

Boletín

*DERECHO
DIGITAL*

2026

CONTENIDO

Protección de datos personales en el ámbito digital	3	— La inteligencia artificial y el Proyecto de Ley Orgánica de protección civil de los derechos al honor, a la intimidad personal y familiar y a la propia imagen.....	14
— Recomendaciones y mejores prácticas para proteger los datos en los videojuegos ...	3	Ciberseguridad	15
— Coordinación entre la presentación de una reclamación ante una autoridad de control y el ejercicio de una acción judicial (STJUE de 18 de junio del 2026, C-414/24) ..	4	— Guía interpretativa sobre el Reglamento de Ciberresiliencia.....	15
— Directrices del Comité Europeo de Protección de Datos sobre anonimización	4	Comercio electrónico	16
— Puesta a disposición del público —en línea y a cambio de una contraprestación económica— de información sobre sentencias penales condenatorias (STJUE de 9 de julio del 2026, C-199/24).....	6	— Sentencia del Tribunal de Justicia de 9 de julio del 2026, C-234/25	16
— Límites de la publicidad registral frente al derecho a la privacidad.....	8	— El Tribunal de Justicia de la Unión Europea avala la verificación de edad en páginas pornográficas para proteger a los menores...	17
Propiedad intelectual.....	9	— Las plataformas que controlan algoritmos de difusión no pueden acogerse a la exención de responsabilidad de alojamiento	19
— La consideración de un post como obra	9	— La responsabilidad de las plataformas de vídeo ante la publicidad de juegos de azar	20
Inteligencia artificial	11	Infraestructuras digitales	22
— Reglamento (UE) 2026/1744 del Parlamento Europeo y del Consejo, de 8 de julio, por el que se modifican los Reglamentos (UE) 2024/1689, (UE) 2018/1139 y (UE) 2023/1230	11	— España: Proyecto de Real Decreto	22
— EU AI Act: la Comisión publica las directrices de transparencia previstas en el artículo 50..	12	Servicios digitales y regulación de plataformas digitales	24
— Directrices del Comité Europeo de Protección de Datos sobre el <i>web scraping</i> en el contexto de la inteligencia artificial generativa	13	— Nuevas designaciones de motores de búsqueda en línea de muy gran tamaño y de plataformas en línea de muy gran tamaño, de acuerdo con el Reglamento de Servicios Digitales (DSA)	24



PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO DIGITAL

Recomendaciones y mejores prácticas para proteger los datos en los videojuegos

La Agencia Española de Protección de Datos y la Autoridad Belga de Protección de Datos han publicado conjuntamente las *Recommendations and best practices for data protection in video games*, el primer documento elaborado por autoridades europeas de protección de datos para promover buenas prácticas destinadas a garantizar el cumplimiento del Reglamento General de Protección de Datos en el diseño, desarrollo y distribución de videojuegos. La guía se dirige a los distintos actores del ecosistema —incluidos desarrolladores, editores, plataformas de distribución, fabricantes de *hardware* y proveedores tecnológicos— y formula recomendaciones para las distintas fases del ciclo de vida del videojuego.

El documento parte de la constatación de que los videojuegos actuales implican tratamientos de datos especialmente complejos. Además de los datos utilizados para la creación y gestión de cuentas, la guía destaca la relevancia de la telemetría y de las inferencias conductuales

obtenidas a partir de la actividad de los jugadores, que pueden utilizarse para personalizar la experiencia de juego, elaborar perfiles o desarrollar estrategias de monetización. La guía analiza los riesgos asociados a estos tratamientos y subraya la necesidad de aplicar los principios de protección de datos desde el diseño y por defecto desde las primeras fases de desarrollo.

Uno de los aspectos destacados de la guía es la atención que presta a los patrones de diseño engañosos y adictivos. El documento advierte de prácticas capaces de orientar o manipular las decisiones de los jugadores, fomentar un uso excesivo o compulsivo del videojuego o explotar determinadas vulnerabilidades relacionadas con el consumo y la monetización. Entre los ejemplos examinados figuran los flujos de consentimiento manipulativos, determinadas mecánicas de *loot boxes* y los estímulos personalizados vinculados a la propensión al gasto.

Asimismo, dedica una atención especial a la protección de los menores. Recomendando que, salvo que un videojuego esté clara y demostrablemente dirigido exclusivamente a adultos, los distintos actores de la industria asuman que

habrá menores entre sus usuarios y adopten sus decisiones de diseño y tratamiento de datos en consecuencia.

Claudia Pérez Moneu

Coordinación
entre la presentación
de una reclamación
ante una autoridad de control
y el ejercicio de una acción judicial
(STJUE de 18 de junio del 2026,
C-414/24)

La Sala Primera del Tribunal de Justicia de la Unión Europea dictó sentencia el 18 de junio del 2026 en el asunto C-414/24, *Datenschutzbehörde y Dra. G S contra Bundesministerin für Justiz y D GmbH* (ECLI:EU:C:2026:493), en respuesta a una petición de decisión prejudicial planteada por el Tribunal Supremo Administrativo de Austria sobre la interpretación de los artículos 77 y 79 del Reglamento General de Protección de Datos.

El caso se refería a un interesado que, tras la denegación de una solicitud de supresión de datos, presentó tanto una reclamación ante la Autoridad Austriaca de Protección de Datos al amparo del artículo 77.1 del Reglamento General de Protección de Datos como una acción judicial con base en el artículo 79.1. La autoridad de control rechazó la reclamación al considerar que ya existían procedimientos judiciales pendientes sobre el mismo objeto. El tribunal remitente preguntó si tal rechazo era compatible con el mencionado reglamento.

El tribunal recuerda que las vías de recurso previstas en los artículos 77 y 79 del Reglamento General de Protección de Datos pueden ejercerse de forma concurrente e independien-

te. Asimismo, subraya que las autoridades de control están obligadas, en virtud del artículo 57.1f de dicho reglamento, a tramitar las reclamaciones con toda la diligencia debida y, cuando proceda, a ejercer las facultades correctivas previstas en el artículo 58.2.

Aunque los Estados miembros pueden establecer mecanismos procesales para coordinar ambas vías de tutela (como permitir que una autoridad de control suspenda el examen de una reclamación hasta que recaiga una resolución judicial), no pueden facultar a dicha autoridad para rechazar la reclamación por el mero hecho de que se hayan iniciado procedimientos judiciales. Un sistema de esta naturaleza podría privar a los interesados de la protección garantizada por el artículo 77 del Reglamento General de Protección de Datos.

El tribunal concluye, por tanto, que los artículos 77.1 y 79.1 del mencionado reglamento se oponen a que una autoridad de control rechace una reclamación únicamente porque estén pendientes procedimientos judiciales relativos al mismo objeto, incluso cuando en dichos procedimientos ya se haya dictado una resolución sobre el fondo que no sea firme. La sentencia confirma la naturaleza independiente de las vías de tutela administrativa y judicial previstas por el Reglamento General de Protección de Datos y aclara los límites de la autonomía procesal de los Estados miembros para coordinar ambos mecanismos.

