



Boletín

DERECHO

DIGITAL

2026

CONTENIDO

Protección de datos personales en el ámbito digital	3	y delimitación de la responsabilidad del anunciante: promoción de canales de compra sin identificación publicitaria	7
— Acción coordinada de aplicación: implementación del derecho de supresión por los responsables del tratamiento	3	— Mención neutral de una marca en contenidos de <i>influencers</i> y ausencia de finalidad publicitaria: exclusión del concepto de <i>publicidad encubierta</i>	8
— Impugnabilidad directa ante los tribunales de la Unión de las decisiones vinculantes el Comité Europeo de Protección de Datos	4	Inteligencia artificial	9
— El abuso del derecho de acceso a los datos personales y sus efectos sobre la responsabilidad civil.....	4	— Inteligencia artificial agéntica desde la perspectiva de protección de datos.....	9
— Tratamiento de datos biométricos en el ámbito policial y límites a la sanción por negativa del interesado	5	— AEPD: El uso de imágenes de terceros en sistemas de inteligencia artificial y sus riesgos visibles e invisibles	10
— Tratamiento de datos procedentes de fuentes públicas y derecho al honor	6	— Informe sobre los derechos de autor y la inteligencia artificial generativa: oportunidades y desafíos.....	10
Publicidad digital	7	Plataformas en línea	12
— <i>Influencers</i> e identificación del carácter publicitario de un post.....	7	— Plataformas y motores de búsqueda en línea de muy gran tamaño designados con arreglo al artículo 33, apartado 4, del Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (ley de servicios digitales).....	12
— Publicidad encubierta en contenidos de <i>influencers</i>			



PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO DIGITAL

Acción coordinada de aplicación:
implementación del derecho
de supresión por los responsables
del tratamiento

El Comité Europeo de Protección de Datos (CEPD) ha publicado recientemente el informe de su Marco Coordinado de Aplicación, dedicado a analizar cómo los responsables del tratamiento están aplicando en la práctica el derecho de supresión o «derecho al olvido» previsto en el artículo 17 del Reglamento General de Protección de Datos. A lo largo del 2025, un total de treinta y dos autoridades de control del Espacio Económico Europeo examinaron la actuación de setecientos sesenta y cuatro responsables, tanto del sector público como del privado, mediante cuestionarios y actuaciones de supervisión. El informe confirma que, pese a tratarse de uno de los derechos más ejercidos por los interesados, su aplicación sigue siendo desigual y presenta deficiencias significativas en diversos ámbitos.

Entre los problemas más recurrentes detectados destacan la ausencia de procedimientos internos documentados y actualizados, la falta de

formación específica del personal, una información insuficiente al interesado sobre cómo y en qué condiciones puede ejercerse el derecho, así como dificultades técnicas y organizativas relacionadas con la supresión de datos en copias de seguridad, la correcta determinación de los plazos de conservación y el uso inadecuado de técnicas de anonimización como alternativa a la supresión efectiva. El informe pone además de relieve la inseguridad jurídica existente en la aplicación de las excepciones al derecho de supresión, lo que en algunos casos conduce a rechazos automáticos o insuficientemente motivados, sin el necesario análisis caso por caso y sin ponderar otros derechos e intereses concurrentes.

Como conclusión, el Comité Europeo de Protección de Datos formula recomendaciones prácticas tanto para los responsables como para las autoridades de control centradas en la necesidad de reforzar la gobernanza interna del derecho de supresión: establecimiento de procedimientos claros y revisables, formación continua y adaptada a los distintos roles, mayor transparencia en la comunicación con los interesados y alineación de las medidas técnicas con estándares reconocidos. Asimismo, el informe

anticipa posibles actuaciones adicionales a nivel europeo, incluida la elaboración de guías prácticas y orientaciones homogéneas, con el objetivo de reducir las divergencias detectadas y garantizar una aplicación más efectiva y coherente del derecho de supresión en toda la Unión Europea.

