Insights y noticias legales

company LEGAL PARTNERS

Novedades

Datos y Nuevas Tecnologías

4º Trimestre 2025

Insights y noticias legales

Novedades datos y nuevas tecnologías de 4º Trimestre 2025

1. Resoluciones de la Agencia Española de Protección de Datos

- La AEPD declara vulnerado el principio de confidencialidad en envíos postales del Ayuntamiento de Vigo.
- La AEPD fija un precedente al sancionar “deepfakes” de menores creados con IA.
- Carrefour PASS, sancionada por la AEPD tras una brecha de seguridad que expuso datos financieros.
- La AEPD impone sanción millonaria a AENA por desplegar sistemas de reconocimiento facial sin una Evaluación de Impacto válida.
- La AEPD sanciona a un hotel por exponer datos identificativos de huéspedes en zonas comunes.

2. Sentencias de órganos judiciales españoles y europeos

- El Juzgado de lo Social nº 3 de A Coruña avala el uso de sistemas biométricos para control laboral y se aparta del criterio de la AEPD.
- Juzgado de lo Mercantil nº 15 de Madrid declara desleal la conducta de Meta .
- Sentencia del Tribunal de Justicia de la Unión Europea analiza el criterio de originalidad en las obras de arte aplicadas.

3. Novedades legislativas

- Propuesta de Reglamento Ómnibus Digital

Resoluciones y publicaciones de la AEPD

La AEPD declara vulnerado el principio de confidencialidad en envíos postales del Ayuntamiento de Vigo

La AEPD vuelve a incidir en la importancia del principio de confidencialidad en tratamientos cotidianos, recordando que incluso elementos externos como sobres postales pueden revelar información sensible y generar una pérdida de confidencialidad.

Un ciudadano interpuso una reclamación ante la AEPD al haber recibido dos notificaciones remitidas por el Ayuntamiento de Vigo mediante correo postal certificado. En el exterior de los sobres figuraban de forma destacada y visible las expresiones **"Diligencia de Embargo"** y **"Notificación Providencia de Apremio"**, acompañadas de referencias numéricas que identificaban los expedientes administrativos en curso.

El reclamante alegó que estos sobres hacían reconocibles ante terceros datos sobre su situación financiera, pues cualquier persona que accediera o manipulase el envío podía conocer que existían actuaciones recaudatorias y un procedimiento ejecutivo contra él. Además, puso de manifiesto que, hasta ese momento, todas las notificaciones relacionadas con el expediente se habían realizado por vía telemática, por lo que no entendía la alteración en el sistema de comunicación ni la necesidad de incluir información que desvelaba el contenido de la actuación administrativa.

El Ayuntamiento, en respuesta al requerimiento de la AEPD, reconoció los hechos y aportó pruebas de haber modificado sus sobres para evitar la reiteración de los incidentes, sustituyendo las referencias explícitas por el término genérico **"Notificación Administrativa"**, acreditando envíos posteriores ya corregidos.

En vista de los hechos alegados y de la inspección realizada, la AEPD determinó que el Ayuntamiento vulneró el artículo 5.1.f) del RGPD, que recoge el principio de integridad y confidencialidad, según el cual los datos personales deben ser tratados de forma que se impida el acceso no autorizado a la información. Para la AEPD, la leyenda impresa en los sobres constituye un tratamiento de datos personales, dado que no solo incluía la identidad y domicilio del interesado, sino que añadía información que permitía inferir la existencia de una deuda en vía ejecutiva, un procedimiento de apremio y, en uno de los casos, un embargo, lo que alcanza al ámbito económico del reclamante.

El acceso potencial por parte de terceros, aunque no materializado, es suficiente para configurar la pérdida de confidencialidad, ya que bastaba con la lectura externa del sobre para descubrir datos protegidos.

Asimismo, la AEPD subrayó que el ayuntamiento no había aplicado las medidas organizativas necesarias para prevenir la difusión innecesaria de información, incumpliendo su deber de responsabilidad proactiva, que exige anticiparse al riesgo y demostrar que se han adoptado sistemas adecuados de protección.

