REVISTA DE
PRIVACIDAD Y DERECHO DIGITAL

DIRECTOR • D. PABLO GARCÍA MEXÍA

AÑO XI • ENERO-ABRIL 2026 • NÚMERO 39

ISSN: 2444-5762

EN RED Nº 39

REVISTA DE

PRIVACIDAD Y DERECHO DIGITAL

I.- NORMATIVA Y DOCUMENTOS DE LA UNIÓN EUROPEA

I.1.- LEY 10/2025, DE 26 DE DICIEMBRE, REGULADORA DE LOS SERVICIOS DE ATENCIÓN A LA CLIENTELA

La Ley 10/2025, de 26 de diciembre, reguladora de los servicios de atención a la clientela, introduce modificaciones relevantes en materia de obligaciones de información, contratación y atención al cliente, con un impacto directo en el comercio electrónico. En particular, se refuerza la transparencia precontractual al exigir que el usuario conozca desde el inicio el precio final completo del producto o servicio, incluyendo impuestos y cualesquiera gastos adicionales; cuando dicho precio no pueda determinarse ex ante, deberá indicarse la base de cálculo y los posibles costes asociados.

Asimismo, en los supuestos de precios personalizados, se impone la obligación de informar al usuario cuando el importe se determine mediante decisiones automatizadas, al tiempo que se limitan las prácticas de fijación dinámica de precios en contextos de urgencia o riesgo. En el ámbito de las suscripciones, se establece la obligación de notificar con una antelación mínima de quince días la renovación automática, así como de garantizar un procedimiento de baja sencillo, accesible y exento de obstáculos.

Por lo que respecta a las reseñas en línea, la norma exige transparencia acerca de su origen - en particular, si proceden de usuarios reales - y sobre los mecanismos de verificación empleados, acotando además su validez a experiencias de compra o uso recientes. Igualmente, se reconoce al afectado el derecho de respuesta y la posibilidad de solicitar su retirada cuando se acredite su falsedad.

En materia de atención al cliente, se imponen plazos máximos de respuesta y la obligación de ofrecer atención humana, excluyendo la prestación exclusiva mediante sistemas automatizados como chatbots. Adicionalmente, se introducen restricciones al marketing telefónico, que deberá identificarse mediante prefijos o códigos específicos; se impone a los operadores el deber de bloquear las comunicaciones que incumplan estas exigencias y se establece la nulidad de los contratos celebrados por esta vía en ausencia de consentimiento debidamente acreditado.

Finalmente, la Ley modifica el régimen de tratamiento de datos personales con fines de exclusión publicitaria, restringiendo la creación de sistemas destinados a tal fin a asociaciones y organismos con alta representatividad conforme al artículo 40.2 del Reglamento (UE) 2016/679 (RGPD). La norma resulta aplicable a grandes empresas —esto es, aquellas con más de 250 empleados o un volumen de negocio superior a 50 millones de euros—, así como a las que prestan servicios básicos de interés general, como los suministros de energía, agua o telecomunicaciones. De acuerdo con la propia definición legal, el concepto de "clientela" se identifica esencialmente con las personas consumidoras o usuarias, cuya posición en el comercio en línea se ve claramente reforzada tras la entrada en vigor de la norma el 28 de diciembre de 2025.

II.- INFORMES, DOCUMENTOS Y RESOLUCIONES DE AUTORIDAD DE CONTROL

II.1.- AESIA PUBLICA GUÍAS PRÁCTICAS PARA FACILITAR EL CUMPLIMIENTO DEL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL (RIA)

La Secretaría de Estado de Digitalización e Inteligencia Artificial, a través de su Dirección General de Inteligencia Artificial y con la colaboración de la Agencia Española de Supervisión de Inteligencia Artificial (AESIA), junto con otras autoridades nacionales de vigilancia del mercado, ha publicado un conjunto de 16 guías prácticas destinadas a facilitar la implementación y el cumplimiento del Reglamento (UE) de Inteligencia Artificial (RIA).