Inês
Lucas Nunes

Directrices
del Comité Europeo
de Protección de Datos
sobre anonimización

El 7 de julio del 2026, el Comité Europeo de Protección de Datos (CEPD o el «Comité») adoptó, para consulta pública, sus Directrices 02/2026 sobre la anonimización, destinadas a sustituir el Dictamen 05/2014 del Grupo de Trabajo sobre Protección de Datos del Artículo 29, que durante más de una década constituyó la principal referencia en esta materia.

Las directrices se fundamentan en un test jurídico en dos fases derivado del artículo 4.1 y del considerando 26 del Reglamento General de Protección de Datos: la información es anónima si no se refiere a una persona física o si dicha persona no está identificada ni es identificable. Siguiendo la sentencia en el asunto C-413/23 P, *Supervisor Europeo de Protección de Datos c. la Junta Única de Resolución (SEPD c. JUR)*, el Comité adopta un enfoque relativo: un mismo conjunto de datos puede ser anónimo para una entidad y personal para otra, de modo que el carácter anónimo debe evaluarse desde la perspectiva de cada entidad pertinente. La probabilidad de identificación no tiene que ser nula, pero ha de resultar insignificante en la práctica. La noción de «medios razonablemente susceptibles de ser utilizados» se interpreta en sentido amplio, incluyendo medios disponibles a través de terceros y cualquier vía legal para obtener información adicional. El Comité advierte contra la confianza en una supuesta falta de motivación para reidentificar y subraya que las prohibiciones contractuales no equivalen a las legales.

En el plano técnico, las directrices precisan los tres criterios establecidos en el dictamen del 2014 transformándolos en «no aislamiento de registros» (*no record isolation*), «no vinculación» (*no linkage*) y «no inferencia» (*no inference*), siendo aplicables tanto en el marco de un enfoque contextual como simplificado. Cabe destacar que el criterio de inferencia se extiende expresamente a los datos agregados, los

datos sintéticos y los modelos de inteligencia artificial.

El Comité recuerda asimismo, como ya se entendía de forma generalizada, que la anonimización constituye en sí misma una operación de tratamiento que requiere una base jurídica conforme al artículo 6 del Reglamento General de Protección de Datos y, cuando se traten categorías especiales de datos, una excepción en virtud del artículo 9.2. Los responsables del tratamiento deben informar a los interesados de que sus datos serán anonimizados, han de documentar el proceso y las pruebas realizadas, y no deben calificar de *anónimos* datos en los que las personas sigan siendo identificables.

El enfoque relativo tiene también un corolario menos evidente con consecuencias prácticas. Según el Comité, cuando sea razonablemente probable que una entidad transmita los datos a un tercero y no pueda descartarse que este tercero disponga de medios razonablemente susceptibles de ser utilizados para identificar a las personas, los datos deben tratarse como personales tanto a efectos de dicha transmisión como del tratamiento ulterior por el destinatario. Apoyándose en la Sentencia *SEPD c. JUR*, el Comité añade que los datos pasan entonces indirectamente a ser personales también para la entidad transmisora, aun cuando ésta no pudiera identificar a nadie por sí sola. Como consecuencia, flujos de datos actualmente considerados fuera del ámbito del Reglamento General de Protección de Datos —porque los datos no son identificables en manos de su primer receptor— podrían quedar comprendidos en su alcance una vez que se tengan en cuenta las comunicaciones sucesivas a lo largo de la cadena. Está por ver si esta posición se mantiene inalterada tras la consulta, pero las organizaciones harían bien en mapear dónde acaban realmente sus datos *anónimos*.

En definitiva, las directrices convierten la anonimización de un ejercicio puntual en una evaluación de riesgos continua, documentada y basada en la perspectiva de cada entidad. Para las organizaciones que se apoyan en datos *anonimizados* con fines de análisis o intercambio de datos —incluidos los datos agregados y, como el Comité expresamente señala, los datos sintéticos y los modelos de inteligencia artificial—, éste es el momento adecuado para revisar las evaluaciones existentes y, en su caso, participar en la consulta pública.

Inês Dias Pinheiro

Puesta a disposición
del público —en línea y a cambio
de una contraprestación
económica— de información
sobre sentencias penales
condenatorias (STJUE de 9 de julio
del 2026, C-199/24)

Según la legislación sueca, la Agencia Sueca de Medios de Comunicación puede expedir certificados de publicación, que confieren protección constitucional. Dichos certificados también pueden abarcar la publicación y el mantenimiento de bases de datos que contengan datos personales. La legislación sueca establece amplias excepciones al Reglamento General de Protección de Datos para determinadas actividades cubiertas por tales certificados, de conformidad con el artículo 85 de dicho reglamento («Tratamiento y libertad de expresión e información»).

Legal Newsdesk gestiona Lexbase. Se negó a suprimir los datos personales relativos a una persona condenada por un delito en el 2011. Posteriormente, dicha persona interpuso una demanda contra la empresa en la que reclama-

ba una indemnización por daños y perjuicios por supuestas infracciones del Reglamento General de Protección de Datos. Legal Newsdesk alegó que Lexbase gozaba de protección constitucional en virtud de un certificado de publicación y que, por consiguiente, ese reglamento no era de aplicación.

En este contexto, el tribunal sueco planteó al Tribunal de Justicia de la Unión Europea las tres cuestiones siguientes para que se pronunciara con carácter prejudicial sobre la interpretación del artículo 85 del Reglamento General de Protección de Datos:

1. ¿Permite el artículo 85, apartado 1, del Reglamento General de Protección de Datos que los Estados miembros adopten medidas legislativas más allá de lo que les incumbe con arreglo al artículo 85, apartado 2, de dicho reglamento y en relación con el tratamiento de datos personales con fines distintos de los periodísticos o de expresión académica, artística o literaria?
2. En caso de respuesta afirmativa a la anterior cuestión prejudicial: ¿permite el artículo 85, apartado 1, del Reglamento General de Protección de Datos una conciliación entre el derecho a la protección de los datos personales previsto en dicho reglamento y la libertad de expresión e información conforme a la cual la persona cuyos datos personales son objeto de tratamiento —al ponerse a disposición del público en internet, a cambio de una con-

traprestación económica, información sobre sentencias penales condenatorias relativas a dicha persona— sólo tiene, como vías de recurso, la posibilidad de ejercitar una acción penal por el delito de difamación o de reclamar una indemnización por daños y perjuicios basada en ese delito?

3. En caso de respuesta negativa a la primera o a la segunda cuestión prejudicial: ¿constituye la actividad de poner a disposición del público en internet, sin ningún tratamiento ni edición, documentos públicos en forma de sentencias penales condenatorias, a cambio de una contraprestación económica, un tratamiento de datos personales que se lleva a cabo con los fines contemplados en el artículo 85, apartado 2, del Reglamento General de Protección de Datos?»