Camino Bustinduy de la Guerra

Impugnabilidad directa ante los tribunales de la Unión de las decisiones vinculantes del Comité Europeo de Protección de Datos

La Gran Sala del Tribunal de Justicia de la Unión Europea ha dictado sentencia el 10 de febrero del 2026 (as. C-97/23P, ECLI:EU:C:2026:81) en la que declara admisible el recurso de anulación interpuesto por WhatsApp Ireland Ltd contra la Decisión Vinculante 1/2021 del Comité Europeo de Protección de Datos (CEPD) y anula el auto del Tribunal General que lo había inadmitido. El litigio tiene su origen en la investigación iniciada en el 2018 por la autoridad irlandesa de protección de datos sobre el cumplimiento por WhatsApp de sus obligaciones de transparencia e información conforme a los artículos 12 a 14 del Reglamento General de Protección de Datos. Al no alcanzarse consenso entre las autoridades de control interesadas, dicho comité adoptó la Decisión 1/2021, en la que constató la infracción de diversas disposiciones del reglamento y obligó a la autoridad irlandesa a modificar las medidas correctivas previstas, incluida la elevación de la multa hasta 225 millones de euros.

El Tribunal de Justicia concluye que dicha decisión constituye un acto recurrible en el sentido del artículo 263 del Tratado de Funcionamiento

de la Unión Europea: emana de un órgano de la Unión, representa la posición definitiva del Comité Europeo de Protección de Datos y produce efectos jurídicos frente a terceros. Asimismo, el Tribunal de Justicia de la Unión Europea aprecia que la decisión afecta directamente a WhatsApp al no dejar margen de apreciación alguno a las autoridades nacionales destinatarias, ni en cuanto a la calificación de la infracción ni respecto de las correcciones que debían aplicarse. El fallo precisa, además, que el plazo para interponer el recurso de anulación debe computarse desde la publicación de la decisión vinculante en el sitio de internet del Comité Europeo, conforme al artículo 65.5 del Reglamento General de Protección de Datos. Se puede afirmar que la sentencia refuerza la tutela judicial efectiva de los responsables del tratamiento frente al mecanismo de coherencia del mencionado reglamento y sienta un precedente relevante para futuras impugnaciones de decisiones vinculantes de dicho comité ante los tribunales de la Unión.

Claudia Pérez Moneu

El abuso del derecho de acceso a los datos personales y sus efectos sobre la responsabilidad civil

La Sala Cuarta del Tribunal de Justicia de la Unión Europea ha dictado sentencia el 19 de marzo del 2026 en el asunto C-526/24, *Brillen Rottler*, resolviendo una cuestión prejudicial planteada por el Amtsgericht (Tribunal de Primera Instancia) de Arnsberg (Alemania) sobre la interpretación de los artículos 12, apartado 5; 15, apartado 1, y 82, apartado 1, del Reglamento (UE) 2016/679, General de Protección de Datos. El litigio principal enfrentaba a Brillen Rottler, una óptica familiar, con un particular residente en Austria que, tras suscribirse a su boletín informativo e

introducir sus datos personales, presentó una solicitud de acceso con arreglo al artículo 15 del citado reglamento tan sólo trece días después. La empresa denegó la solicitud por considerarla excesiva, alegando que el interesado seguía un *modus operandi* sistemático: suscribirse a boletines, ejercer el derecho de acceso y, a continuación, reclamar una indemnización por la supuesta infracción. El Tribunal de Justicia de la Unión Europea declara, en primer lugar, que una primera solicitud de acceso puede ser calificada de «excesiva» a efectos del artículo 12, apartado 5, del reglamento cuando el responsable del tratamiento demuestre que, pese al cumplimiento formal de los requisitos del artículo 15, dicha solicitud no fue presentada con el propósito de conocer el tratamiento de los datos y verificar su licitud, sino con una intención abusiva, como la creación artificial de los requisitos exigidos para obtener una indemnización. No obstante, esta excepción debe interpretarse de manera restrictiva.