Estas guías, elaboradas en el marco del denominado Sandbox de IA, tienen por finalidad apoyar al tejido productivo español -en particular, a aquellas entidades que desarrollan o implementan sistemas de inteligencia artificial de alto riesgo- en la adaptación a las exigencias normativas. A tal efecto, proporcionan orientaciones alineadas con los requisitos regulatorios vigentes, en tanto se aprueban las

correspondientes normas armonizadas a escala europea. Asimismo, pretenden contribuir al desarrollo de sistemas de IA innovadores, fiables y respetuosos con los derechos fundamentales, resultando de especial utilidad para pymes, start-ups y grandes empresas.

Conviene subrayar que estas guías carecen de carácter vinculante y no sustituyen ni desarrollan la normativa aplicable, sino que constituyen instrumentos de apoyo interpretativo y técnico. Su contenido se estructura en tres grandes bloques:

1. Guías introductorias

En primer lugar, se incluyen dos documentos de carácter general. Por un lado, la Introducción al Reglamento de IA, que ofrece una visión de conjunto sobre su alcance, ámbito de aplicación y principales obligaciones. Por otro, la Guía práctica y ejemplos para entender el Reglamento de Inteligencia Artificial, que adopta un enfoque más aplicado, incorporando ejemplos hipotéticos de sistemas de IA de alto riesgo y facilitando la comprensión operativa del marco regulador.

2. Guías técnicas

El segundo bloque agrupa trece guías de naturaleza técnica, orientadas a la implementación de los requisitos del RIA. Entre ellas destacan: la evaluación de conformidad (incluido el marcado CE), los sistemas de gestión de la calidad (art. 17) y de gestión de riesgos (art. 9), la supervisión humana (art. 14), así como la gobernanza de datos (art. 10). Igualmente, se abordan aspectos clave como la transparencia y la información al usuario (art. 13), y los requisitos de precisión, solidez y ciberseguridad (art. 15), desglosados en guías específicas.

Asimismo, se incluyen orientaciones sobre registros y trazabilidad, documentación técnica, planes de vigilancia poscomercialización y notificación de incidentes graves (art. 73), configurando un conjunto integral de herramientas destinadas a garantizar el cumplimiento normativo a lo largo de todo el ciclo de vida del sistema de IA.

3. Checklist de requisitos

Finalmente, el tercer bloque incorpora un manual de checklist que permite realizar un diagnóstico sistemático del grado de cumplimiento de los principales requisitos del RIA. Este instrumento, acompañado de ejemplos y plantillas (incluidos archivos Excel), cubre ámbitos como la gestión de calidad y riesgos, la supervisión humana, la gobernanza de datos, la transparencia, la precisión, la solidez, la ciberseguridad, los registros, la documentación técnica, la vigilancia poscomercialización y la gestión de incidentes graves.

En último término, estas guías se conciben como documentos dinámicos, sujetos a un proceso continuo de evaluación y actualización, en función de la evolución de los estándares técnicos y de las directrices que emanen de la Comisión Europea. En este sentido, se prevé su revisión una vez se aprueben las iniciativas normativas en curso, incluido el denominado paquete "Ómnibus digital", que introducirá modificaciones en el Reglamento de Inteligencia Artificial.

II.2.- EL COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (CEPD) Y LA COMISIÓN EUROPEA AVALAN DE FORMA CONJUNTA UNAS DIRECTRICES SOBRE LA INTERACCIÓN ENTRE LA LEY DE MERCADOS DIGITALES (DMA) Y EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD).

El 9 de octubre de 2025 se publicaron unas primeras directrices elaboradas conjuntamente por el Comité Europeo de Protección de Datos (CEPD) y la Comisión Europea, con el objetivo de facilitar una aplicación coherente del Digital Markets Act (DMA) y del Reglamento General de Protección de Datos (RGPD), reforzar la seguridad jurídica y simplificar el cumplimiento normativo para usuarios, beneficiarios y personas interesadas en general.

Estas primeras orientaciones persiguen armonizar criterios interpretativos y reducir fricciones en la aplicación conjunta de ambos marcos regulatorios. En particular, las directrices clarifican los elementos que deben tenerse en cuenta para cumplir los requisitos de "elección específica" y "consentimiento válido", previstos en el artículo 5.2 de la DMA y en el RGPD, especialmente en relación con la

combinación o el uso cruzado de datos personales en los servicios de plataforma esenciales.