En respuesta a estas cuestiones, el Tribunal de Justicia de la Unión Europea sostuvo que el artículo 85, apartado 1, del Reglamento General de Protección de Datos no permite a los Estados miembros establecer excepciones a dicho reglamento más allá de las expresamente permitidas por el artículo 85, apartado 2. El artículo 85, apartado 1, exige a los Estados miembros que concilien la protección de datos con la libertad de expresión y de información, pero no autoriza por sí mismo excepciones al reglamento. Dichas excepciones sólo pueden introducirse en virtud del artículo 85, apartado 2, y únicamente para el tratamiento realizado con fines periodísticos o para la expresión académica, artística o literaria. Por lo tanto, el Tribunal de Justicia

européu consideró que los Estados miembros no pueden invocar el artículo 85, apartado 1, para excluir otras formas de tratamiento de la aplicación del mencionado reglamento.

El tribunal europeo también dictaminó que el artículo 85 del Reglamento General de Protección de Datos no permite a los Estados miembros restringir las vías de recurso de que disponen los interesados en virtud del capítulo VIII de este cuerpo normativo. Por lo tanto, la legislación nacional no puede establecer los procedimientos por difamación como única vía de defensa para un interesado cuyos datos sobre condenas penales se publiquen en línea. El interesado debe conservar el acceso a las vías de recurso previstas en los artículos 77, 78, 79 y 82 del reglamento, incluidos los derechos a presentar una reclamación ante la autoridad de protección de datos, a solicitar un recurso judicial efectivo y a reclamar una indemnización.

En lo que respecta a los *finés periodísticos*, el Tribunal de Justicia de la Unión Europea confirmó que dicho concepto debe interpretarse de manera amplia. El hecho de que el tratamiento se lleve a cabo en línea, a título oneroso o en relación con condenas penales no excluye, por sí mismo, dicho tratamiento del ámbito de aplicación del artículo 85, apartado 2.

Sin embargo, la mera publicación no es suficiente. El tratamiento de la información sólo se considera periodístico si tiene por objeto informar al público y se lleva a cabo de conformidad con las normas profesionales y éticas del periodismo. Debe implicar un trabajo editorial o una adaptación, o al menos regirse por una política editorial, y la información fáctica pertinente debe estar verificada.

El Tribunal de Justicia de la Unión Europea consideró que poner a disposición de cualquier usuario de pago sentencias penales sin editar

no parecía cumplir dichos requisitos. En particular, la actividad no parecía implicar una evaluación editorial, una adaptación ni una política periodística. El hecho de que los documentos pudieran resultar útiles para los periodistas no bastaba para que el tratamiento entrara en el ámbito de aplicación del artículo 85, apartado 2.

Daniel Reis

Límites de la publicidad registral frente al derecho a la privacidad

El Tribunal de Justicia —en su Sentencia de 3 de septiembre del 2026, *Jautiva*, C-798/24— ha analizado si la legislación letona sobre el Registro Mercantil en virtud de la cual se pone a disposición del público (que puede acceder en línea y descargarla, incluso sin necesidad de identificarse) determinada información relativa a los accionistas de sociedades anónimas (incluyendo el nombre, los apellidos de los socios personas físicas; el número de identificación personal o, en su defecto, su fecha de nacimiento, el número y la fecha de expedición del documento de identidad, el país y la autoridad de expedición de dicho documento; una dirección de contacto; la categoría, el número y el valor nominal de sus acciones, y el número de votos asociados a esas acciones). La finalidad de esta legislación es incrementar la transparencia en el ámbito empresarial para prevenir el blanqueo de capitales, la financiación del terrorismo y la proliferación de armas de destrucción masiva, así como proporcionar la información necesaria para la aplicación de sanciones nacionales, internacionales y de la Unión Europea.

Pues bien, lo primero que destaca el Tribunal de Justicia es que este grado de transparencia no

viene impuesto por la Directiva (UE) 2017/1132 del Parlamento Europeo y del Consejo, de 14 de junio, sobre determinados aspectos del Derecho de sociedades, cuyo artículo 14d restringe la obligación de publicar datos personales a «la identidad de las personas que, como órgano legalmente previsto, o como miembros de tal órgano: i) tengan el poder de obligar a la sociedad con respecto a terceros y representarla en juicio; las medidas de publicidad precisarán si las personas que tengan poder de obligar a la sociedad pueden hacerlo por sí solas o deben hacerlo conjuntamente, ii) participen en la administración, la vigilancia o el control de la sociedad». No se exige, por tanto, la publicación de información sobre todos los accionistas de las sociedades.

Por lo demás, la publicidad indiscriminada de dicha información entra en conflicto, según el Tribunal de Justicia, con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos), porque el acceso a dichos datos no está supeditado a ningún requisito, como la demostración de un interés legítimo.

Destaca a este respecto el tribunal que la normativa letona analizada «no parece ni necesaria ni proporcionada en relación con el objetivo» que pretende, porque no va acompañada de garantías suficientes que permitan proteger eficazmente a las personas afectadas contra los riesgos de abuso, ya que «sus datos personales son accesibles en internet y pueden ser objeto de descargas masivas, en particular por cualquier usuario no identificado, lo que aumenta dichos riesgos».

Ángel
García Vidal



PROPIEDAD INTELLECTUAL

La consideración de un post como obra

En su Sentencia de 3 de septiembre del 2026 (*Gándul Media Network*, C-598/24), el Tribunal de Justicia ha declarado que un post o texto publicado en una red social en el que se expresa una opinión sobre prácticas sociales consideradas inadecuadas puede constituir una obra protegida por derechos de propiedad intelectual, conforme a la Directiva 2001/29/CE de 22 de mayo, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información. Para ello será necesario que dicho texto cumpla los dos requisitos que el Tribunal de Justicia viene exigiendo para estar ante una obra protegible: que sea original, en el sentido de constituir una creación intelectual propia de su autor, y que sea identificable con suficiente precisión y objetividad.

Recuerda a estos efectos el Tribunal de Justicia que la Unión Europea está vinculada por lo dispuesto en el Tratado de la Organización Mundial de la Propiedad Intelectual (OMPI) sobre

Derecho de Autor, según el cual (art. 2.1), las obras literarias y artísticas comprenden todas las producciones en el campo literario, científico y artístico, cualquiera que sea el modo o forma de expresión, tales como los libros, folletos y «otros escritos», como es el caso de los textos publicados en las redes sociales.

