas se encuentra en la posibilidad de discriminar la difusión de los contenidos, por lo que la obligación de diligencia de estos prestadores de servicio presenta una directa relación con las que son exigidas en materia de protección de datos. Esta se concreta en la capacidad de respuesta ante las irregularidades que eventualmente le sean puestas en su conocimiento.

---

[40] Buiten, C.M. «The Digital Service Act from Intermediary Liability to platform regulation», 12, *JIPITEC* (2021): 360.

[41] *Ibid.*: 361.

8.3. Plataformas de almacenamiento de datos (online platforms)

En lo que se refiere a los servicios de alojamiento de datos, la exoneración de las prestadoras de servicios digitales queda condicionado a que no tenga conocimiento de la existencia de una actividad ilícita y caso de detectar dichos contenidos ilícitos procedan con prontitud retirar el contenido ilícito alojado o se bloqueé su acceso. Tal deber de diligencia en orden a retirar dichos contenidos ilícitos, en todo caso, no se hace extensiva como hemos indicado a un seguimiento o monitorización de la información que transmitan o almacenen, ni menos aún, a buscar activamente hechos o circunstancias que indiquen la existencia de actividades ilícitas (art. 8 RMSD). Entre estos servicios se encontraría «*la computación en nube, el alojamiento web, los servicios remunerados de referenciación o los servicios que permiten compartir información y contenidos en línea, incluido el almacenamiento y el intercambio de archivos*».

Conforme a lo dispuesto en el apartado 3º del art. 6 del Reglamento, una plataforma de ese tipo no puede beneficiarse de la exención de responsabilidad en esa materia cuando «*presente el elemento de información concreto, o haga posible de otro modo la transacción concreta de que se trate, de manera que pueda inducir a un consumidor medio a creer que esa información, o el producto o servicio que sea el objeto de la transacción, se proporcione por la propia plataforma en línea o por un destinatario del servicio que actúe bajo su autoridad o control*». El reglamento establece dentro de estas últimas diversas especialidades según se trate de plataforma en línea, plataforma en línea que permita a los consumidores celebrar contratos a distancia con comerciantes o motor de búsqueda en línea. Estas subdivisiones, según De Miguel Asensio, son relevantes básicamente para concretar el alcance de las obligaciones de diligencia debida establecidas en el Capítulo III, pero no inciden, en principio, a la hora de fijar los beneficiarios de la exención de responsabilidad prevista en el art. 6 RMSD[42].

8.4. Grandes plataformas de transmisión de contenidos digitales.

El reglamento establece una legislación particularizada para los prestadores de servicio que presenten un gran volumen de tráfico de datos, entendiendo por tales a las plataformas en línea y motores de búsqueda que tengan un promedio mensual de destinatarios del servicio activos en la Unión igual o

[42] De Miguel Asensio, P. «Obligaciones de diligencia y responsabilidad de los intermediarios: El Reglamento (UE) de Servicios Digitales». *La Ley Unión Europea*, núm. 109, diciembre (2022): 9.

superior a cuarenta y cinco millones y a los que se designe como de tal condición por la Comisión a través del procedimiento establecido en el propio Reglamento (art. 33.4 RMSD)[43].

La posición de dominio que ejercen en el mercado digital ha determinado que el legislador europeo les haya impuesto especiales obligaciones de diligencia, por lo que se ha venido en llamar riesgo sistémico, atendido el hecho de su singular posición respecto de la difusión de contenidos y el acceso a información en línea[44]. De este modo se establece un régimen específico de supervisión, investigación y control con respecto a las plataformas de grandes dimensiones, respecto del que las competencias de la Comisión resultan determinantes[45]. Esta se reserva competencias de supervisión tanto en orden a la determinación su contenido y alcance, como en lo relativo a las situaciones de excepción contenidas bajo el ambiguo epígrafe «respuesta a las crisis»[46].

Dentro de este ámbito de diligencia de las grandes empresas de servicios digitales el artículo 22 se refiere a la exigencia de que estas empresas cuenten con especiales medidas técnicas y organizativas. Entre estas, se prevé que se dé prioridad a las notificaciones enviadas por alertadores fiables a través de los mecanismos a que se refiere el artículo 16, y de que se tramitan y resuelvan dichas alertas sin dilación indebida. La condición de «alertador fiable» será otorgada por el coordinador de servicios digitales del Estado miembro donde el solicitante esté establecido, previa solicitud de cualquier entidad interesada en prestar estos servicios que haya demostrado que posee conocimientos y competencias específicos para detectar, identificar y notificar contenidos ilícitos. Se exige también que no dependan de ningún prestador de plataformas en línea y que realicen sus actividades con el fin de enviar notificaciones de manera diligente, precisa y objetiva.

---

[43] La Comisión Europea procedió a la designación el 25 de abril de 2022, de las 17 compañías que tendrían la consideración de Grandes plataformas *on line*, así como dos motores de búsqueda todos los cuales quedarán sometidos a las especiales previsiones contenidas para este tipo de compañías. *https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413*

[44] De Miguel Asensio, P. «Obligaciones de diligencia y responsabilidad de los intermediarios: El Reglamento (UE) de Servicios Digitales». La Ley Unión Europea, Nº 109, (diciembre 2022): 6.

[45] *Ibid.*

[46] Para De Miguel Asensio, la referencia específica a los ilícitos derivados de la vulneración del «Derecho en materia de protección de los consumidores» en el art. 6.3º RSD, no debería impedir que se lograse ese mismo resultado respecto de otro tipo de ilícitos en circunstancias similares, y en las que, por cierto, tampoco resultará extraño que los intereses de los consumidores puedan verse afectados, como suceden en el ámbito de la competencia desleal o de la protección de marcas. *Ibid*: 9.