En segundo lugar, el Tribunal de Justicia de la Unión Europea confirma que el artículo 82, apartado 1, del reglamento confiere al interesado un derecho a indemnización por los daños y perjuicios derivados de la vulneración del derecho de acceso, sin que resulte necesario que la infracción implique una operación de tratamiento. En cuanto a los daños inmateriales, la pérdida de control sobre los datos personales o la incertidumbre sobre su tratamiento pueden constituir un perjuicio indemnizable siempre que se acredite que el interesado sufrió efectivamente dicho daño y que su propia conducta no fue la causa determinante de éste. La sentencia reviste especial relevancia en el contexto del fenómeno de abuso instrumentalizado del Reglamento General de Protección de Datos, mediante el cual determinados particulares provocan deliberadamente infracciones del reglamento con el fin de obtener indemnizaciones. El pronunciamiento ofrece a los responsables

del tratamiento un instrumento de defensa frente a solicitudes de acceso instrumentalizadas, al tiempo que preserva el alto estándar de protección del derecho de acceso consagrado en tal reglamento.

Iratze Arrigain García

Tratamiento de datos biométricos en el ámbito policial y límites a la sanción por negativa del interesado

En su Sentencia de 19 de marzo del 2026 (as. C-371/24, *Comdribus*), el Tribunal de Justicia de la Unión Europea se pronuncia sobre los límites al tratamiento de datos biométricos por parte de las autoridades policiales en el marco de la Directiva (UE) 2016/680, como consecuencia de las cuestiones prejudiciales planteadas por la Cour d'Appel de Paris (Tribunal de Apelación de Paris) en el procedimiento principal, en el que una persona fue condenada penalmente no por el delito que motivó su detención, sino exclusivamente por negarse a que se le tomaran huellas dactilares y fotografías, pese a haber sido posteriormente absuelta del delito principal.

El Tribunal de Justicia recuerda que los datos biométricos constituyen categorías especiales de datos personales y que su tratamiento con fines de prevención e investigación penal sólo es lícito cuando resulte estrictamente necesario, de conformidad con el artículo 10 de la Directiva 2016/680. Este juicio de necesidad exige una evaluación concreta y motivada vinculada a la situación individual de la persona afectada y no puede basarse en presunciones generales ni en automatismos legales. En este contexto, dicho tribunal subraya que la mera existencia de razones plausibles de sospecha no exonera a las autoridades de justificar por qué la



recogida de datos biométricos es imprescindible en el caso concreto.

Asimismo, este tribunal subraya que la recogida de datos biométricos constituye una injerencia particularmente grave en los derechos fundamentales reconocidos por la normativa europea, por lo que exige un control riguroso de proporcionalidad. En este sentido, las autoridades deben valorar si existen medidas menos intrusivas que permitan alcanzar el mismo objetivo y garantizar que la captación de huellas, imágenes u otros datos biométricos no se convierta en una práctica sistemática o automática.

Camino Bustinduy de la Guerra

Tratamiento de datos procedentes de fuentes públicas y derecho al honor

La Sala Primera del Tribunal Supremo, en su Sentencia 333/2026, de 3 de marzo (rec. 8978/2024), ha estimado el recurso de casación interpuesto por Equifax Ibérica, S.L., declarando la inexistencia de intromisión ilegítima en el derecho al honor del demandante por la inclusión de sus datos personales en el Fichero de Incidencias Judiciales y Reclamaciones de Organismos Públicos (FIJ). El supuesto enjuiciado versa sobre la incorporación a este fichero de los datos del demandante relativos a una deuda tributaria con el Ayuntamiento de Madrid, obtenidos del *Boletín Oficial del Estado*, en el que se había publicado un anuncio de

embargo de sueldos y pensiones. La Audiencia Provincial de Madrid había estimado la demanda al considerar que el tratamiento de los datos no cumplía los requisitos de veracidad, exactitud y notificación previstos en los artículos 29.2 y 29.4 de la LOPD 1999 y en los artículos 38 a 40 del RLOPDGP.