Por lo demás, a la hora de calificar un determinado texto de obra protegida por propiedad intelectual, debe comprobarse si, al elaborar ese texto, «el autor ha podido tomar decisiones libres y creativas aptas para transmitir al lector la singularidad de la prestación de que se trate, singularidad que se derivará de la elección, la disposición y la combinación de las palabras mediante las que el autor haya expresado su espíritu creador de manera original y haya obtenido un resultado que constituya una creación intelectual». Y, a este respecto, son irrelevantes, en cambio, elementos como su extensión, su publicación en línea y su eventual pertenencia a un género literario predeterminado, a menos que tales elementos sean el resultado de reglas, consideraciones técnicas o condicionantes que no hayan dejado lugar al ejercicio de una libertad creativa por parte de su autor, en cuyo caso no puede considerarse que este texto



presente la originalidad necesaria para constituir una obra.

Por lo demás, en la misma sentencia ahora reseñada, el Tribunal de Justicia también interpreta el límite establecido en el artículo 5.3c de la citada Directiva 2001/29/CE, según el cual, los Estados miembros pueden establecer excepciones o limitaciones a los derechos derivados de la propiedad intelectual «cuando la prensa reproduzca o se quiera comunicar o poner a disposición del público artículos publicados sobre temas de actualidad económica, política o religiosa, o emisiones de obras o prestaciones del mismo carácter, en los casos en que dicho uso no esté reservado de manera expresa, y siempre que se indique la fuente, incluido el nombre del autor, o bien cuando el

uso de obras o prestaciones guarde conexión con la información sobre acontecimientos de actualidad, en la medida en que esté justificado por la finalidad informativa y siempre que, salvo en los casos en que resulte imposible, se indique la fuente, con inclusión del nombre del autor».

Pues bien, según el tribunal, esta disposición de la directiva «no se opone a una normativa nacional que restringe la excepción o limitación contemplada en dicha disposición a la reproducción de breves extractos de una obra protegida, pero sí se opone a la prohibición de obtener cualquier beneficio comercial o económico, directo o indirecto, de esa reproducción».

Ángel García Vidal



INTELIGENCIA ARTIFICIAL

Reglamento (UE) 2026/1744 del Parlamento Europeo y del Consejo, de 8 de julio, por el que se modifican los Reglamentos (UE) 2024/1689, (UE) 2018/1139 y (UE) 2023/1230 en lo que respecta a la simplificación de la aplicación de normas armonizadas en materia de inteligencia artificial (Ómnibus digital sobre IA)

El 24 de julio del 2026 se publicó el Reglamento (UE) 2026/1744 del Parlamento Europeo y del Consejo, de 8 de julio, por el que se modifican los Reglamentos (UE) 2024/1689, (UE) 2018/1139 y (UE) 2023/1230 en lo que respecta a la simplificación de la aplicación de normas armonizadas en materia de inteligencia artificial (Ómnibus digital sobre IA).

La norma introduce diversas modificaciones en el Reglamento (UE) 2024/1689 (Reglamento de Inteligencia Artificial) con el objetivo de facilitar y aclarar su aplicación, reducir cargas administrativas y evitar duplicidades con otras normas de la Unión Europea. Entre otras cuestiones, precisa el concepto de *componente de seguridad*, reformula la obligación de alfabeti-

zación en materia de inteligencia artificial, amplía el régimen aplicable al tratamiento excepcional de categorías especiales de datos personales para la detección y corrección de sesgos e incorpora nuevas prácticas prohibidas. Asimismo, simplifica determinados requisitos de registro y documentación y modifica las reglas relativas a los organismos notificados y a los procedimientos de evaluación de la conformidad.

Una de las principales novedades es el aplazamiento de la aplicación de las obligaciones previstas en las secciones 1, 2 y 3 del capítulo III del Reglamento (UE) 2024/1689 para los sistemas de inteligencia artificial de alto riesgo. Estas disposiciones serán aplicables desde el 2 de diciembre del 2027 a los sistemas clasificados como de alto riesgo conforme al artículo 6.2 y al anexo III, y desde el 2 de agosto del 2028 a los sistemas de alto riesgo vinculados a productos regulados por la legislación de armonización de la Unión Europea, conforme al artículo 6.1 y al anexo I.

El Ómnibus también amplía algunas medidas de apoyo y simplificación previstas para las pymes —incluidas las empresas emergentes— y las

pequeñas empresas de mediana capitalización. Entre ellas, se encuentran la posibilidad de presentar documentación técnica simplificada, la aplicación proporcionada de determinados requisitos, el acceso prioritario a espacios controlados de pruebas y la consideración de su situación económica en materia sancionadora. Además, se refuerzan las competencias de supervisión y garantía del cumplimiento de la Oficina Europea de Inteligencia Artificial y se amplía la posibilidad de realizar pruebas de sistemas de inteligencia artificial en condiciones reales.

Por último, se modifican los reglamentos sobre seguridad aérea y sobre máquinas para coordinar sus requisitos con los establecidos en el Reglamento de Inteligencia Artificial. En particular, se prevé que la normativa sectorial tenga en cuenta los requisitos aplicables a los sistemas de inteligencia artificial de alto riesgo y que, respecto de las máquinas, la Comisión incorpore los correspondientes requisitos de salud y seguridad mediante actos delegados aplicables, a más tardar, el 2 de agosto del 2028.

Camino Bustinduy de la Guerra

EU AI Act: la Comisión publica las directrices de transparencia previstas en el artículo 50

El 20 de julio del 2026, la Comisión Europea publicó sus directrices no vinculantes sobre las obligaciones de transparencia establecidas en el artículo 50 del Reglamento (UE) 2024/1689 (conocida como «ley de inteligencia artificial» o «ley de IA»). El objetivo declarado de las directrices es ayudar a las autoridades competentes, a los proveedores y a los responsables del despliegue a garantizar el cumplimiento del marco

de transparencia, aplicable desde el 2 de agosto del 2026 —dos años después de la entrada en vigor de la ley de inteligencia artificial—.

Una aclaración clave se refiere al concepto de *responsable del despliegue*. La ley de inteligencia artificial define a los responsables del despliegue como aquellos que utilizan un sistema de inteligencia artificial «bajo su *autoridad*», pero no explica qué se entiende por *autoridad*. Las directrices aclaran ahora que la *autoridad* sobre un sistema de inteligencia artificial implica la responsabilidad de la decisión de implantar el sistema y la forma de su uso respectivo, sin que ello requiera necesariamente un control técnico sobre su funcionamiento. Se aclara además que los empleados a título individual no son implantadores independientes de su empleador y que una persona jurídica sigue siendo implantadora incluso cuando terceros —como contratistas o autónomos— operan el sistema de inteligencia artificial en su nombre.