En consecuencia, la autoridad concluyó que se produjo un tratamiento indebido y desproporcionado, pues la inclusión de las expresiones “embargo” y “apremio” no resultaba necesaria para la finalidad de la notificación y exponía información personal a terceros.

Sanciones aplicables

La conducta fue calificada como infracción del artículo 5.1.f del RGPD, tipificada como vulneración muy grave conforme al artículo 83.5 RGPD y artículo 72.1 Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales (“**LOPDGDD**”), al afectar a principios esenciales de la normativa.

No obstante, al tratarse de una Administración Local, la AEPD aplicó el régimen especial del artículo 77 LOPDGDD, que impide imponer multas económicas a las entidades públicas incluidas en su ámbito. En su lugar, la Agencia declaró formalmente la infracción y pudo haber ordenado medidas correctivas para garantizar la adecuación futura del tratamiento.

En este caso, como el Ayuntamiento demostró que había adoptado medidas correctoras antes de la resolución (suprimió la información visible en sobres y utilizó únicamente descripciones neutras), la AEPD consideró que no resultaba necesario imponer obligaciones adicionales, limitándose a:

- Declarar la infracción cometida,
- Notificar al Defensor del Pueblo,
- Establecer su publicación en la web de la AEPD una vez adquiriese firmeza.

Puedes consultar la resolución a través del siguiente enlace.

La AEPD fija un precedente al sancionar “deepfakes” de menores creados con IA

Esta resolución marca un precedente relevante al aplicar el RGPD a la generación de imágenes sintéticas mediante inteligencia artificial, reforzando la protección de los menores frente a usos ilícitos de tecnologías de fácil acceso.

El 6 de noviembre de 2025, la AEPD dictó resolución aplicando el RGPD a la generación de imágenes sintéticas mediante inteligencia artificial o IA. La AEPD concluye que la modificación y utilización del rostro de una persona para crear imágenes artificiales configura un tratamiento de datos personales y queda plenamente sujeta al régimen jurídico del RGPD.

Los hechos tienen lugar en septiembre de 2023, cuando varios menores utilizaron una aplicación de IA, para producir imágenes sintéticas de contenido sexual en las que se insertaba el rostro real de compañeras menores de edad sobre cuerpos desnudos ajenos, configurando material falso, pero visualmente verosímil. La generación de estas imágenes no requería conocimientos técnicos avanzados, y la herramienta operaba en la nube sin salvaguardas eficaces para impedir su uso con fines ilícitos. Las imágenes generadas

fueron difundidas masivamente en redes sociales ampliando la exposición y el daño potencial para las víctimas.

La intervención de la AEPD se orientó exclusivamente al análisis de la eventual vulneración del derecho fundamental a la protección de datos personales. En este sentido, la AEPD aprecia una vulneración del artículo 6.1 del RGPD al constatar que las actuaciones analizadas constituyen un tratamiento de datos personales desprovisto de cualquier base legitimadora.

En primer término, la AEPD identifica el rostro de las menores como dato personal en el sentido del artículo 4.1 RGPD, dado que permite su identificación directa, precisando que la manipulación algorítmica o la naturaleza sintética del resultado no alteran dicha calificación mientras la imagen resultante mantenga un vínculo identificable con la afectada.

En segundo lugar, califica como tratamiento todas las operaciones realizadas (captación, transformación mediante sistemas de inteligencia artificial, generación de contenido sintético y difusión posterior) en aplicación del artículo 4.2 RGPD, subrayando que su existencia es independiente de la intencionalidad, madurez o ausencia de lucro del infractor.

Finalmente, destaca la inexistencia absoluta de una base jurídica válida conforme al artículo 6.1 RGPD, por no concurrir consentimiento, obligación legal, interés público, interés contractual ni interés legítimo prevalente, prohibido expresamente cuando se ven comprometidos los derechos de menores.