9. LA ORDEN DE ACTUACIÓN CONTRA CONTENIDOS ILÍCITOS

Junto a las obligaciones de cumplimiento normativo, vinculadas al deber de diligencia debida, la nueva ordenación de los servicios digitales contenida en el Reglamento de 2022 no se limita a condicionar la intervención de los prestadores de servicios intermediarios, sino que habilita a las autoridades de los Estados miembros para la emisión de órdenes de actuación para la supresión contenidos ilícitos, punto que constituye la gran novedad del Reglamento respecto del régimen existente en la Directiva. La exclusión de los contenidos digitales no se ampara en una transgresión que ponga en riesgo los derechos fundamentales de la persona, sino que puede hacerse extensiva a cualquier tipo de ilícito civil o administrativo que comprometa la seguridad del tráfico jurídico en el mercado de servicios digitales.

La declaración de ilicitud lo es en principio al ordenamiento nacional que resulte afectado, sin perjuicio, de la normativa europea que pueda ser aplicación. Como consecuencia de ello, el Reglamento no define que tipo de contenidos justifica la adopción de este tipo de órdenes, ni su ámbito de aplicación territorial, ni su eficacia transfronteriza, ni tampoco la condición de quien pueda expedir dichos mandamientos, admitiendo que puedan serlo autoridades judiciales o administrativas. De hecho, en principio, en lo que se refiere a la intervención judicial, el Reglamento únicamente habrá de suponer un mecanismo que permita simplificar el procedimiento para la supresión o entrega de contenidos digitales por cuanto tales facultades se presumen como propias del ejercicio de la jurisdicción.

La finalidad según De Miguel Asensio es armonizar ciertas condiciones mínimas de esas órdenes a fin de adecuar su cumplimiento al contexto transfronterizo y evitar así cargas excesivas a los intermediarios. A este objeto impone ciertas obligaciones con respecto a su configuración por las autoridades competentes, así como obligaciones a los intermediarios en relación con tales mandamientos. Tales condiciones y los requisitos que establece el art. 9 RMSD se entienden sin perjuicio del Derecho procesal nacional (art. 9. 6º)[47].

En todo caso se trata de una herramienta de carácter subsidiaria y limitada (arts. 5.1 y 5.3 del Tratado de la Unión Europea). Así, a tenor de lo previsto en el apartado segundo b del artículo 9, los Estados miembros deben velar por «*que el ámbito de aplicación territorial de dicha orden, en virtud de las disposiciones aplicables del Derecho de la Unión y nacional, incluida la Carta y, en su caso, los principios generales del Derecho internacional, se limite a lo estrictamente necesario para alcanzar su objetivo*[48]».

---

[47] De Miguel Asensio, P. «Obligaciones de diligencia y responsabilidad de los intermediarios: El Reglamento (UE) de Servicios Digitales». La Ley Unión Europea, Nº 109, diciembre (2022): 11.

[48] Véase en este sentido también el informe 22/2021 de la comisión mixta para la Unión Europea, de 16 de marzo de 2021, sobre la aplicación del principio de subsi-

La competencia con respecto a la expedición de la orden se atribuye al Estado miembro en el que se encuentre el establecimiento principal del prestador de servicios intermediarios, o en su defecto, el lugar de residencia o establecimiento del representante designado. Desconociéndose éste, todos los Estados miembros tendrán competencia. En cuanto, a la condición de la autoridad que expida la orden el Reglamento se refiere indistintamente a autoridades judiciales y administrativas, cuestión abordaremos con más detalle a continuación.

Con relación a la configuración de este tipo de órdenes, el art. 9.2º RMSD prevé que deben cumplir una serie de requisitos antes de ser transmitidas al prestador de servicios intermediarios al que se dirige la orden, debiendo concretar en aquel uno o varios elementos concretos de contenido ilícito y ajustarse a los trámites que en el propio precepto se establece.

En primer término, y con respecto a su contenido, se prevé que la orden debe incluir los siguientes elementos:

— En primer lugar, una referencia a su fundamento jurídico y motivación acerca de la calificación como ilícita de la información en cuestión; la identificación de la autoridad emisora.
— La identificación y localización del contenido ilícito (con indicación de la URL donde se ubican dichos contenidos).
— Los mecanismos de recurso disponibles para el intermediario y para el destinatario del servicio que haya proporcionado el contenido de que se trate; y, en su caso,
— Información sobre qué autoridad debe recibir la información sobre el curso dado las órdenes.

Respecto de su ámbito territorial, el art. 9.2º. b) acoge como veremos un criterio restrictivo al disponer que el ámbito territorial de la orden se limite a lo estrictamente necesario para alcanzar su objetivo.

En lo que atañe al procedimiento para llevarla efecto, se prevé en el reglamento un procedimiento extraordinariamente expeditivo, que obliga a los intermediarios que reciban una orden de actuación contra contenidos ilícitos de ese tipo a informar sin dilación a la autoridad que haya dictado la orden, o a cualquier autoridad especificada en ella, de cualquier curso que se pueda haber dado a aquella. Se simplifica además la trasmisión de la orden mediante su remisión a través de un sistema de corresponsalías bien conocido, y que se viene aplicando en diversos ámbitos en materia de cooperación internacional. Conforme a este mecanismo la orden expedida por la autoridad competente es remitida al coordinador de servicios digitales de su Estado miembro (art. 9.3 RMSD), quien la transmitirá, a todos los demás coordinadores de servicios digitales presentes en la propia oficina y estos a su vez a los prestadores de servicio intermediarios (arts. 9.4 y 95 RMSD).

---

diariedad en relación con la propuesta de Reglamento sobre mercados disputables y equitativos en el Sector Digital,

En todo caso, tal como se ve en el apartado 34 de los considerandos las disposiciones en este ámbito deben entenderse, sin perjuicio del Reglamento Bruselas I bis y del Derecho procesal nacional, lo que como señala De Miguel Asensio puede llevar a que resulten aplicables condiciones adicionales o incluso que deban adaptarse o no aplicarse algunas de las condiciones previstas en el RMSD[49].

Se impone asimismo al prestador de servicios de intermediación la obligación de informar al destinatario afectado del curso dado a la orden recibida, sino al tiempo del dictado de aquella o a lo más tardar en el momento que determine la autoridad emisora en su orden (art. 9.5º). No obstante, se contempla que algunas de estas obligaciones de información pueden retrasarse en atención a la legislación que resulte aplicable, en particular en el marco de un proceso penal, civil o administrativo (cdo. art. art. 34 RSD). Entre la información remitida deberá de incluirse la motivación para el dictado de la orden, vías de recurso disponibles y ámbito territorial.