En su artículo 50, la ley de inteligencia artificial establece cuatro obligaciones de transparencia. Dos de ellas recaen sobre los proveedores, los cuales, por una parte, deben diseñar los sistemas de inteligencia artificial interactivos entre humanos e inteligencia artificial de tal manera que los usuarios sepan que están interactuando con ella, y, por otra, deben marcar el contenido de audio, imagen, vídeo o texto generado o manipulado por la inteligencia artificial en un formato legible por máquina para garantizar que sea detectable. Las directrices aclaran, en concreto, que la «interacción directa» requiere un intercambio bidireccional genuino, en tiempo real o casi en tiempo real, y excluye la interacción indirecta o mediada, en la que una persona se limita a estar expuesta a los resultados de la inteligencia artificial, y que los proveedores de agentes de inteligencia artificial, en particular, deben revelar tanto su naturaleza artificial como la identidad de la persona en

cuyo nombre actúan. Las directrices confirman asimismo que el contenido 3D, la realidad virtual, aumentada o mixta y los gemelos digitales entran dentro de su ámbito de aplicación, mientras que excluyen, específicamente, las secuencias cortas de números, símbolos o letras, tales como subtítulos, código fuente, resultados de máquina a máquina no expuestos a seres humanos y resultados utilizados en flujos de trabajo industriales de bucle cerrado, a menos que constituyan el resultado final.

Recae una doble obligación adicional sobre los responsables del despliegue, quienes deben informar a las personas expuestas a sistemas de reconocimiento de emociones o de categorización biométrica, así como etiquetar los *deepfakes* ('ultrafalsos') y los textos generados por inteligencia artificial que se publiquen para informar sobre asuntos de interés público. Las directrices proporcionan una prueba práctica de cuatro partes para evaluar la existencia de un *deepfake* y, en particular, exigen que la evaluación de la apariencia falsa tenga en cuenta la composición diversa de la audiencia previsible —incluidos los grupos vulnerables, como los niños y las personas mayores— en lugar de aplicar un único criterio de «consumidor medio».

De conformidad con el artículo 50, apartado 5, toda información debe transmitirse de forma clara y distinguible, a más tardar en el momento de la primera interacción con el sistema o de la primera exposición a él, y de conformidad con los requisitos de accesibilidad aplicables.

Las diversas obligaciones pueden aplicarse de forma acumulativa a un único sistema de inteligencia artificial, lo que podría implicar tanto a los proveedores como a los responsables de su implantación. En este contexto, las directrices destacan el papel de los códigos de buenas prácticas: los signatarios de un código consi-

derado adecuado con arreglo al artículo 50, apartado 7, se benefician de una vía predecible de cumplimiento y de un escrutinio supervisor menos riguroso, mientras que los no signatarios deben demostrar el cumplimiento por otros medios y pueden esperar solicitudes de información más detalladas. Las directrices también aclaran que las autoridades competentes pueden considerar la adhesión a un código adecuado como un factor atenuante a la hora de fijar las multas.

Cabe destacar que los contenidos generados por inteligencia artificial y los *deepfakes* producidos antes del 2 de agosto del 2026 no tienen que marcarse ni etiquetarse con carácter retroactivo, aunque los textos generados antes de esa fecha, pero publicados a partir de ella, sí deben etiquetarse.

Las empresas que suministren o implementen sistemas de inteligencia artificial en la Unión Europea deben considerar estas directrices como una guía práctica para el cumplimiento normativo. Entre las medidas prioritarias se incluyen determinar si la organización cumple los requisitos para ser considerada proveedora, implementadora o ambas; revisar las prácticas actuales de divulgación y etiquetado a la luz de las directrices, y considerar la adhesión temprana a un código de buenas prácticas para beneficiarse de la protección que ofrece, especialmente teniendo en cuenta que el incumplimiento conlleva multas administrativas de hasta 15 millones de euros o el 3 % de la facturación anual mundial, lo que sea mayor.

Rita Fraga Dornellas

Directrices del Comité Europeo de Protección de Datos sobre el *web scraping* en el contexto de la inteligencia artificial generativa

El Comité Europeo de Protección de Datos (CEPD) ha publicado las *Guidelines 03/2026 on web scraping in the context of generative AI*, unas directrices, actualmente en consulta pública, que abordan específicamente el uso de técnicas de *web scraping* ('raspado web') para recopilar datos destinados al entrenamiento de modelos de inteligencia artificial generativa. Con este documento, el Comité analiza la aplicación del Reglamento General de Protección de Datos a una práctica ampliamente utilizada en el desarrollo de sistemas de inteligencia artificial.

Las directrices parten de una idea clara: el hecho de que la información esté accesible públicamente en internet no excluye la aplicación de las normas de protección de datos. Por ello, el Comité recuerda que las organizaciones que utilizan datos obtenidos mediante *web scraping* deben garantizar el cumplimiento de los principios del mencionado reglamento.

Uno de los aspectos más relevantes del documento es el análisis del interés legítimo como posible base jurídica para este tipo de tratamientos. El Comité señala que esta base jurídica es utilizada con frecuencia por entidades privadas para el *web scraping* destinado al entrenamiento de inteligencia artificial generativa, pero subraya que su aplicación exige una evaluación rigurosa de la necesidad del tratamiento, de las expectativas razonables de los interesados y de los riesgos para sus derechos y libertades.

Iratze Arrigain García

La inteligencia artificial
y el Proyecto de Ley Orgánica
de protección civil de los derechos
al honor, a la intimidad personal
y familiar y a la propia imagen

El Proyecto de Ley Orgánica de protección civil de los derechos al honor, a la intimidad personal y familiar y a la propia imagen, publicado en el *Boletín Oficial de las Cortes Generales* de 27 de julio del 2026, introduce varias disposiciones sobre la manipulación con medios técnicos (como es el caso de la inteligencia artificial) de la imagen o la voz de una persona.

Así, se prevé la consideración como intromisión ilegítima en el ámbito de protección del honor, de la intimidad y de la propia imagen, «la utilización o difusión de la imagen o la voz de una persona que haya sido creada, simulada o manipulada tecnológicamente para dotarla de una apariencia extremadamente realista», así como «la utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga, aunque la voz o la imagen hubieran sido simuladas o manipuladas».

De igual modo, también se prevé que el derecho a la propia imagen no impedirá la utilización de imágenes o voces extremadamente realistas de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública (siempre que no sean autoridades o personas que desempeñen funciones que por su naturaleza necesiten el anonimato de la persona que las ejerza) «generadas o manipuladas tecnológicamente como parte de una obra o programa manifiestamente creativos, satíricos, artísticos, de ficción o análogos». Pero se introduce la salvedad de que, «cuando este contenido pueda inducir a una persona a pensar erróneamente que es auténtico o verídico, el responsable de su divulgación deberá hacer pública la existencia de dicho contenido generado o manipulado artificialmente de una manera adecuada que no dificulte la exhibición o el disfrute de la obra».

Ángel García Vidal



CIBERSEGURIDAD

Guía interpretativa sobre el Reglamento de Ciberresiliencia

La Comisión Europea ha publicado una guía interpretativa sobre el Reglamento de Ciberresiliencia (*Cyber Resilience Act* o CRA) con el objetivo de facilitar su aplicación práctica por parte de fabricantes y otros operadores económicos con vistas a la plena aplicación de sus principales obligaciones. La guía no tiene carácter vinculante, pero ofrece la interpretación de la Comisión sobre algunas de las cuestiones que más dudas han suscitado desde la adopción del reglamento.