La resolución añade factores agravantes que intensifican la ilicitud: la condición de menores de las víctimas, cuyo tratamiento exige salvaguardas reforzadas (Considerando 38 RGPD), la tipología del contenido generado, con afectación directa a su dignidad e indemnidad, y la amplia difusión del material, que multiplica el impacto y la persistencia del daño.

Sanción aplicable

La AEPD califica la conducta como infracción muy grave, de acuerdo con lo previsto en el artículo 83.5.a del RGPD y el artículo 72.1.b de la LOPDGDD, al tratarse de un tratamiento de datos personales realizado sin base legitimadora sobre la imagen de una menor. En ejercicio de sus potestades sancionadoras del artículo 58.2 RGPD, la AEPD impone una multa administrativa de 2.000 euros, reducida a 1.200 euros tras la aplicación de los descuentos previstos por reconocimiento de responsabilidad y pago voluntario.

Dado que el infractor es menor de edad y carece de capacidad económica, la obligación pecuniaria se traslada a sus representantes legales. La resolución precisa igualmente que la responsabilidad recae exclusivamente en quien determinó los fines y medios del tratamiento (en este caso, el menor autor de la manipulación y difusión), descartándose cualquier imputación a las plataformas digitales o a la aplicación de inteligencia artificial utilizada, al no ostentar estas la condición de responsables según la definición contenida en el artículo 4.7 del RGPD.

Puedes consultar la resolución a través del siguiente enlace

Carrefour PASS, sancionada por la AEPD tras una brecha de seguridad que expuso datos financieros

La AEPD refuerza su enfoque estricto en materia de seguridad de datos financieros, subrayando que los responsables deben contar con medidas técnicas y organizativas efectivas, proporcionales al riesgo y verificables en la práctica.

Servicios Financieros Carrefour notificó a la AEPD la existencia de una brecha de seguridad, tras detectar accesos no autorizados a sus sistemas que habrían comprometido datos personales de clientes titulares de productos financieros. Según la comunicación oficial (realizada en cumplimiento del art. 33 RGPD) un tercero habría logrado acceder a información identificativa y contractual de usuarios, lo que incrementaba el riesgo de usos fraudulentos, suplantaciones y operaciones no consentidas. Posteriormente, varios afectados remitieron reclamaciones a la AEPD describiendo correos y actividades sospechosas coincidentes temporalmente con el incidente.

Ante estos indicios, la AEPD abrió actuaciones previas y requirió a la compañía información exhaustiva sobre el incidente, sus causas y las medidas técnicas y organizativas de seguridad vigentes, así como sobre las acciones adoptadas para contener el incidente y mitigar sus efectos.

El análisis de la documentación reveló deficiencias estructurales en el modelo de seguridad de Carrefour, entre ellas:

- controles insuficientes en accesos externos, que permitieron una intrusión explotable;
- falta de medidas de protección robustas en sistemas con datos financieros especialmente sensibles;
- ausencia de mecanismos preventivos eficaces para detectar la brecha en tiempo real;
- y reacción tardía y limitada en la contención del incidente, lo que extendió su impacto potencial.

A la luz de las comprobaciones realizadas en el expediente, la AEPD concluye que Servicios Financieros Carrefour vulneró las obligaciones del artículo 32 del RGPD, al no implementar medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad proporcional al riesgo asociado al tratamiento.

La AEPD observa que, pese a tratar datos especialmente sensibles por su vinculación con productos financieros y riesgo de suplantación de identidad, el responsable:

- no disponía de mecanismos de prevención suficientes para impedir accesos ilícitos previsibles;

- carecía de herramientas de monitorización capaces de detectar anomalías en tiempo real;
- y mantenía arquitecturas tecnológicas con niveles de protección inferiores a los exigibles en el sector financiero.

La AEPD recalca que la obligación del responsable no se satisface con medidas genéricas, sino con controles efectivos, documentados y verificables, adaptados al nivel de exposición y al impacto potencial sobre los titulares.

Sanciones aplicables

La AEPD califica los hechos como vulneración del artículo 32 del RGPD, integrándolos en el régimen sancionador del artículo 83.4 RGPD, al constatar la falta de medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos frente a accesos no autorizados.