10. LA ORDEN DE ENTREGA DE INFORMACIÓN.

Junto a la orden de actuación la ley prevé una nueva herramienta a disposición tanto de las autoridades judiciales como de las administrativas destinada a facilitar la obtención de información digital de características muy similares al previsto en el art. 9 RMSD, pero orientada en este caso a obtener información específica sobre uno o varios destinatarios individuales del servicio.

En este caso, como afirma De Miguel Asensio, el ámbito territorial de la orden no se considera un elemento relevante, sino que se impone la exigencia de que la orden «*solo requiera que el prestador aporte información ya recabada para los fines de la prestación del servicio y que esté bajo su control*» (art. 10.2º.b RMSD).

La regulación se limita al procedimiento a seguir sin entrar a conocer sobre cuales sean los contenidos digitales a los que pueda accederse o cual puedan ser las facultades de las autoridades autorizadas a enviarla. Su objeto es la identificación de las personas que reenvían dicha información, así como del tracto de los contenidos digitales recibidos. En tal supuesto, a diferencia de la intervención de las comunicaciones propiamente dichas, nos encontramos ante la transmisión informaciones en abierto cuyos contenidos son directamente accesibles, pero cuyo emisor es desconocido.

La orden de entrega de información tal como se presenta en el Reglamento es una normativa de carácter instrumental cuya concreta extensión y alcance va a venir determinada por la efectiva entrada en vigor de las previsio-

[49] De Miguel Asensio, P. «Obligaciones de diligencia y responsabilidad de los intermediarios: El Reglamento (UE) de Servicios Digitales». *La Ley Unión Europea*, núm. 109, (diciembre 2022): 11.

nes contenidas en el segundo protocolo de Budapest, en el que se contienen disposiciones muy concretas sobre el contenido y alcance de la entrega de información de contenidos ofrecidos en abierto, como son el acceso en directo a los nombres de domino de internet o la identificación de los abonados[50].

11. APLICACIÓN DE LA ORDEN DE ACTUACIÓN Y LA ORDEN DE ENTREGA DE INFORMACIÓN AL ÁMBITO PENAL

Como hemos señalado la regulación contenida en el Reglamento de prestación de servicios en los mercados digitales se halla dirigida a combatir cualquier tipo de contenidos que sean contrarios al orden público, no necesariamente penal, y de hecho las referencias presentes en aquel abarcan materias tan distintas como son el Derecho de consumo o el Derecho de propiedad intelectual. Con todo, no se debe desconocer que aún en estos casos la referencia última al orden penal se encuentra implícita, como pueda ser con relación a los ámbitos indicados, el delito de estafa o los delitos contra la propiedad intelectual.

De hecho el considerando 12 establece concretamente, como el concepto de «contenido ilícito» debe definirse de manera amplia para abarcar la información relacionada con contenidos, productos, servicios y actividades de carácter ilícito «*en particular, debe entenderse que dicho concepto se refiere a información, sea cual sea su forma, que sea de por sí ilícita en virtud del Derecho aplicable, como los delitos de incitación al odio o los contenidos terroristas y los contenidos discriminatorios ilícitos, o que las normas aplicables consideren ilícita por estar relacionada con actividades ilícita*»

Para Arangüena Fanego las nuevas órdenes de retirada de este tipo de contenidos en línea si bien se revelan como especialmente eficientes, «*generan cierto recelo sobre si realmente guardan el delicado y debido equilibrio entre velar por la seguridad de la ciudadanía frente al terrorismo mediante su prevención y el respeto de los derechos fundamentales garantizados por el artículo 11 de la Carta*[51]». Teruel Lozano, como hemos visto se cuestiona también la constitucionalidad de la habilitación a las autoridades administrativas y de policía para limitar un derecho fundamental como es el derecho a la libre transmisión de información, y se pregunta en concreto si esto pudiera cons-

[50] Sobre este particular y las nuevas herramientas que ofrece el segundo protocolo de Budapest, véase Gudín Rodríguez-Magariños, A.E. «El nuevo protocolo del Convenio de Budapest de lucha contra la cibercriminalidad». *Revista General de Derecho Procesal*, núm. 58, (2022): 26.

[51] Arangüena Fanego, C. «Nuevos pasos contra el terrorismo en la UE: Reglamento (UE) 2021/1784 y la orden de retirada de contenidos terroristas en línea». *Revista de Estudios Europeos*, n.º Extraordinario monográfico 1 (2023): 91.

tituir un tipo de censura previa proscrito por el art. 20.5 de la CE[52]. Cabría apuntar también la quiebra del principio de presunción inocencia, en la medida que las órdenes dictadas se justificarían en la presunción de que unos determinados hechos son constitutivos de delito, presunción cuyo conocimiento está reservado a los tribunales.

Estas limitaciones no dejan de constituir una limitación a la libre transmisión de información, pero el que esto sea así no tiene por qué suponer una vulneración de un derecho fundamental. La diferencia respecto de los supuestos tradicionales de secuestro de ediciones es que la difusión que otorgan los mercados digitales no atiende a un hecho ya sucedido del que se han adquirido ya derechos, como es una edición de una publicación, sino a un proceso que se está produciendo y cuya proyección depende de la difusión que el prestador del servicio pueda facilitar. La transmisión y el acceso a la información no es enteramente libre, sino que viene condicionada por la difusión de los contenidos dentro del marco de cumplimiento normativo a las que las propias empresas de servicios digitales se encuentran sometidas.