El Tribunal Supremo, reiterando la doctrina fijada en la STS 434/2023, de 29 de marzo, establece que los ficheros contemplados en el artículo 29.1 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, que tratan datos obtenidos de registros y fuentes accesibles al público, quedan al margen de las exigencias previstas en los apartados 2 y 4 del mismo precepto, aplicables únicamente a los ficheros que se nutren de datos facilitados por el acreedor o por quien actúe por su cuenta o interés. La Sala razona que el legislador, al autorizar el tratamiento de datos provenientes de fuentes públicas, ya ponderó los intereses en juego, y que hubo de considerar que la afectación es menor al tratarse de datos divulgados previamente. Asimismo, la información se incorporó con los mismos datos que figuraban en la fuente pública, con indicación del organismo acreedor y de la naturaleza tributaria de la deuda. A mayor abundamiento, la propia conducta del demandante, que se negó a facilitar la verificación de la deuda, impidió cuestionar la exactitud de los datos inscritos. En consecuencia, se casa la sentencia de apelación y se confirma la desestimación íntegra de la demanda.

Claudia Pérez Moneu



PUBLICIDAD DIGITAL

Influencers e identificación del carácter publicitario de un post

El Jurado de la Publicidad de Autocontrol —en su Resolución de la Sección Primera de 20 de febrero del 2026, confirmada por el Pleno en Resolución de 20 de marzo— se ha ocupado de un problema recurrente en la práctica: cómo indicar que una publicación en una red social por parte de un *influencer* tiene carácter publicitario.

El caso concreto versa sobre una publicación en Instagram en la que una *influencer* aparece junto a otras chicas comiendo un *croissant* gigante y luciendo diversas joyas de una determinada marca, todo ello acompañado de un post en el que se dice: «EXXXXCUSE-MOI [...] paris [sic], croissants, gente buena y las mejores joyas de @singularu <333 no puedo pedir más !!!!! publi invitación». Y, con ese presupuesto, lo que se discute es si la indicación en el post de su carácter publicitario es suficiente o no.

Pues bien, según el Jurado de Autocontrol, considera que no se ha identificado adecuadamente el carácter publicitario del mensaje, porque la «la mención “publi” aparece en el texto que

acompaña a la publicación. Sin embargo, su ubicación no permite desvelar a primera vista el carácter promocional del contenido, en tanto no se incluye de manera inmediata junto al título o al inicio del mensaje, lo que habría permitido al destinatario conocer desde el primer momento que se trata de publicidad. Por el contrario, la advertencia figura al final del texto, con dos consecuencias claras: por un lado, el usuario no advierte la naturaleza publicitaria del mensaje hasta el final, ignorándola por lo tanto durante su visionado y lectura; por otro lado, en función del dispositivo que se emplee para acceder al mensaje, en algunos casos el usuario deberá pinchar en el enlace “más”, acceder al texto completo y encontrar la mención al final, con un elevado riesgo de que pase fácilmente desapercibida».

Ángel García Vidal

Publicidad encubierta en contenidos de *influencers* y delimitación de la responsabilidad del anunciante: promoción de canales de compra sin identificación publicitaria

La Resolución del Jurado de Autocontrol, Sección Segunda, de 27 de febrero del 2026, asunto 102/R/Febrero 2026, se ha ocupado de un supuesto en el que un *influencer* hace publicidad de los productos de una marca (Philips) y de la posibilidad de adquirirlos en una plataforma de venta (Amazon).

Tras reconocer el carácter publicitario de las publicaciones y constatar que no se ha declarado expresamente tal naturaleza publicitaria, con la consiguiente infracción de la obligación de advertir claramente del carácter publicitario de los mensajes, el jurado examina si dicha infracción es imputable o no al titular de la marca promocionada.