Tras ponderar los factores de graduación previstos en el artículo 83.2 RGPD (naturaleza de los datos afectados, riesgo de perjuicio patrimonial, y deficiencias estructurales en el sistema de protección) la Agencia fija una multa inicial de 2.500.000 euros. No obstante, Servicios Financieros Carrefour se acogió a las opciones previstas en el artículo 85 de la Ley 39/2015, aplicables en el marco del procedimiento sancionador, obteniendo dos reducciones acumulables:

- un 20% por reconocimiento de responsabilidad,
- un 20% adicional por pago voluntario anticipado.

Puedes consultar la resolución a través del siguiente enlace.

La AEPD impone sanción millonaria a AENA por desplegar sistemas de reconocimiento facial sin una Evaluación de Impacto válida

La resolución constituye una de las decisiones más relevantes en España sobre el uso de biometría a gran escala, poniendo el acento en la necesidad de evaluaciones de impacto previas, completas y coherentes con la evolución real del tratamiento.

En 2019, AENA inició el desarrollo de un sistema de reconocimiento facial para agilizar los procesos aeroportuarios, que se implantó inicialmente en fase piloto entre 2019 y 2022 en los aeropuertos de Menorca, Madrid-Barajas y Barcelona-El Prat. El sistema permitía a los pasajeros acceder a controles y embarque mediante identificación facial, previa inscripción voluntaria y generación de una plantilla biométrica.

Durante esta fase, AENA remitió a la AEPD borradores de la Evaluación de Impacto en la Protección de Datos (EIPD), recibiendo reiterados informes desfavorables por no justificar la necesidad del uso de biometría, no acreditar su proporcionalidad frente a alternativas menos intrusivas ni analizar adecuadamente los riesgos asociados. Pese a ello, el sistema

se mantuvo operativo y, a partir de 2023, se extendió progresivamente a otros aeropuertos, superando el ámbito propio de un piloto.

La AEPD concluye que este paso a un tratamiento de alcance masivo se realizó sin una EIPD válida ni la corrección de los riesgos advertidos, infringiendo el artículo 35 del RGPD. La Agencia subraya que la evaluación era materialmente insuficiente y que AENA amplió el sistema con pleno conocimiento de sus déficits, vulnerando los principios de responsabilidad proactiva y privacidad desde el diseño. La gravedad del incumplimiento se ve reforzada por el contexto aeroportuario y por la naturaleza especialmente sensible e irreversible de los datos biométricos faciales.

Sanciones aplicables

La AEPD califica la infracción como incumplimiento del artículo 83.4 del RGPD, relativo a la obligación de realizar una EIPD, y activa el régimen sancionador económico aplicable a tratamientos de alto riesgo. En consecuencia, impone a AENA una multa de 10.043.002 euros, teniendo en cuenta, entre otros factores agravantes: (i) la especial sensibilidad de los datos tratados, consistentes en biometría facial para identificación inequívoca; (ii) el alcance territorial creciente del sistema, inicialmente limitado a tres aeropuertos y posteriormente en expansión; (iii) la continuidad del tratamiento durante varios años; (iv) la afectación real de miles de pasajeros nacionales e internacionales; y (v) la persistencia en el despliegue del sistema pese a advertencias desfavorables previas de la AEPD.

Además, la resolución ordena la suspensión inmediata del sistema de reconocimiento facial hasta que AENA elabore una EIPD completa y adecuada y acredite la supresión de los datos tratados, quedando prohibida su reactivación mientras no se demuestre el pleno cumplimiento del RGPD.

Finalmente, la AEPD descarta la aplicación del artículo 77 LOPDGDD y confirma que AENA, como sociedad mercantil estatal, está plenamente sujeta al régimen sancionador económico del RGPD, con independencia de la titularidad pública de su capital.

Puedes consultar la resolución a través del siguiente enlace.

La AEPD sanciona a un hotel por exponer datos identificativos de huéspedes en zonas comunes

La AEPD recuerda que las obligaciones de seguridad y confidencialidad también se aplican plenamente al tratamiento de datos en soporte papel, especialmente en entornos con tránsito elevado de personas.