La STJUE de 6 de octubre de 2020, caso Quadrature du Net, C-5212/18 [ECLI:EU:C:2020:791] fue la primera en abordar la problemática respecto de la protección que deba merecer el sólo hecho de acceder a un sistema informático en abierto. Se trata en la sentencia, concretamente en los cdos. 193 a 214, de si resultaba contrario al derecho a la protección de datos una normativa nacional que impone a los proveedores de acceso a los servicios de comunicación al público en línea y a los proveedores de servicios de almacenamiento la obligación de proceder a la conservación generalizada e indiferenciada, en particular, de los datos de carácter personal correspondientes a estos servicios. En dicha resolución, si bien se pone de manifiesto que no son aplicables las previsiones en materia de protección de la confidencialidad de las comunicaciones, a los servicios de comunicación al público en línea y a los proveedores de servicios de almacenamiento, concretamente del art. 15 de la Directiva (CE) 2002/58, estima, sin embargo, que cabría llegar a la misma conclusión al amparo de las previsiones contenidas en el artículo 23, apartado 1, del Reglamento 2016/679, en relación con los artículos 7, 8 y 11 y el artículo 52, apartado 1, de la Carta (véase cdo. 212[53]). La sentencia co-

---

[52] Se señala por dicho autor: «… *las órdenes de retirada previstas por la propuesta de normativa europea entrarían dentro de lo que en sentido constitucional se considera secuestro de publicaciones: son medidas adoptadas de forma cuasicautelar por una autoridad, siguiendo un procedimiento expedito y que operan sobre el medio de publicación para evitar la difusión de un determinado mensaje*». Teruel Lozano, G. «Una lectura garantista de las nuevas tendencias en la lucha europea contra la difusión de mensajes terroristas en Internet». *Revista de Derecho Constitucional Europeo*, núm. 34 (2020): 4 y 5.

[53] Según la sentencia comentada, todo tratamiento de datos personales debe, sin perjuicio de las excepciones admitidas al amparo del artículo 23 del Reglamento 2016/679, respetar los principios que regulan el tratamiento de los datos de carácter personal, así como los derechos de la persona afectada previstos, respectivamente, en

mentada, desestima en base a dicho precepto las alegaciones efectuadas por los Gobiernos Belga y Francés, de asimilar la orden de retención de datos de las comunicaciones establecida por la legislación antiterrorista, con el caso que se trata en el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017[54] y que se ratifica en la sentencia de 3 de octubre de 2019, C-70/18[55], en el que se había admitido como lícito la posibilidad de retención por las aerolíneas de los datos de los pasajeros, estimando que en aquel caso existían razones de orden público que precedían a la orden de retención. De este modo, la retención debe responder en todo caso a criterios objetivos y ha de existir una relación entre los datos que deban conservarse y el objetivo que se pretende lograr (véase cdo. 133). La existencia de una relación antecedente y directa con la norma de orden público resulta determinante en orden a avalar una intromisión en materia de protección de datos.

El hecho es que la sentencia comentada no tiene presente la evolución la normativa de cumplimiento que condiciona el acceso a los mercados digitales. Se desconoce en concreto la existencia de normas de orden público que habilitan las potestades extraordinarias con las que cuentan las plataformas de prestación de servicios.

Como hemos visto una gran mayoría de la doctrina estima que la habilitación conferida se sustenta en una especial delegación de potestades de derecho público[56]. Es por tal razón, por las que estas objeciones no han supuesto hasta el presente un obstáculo en el ámbito de las facultades conferidas a las empresas de servicios digitales y particularmente de los motores de búsqueda, las cuales se encuentran habilitadas para suprimir el acceso a contenidos ilícitos. La razón de esta habilitación extraordinaria obedece al hecho de que no se pretende tanto suprimir la información, que de hecho se conserva en los sistemas, como eliminar los vínculos que permiten su difusión en los entornos digitales. Estas facultades, establecidas originariamente en orden a la tutela del derecho al olvido en la legislación de protección de datos, se desplaza a una norma de orden público que nace del solo hecho de la difusión de contenidos en la red más allá de la previsión inicial del emisor de la información.

---

los capítulos II y III de dicho Reglamento a cuyo efecto equipara las previsiones contenidas en el artículo 23, apartado 1 RGPD con las contenidas en el artículo 15, apartado 1, de la Directiva 2002/58 permite a los Estados miembros limitar, en relación con los fines que prevé y mediante medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en el mismo «cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar» (véase cdo. 208 y 209).

[54] EU:C:2017:592, cdo. 191.

[55] EU:C:2019:823, cdo. 63.

[56] Véase, Kuner, C. «The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges» in Burkhard Hess and Cristina M. Mariottini (eds), *Protecting Privacy in Private International and Procedural Law and by Data Protection* Ashgate/Nomos, (2015): 19.

La jurisprudencia del TJUE ha venido delimitando claramente entre las distintas actividades de tratamiento del editor y del gestor del motor de búsqueda y las posibles consecuencias respecto de los interesados en la información transmitida. Esto ha permitido la concesión de solicitudes de exclusión de las búsquedas contra los operadores en aquellos supuestos en que los datos pertinentes no se hubieran eliminado previa o simultáneamente de la página web de origen y cuando se hubieran publicado ilícitamente.

De hecho, cuando judicialmente se acuerda la supresión de contenidos ilícitos en la red, la acción de las autoridades se concreta en comisionar uno a uno a los distintos operadores afectados, sin que por lo demás exista, ni pueda existir una acción dirigida a la supresión de los archivos que eventualmente puedan obrar en los servidores.

Ciertamente, el Reglamento excluye una declaración formal de responsabilidad por las empresas de servicios digitales, y en tal sentido redunda una vez más en la inexigibilidad de una obligación de monitorización o búsqueda de archivos, pero el que esto sea así, no supone que las empresas de prestación de servicios digitales estén absolutamente al margen de las exigencias de orden público que exigen la supresión de los contenidos ilícitos que ponen en peligro la seguridad del mercado digital.

Cabe concluir, por tanto, en que la valoración de la ilicitud de estos contenidos se traslada del contenido en sí mismo de la información, a la ilicitud de su difusión mediante la incorporación de dichos contenidos a un sistema digital cuyo acceso se encuentra sujeto a sus propias normas de orden público.