Asimismo, el documento aborda otras cuestiones relevantes, como la distribución de aplicaciones a través de tiendas de terceros, la portabilidad de datos, las solicitudes de acceso a la información y la interoperabilidad de los servicios de mensajería, configurando un marco interpretativo que facilita la aplicación coordinada de ambas normativas.

El texto definitivo, que incorporará las observaciones recabadas durante el proceso de consulta pública promovido por el CEPD y la Comisión Europea, será elaborado de forma conjunta por ambas instituciones.

II.3.- GUÍA DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) SOBRE AUTÓNOMOS Y PYMES.

El uso de herramientas digitales como aplicaciones de asignación de tareas, sistemas de control horario, dispositivos de geolocalización o sistemas de videovigilancia se ha generalizado en la gestión cotidiana de muchos autónomos con empleados y pequeñas empresas. Si bien estas soluciones contribuyen a mejorar la organización y la eficiencia, también plantean relevantes implicaciones en materia de protección de datos personales.

En este contexto, de cara a 2026, la AEPD ha actualizado su guía sobre protección de datos en las relaciones laborales, con el objetivo de delimitar el alcance del control empresarial y clarificar los límites dentro de los cuales puede ejercerse sin vulnerar los derechos de las personas trabajadoras. Aunque el documento se dirige a organizaciones de cualquier tamaño, reviste especial importancia para autónomos y pymes, donde la implantación de estas tecnologías suele realizarse sin un análisis jurídico previo. La idea central es clara: el control laboral es legítimo, pero no ilimitado.

Revista de Privacidad y Derecho Digital
ISSN digital 2444-5762, NÚM. 39, Madrid, Enero-Abril (2026), págs. 215-230

1. Software, algoritmos y decisiones automatizadas

Uno de los ámbitos de mayor expansión es el uso de aplicaciones destinadas a medir la productividad, asignar tareas o evaluar el rendimiento. La AEPD advierte de que estas herramientas pueden generar riesgos cuando decisiones con efectos relevantes sobre el empleo se basan exclusivamente en procesos automatizados o algoritmos.

En este sentido, se exige que las personas trabajadoras sean informadas de la existencia de tales sistemas y comprendan, al menos de forma general, su funcionamiento. Asimismo, las decisiones no pueden adoptarse sin intervención humana, en línea con el derecho a no quedar sometido a decisiones exclusivamente automatizadas sin una explicación adecuada ni posibilidad de revisión.

2. Uso de dispositivos digitales y comunicaciones corporativas

La provisión de medios digitales por parte de la empresa —como correo electrónico, teléfonos móviles u ordenadores— no legitima un acceso indiscriminado a su contenido. La AEPD recuerda que cualquier control debe responder a una finalidad legítima vinculada a la actividad laboral y respetar, en todo caso, la privacidad del trabajador.

Entre las prácticas más problemáticas se encuentran la ausencia de información previa sobre posibles controles, el uso de los datos obtenidos para finalidades distintas de las inicialmente previstas o el acceso injustificado a contenidos personales, especialmente en aplicaciones de mensajería o navegación por internet. La definición de políticas internas claras y la limitación del control a lo estrictamente necesario resultan esenciales para minimizar riesgos.

3. Videovigilancia: límites al control continuo

La videovigilancia constituye una de las herramientas más extendidas, pero también una de las que mayor conflictividad genera. La AEPD subraya que su utilización debe responder a finalidades específicas,

como la seguridad de personas, bienes o instalaciones, y no puede convertirse en un mecanismo de supervisión permanente del desempeño laboral.

Se consideran contrarias a la normativa prácticas como la instalación de cámaras en zonas especialmente protegidas (vestuarios o áreas de descanso), la falta de información adecuada a los trabajadores o el uso de las grabaciones para fines distintos de los comunicados. Asimismo, la captación excesiva de imágenes o su conservación durante plazos desproporcionados vulnera el principio de proporcionalidad.

4. Geolocalización y control horario digital

Los sistemas de geolocalización y registro horario digital se han consolidado en sectores como el reparto o la actividad comercial. No obstante, la AEPD insiste en que su uso debe limitarse a supuestos en los que resulte necesario para la organización del trabajo o el cumplimiento de obligaciones legales, y no como instrumento de vigilancia constante.