La AEPD declara responsable a un establecimiento hotelero por permitir que listados físicos con datos personales de los huéspedes permanecieran visibles en zonas comunes accesibles a terceros, generando un riesgo real de acceso indebido y divulgación no autorizada de información identificativa y contractual.

Tras la reclamación de un huésped, la AEPD constató que la documentación se dejaba de forma transitoria en mostradores y dependencias internas sin supervisión ni custodia

efectiva, facilitando su visualización o captación por personas ajenas al tratamiento. El hotel reconoció esta práctica por motivos operativos, pero no acreditó la existencia de procedimientos adecuados de control documental.

La Agencia concluye que estas prácticas vulneran los artículos 5.1.f) y 32 del RGPD, al suponer una pérdida de confidencialidad y la ausencia de medidas técnicas y organizativas proporcionadas al riesgo. Asimismo, recuerda que el cumplimiento de la normativa exige una actuación preventiva y no meramente reactiva, en aplicación del principio de responsabilidad proactiva.

Sanciones aplicables

La AEPD califica la conducta como infracción del artículo 32 RGPD, incluida entre las infracciones sancionables del artículo 83.4 RGPD, al apreciarse insuficiencia de medidas de seguridad que comprometieron el principio de integridad y confidencialidad del artículo 5.1.f). Tras ponderar los criterios del artículo 83.2 RGPD (naturaleza del incidente, alcance, riesgo para los afectados y retraso en la adopción de medidas correctoras), la Agencia impone una multa de **50.000 euros**, sin reducciones ni sustitución por apercibimiento al tratarse de una entidad privada plenamente sujeta al régimen sancionador económico del RGPD.

Puedes consultar la resolución a través del siguiente enlace.

Sentencias de órganos judiciales españoles y europeos

El Juzgado de lo Social nº 3 de A Coruña avala el uso de sistemas biométricos para control laboral y se aparta del criterio de la AEPD

Esta sentencia introduce un criterio judicial relevante al avalar el uso de sistemas biométricos para el control horario, matizando la posición restrictiva mantenida tradicionalmente por la AEPD en el ámbito laboral.

El Juzgado de lo Social nº 3 de A Coruña ha declarado lícito el uso de sistemas biométricos (huella dactilar) para registrar la jornada laboral del personal sanitario de un centro hospitalario, aceptando su utilización como medida proporcionada y ajustada al RGPD.

Antecedentes de hecho

Un centro hospitalario implantó un sistema de control de acceso y registro horario basado en huella dactilar. Este sistema se configuró para no conservar imágenes completas de las huellas, sino plantillas matemáticas cifradas que impiden identificar o reconstruir la huella original.

El comité de empresa y los sindicatos formularon demanda al considerar que el centro debía emplear métodos menos invasivos y que el tratamiento infringía la normativa de protección de datos. Para sustentar su posición, se apoyaron en las guías de la AEPD, tradicionalmente muy restrictivas con el uso de biometría en el ámbito laboral. Alegaron también que la empresa no había recabado el consentimiento de los trabajadores y que, en ausencia de dicho consentimiento (considerado inválido en relaciones de dependencia), el fichaje no podía considerarse lícito.

El centro sostuvo que el sistema era necesario para la correcta organización del personal y la seguridad asistencial, especialmente en un entorno sanitario, defendiendo que la medida se ajustaba al RGPD porque trataba únicamente la información imprescindible para verificar la identidad del trabajador. Añadió que el consentimiento no es la base legal aplicable en estos casos, sino las obligaciones derivadas de la relación contractual y la necesidad de garantizar la continuidad y trazabilidad del servicio sanitario.

Fundamento Jurídico

El análisis del Juzgado se centró en determinar si el tratamiento biométrico podía considerarse lícito en el marco del RGPD y si la empresa contaba con una base legal suficiente para su implantación. En este sentido, aclaró que el consentimiento no resultaba exigible, ya que en el ámbito laboral no suele considerarse libre debido al desequilibrio entre empresa y trabajador. Por ello, concluyó que la base legal adecuada era la ejecución del contrato de trabajo y la necesidad organizativa inherente a la prestación de servicios.