El documento aporta aclaraciones sobre aspectos esenciales del reglamento, como su ámbito de aplicación, el tratamiento del *software*

libre y de código abierto, el concepto de *modificación sustancial de productos* y la determinación de los periodos de soporte. También ofrece orientaciones específicas sobre las soluciones de procesamiento remoto de datos y sobre productos que incorporan componentes o *software* desarrollados por terceros.

Un mensaje transversal de la guía es la importancia de la evaluación de los riesgos de ciberseguridad durante todo el ciclo de vida del producto. La Comisión recuerda que los fabricantes deben identificar, documentar y mitigar los riesgos relevantes atendiendo a la finalidad y al uso razonablemente previsible del producto, y revisar dicha evaluación cuando resulte necesario a lo largo de su ciclo de vida.

Claudia
Pérez Moneu



COMERCIO ELECTRÓNICO

Suscripciones de *streaming*:
¿servicio digital o suministro
de contenido digital?
Sentencia del Tribunal de Justicia
de 9 de julio del 2026,
C-234/25

La Directiva 2011/83/UE, sobre los derechos de los consumidores, reconoce con carácter general un plazo de catorce días para desistir de los contratos celebrados a distancia, aunque prevé determinadas excepciones. Entre ellas se encuentra la relativa al suministro de contenido digital que no se preste en un soporte material, siempre que la ejecución haya comenzado y se cumplan las condiciones de consentimiento, conocimiento y confirmación exigidas por la propia directiva. Esta excepción ha planteado dudas sobre si una suscripción de *streaming* que permite a los usuarios descargar contenidos para verlos más tarde debe tratarse como suministro de «contenido digital» o como prestación de un «servicio digital». Conforme a la Directiva 2011/83/UE, por remisión a la Directiva 2019/770/UE, el *contenido digital* se refiere a datos producidos y suministrados en formato digital, mientras que un *servicio digital* incluye

un servicio que permite al consumidor crear, tratar, almacenar o acceder a datos en formato digital, o compartir o interactuar de otro modo con dichos datos.

La cuestión fue analizada por el Tribunal de Justicia en la Sentencia de 9 de julio del 2026, *Sky Österreich Fernsehen*, C-234/25. El litigio enfrentaba a Sky Österreich, que ofrecía en Austria los paquetes «Sport & Live TV» y «Fiction & Live TV», con la asociación de consumidores Verein für Konsumenteninformation (VKI), que cuestionaba una cláusula según la cual el consumidor aceptaba el inicio de la ejecución antes de que expirase el plazo de desistimiento y reconocía que por ello perdía tal derecho. El Tribunal Supremo austriaco planteó al Tribunal de Justicia de la Unión Europea si una oferta de *streaming* de esas características constituía suministro de contenido digital a los efectos del artículo 16, párrafo primero, letra *m*, de la Directiva 2011/83/UE, como sostenía Sky Österreich, o prestación de un servicio digital, como sostenía VKI.

El tribunal rechazó que la calificación dependa únicamente del medio técnico de acceso a los datos digitales o de la duración continua del

suministro. El criterio decisivo es si la oferta del proveedor de servicios presenta un carácter dinámico que va más allá de la mera provisión estable y, en su caso, continua de contenidos específicos. Así ocurre cuando, sobre la base de un seguimiento de los contenidos a los que el consumidor ha accedido o de sus listas de reproducción o favoritos, la oferta se adapta al comportamiento o expectativas individuales del consumidor o influye en la forma en que éste utiliza el servicio. Serían indicios de ese carácter dinámico, por ejemplo, la actualización continua del catálogo ofrecido, las recomendaciones personalizadas, los perfiles de usuario, las listas de favoritos o las funcionalidades que ordenan o priorizan contenidos en función de la actividad del usuario.

Sobre esa base, el tribunal concluye que un servicio de *streaming* no constituye suministro de «contenido digital», sino prestación de un «servicio digital», si la oferta tiene ese carácter dinámico. En consecuencia, el proveedor no puede ampararse en la excepción del artículo 16, párrafo primero, letra *m*, para excluir el derecho de desistimiento desde el inicio de la ejecución. No obstante, el tribunal recuerda que el artículo 14, apartado 3, de la Directiva 2011/83 permite al comerciante reclamar un importe proporcional por la parte ya prestada del servicio si el consumidor solicitó el inicio de la ejecución durante el plazo de desistimiento. Esa compensación puede atender no sólo al tiempo de uso, sino también al valor económico de los contenidos efectivamente puestos a disposición y visionados.

La sentencia exige a los proveedores de servicios en línea mirar más allá de la redacción de sus condiciones generales y atender a la configuración efectiva de sus productos. Las funcionalidades de personalización, recomendación, actualización frecuente del catálogo y adaptación de la experiencia de usuario pueden ser

decisivas para calificar su oferta como un servicio digital en lugar de como un suministro de contenido digital. La consecuencia práctica es que, en las ofertas que se incluyen en la categoría de «servicios digitales», el consentimiento del consumidor para el inicio de la prestación no implica necesariamente la pérdida del derecho de desistimiento, aunque puede dar lugar al pago de una cantidad proporcional si el consumidor decide ejercerlo después de haber utilizado el servicio.

Duarte Rocha Manso

El Tribunal de Justicia de la Unión Europea avala la verificación de edad en páginas pornográficas para proteger a los menores

En su Sentencia de 16 de junio del 2026, en los asuntos acumulados C-188/24 y C-190/24, *WebGroup Czech Republic* y *Coyote System*, el Tribunal de Justicia de la Unión Europea ha analizado si se ajustan a la Directiva de comercio electrónico y a los referidos principios de control en origen y de reconocimiento mutuo en ella establecidos una normativa francesa que establece la obligación de los sitios pornográficos de implantar sistemas eficaces de verificación de edad para impedir el acceso de menores y, en segundo lugar, otra que establece la prohibición temporal de difundir información sobre determinados controles policiales y de tráfico mediante aplicaciones de asistencia a la conducción.

Pues bien, lo primero que hace el Tribunal de Justicia es analizar si las referidas normativas encajan en el ya mencionado «ámbito coordinado» de la directiva, que es donde, como regla general, operan los principios de control en



origen y de reconocimiento mutuo. Y la conclusión a la que llega el tribunal es que las disposiciones penales destinadas a garantizar la protección de los menores, así como las medidas que imponen la implantación de mecanismos técnicos para bloquear el acceso de los menores a contenidos pornográficos, entran en el «ámbito coordinado» y constituyen una «exigencia» relativa al ejercicio de la actividad de los servicios de la sociedad de la información, en el sentido de la Directiva 2000/31.