Pues bien, el jurado exonera de responsabilidad al titular de la marca sobre la base de la norma 12 del Código de *Influencers*, según la cual: «La responsabilidad por la infracción de lo dispuesto en el presente código podrá alcanzar a todos los sujetos implicados en la comunicación comercial. No obstante, un sujeto podrá exonerar su responsabilidad si acredita de forma suficiente que la infracción es consecuencia de un incumplimiento puntual y manifiesto de las indicaciones o instrucciones dadas al *influencer*. Cuando se concluya que la mención o contenido promocional ha sido difundido por iniciativa exclusiva del *influencer*, sin intervención ni relación alguna por parte del anunciante o sus agentes, la responsabilidad, en su caso, podrá ser atribuida en exclusiva al *influencer* o sus agentes».

Destaca el jurado que el mensaje analizado pone el acento principal en la adquisición del producto a través de la plataforma de venta, lo que permite concluir que la publicidad se orienta al canal de compra y no al producto. Esta conclusión es coherente con el historial del *influencer*, centrado mayoritariamente en recomendaciones de compra en dicha plataforma. Finalmente, el jurado también tienen en cuenta

que el titular de la marca ha acreditado que no existe relación contractual con dicho *influencer*, pues su publicidad se gestiona exclusivamente a través de una agencia que ha negado cualquier vínculo con él.

Ángel García Vidal

Mención neutral de una marca en contenidos de *influencers* y ausencia de finalidad publicitaria: exclusión del concepto de *publicidad encubierta*

El Jurado de Autocontrol —en su Resolución de la Sección Quinta de 9 de enero del 2026, asunto 393/R/Diciembre 2025, confirmada por la Resolución del Pleno de 13 de febrero del 2026— ha conocido de un caso en el que un *influencer* menciona una marca en una publicación en redes sociales, sin que eso implique la existencia de publicidad.

En concreto, en la publicación en cuestión, donde se puede ver al *influencer* en un partido de fútbol con su familia, se hace esta afirmación: «iamperea. Os traemos el partido dentro del partido. Ése que se juega en la butaca, el que comentas con el que tienes al lado, el que te deja sin voz y te pone la piel de gallina... Gracias @larocheposay por hacernos vivir así el fútbol». Aunque, como se puede comprobar, se menciona una marca, no se alude a ningún tipo de productos o servicios de esa marca, incluyendo «sólo una sucinta referencia al nombre de la marca que le ha invitado a esa experiencia, expresando su agradecimiento. Más allá de esta mención, insistimos, el mensaje es completamente ajeno a dicha empresa o a sus productos o servicios, centrándose únicamente en mostrar como disfrutaban del evento en familia».

Ángel García Vidal



INTELIGENCIA ARTIFICIAL

Inteligencia artificial agéntica desde la perspectiva de protección de datos

La Agencia Española de Protección de Datos (AEPD) ha publicado, en febrero del 2026, unas orientaciones pioneras sobre la inteligencia artificial agéntica desde la perspectiva de protección de datos. El documento aborda las implicaciones que la integración de agentes de inteligencia artificial (sistemas que utilizan modelos de lenguaje para alcanzar objetivos de forma autónoma) tiene para los responsables y encargados del tratamiento que decidan implementar esta tecnología en aquellas de sus operaciones que involucren datos personales. A diferencia de los modelos generativos convencionales, la inteligencia artificial agéntica no se limita a generar contenido, sino que define planes, interactúa con múltiples fuentes de datos, se conecta con servicios externos y ejecuta acciones sin intervención humana constante. Esta autonomía operativa amplía considerablemente la extensión del riesgo para los derechos y libertades de los interesados, por cuanto dificulta la determinación de las figuras de responsable y de encargado del tratamiento, la aplica-

ción del principio de minimización de datos y el cumplimiento de las obligaciones de transparencia e información.