El tribunal reconoció la posición cautelosa de la AEPD respecto a la biometría e incluso su recomendación de utilizar mecanismos alternativos cuando existan opciones menos intrusivas. No obstante, subrayó que estas guías interpretativas carecen de carácter normativo y no pueden prevalecer sobre el RGPD ni vaciar de contenido sus habilitaciones legales. En palabras del juzgado, la autoridad administrativa puede orientar, pero no restringir por sí solas tecnologías admitidas expresamente por el derecho europeo.

El examen de proporcionalidad fue determinante para el fallo. La sentencia destacó que el sistema implantado:

- no almacenaba imágenes completas de la huella dactilar,
- generaba plantillas biométricas cifradas e irreversibles,
- limitaba el tratamiento a control horario y acceso, sin usos adicionales,
- y resultaba eficaz para asegurar organización, trazabilidad y cobertura de turnos en el hospital.

El Juzgado añadió que la existencia de alternativas hipotéticas (tarjetas, firmas o aplicaciones móviles) no obliga a adoptar necesariamente dichas vías si la opción elegida cumple con garantías técnicas, responde a una finalidad legítima y no genera un perjuicio desproporcionado para los derechos de los trabajadores.

Además, el Tribunal valoró positivamente que la empresa hubiera realizado la EIPD antes y después de la implantación del sistema, analizando riesgos, medidas de mitigación y alternativas disponibles, lo que evidencia el cumplimiento del deber de responsabilidad proactiva. También destacó la existencia de información clara y accesible dirigida a la plantilla.

Otro elemento relevante para la decisión fue el contexto en el que opera el centro: el juzgado subrayó que un hospital constituye un entorno especialmente sensible, donde resulta legítimo exigir un control fiable sobre acceso y presencia del personal para garantizar la seguridad asistencial, prevenir accesos indebidos y asegurar la continuidad operativa. Señaló que este razonamiento no sería necesariamente extrapolable a otros sectores con menor exigencia en materia de presencia física y seguridad.

La sentencia también aludió al reciente Reglamento Europeo de Inteligencia Artificial para ilustrar que la verificación biométrica presencial, utilizada en entornos controlados y bajo garantías adecuadas, puede considerarse de riesgo relativamente bajo. Aunque esta referencia no condiciona directamente el fallo, revela la apertura del tribunal a integrar en su análisis el marco regulatorio tecnológico emergente.
Situación y alcance

La sentencia no es firme y puede ser recurrida ante el Tribunal Superior de Justicia de Galicia. Su impacto real dependerá de si es confirmada o si se revierte, pero por ahora introduce un precedente destacable que podría influir en futuros litigios y en la interpretación judicial del uso de biometría en el ámbito laboral, especialmente en sectores críticos como el sanitario.

Puedes consultar la resolución en el siguiente enlace.

Juzgado de lo Mercantil nº 15 de Madrid declara desleal la conducta de Meta en el mercado publicitario *online* en INSTAGRAM y FACEBOOK

La resolución sienta un precedente significativo al vincular la infracción de la normativa de protección de datos con una conducta de competencia desleal, proyectando el RGPD más allá del ámbito estrictamente sancionador.

La sentencia dictada por el Juzgado de lo Mercantil nº 15 de Madrid declara desleal la conducta de Meta Platforms Ireland Ltd. ("**Meta**") en el mercado publicitario *online* en *display* debido al tratamiento de datos de los usuarios de INSTAGRAM y FACEBOOK para la realización de publicidad personalizada sin base legal infracción del artículo 6.1.b) del RGPD. Por estos hechos se le condenó a abonar 479.120.000 euros a 87 editoras de prensa digital y agencias de noticias integradas en la Asociación de Medios de Información (AMI).