12. HABILITACIÓN DE LAS AUTORIDADES GUBERNATIVAS PARA LA EMISIÓN DE ÓRDENES DE ACTUACIÓN Y DE ENTREGA DE INFORMACIÓN

Al igual que sucede en el Reglamento de 2021 de lucha contra los contenidos terroristas, el Reglamento de Mercados de Servicios Digitales habilita la posibilidad de que las órdenes que regula puedan ser emitidas tanto por autoridades gubernativas como judiciales, quedando al criterio de las legislaciones nacionales la determinación de la autoridad competente que en cada caso corresponda la emisión de aquellas

La extensión de estas facultades directamente a la Administración no está exenta de dudas, sobre todo cuando los contenidos ilícitos objeto de estas órdenes se encuentran relacionados con la investigación penal. Se presenta en estos supuestos una problemática especialmente ardua y compleja al incidir en el derecho a la presunción de inocencia e interferir en la exclusividad de la jurisdicción penal para la represión de las conductas delictivas.

Como hemos visto la cuestión resultó manifiestamente polémica, y contrariamente a la interpretación general de la doctrina, la mayoría de los Estados encomendaron estas funciones a servicios o agencias estatales dependientes

de la policía o del Ministerio del Interior. En el caso del RMSD como se ha señalado repetidamente el Reglamento atiende a una diversidad de ilícitos que no permiten dar una solución uniforme para todos los supuestos.

Un correcto entendimiento de estas cuestiones exige distinguir alcance de los poderes públicos en un Estado de Derecho respecto de la investigación de los delitos que ya se han cometido y las facultades en orden a prevenir un riesgo para la seguridad ciudadana. En el primero de los casos, el principio de presunción de inocencia excluye cualquier actuación prospectiva que cree una infundada sospecha genérica sobre grupos o colectivos de población. En tal caso, resultaría inevitable poner los hechos en conocimiento de la autoridad judicial y la ratificación de las medidas que pudiesen acordarse al amparo de la habilitación conferida a la fuerza actuante. Fuera de estos supuestos, la actuación propiamente de prevención solo está justificada por el riesgo de lesión real y concreto de los intereses de la población general o por el riesgo que determinados ilícitos pueden suponer para la seguridad pública o los derechos fundamentales de las personas[57].

Sobre el alcance de esta actuación a prevención, la sala cuarta del Tribunal Supremo se ha pronunciado recientemente en la STS 1231/2022, de 3 de octubre, poniendo de manifiesto las limitaciones de la actuación policial. Se trataba en el caso de la decisión de la Agencia Española de Medicamentos y Productos Sanitarios de proceder a la suspensión del sitio web, Women on Web International Foundation dedicada a la venta de productos farmacéuticos y concretamente a la adquisición de unos medicamentos prohibidos en España sin receta. El Tribunal Supremo estimó en parte el recurso interpuesto, limitando el bloqueo de aquellas partes de la web destinadas a ofrecer los medicamentos prohibidos, pero anulando el cierre de la página web ordenada por la autoridad gubernativa. La sentencia estima que «*los sitios web no pueden caracterizarse como "medios de información" cuando no contienen ninguna información ni expresión, sino que son un mero instrumento para realizar otra actividad", de tal manera que el art. 20.5 CE sólo "entra en juego cuando las publicaciones, las grabaciones o los otros medios de información son canales para la emisión y circulación de ideas, tanto si versan sobre hechos como si versan sobre valores" (FJ. 9)*». Esta condición, determina que la prohibición debe quedar restringida al hecho de las transacciones de productos farmacéuticos sin receta, pero no puede hacerse extensiva al sitio web en cuanto instrumen-

[57] El antiguo artículo 22 de la Ley 15/1999, de 13 de diciembre, distinguía así entre los supuestos que el tratamiento de datos respondiese a la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad, de aquellos supuestos en que se procediese a la investigación en concreto a hechos criminales ya sucedidos, solo en este supuesto admitía el acceso a los datos sensibles en estos supuestos, respecto de los que requería la intervención de una autoridad judicial. La directiva y la Ley 7/2021, de 26 de mayo, no distinguen en este punto, quedando al criterio de las autoridades nacionales concretar la intervención judicial en función de los intereses afectados.

to de difusión de información. El tribunal señaló entonces que la valoración de los hechos y la ponderación de los intereses que determinen el cierre de un medio de comunicación, como lo es una página web, si bien no está amparado en la libertad de expresión, en cuanto que su objeto no se constriñe a hacer valoraciones sino a dar información comercial, debe someterse necesariamente a una autoridad imparcial e independiente en cuanto limitación del derecho a transmitir y recibir libremente información[58].

Lo relevante de la sentencia es la distinción entre el instrumento de difusión de información, en este caso una página web, y los contenidos obrantes en aquel medio. Tal interpretación debe hacerse especialmente extensiva en relación con la creación de perfiles, cuentas de usuario, etc. En todos estos supuestos la acción policial de carácter preventivo debe limitarse al señalamiento de los contenidos ilícitos como antecedente necesario a la intervención judicial, pero sin que en modo alguno pueda hacerse extensiva al medio de difusión empleado.

El CITCO en este sentido lo ha venido entendiendo así, estimando que las facultades que se le atribuye se aplican únicamente a la retirada de concretos «contenidos terroristas» según la definición del reglamento por lo que, en principio, no permitiría la retirada de perfiles completos a menos que dichos perfiles pudieran considerarse como «contenidos terroristas» de manera global[59].

El caso es que en el medio informático lo relevante no es tanto los contenidos, o el lugar donde se ubican, como la difusión de la información. Una página web, de por si no representa mayor eficiencia en orden a la transmisión de contenidos digitales que pueda tener una publicación escrita. Lo que singulariza la información en medio del universo digital, en que las posibilidades de acceso de forma casual a esos contenidos son mínimas, es la capacidad de reconocer dicha información mediante la indexación de sus contenidos. Es esta condición la que permite que la información pueda ser reconocida por los usuarios.