Las orientaciones se estructuran abordando, en primer lugar, la descripción técnica de los sistemas agénticos. En segundo lugar, describen las vulnerabilidades específicas que afectan a la protección de datos y ciertas amenazas que pueden cernirse sobre el tratamiento, como la falta de madurez en el desarrollo o la pérdida de control sobre los flujos de datos hacia terceros. Finalmente, el documento enumera medidas técnicas y organizativas, entre las que destacan la gobernanza de la información como medida nuclear y la aplicación proactiva de la protección de datos desde el diseño y por defecto conforme al Reglamento General de Protección de Datos. La Agencia Española de Protección de Datos enfatiza que tanto el rechazo irracional de esta tecnología como su aceptación acrítica pueden resultar perjudiciales, e insta a aprovechar las oportunidades que ofrece la inteligencia artificial agéntica como herramienta de mejora de la privacidad.

Iratze Arrigain García

AEPD: El uso de imágenes de terceros en sistemas de inteligencia artificial y sus riesgos visibles e invisibles

En enero del 2026, la Agencia Española de Protección de Datos (AEPD) ha publicado su guía sobre el uso de imágenes de terceros en sistemas de inteligencia artificial y sus riesgos visibles e invisibles. La agencia recuerda que cualquier imagen o vídeo en el que una persona sea identificada o identificable constituye un dato personal, con independencia de que el contenido sea real, generado o modificado mediante inteligencia artificial o de que el uso tenga una finalidad aparentemente trivial o lúdica. Subir imágenes de terceros a herramientas de inteligencia artificial supone siempre un tratamiento de datos personales, incluso cuando el resultado no se difunde posteriormente. La Agencia Española de Protección de Datos insiste en que el hecho de que una imagen haya sido compartida previamente en redes sociales, mensajería u otros entornos no legitima automáticamente su reutilización para entrenar, generar o transformar contenidos mediante sistemas de inteligencia artificial.

La guía distingue entre impactos visibles (derivados de la generación y difusión de contenidos) y riesgos menos perceptibles asociados al mero hecho de subir una imagen a un sistema de inteligencia artificial. Entre los primeros, la Agencia Española de Protección de Datos identifica factores como la pérdida de contexto, la facilidad de difusión, la persistencia del contenido, la atribución de hechos no reales con efectos reputacionales o la especial gravedad de los supuestos de sexualización y uso de imágenes de personas vulnerables. Desde la perspectiva del impacto no visible, se subrayan riesgos estructurales como la pérdida efectiva de control sobre la imagen al intervenir un

proveedor tecnológico, la posible retención técnica y generación de copias, la participación de múltiples actores en el tratamiento, la creación de metadatos e inferencias internas y la dificultad real de que la persona afectada conozca qué ha ocurrido con su imagen o pueda ejercer sus derechos de protección de datos de forma efectiva.

Finalmente, la agencia aclara que no todos los usos de imágenes con inteligencia artificial constituyen automáticamente una infracción, especialmente cuando se desarrollan en un ámbito estrictamente personal o doméstico. No obstante, advierte de que determinadas circunstancias (como la creación de contenidos verosímiles que atribuyan hechos no sucedidos, la implicación de menores o colectivos vulnerables, la introducción de elementos de humillación o sexualización, o la difusión en entornos con alto impacto social o profesional) elevan significativamente el nivel de riesgo desde la perspectiva de la protección de datos.

Camino Bustinduy de la Guerra

Informe sobre los derechos de autor y la inteligencia artificial generativa: oportunidades y desafíos

El Parlamento Europeo aprobó el 10 de marzo del 2026, con cuatrocientos sesenta votos a favor, setenta y uno en contra y ochenta y ocho abstenciones, la «Resolución sobre derechos de autor e inteligencia artificial generativa: oportunidades y desafíos», elaborada por la Comisión de Asuntos Jurídicos, con la ponencia del eurodiputado Axel Voss (A10-0019/2026). La resolución parte del reconocimiento de que la legislación vigente en materia de derechos de autor resulta insuficiente para abordar las cuestiones derivadas del uso de material protegido en el



entrenamiento de modelos de inteligencia artificial generativa, y constata la existencia de infracciones generalizadas por parte de determinados proveedores consistentes en la recopilación de obras sin autorización y el incumplimiento de las reservas de derechos en materia de minería de textos y datos.