En particular, se consideran prácticas indebidas la activación de la geolocalización fuera del horario laboral, la recopilación de datos excesivos o la falta de transparencia respecto a la finalidad del tratamiento, su alcance y el periodo de conservación. El control debe circunscribirse estrictamente al ámbito y tiempo de la relación laboral.

5. Principios rectores del control empresarial

Más allá de las tecnologías concretas, la guía refuerza tres principios esenciales que deben regir cualquier medida de control laboral: necesidad, proporcionalidad y transparencia. La existencia de una relación laboral no habilita para tratar cualquier dato personal ni para implantar mecanismos intrusivos si existen alternativas menos invasivas.

En este sentido, el endurecimiento de los estándares en materia de privacidad laboral convierte el cumplimiento de estos principios en un elemento clave para la gestión empresarial, especialmente

Revista de Privacidad y Derecho Digital
ISSN digital 2444-5762, NÚM. 39, Madrid, Enero-Abril (2026), págs. 215-230

en el caso de autónomos y micropymes. La evaluación previa de la necesidad de las medidas, así como su adecuada implementación, resulta imprescindible para evitar riesgos sancionadores y garantizar un funcionamiento conforme a Derecho en el nuevo escenario regulatorio de 2026.

II.4.- SANCIONES DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS POR EL USO DE RECONOCIMIENTO BIOMÉTRICO.

a) Sanción de la Agencia Española de Protección de Datos a AENA por el uso de reconocimiento biométrico.

El 25 de noviembre de 2025, la Agencia Española de Protección de Datos (AEPD) resolvió imponer una multa de 10 millones de euros a AENA por incumplir el artículo 35 del Reglamento General de Protección de Datos (RGPD), al considerar que las Evaluaciones de Impacto en Protección de Datos (EIPD) realizadas para sus proyectos de embarque biométrico no cumplían con los requisitos legales. La sanción se basa en la falta de una descripción detallada de las operaciones de tratamiento y finalidades específicas, además de la ausencia de evidencia formal de su realización previa al inicio del tratamiento. AENA ha anunciado que recurrirá la sanción ante los tribunales por discrepar tanto en el fondo como en la forma, y sostiene que no se han producido brechas de seguridad ni filtraciones, que el consentimiento fue informado y que los datos se han tratado conforme al RGPD y la LOPDGDD (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales). El programa, desarrollado con aerolíneas, busca mejorar la experiencia del pasajero mediante el uso voluntario de tecnologías de reconocimiento facial. Una vez más, el uso de la biometría, en particular el relativo al control de accesos a espacios públicos, se sitúa en el centro de una actuación sancionatoria (tras el conocido asunto Club Atlético Osasuna de la propia Agencia). Es de esperar que la previsible sentencia arroje definitivamente luz sobre la legitimidad de uso de una tecnología que presenta obvios riesgos, pero a la vez presenta indudables ventajas en forma de autenticidad y de comodidad para los interesados.

b) Sanción a una universidad por el uso de biometría en sistemas de "proctoring".

La Agencia Española de Protección de Datos (AEPD) ha sancionado a una universidad por el tratamiento de datos biométricos mediante un sistema de *proctoring* basado en reconocimiento facial, impuesto al alumnado sin ofrecer alternativas equivalentes.

La resolución declara la infracción del artículo 9 del Reglamento General de Protección de Datos (RGPD), al haberse tratado categorías especiales de datos personales sin concurrir una base de legitimación válida ni una excepción habilitante. En particular, la AEPD considera que la autenticación 1:1 mediante patrones de geometría facial constituye un tratamiento de datos biométricos a los efectos del RGPD.

La universidad alegó que el uso del reconocimiento facial respondía a exigencias de la Agencia Nacional de Evaluación de la Calidad y Acreditación (ANECA) para prevenir el fraude académico. No obstante, la AEPD rechaza esta justificación al constatar que no existe norma con rango suficiente que imponga dicho tratamiento y que, en todo caso, las directrices de la ANECA carecen de fuerza jurídica para habilitarlo.

En relación con el consentimiento de los estudiantes, la Agencia concluye que no puede considerarse libre, al no existir alternativas reales y concurrir un evidente desequilibrio de poder entre la institución y el alumnado, equiparable al que se produce en el ámbito laboral. Asimismo, se destaca que la universidad descartó soluciones tecnológicas menos intrusivas que no requerían el uso de datos biométricos.