---

[58] Para Teruel Lozano esta decisión debe tener un importante impacto ahora que se están definiendo los órganos de control de las plataformas digitales en el marco de la más reciente legislación europea, especialmente la *Digital Service Act*. A juicio de este autor, de acuerdo con esta jurisprudencia, debe reputarse inconstitucional la atribución al CITCO de la competencia de dictar órdenes de bloqueo y retirada de mensajes terroristas en Internet, prevista de conformidad con el Reglamento (UE) 2021/784 del Parlamento Europeo y del Consejo, de 29 de abril de 2021. Es más, para dicho autor, tendría dudas de la constitucionalidad de esta atribución, aunque la decisión de bloqueo se adoptara previa autorización judicial, pero sin que fuera el juez la autoridad decisoria, cualquier decisión restrictiva de la libertad de información debería ser llevada a cabo por un juez imparcial, en un proceso contradictorio con todas las garantías. Teruel Lozano, G.M. (15 de diciembre de 2022). «Bloqueo de contenidos en Internet y reserva de jurisdicción». *Blog del CEPC https://www.cepc.gob.es/blog/bloqueo-de-contenidos-en-internet-y-reserva-de-jurisdiccion*

[59] Contestación de fecha de 1 de agosto de 2023, a consulta del Servicio de Ejecutorias de la Audiencia Nacional, en el marco del procedimiento EJP 37/2023.

Debe tenerse presente que la indexación es una actuación que ofrecen los servicios de internet, pero que debe ser preparada por el usuario, eligiendo los algoritmos adecuados que permitan identificar los metadatos que definen los contenidos que son ofrecidos de forma pública. Esta facultad no resulta inherente a la adquisición del dominio sobre una dirección de internet o a la gestión de una cuenta de usuario. La inclusión de la información en un motor de búsqueda es una prestación que se ofrece por las empresas prestadoras de servicio de internet y que está sometida como hemos visto a las exigencias de orden público de los mercados digitales.

El debate que se presenta hoy es saber cuales sean las facultades de la autoridades gubernativas y judiciales para interferir en la prestación de este servicio, atendidas las obligaciones de cumplimiento normativo y los principios de orden público a los que están sometidos los mercados digitales. Como hemos visto esta es una cuestión de la mayor importancia en orden a la ejecución de determinadas penas de inhabilitación, y que como hemos señalado fue sometida al pleno del Tribunal Supremo en la sentencia de la sala segunda en la STS 547/2022, de 2 de junio, anteriormente citada. En dicha sentencia se incide sobre la posibilidad de proceder al cierre de una entrada de Youtube al amparo de la prohibición de concurrir a determinados lugares contenida en el art. 48 del CP. La sentencia se muestra conforme con la aplicación de una medida de esta naturaleza, pero señala una vía alternativa que debería ser la adecuada a estos casos, cuál es la de que, «*una vez verificado el oportuno juicio de proporcionalidad, considerar que el canal de Youtube, mediante el que se hacía posible la difusión de las lacerantes imágenes captadas por el acusado, pueda ser considerado como un instrumento del delito y, por tanto, sometido al decomiso previsto en el art. 127.1 del CP*». No se trata tanto de restringir contenidos informativos o de limitar la capacidad de emitir información, como la de excluir la capacidad de acceder a un medio especialmente idóneo para la difusión de dichos contenidos. Y cuando digo medio, no me refiero tan sólo a la ubicación web del sitio (url), sino al conjunto de algoritmos y metadatos asociados a dicha dirección que permiten acceder y reconocer dicha información y que definen el perfil del usuario.

13. EFECTIVIDAD DE LA ORDEN DE ACTUACIÓN Y DE ENTREGA DE INFORMACIÓN RESPECTO DE CONTENIDOS ALOJADOS EN TERCEROS PAÍSES.

La represión de las acciones penales en los entornos digitales resulta especialmente compleja cuando los usuarios están sujetos a leyes diferentes dependiendo de donde sus datos se encuentren en un momento determinado.

La regla general es que la eventual adopción de medidas de retirada de contenidos fuera del territorio de la Unión queda limitada a aquellos supuestos que la autoridad que lo solicite tenga competencia judicial internacional para adoptarlas. La protección de la legalidad y los intereses de la Unión en

un mercado global hace necesario el examen en conjunto del impacto producido por los prestadores servicios digitales por el sólo hecho de la emisión de dichos contenidos.

Estas limitaciones pueden surgir de acuerdos internacionales en determinadas materias, como pueda ser en materia de protección de la propiedad intelectual, pero no excluye tampoco decisiones discrecionales de las empresas de servicios digitales en orden a la mayor implantación de su negocio. Estas pueden libremente hacer suyos los intereses de orden público de otros Estados y condicionar la prestación de servicios al objeto de obtener una mayor difusión de su negocio en el conjunto de los mercados digitales.

En este sentido, debe tenerse presente el carácter voluntarista de los límites de la jurisdicción conforme resulta de las previsiones contenidas en el art. 32.b del Convenio de Budapest. Este precepto, que resulta clave en orden a definir la jurisdicción de los Estados en los entornos digitales, habilita el acceso a los datos desde una jurisdicción distinta no sólo cuando se trata de datos obtenidos en abierto, sino también cuando se obtiene el consentimiento legal y voluntario de la persona autorizada para divulgarlos a través de un sistema informático.

En este sentido el considerando 36 del RMSD establece como criterio «*el efecto de la orden debe limitarse, en principio, al territorio del Estado miembro emisor, a menos que el carácter ilícito del contenido se derive directamente del Derecho de la Unión o la autoridad emisora considere que los derechos en cuestión requieren un ámbito territorial más amplio, de conformidad con el Derecho de la Unión y el Derecho internacional, teniendo en cuenta al mismo tiempo los intereses de la cortesía internacional*».

Esta referencia a los intereses de la cortesía internacional a los que se refiere el Reglamento admite que la orden pueda producir efectos fuera del territorio de la Unión, si la extensión de la orden no es contraria al Derecho Internacional aplicable al caso. El Tribunal de Justicia en la STJUE de 3 de octubre de 2019, caso Glawishing-Piesczek, C-18/18, declaró expresamente que habida cuenta de la dimensión mundial del servicio electrónico, el legislador europeo ha estimado necesario garantizar la coherencia de las normas de la Unión en ese ámbito con las normas aplicables a nivel internacional, correspondiendo a los Estados miembros velar por que las medidas que adopten y que producen efectos a escala mundial tengan debidamente en cuenta estas últimas previsiones[60].