Ahora bien, aunque esas disposiciones nacionales encajen en el ámbito coordinado de la directiva, es posible que los Estados miembros adopten, respecto de un servicio concreto de la sociedad de la información, medidas que constituyan una excepción a los principios de control en origen y de reconocimiento mutuo cuando sean necesarias para garantizar el orden público, la protección de la salud pública, la seguridad pública o la protección de los consumidores, o cuando se adopten respecto de un servicio de la sociedad de la información que perjudique efectivamente esos objetivos o constituya un riesgo serio y grave de perjuicio para ellos, y sean proporcionadas a dichos objetivos.

Según el Tribunal de Justicia, los objetivos perseguidos por la primera normativa controvertida encajan en el concepto de *orden público*, pues éste comprende, en particular, la protección de los menores y la lucha contra las vulneraciones de la dignidad de la persona humana, así como la prevención, investigación, detección y persecución de infracciones penales. De igual modo, motivos de orden público, así como de seguridad pública o protección de las personas, pueden justificar prohibiciones de difusión de información relativa a controles de tráfico.

Ahora bien, en este punto es muy relevante el matiz que realiza el Tribunal de Justicia al des-

tacar que estas normas no quedan excluidas automáticamente del principio del control en origen por el mero hecho de ser normas penales o de seguridad pública. Según el tribunal, la directiva se opone a que un Estado miembro imponga directamente a todos los operadores establecidos en otro Estado una obligación general de impedir el acceso de menores a contenidos pornográficos así como una prohibición general de difundir determinada información sobre controles policiales. Por el contrario, lo que sí es posible es que, en aplicación de dicha normativa general, un Estado miembro adopte medidas —individuales y específicas— contra un prestador establecido en otro Estado. Y, sobre esa base, el Tribunal de Justicia constata que en las referidas normativas francesas, además de las correspondientes prohibiciones generales, se prevé que la autoridad administrativa remitirá un requerimiento individualizado a cada operador para instarlo al cumplimiento de la normativa.

Por lo tanto, aunque las disposiciones generales no, los requerimientos individuales dirigidos a los prestadores de servicios de comunicación al público que difunden contenidos pornográficos o las decisiones de prohibición dirigidas a los operadores de un servicio determinado para que no difundan ciertas informaciones sí pueden calificarse de medidas relativas a un servicio concreto de la sociedad de la información a efectos del artículo 3, apartado 4, letra a, de la Directiva 2000/31, permitiendo así que el Estado de destino excepcione el principio de control en origen, siempre que se respeten las exigencias de proporcionalidad y las garantías procedimentales establecidas por el Derecho de la Unión.

Ángel
García Vidal

Las plataformas que controlan
algoritmos de difusión
no pueden acogerse
a la exención de responsabilidad
de alojamiento

En su Sentencia de 16 de junio del 2026, en los asuntos acumulados C-188/24 y C-190/24, *WebGroup Czech Republic* y *Coyote System*, el Tribunal de Justicia también analiza si la normativa francesa que impide a los operadores de servicios electrónicos de ayuda a la conducción o a la navegación mediante geolocalización difundir determinadas informaciones sobre controles en carretera en realidad no supone imponerles una obligación general de supervisar la información que transmiten, obligación general de supervisión que prohíbe el artículo 15 de la directiva (artículo hoy derogado por el Reglamento (UE) 2022/2065, de Servicios Digitales, que sienta tal prohibición en su artículo 8).

En primer lugar, el tribunal recuerda su jurisprudencia previa (Sentencia de 3 de octubre del 2019, *Glawischnig-Piesczek*, C-18/18), según la cual la prohibición impuesta a los Estados miembros de establecer para los prestadores intermediarios de servicios una obligación general de supervisión no afecta a las obligaciones de supervisión en «casos concretos» y, en particular, deja intactas las órdenes dictadas por las autoridades nacionales con arreglo a sus respectivas legislaciones y relativas a un caso de esa naturaleza. Una orden de este tipo no obliga al prestador a realizar una evaluación autónoma del contenido almacenado, puesto que puede limitarse a identificar los contenidos afectados por la orden mediante búsquedas automatizadas.

Con estos presupuestos, la prohibición de control general se aplica a los prestadores intermediarios de servicios y una cuestión previa sería

la de determinar si el prestador del servicio de ayuda a la conducción tiene tal condición. Es ésta una cuestión cuya determinación el Tribunal de Justicia deja al juez nacional. Pero, en todo caso, hace una consideración muy relevante para determinar si es de aplicación la exención de responsabilidad de los intermediarios de *hosting*, regulada inicialmente en el artículo 14 de la directiva (y, en la actualidad, en el artículo 6 del Reglamento de Servicios Digitales). Según esta exención, los Estados miembros garantizarán que, cuando se preste un servicio de la sociedad de la información consistente en almacenar datos facilitados por el destinatario del servicio, el prestador de servicios no pueda ser considerado responsable de los datos almacenados a petición del destinatario si se cumplen estas condiciones:

- a) que el prestador de servicios no tenga conocimiento efectivo de que la actividad a la información es ilícita y, en lo que se refiere a una acción por daños y perjuicios, no tenga conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito;
- b) o que, en cuanto tenga conocimiento de estos puntos, el prestador de servicios actúe con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible.

Pues bien, según el Tribunal de Justicia, las condiciones de conocimiento y control deben entenderse como alternativas y autónomas entre sí. Por consiguiente, el operador de un servicio de la sociedad de la información que controle la información almacenada queda excluido del beneficio incluso aunque no llegue a conocer esa información debido a la automatización de su tratamiento.

Y, a este respecto, es especialmente relevante el hecho de que en la sentencia ahora comen-

tada el Tribunal de Justicia declare que el control puede ejercerse por medio de un algoritmo, afirmando que es precisamente a través del algoritmo utilizado como dicho operador ejerce un control sobre la información almacenada. En consecuencia, mientras haya predeterminado, mediante ese algoritmo, las condiciones conforme a las cuales dicha información será o no difundida, carece de relevancia que el operador no realice por sí mismo intervenciones adicionales destinadas a promover, modificar o eliminar la información almacenada para su difusión.

Por lo tanto, si más allá de una mera clasificación e indexación de la información para facilitar su accesibilidad, el algoritmo utilizado determina, en interés del operador o de su servicio, en qué condiciones, de qué manera y con qué orden de prioridad se difunde o no dicha información, ese operador ejerce un control sobre aquélla. En consecuencia, el servicio que presta no puede calificarse de «servicio de la sociedad de la información consistente en el almacenamiento de información proporcionada por un destinatario del servicio», por lo que no sería de aplicación la exención de responsabilidad.

Ángel García Vidal

La responsabilidad de las plataformas de vídeo ante la publicidad de juegos de azar

La Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), no resulta de aplicación a las actividades de juegos

de azar que impliquen apuestas de valor monetario, incluidas loterías y apuestas. Así se dispone en el artículo 1.5 de la directiva.