No obstante, la AEPD reconoce que, con anterioridad a la publicación de su Guía sobre tratamientos de datos biométricos en noviembre de 2023, existían incertidumbres interpretativas razonables en torno a este tipo de sistemas. En consecuencia, limita el período sancionable a partir de dicha fecha, imponiendo por esta infracción una multa de 300.000 euros.

Adicionalmente, la Agencia aprecia la vulneración del artículo 5.1.c) del RGPD, relativo al principio de minimización de datos, al considerar

que el sistema empleado resultaba innecesariamente intrusivo, existiendo alternativas eficaces que no implicaban el tratamiento de datos biométricos. En este sentido, la AEPD subraya la desproporción de la medida, al no quedar justificado que el fin perseguido legitime el medio utilizado, y concluye que la elección del sistema respondió fundamentalmente a criterios de conveniencia organizativa.

III.- JURISPRUDENCIA

III.1.- EL TJUE AVALA RECHAZAR SOLICITUDES ABUSIVAS DE ACCESO A DATOS Y EXIGE DAÑO REAL PARA INDEMNIZAR.

La Sentencia del Tribunal de Justicia de la Unión Europea de 19 de marzo de 2026 (asunto C-526/24) delimita el alcance del derecho de acceso a los datos personales reconocido en el Reglamento General de Protección de Datos (RGPD), introduciendo criterios relevantes tanto para la apreciación de solicitudes abusivas como para el reconocimiento del derecho a indemnización.

La Sala Cuarta resuelve un litigio entre una empresa alemana y un particular que, tras facilitar sus datos con ocasión de la suscripción a un boletín informativo, ejercitó su derecho de acceso con una finalidad primordialmente orientada a fundamentar una reclamación indemnizatoria.

1. El carácter abusivo del derecho de acceso

El Tribunal examina si una solicitud inicial de acceso puede calificarse como excesiva o abusiva y concluye que, en determinadas circunstancias, incluso una única petición puede revestir tal carácter. Para ello, exige una valoración estricta y casuística, en la que corresponde al responsable del tratamiento acreditar, mediante elementos objetivos y subjetivos, que la solicitud no persigue el conocimiento del tratamiento de los datos, sino la generación artificiosa de una reclamación.

Asimismo, admite que pueden tenerse en cuenta indicios adicionales, como un comportamiento reiterado del interesado frente a distintos responsables, siempre que tales elementos queden debidamente corroborados por las circunstancias del caso concreto.

2. Alcance del derecho a indemnización

La sentencia precisa igualmente el alcance del derecho a indemnización previsto en el artículo 82 del RGPD. En este sentido, el Tribunal afirma que dicho derecho no se limita a los supuestos de tratamiento ilícito, sino que también puede derivarse de la vulneración de derechos reconocidos en el Reglamento, como el derecho de acceso. Así, una negativa injustificada a facilitar la información solicitada puede generar responsabilidad.

3. Exigencia de daño real y relación de causalidad

No obstante, el Tribunal subraya que la mera infracción del RGPD no basta, por sí sola, para fundamentar una indemnización. El interesado debe acreditar la existencia de un perjuicio real, así como la correspondiente relación de causalidad entre la infracción y el daño sufrido. Quedan, por tanto, excluidos los supuestos en los que la situación haya sido provocada artificialmente por el propio solicitante.

En cuanto al daño inmaterial, el Tribunal reconoce que puede consistir, entre otros supuestos, en la pérdida de control sobre los datos personales o en la incertidumbre acerca de su tratamiento, siempre que dicho perjuicio sea efectivo y no meramente hipotético.

En definitiva, la resolución introduce un equilibrio entre la tutela efectiva de los derechos de las personas interesadas y la necesidad de prevenir prácticas abusivas. De este modo, refuerza el derecho de acceso, pero, al mismo tiempo, legitima a los responsables del tratamiento para rechazar solicitudes cuando acrediten un uso instrumental o fraudulento del RGPD con fines exclusivamente lucrativos.