Debe tenerse presente que en el marco de los entornos digitales el principio de territorialidad se encuentra condicionado por la posibilidad real de acceso a los contenidos digitales. La vinculación de la información almacenada con su soporte físico es algo meramente convencional, no depende de la naturaleza de las cosas sino de una mera convención lógica. Esta falta de vinculación de la información a su soporte determina una reconsideración

[60] ECLI:EU:C:2019:821

del problema al objeto de afirmar algo, qué por sabido, no deja de ser obvio: allí donde se exterioriza la información y es reconocible, la información existe y produce efecto. El problema viene determinado en aquellos supuestos en que quien detenta la información o cuando menos tiene acceso condiciona su acceso por las normas de orden público a las que se encuentra afecto[61].

El problema se planteó por primera vez ante el Tribunal Supremo de los Estados Unidos en el caso Microsoft c. Ireland. Los hechos nacen como consecuencia de la impugnación por la empresa Microsoft de una orden de la Oficina Federal de Investigación (FBI) para entregar los correos electrónicos de una cuenta de destino almacenados en Irlanda, argumentando que una orden emitida en virtud de la Sección 2703 de la Ley de Comunicaciones Electrónicamente Almacenadas, (Stored Communications Act) no podía obligar a las empresas estadounidenses a presentar datos almacenados en servidores fuera de Estados Unidos. Microsoft perdió el caso inicialmente en el Distrito Sur de Nueva York, y el juez declaró que la naturaleza de la orden de la Ley de Comunicaciones Almacenadas, tal como se aprobó en 1986, no estaba sujeta a restricciones territoriales[62]. La nueva reforma legal, Cloud Act, que fue aprobada como consecuencia de aquel caso, afirmó que las empresas de datos y comunicaciones estadounidenses deben proporcionar los datos almacenados de un cliente o abonado en cualquier servidor que posean y operen cuando se les solicite mediante una orden judicial, pero establece mecanismos para que las empresas o los tribunales puedan rechazarlos o impugnarlos si consideran que la solicitud viola los derechos de privacidad del país extranjero en el que se almacenan los datos

La interpretación de la extensión de la jurisdicción en la Unión Europea en los mercados digitales ha sufrido también un cambio radical tras la entrada en vigor del Reglamento 2023/1543, de 12 de julio, sobre las órdenes europeas de producción y conservación de datos a efectos de prueba electrónica. Esta normativa fija como criterio delimitador de la competencia de los órganos judiciales el hecho de que los servicios prestados produzcan efecto en el territorio de la Unión Europea con independencia de donde se encuentre establecido el prestador de servicios (art. 2.3). El legislador europeo se suma así a las corrientes doctrinales más modernas que fijan el criterio para deter-

---

[61] Sobre la extensión de la jurisdicción tras la aprobación del Convenio de Bruselas II, pusimos de manifiesto la necesidad de deslindar la información sensible susceptible de ser reconocida de su soporte, la cognoscibilidad de dicha información y el efecto que pueda producir respecto de tercero es lo que es relevante al derecho y determinante de los límites de la jurisdicción, véase Gudín Rodríguez-Magariños, A.E. «El nuevo protocolo del Convenio de Budapest de lucha contra la cibercriminalidad». Revista General de Derecho Procesal, núm. 58, (2022):7.

[62] Microsoft recurrió al Tribunal de Apelación del Segundo Circuito de los Estados Unidos, que dio la razón a Microsoft en 2016 e invalidó la orden. En respuesta, el Departamento de Justicia de los Estados Unidos recurrió al Tribunal Supremo, sin embargo, antes de que aquel se pronunciase las autoridades norteamericanas vinieron a promulgar una reforma legal sin precedentes la denominada *Cloud Act*.

minar la jurisdicción no tanto en el lugar de donde proceden los datos, como en aquel donde aquellos producen efecto. Los contenidos que permanecen ocultos y que no producen efecto o trascienden a terceros quedan al margen de las normas que regulan los mercados de servicios digitales. Podrán quedar sujetos en su caso al derecho de propiedad intelectual o industrial, pero en sí mismos considerados, no trascendiendo resultan inocuos a la acción del Derecho.

14. CONCLUSIONES.

A lo largo de nuestra exposición hemos puesto de relieve las consecuencias que implica la difusión de forma indiscriminada de determinados contenidos fuera del contexto en que dicha información se encontraba dirigida. Los efectos de transmitir información desconociendo quienes sean sus destinatarios ha dado lugar a que la difusión de información esté sometida a previsiones de orden público que regulan el mercado digital. Hemos visto también como la normativa europea que habilita a los prestadores de servicio para la retirada de contenidos ilícitos presenta una larga trayectoria que se hace extensiva a ámbitos tan dispares como puedan ser el terrorismo, la pornografía infantil, la propiedad intelectual o el derecho de consumo.

De esta suerte, difusión y transmisión de información son cuestiones distintas que deben ser distinguidas. Solo la primera exige la actuación de las autoridades para la seguridad de los mercados digitales. Se entiende así que las obligaciones de diligencia debida y las potestades de policía que se encuentran implícitas en aquellas resultan transcendentales en orden a limitar la difusión de contenidos ilícitos más allá del marco prestablecido.

En lo que se refiere a las nuevas órdenes de actuación y entrega de información, las garantías que deban acompañarse no son necesariamente distintas a las obligaciones de diligencia debida a las que están afectan las empresas prestadoras de servicio. La emisión de estas órdenes implica el ejercicio de potestades de policía que se justifican en los mismos principios que subyacen en las normas de cumplimiento normativo a que aquellas se encuentran afectas. Cabe apreciar en ambos casos una normativa de orden público que tutela la seguridad de los mercados digitales y que no se dirige directamente a reprimir la transmisión de la información en sí misma, sino la limitación de la difusión de aquella de forma indiscriminada y fuera del marco prestablecido.