No obstante, se le ha planteado al Tribunal de Justicia si la directiva es aplicable en los casos en que en una plataforma de vídeos en línea un creador de contenido suba vídeos en los que promocione sitios de internet de juegos de azar. La cuestión ha sido resuelta en la Sentencia de 16 de julio del 2026, AGCOM (*Jeux d'argent en ligne*), C-421/24, ECLI:EU:C:2026:592, en la que el tribunal ha declarado que un servicio de la sociedad de la información consistente en alojar vídeos en línea está comprendido en el ámbito de aplicación de dicha directiva cuando esos vídeos contengan publicidad de juegos de azar que impliquen apuestas de valor monetario.

Con esa premisa, y partiendo de la aplicación de la directiva, el Tribunal de Justicia examina si estos proveedores del servicio de alojamiento de vídeos pueden ampararse en la exención de responsabilidad prevista en el artículo 14 de la directiva (y, en la actualidad, en el artículo 6 del Reglamento (UE) 2022/2065, de Servicios Digitales).

Pues bien, según el tribunal, dicha exención «no se aplica al operador de una plataforma de vídeos en línea que ha celebrado, con una persona que utiliza esa plataforma para difundir vídeos en un canal específico, un contrato de asociación comercial que establece un reparto de ingresos publicitarios y que, en el marco de la celebración o de la ejecución de dicho contrato, ha examinado el contenido de ese canal y, en particular, su tema principal, los vídeos más vistos o los más recientes, o incluso los metadatos de esos vídeos».

A este respecto y como se explica en la sentencia, «aun cuando dicho examen del contenido,



ya sea automatizado o efectuado por personas físicas, esté destinado a comprobar que el creador de contenido que solicita ese contrato de asociación comercial respeta las normas establecidas por la plataforma para acceder a tal asociación, proporciona al operador de dicha plataforma un conocimiento concreto del con-

tenido esencial de un conjunto de vídeos, de modo que no puede sostener ejercer una actividad meramente técnica, automática y pasiva y desempeñar, por ende, un papel de intermediario neutral».

Ángel García Vidal



INFRAESTRUCTURAS DIGITALES

España: Proyecto de Real Decreto por el que se regulan los requisitos de sostenibilidad energética, medioambiental y de resiliencia y soberanía digital aplicables a los centros de datos

El Ministerio para la Transición Ecológica y el Reto Demográfico ha sometido a audiencia pública el Proyecto de Real Decreto por el que se regulan los requisitos de sostenibilidad energética, medioambiental, y de resiliencia y soberanía digital aplicables a los centros de datos (Proyecto de Real Decreto). La norma proyectada tiene por objeto establecer las condiciones aplicables a estas infraestructuras, incluidos los requisitos que deberán observarse para solicitar, obtener y mantener los permisos de acceso y conexión a las redes de transporte y distribución de energía eléctrica.

Con carácter general, el régimen previsto se aplicará a los centros de datos con una potencia de acceso igual o superior a un megavatio, así como a los grupos de centros situados en una misma ubicación y pertenecientes al mismo titular que alcancen conjuntamente dicho

umbral. Se excluyen los centros destinados exclusivamente a la defensa, la protección civil y la seguridad pública. Por su parte, las obligaciones de comunicación y publicidad de información se extenderán a los centros cuya potencia de tecnología de la información sea igual o superior a quinientos kilovatios (500 kW), con independencia de su potencia de acceso.

El proyecto de real decreto establece requisitos en materia de resiliencia y soberanía digital, eficiencia energética y eficiencia en el uso del agua. Asimismo, incorpora exigencias relativas al consumo de electricidad de origen renovable que incluyen criterios de adicionalidad y correlación horaria entre el consumo del centro y la generación renovable empleada para cubrirlo. La acreditación de estos requisitos se articula mediante declaraciones responsables, etiquetas o documentación justificativa, según la obligación de que se trate.

En materia de soberanía digital, se prevén, entre otras obligaciones, el establecimiento del operador en la Unión Europea, la permanencia en ella de determinados datos operativos sometidos a su control y la adopción de medidas respecto de accesos o transferencias requeridos



por autoridades de terceros países. Los centros que alojen sistemas de información del sector público sujetos al Esquema Nacional de Seguridad deberán garantizar que los datos correspondientes —incluidos metadatos, registros, réplicas y copias de seguridad— sean tratados, almacenados y transferidos exclusivamente dentro de la Unión Europea.

El proyecto de real decreto prevé mecanismos de supervisión y control durante la explotación de las instalaciones. El incumplimiento de las

obligaciones podrá dar lugar a la aplicación de recargos sobre los cargos y peajes eléctricos y, en determinados supuestos de incumplimiento significativo y reiterado, a la pérdida de los permisos de acceso y conexión. También se establecen obligaciones de recogida, comunicación y publicación de información sobre el rendimiento energético, el uso de energías renovables, la huella hídrica y la demanda eléctrica.

Camino Bustinduy de la Guerra



SERVICIOS DIGITALES Y REGULACIÓN DE PLATAFORMAS DIGITALES

Nuevas designaciones de motores de búsqueda en línea de muy gran tamaño y de plataformas en línea de muy gran tamaño, de acuerdo con el Reglamento de Servicios Digitales (DSA)

La Comisión Europea ha designado a ChatGPT motor de búsqueda en línea de muy gran tamaño (*very large online search engine* o VLOSE) y a Reddit y Roblox plataformas en línea de muy gran tamaño (*very large online platforms* o VLOP) en virtud del Reglamento de Servicios Digitales (DSA), tras constatar que cada uno de estos servicios supera el umbral de cuarenta y cinco millones de usuarios activos mensuales en la Unión Europea.

Como consecuencia de esta designación, las tres plataformas deberán cumplir, en un plazo de cuatro meses desde su notificación y, por tanto, a más tardar, en enero del 2027, las obligaciones reforzadas previstas para los servicios de mayor tamaño. Entre otras cuestiones, deberán evaluar y mitigar los riesgos sistémicos

asociados a sus servicios y a sus sistemas algorítmicos. Entre estos riesgos se incluyen los relacionados con la difusión de contenidos ilícitos, la protección de los menores, el bienestar físico y mental de los usuarios, los derechos fundamentales, los procesos electorales y la seguridad pública.

La decisión resulta especialmente relevante en el caso de ChatGPT al haber sido considerado por la Comisión motor de búsqueda en línea a efectos del citado reglamento. Por su parte, Reddit y Roblox han sido calificados de plataformas en línea.

Estas designaciones amplían el grupo de los servicios sujetos a la supervisión reforzada prevista en el Reglamento de Servicios Digitales y reflejan la creciente atención de las autoridades europeas hacia plataformas digitales que desempeñan un papel relevante en el acceso a la información, la interacción social y el consumo de contenidos en línea.

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.