Antecedentes de hecho

La demanda se centra en señalar que la conducta de Meta ha incurrido en dos conductas tipificadas como desleales, por una parte, prevalerse en el mercado de una ventaja competitiva adquirida mediante la infracción de leyes y, la infracción de normas jurídicas que tengan por objeto la regulación de la actividad concurrencial.

Los demandantes alegan que la infracción de las obligaciones derivadas del RGPD a efectos de las acciones de publicidad comportamental llevadas a cabo por FACEBOOK e INSTAGRAM dieron lugar a las conductas sancionadas por la autoridad de protección de datos de Irlanda pusieron a Meta en una posición de clara desventaja competitiva, ya que los editores no podían competir en igualdad de condiciones en el mercado de la publicidad online sin incurrir en infracciones del RGPD.

Fundamentos jurídicos

El Juzgado analiza si Meta infringió la normativa aplicable y si dicha infracción le otorgó una ventaja competitiva relevante. Aunque no es imprescindible una declaración previa de infracción, en este caso existen resoluciones firmes de la autoridad de protección de datos irlandesa que constatan infracciones del RGPD por parte de Meta en relación con Facebook e Instagram, vinculadas a la realización de publicidad comportamental sin base legal válida.

A partir de estas resoluciones, la sentencia estima parcialmente la demanda y declara desleal la conducta de Meta por obtener una ventaja competitiva mediante la infracción del RGPD, condenándola a indemnizar a la Asociación de Medios de Información (AMI) con 479.120.000 euros, conforme al artículo 15.1 de la Ley de Competencia Desleal.

Un elemento determinante del fallo es la negativa de Meta a aportar las cuentas de su negocio publicitario en España, lo que lleva al tribunal a presumir ciertos los datos

aportados por los demandantes y a considerar acreditados ingresos publicitarios superiores a 5.281 millones de euros durante el periodo infractor.

Para cuantificar la indemnización, el Juzgado toma como referencia la cuota de mercado de la prensa digital española, apoyándose en datos de la CNMC, y concluye que el daño puede acreditarse con una razonable verosimilitud, aun sin una cuantificación exacta.
La sentencia no es firme y puede ser recurrida ante el Tribunal Superior de Justicia de Madrid, si bien constituye un precedente relevante al vincular la infracción del RGPD con una conducta de competencia desleal en el ámbito de la publicidad digital.

Se puede consultar la sentencia en este enlace.

Sentencia del Tribunal de Justicia de la Unión Europea analiza el criterio de originalidad en las obras de arte aplicadas

El TJUE aporta claridad sobre los criterios de originalidad aplicables a las obras de arte aplicadas, reforzando la seguridad jurídica en la protección por derechos de autor de objetos con función utilitaria.

El Tribunal de Justicia de la Unión Europea (“**TJUE**”), en los asuntos acumulados C-580/23 y C-795/23, analiza el concepto de obra con arreglo a la normativa de derechos de autor relativo a las obras de arte aplicadas. Para ello, realiza un examen de la originalidad de un objeto de artes aplicadas.

Antecedentes

En los asuntos acumulados C-580/23 y C-795/23, el TJUE analiza dos litigios relativos a la protección por derechos de autor de obras de arte aplicadas en el sector del mobiliario. En el primero, Asplund demanda a Mio por la comercialización de mesas presuntamente similares a su serie “Palais Royal”. En el segundo, USM acciona contra Konektra por la venta, promoción y montaje de componentes compatibles con su sistema modular “USM Haller”.

Ante estos conflictos, los tribunales nacionales plantean cuestiones prejudiciales al TJUE para determinar qué criterios deben aplicarse para apreciar la originalidad de un objeto de artes aplicadas y establecer si puede calificarse como obra protegida por derechos de autor.

Decisión del TJUE

Para el TJUE la norma es clara en admitir la acumulación de protecciones: la protección por dibujos y modelos y la protección por derecho de autor las cuales pueden coexistir, sin existir una relación de regla-excepción ni jerarquía entre ambas.