Es por tales razones, que la justificación de una orden que puede dar lugar a graves restricciones a la difusión de los contenidos digitales no viene dada tanto por el riesgo de la alteración del orden público, como por la necesidad de evitar la instrumentalización de los mercados digitales por los criminales al margen del Estado de Derecho.

La extensión de estas facultades a las autoridades estatales y en particular a la autoridad gubernativa no está exenta de dificultades en un ámbito en el

que los usuarios y los prestadores de servicios están sometidos a criterios de orden público cuyo contenido y alcances no se encuentra perfectamente definido. La sentencia del Tribunal de Justicia de la Unión Europea Quadrature du Net, aun refiriéndose principalmente a la transmisión de información en el marco de las comunicaciones sujetas a confidencialidad, abordó por primera vez cuestiones tales como la monitorización del acceso a la red y la vigilancia y control en el entorno digital. Desde entonces son muchas las incógnitas que se presentan para el intérprete acerca de cuál sea el alcance de las facultades de las autoridades gubernativas respecto de la emisión de contenidos en línea, haciéndose precisa una definición de conceptos básicos como es el derecho al entorno digital o la limitación de la difusión de las comunicaciones en entornos abiertos[63].

BIBLIOGRAFÍA

Arangüena Fanego, C., «Nuevos pasos contra el terrorismo en la UE: Reglamento (UE) 2021/784». *Revista de Estudios Europeos*, núm. extraordinario monográfico 1 (2023).

Buiten, M.C. «Digital Service Act: form Intermediary Liability to Plattform Regulation», *Journal of Intellectual Property Informacion, Technology and E-Commerce*, (dic. 2021).

De Miguel Asensio, P. «Aplicación del derecho a la supresión de enlaces por buscadores», *blog Pedro de Miguel Asensio*, 27.01.2020 (consultado: 13/11/2023). *https://pedrodemiguelasensio.blogspot.com/2020/01/aplicacion-del-derecho-la-supresion-de.html*.

De Miguel Asensio, P. «Obligaciones de diligencia y responsabilidad de los intermediarios: El Reglamento (UE) de Servicios Digitales». *La Ley Unión Europea*, núm. 109, diciembre (2022).

Frosio, G. and Geiger, C. «Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime», *European Law Journal* (forthcoming, November 2023), Available at SSRN: *https://ssrn.com/abstract=3747756 or http://dx.doi.org/10.2139/ssrn.3747756*.

Galán Muñoz, A. «Redes sociales discurso terrorista y Derecho Penal. Entre la prevención, las libertades fundamentales y los ¿los negocios?» en la obra colectiva *La represión y persecución penal del discurso terrorista*, editorial Tirant Lo Blanc, Valencia, (2022).

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 la obra colectiva *Estudios sobre tecnologías disruptivas y justicia* / coord. por Irene González Pulido; Federico Bueno de Mata (dir.), Lorenzo Mateo Bujosa Vadell (pr.), 2020): 345 y 356.

Gudín Rodríguez-Magariños, A. E. «Derecho al Recuerdo: examen comparado de la normativa de preservación de datos en los Estados Unidos y en la Unión Europea» *Revista Jurídica de Castilla y León*, núm. 55, (2021).

[63] STJUE (Gran Sala), de 5 de abril de 2022 (LA LEY 39345/2022) (caso Garda SíoChána), asunto C-140/20) y SJUEZ (Gran Sala), de 20 de septiembre de 2022 (SpaceNet C-793/19 y telekom GmBH asunto C-794/19)

Gudín Rodríguez-Magariños, A.E. «El nuevo protocolo del Convenio de Budapest de lucha contra la cibercriminalidad». *Revista General de Derecho Procesal*, núm. 58, (2022).

Kuner, C. «The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges» in Burkhard Hess and Cristina M. Mariottini (eds), *Protecting Privacy in Private International and Procedural Law and by Data Protection* Ashgate/Nomos, (2015).

Moreno Blesa, L. «La retirada de los contenidos ilícitos prestadores de servicios en línea». *Themis-Revista de Derecho*, UCM (2021). *https://doi.org/10.18800/themis.202101.004*

Rodríguez Lainz, J.L. «La evolución de la jurisprudencia del Tribunal de Justicia de la Unión Europea en materia de conservación indiscriminada de datos de comunicaciones electrónicas en la STJUE del Caso G.D. y Comissioner an Garda Síochána» *Diario La Ley,* No 10058, Sección Tribuna (28 de Abril de 2022).

Savin, A., «The EU Digital Services Act: Towards a More Responsible Internet» (February 16, 2021), *CBS LAW Research Paper*, núm. 21-04, *Journal Internet Law*, disponible en *https://ssrn.com/abstract=3786792* (consultado: 09/10/2022)

Teruel Lozano, G. «Una lectura garantista de las nuevas tendencias en la lucha europea contra la difusión de mensajes terroristas en Internet», *Revista de Derecho Constitucional Europeo*, núm. 34 (2020).

Teruel Lozano, G.M. «Bloqueo de contenidos en Internet y reserva de jurisdicción». *Blog del CEPC*, 15 de diciembre de 2022 (consultado: 13/11/2023). *https://www.cepc.gob.es/blog/bloqueo-de-contenidos-en-internet-y-reserva-de-jurisdiccion.*

Teruel Lozano, G. «Libertad de expresión, censura y pluralismo en las redes sociales: algoritmos y el nuevo paradigma regulatorio europeo», en la obra colectiva *Derecho Público de la inteligencia artificial*, coord. Balaguer Callejón, F. y Cotino Hueso, L., Fundación Giménez Abad: Zaragoza (2023): 181-222, Accesible en: *https://www.fundacionmgimenezabad.es/es/derecho-publico-de-la-inteligencia-artificial.*

Wilman, F., «The EU's system of knowledge-based liability for hosting service providers in respect of illegal user content — between the e-Commerce Directive and the Digital Services Act», *JIPITEC*, vol. 12, (2021): pp. 317-341.