Entre sus principales pronunciamientos, el Parlamento insta a la Comisión a establecer un marco de concesión de licencias que garantice tanto la transparencia plena sobre las obras protegidas utilizadas para el entrenamiento como una remuneración justa y proporcionada a los creadores. Se propone asimismo una presunción *iuris tantum* de que todo modelo de inteligencia artificial generativa introducido en el

mercado de la Unión ha utilizado obras protegidas cuando no se hayan cumplido las obligaciones de transparencia.

Igualmente, la resolución declara que los contenidos generados íntegramente por inteligencia artificial que no satisfagan los criterios de originalidad no pueden acogerse a la protección de los derechos de autor, debiendo considerarse de dominio público. El texto destaca, por último, la necesidad de que el Derecho de la Unión resulte aplicable aun cuando el entrenamiento se lleve a cabo fuera de su territorio con contenidos europeos.

Claudia Pérez Moneu



PLATAFORMAS EN LÍNEA

Plataformas y motores de búsqueda en línea de muy gran tamaño designados con arreglo al artículo 33, apartado 4, del Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (ley de servicios digitales)

La Comisión Europea ha publicado (DOUE núm. 1654, de 11 de marzo del 2026) la lista actualizada de plataformas en línea de muy gran tamaño (VLOP) y motores de búsqueda en línea de muy gran tamaño (VLOSE) designados con arreglo al artículo 33, apartado 4, del Reglamento (UE) 2022/2065 (ley de servicios digitales o DSA, por sus siglas en inglés).

Dicha publicación reviste carácter obligatorio y constituye el instrumento formal mediante el cual se identifican los servicios sujetos a las obligaciones reforzadas previstas en la sección 5 del capítulo III del citado reglamento. La principal novedad radica en la incorporación de WhatsApp como plataforma en línea de muy gran tamaño, en virtud de la decisión de designación de 26 de enero del 2026, por haber alcanzado su funcionalidad «Channels» el umbral

de cuarenta y cinco millones de usuarios activos mensuales en la Unión Europea. Cabe precisar que el servicio de mensajería privada de WhatsApp queda expresamente excluido del ámbito de aplicación de la ley de servicios digitales, pues no se subsume en la definición de *plataforma en línea*.

Meta, como prestador del servicio, dispone de un plazo de cuatro meses desde la designación para garantizar el cumplimiento de las obligaciones adicionales que corresponden a las plataformas en línea de muy gran tamaño, entre las que destacan la evaluación y mitigación de riesgos sistémicos, las obligaciones reforzadas de transparencia y la protección de los menores en línea.

Con esta actualización, la lista comprende un total de veintitrés plataformas en línea de muy gran tamaño (AliExpress, Amazon Store, App Store, Booking.com, Facebook, Google Maps, Google Play, Google Shopping, Instagram, LinkedIn, Pinterest, Pornhub, Shein, Snapchat, Temu, TikTok, WhatsApp, Wikipedia, X —anteriormente Twitter—, XNXX, XVideos, YouTube y Zalando) y dos motores de búsqueda en línea de muy gran tamaño (Bing y Google Search).

Iratze Arrigain García



Para más información, contacte con las siguientes letradas del Grupo de Propiedad Intelectual:

Sofía Martínez-Almeida y Alejos-Pita

Socia
smartinez@ga-p.com

Rais Amils Arnal

Socia
ramils@ga-p.com

Advertencia legal: Este boletín sólo contiene información general y no se refiere a un supuesto en particular. Su contenido no se puede considerar en ningún caso recomendación o asesoramiento legal sobre cuestión alguna.

© Gómez-Acebo & Pombo Abogados, 2026. Todos los derechos reservados.