Respecto de la apreciación de la originalidad en este tipo de obras, el TJUE señala que no pueden exigirse requisitos de originalidad más elevados a las obras de arte aplicada que a

cualquier otra obra protegida por la Directiva 2001/29/CE. En este sentido, merecerá la categoría de obra la creación intelectual propia que refleje decisiones libres y creativas del autor, quedando excluidos los elementos impuestos exclusivamente por exigencias técnicas o funcionales. La apreciación de la originalidad deberá basarse en los elementos perceptibles del objeto que expresan la aportación creativa, sin que factores como la intención del autor o el reconocimiento experto sean determinantes.

De igual manera, la protección solo recae sobre los elementos originales aportados por el autor, y la posible existencia de obras similares independientes no excluye la protección.

El TJUE refuerza con esta interpretación la seguridad jurídica en el ámbito de las obras de arte aplicadas, además de armonizar el estándar del concepto de originalidad en la Unión Europea.

Se puede consultar la sentencia en este enlace.

Novedades legislativas

Propuesta de Reglamento Ómnibus Digital

La Comisión Europea avanza hacia una simplificación del marco regulatorio digital mediante una propuesta transversal que busca reducir solapamientos normativos sin rebajar los estándares de protección de derechos fundamentales.

El pasado mes de noviembre de 2025 la Comisión Europea presentó su Propuesta de Reglamento Ómnibus Digital que tiene como propósito simplificar, armonizar y hacer más eficiente la regulación digital vigente en la Unión Europea en materias clave como protección de datos, inteligencia artificial, privacidad electrónica, ciberseguridad y gobernanza de datos.

La Propuesta de Reglamento Ómnibus Digital no crea un nuevo cuerpo normativo autónomo, sino que actúa como un instrumento modificador y transversal de múltiples Reglamentos y Directivas ya en vigor. Con esto se busca reducir la fragmentación, aclarar solapamientos y disminuir carga administrativa, sin que ello afecte el cumplimiento de los objetivos fundamentales de las mencionadas normativas. Entre los cambios se plantea la Propuesta de Reglamento Ómnibus Digital podemos reseñar:

- **En materia de protección de datos**: En lo que se refiere a los datos personales regulados en el RGPD, la Propuesta de Reglamento Ómnibus busca aclarar **(i)** definiciones clave, por ejemplo, el concepto de datos personales, por ejemplo, respecto de los criterios y medios para determinar si los datos resultantes de la seudonimización constituyen o no datos personales; y, **(ii)** aspectos del tratamiento de datos para el entrenamiento y desarrollo de la inteligencia artificial. También se propone ampliar las excepciones a la obligación de información para el tratamiento.

- **Normativa de cookies:** Se propone simplificar la interacción de las normas aplicables. Se prevén determinados fines para los que no debe ser necesario obtener el consentimiento y para los que el tratamiento posterior debe considerarse lícito. También se allana el camino para las indicaciones automatizadas y legibles por máquina de las preferencias individuales y el respeto de dichas indicaciones por parte de los proveedores del sitio web y Apps.

- **En materia de inteligencia artificial**: La Propuesta de Reglamento Ómnibus Digital propone ajustes al Reglamento de IA, entre ellos la flexibilización de plazos de aplicación para sistemas de alto riesgo, la ampliación de alivios regulatorios para pymes y empresas medianas, y la introducción de una base jurídica específica para el tratamiento de datos sensibles, por ejemplo, a efectos de detección y corrección de sesgos, siempre con las debidas garantías de derechos fundamentales.

- **Creación de un mecanismo único y simplificado de notificación de incidentes** de ciberseguridad, violación de datos personales, y/o obligaciones sectoriales a nivel de la UE. El objetivo es reducir duplicidad en normas manteniendo las salvaguardas específicas de cada sector. También se propone ampliar el plazo para notificar una violación de seguridad de los datos personales en virtud del RGPD de 72 a 96 horas.

Publicada la Propuesta de Reglamento Ómnibus Digital se presentó al Parlamento Europeo y al Consejo para su adopción. Daremos seguimiento al trámite hasta tener el texto definitivo.

Se puede consultar el anteproyecto en este enlace.

Síguenos en