Revista de Privacidad y Derecho Digital
ISSN digital 2444-5762, NÚM. 39, Madrid, Enero-Abril (2026), págs. 215-230

III.2.- SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA SOBRE PROTECCIÓN DE DATOS EN ANUNCIOS DE MERCADOS EN LÍNEA

La Sentencia del Tribunal de Justicia de la Unión Europea, de 2 de diciembre de 2025, As. C-492/23, aborda la responsabilidad de los operadores de mercados en línea en relación con la publicación de anuncios que incorporan datos personales, en particular cuando se trata de categorías especialmente protegidas conforme al Reglamento General de Protección de Datos (RGPD).

El litigio tiene su origen en la publicación de un anuncio de contenido sexual que incluía fotografías y el número de teléfono de una mujer sin su consentimiento. Aunque el operador de la plataforma procedió a retirar el anuncio tras la solicitud de la afectada, este ya había sido replicado en otros sitios web, permaneciendo accesible fuera del entorno original.

En este contexto, el Tribunal establece que el operador de un mercado en línea está obligado a adoptar medidas técnicas y organizativas adecuadas para prevenir y detectar la publicación de anuncios que contengan datos personales sensibles. En particular, debe verificar que los datos publicados pertenecen al anunciante o que su difusión se encuentra amparada por alguna de las excepciones previstas en el artículo 9 del RGPD.

Asimismo, el TJUE impone a los operadores el deber de actuar para evitar la reproducción y difusión ilícita de tales contenidos en otros sitios web, extendiendo así su responsabilidad más allá de la mera retirada del anuncio en la propia plataforma.

La sentencia aclara, además, que estas obligaciones no pueden eludirse mediante la invocación de las exenciones de responsabilidad previstas en la Directiva sobre el comercio electrónico, en particular las relativas a la mera transmisión de contenidos o a la ausencia de una obligación general de supervisión.

Desde una perspectiva material, resulta especialmente relevante la primacía que el Tribunal reconoce a la protección de los datos personales frente a dichas exenciones. En particular, considera que la ausencia de obligación general de supervisión deviene inaplicable

una vez que el operador tiene conocimiento efectivo de la ilicitud -como ocurre tras la notificación de la persona afectada-. La principal novedad de la resolución radica, no obstante, en la extensión de esta lógica más allá del propio entorno de la plataforma, proyectando deberes de actuación sobre la difusión ulterior de los contenidos en terceros sitios web.

En definitiva, la sentencia refuerza de manera significativa las obligaciones de diligencia de los intermediarios digitales, consolidando un estándar elevado de protección de los datos personales en el ecosistema de los mercados en línea.

III.3.- SENTENCIA CONDENATORIA A META PLATFORMS IRELAND LIMITED POR COMPETENCIA DESLEAL DERIVADA DE INFRACCIONES DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

La sentencia del Juzgado de lo Mercantil nº 15 de Madrid, de 19 de noviembre de 2025, resuelve la demanda interpuesta por 87 empresas editoras de prensa, agencias de noticias y cadenas de radio españolas frente a Meta Platforms Ireland Limited, en la que se alegaba la existencia de actos de competencia desleal derivados de infracciones en materia de protección de datos. El período objeto de análisis se extiende desde el 25 de mayo de 2018 -fecha de plena aplicabilidad del RGPD- hasta el 31 de julio de 2023.

El órgano judicial concluye que Meta vulneró el RGPD en el marco de sus servicios Facebook e Instagram mediante la implementación de prácticas de publicidad comportamental, entendida como aquella basada en la observación sistemática del comportamiento de los usuarios con el fin de elaborar perfiles y ofrecer publicidad personalizada.

En particular, la sentencia identifica las siguientes infracciones:

a. Vulneración del artículo 6.1.b) del RGPD (ejecución de un contrato): Meta invocó indebidamente la base jurídica de la necesidad contractual para legitimar el tratamiento de datos con fines publicitarios, pese a que dicha finalidad no resulta necesaria ni esencial para la prestación del servicio de red social. En esta lí-

Revista de Privacidad y Derecho Digital
ISSN digital 2444-5762, NÚM. 39, Madrid, Enero-Abril (2026), págs. 215-230

nea, el Comité Europeo de Protección de Datos (CEPD) ya había descartado la validez de esta base jurídica para la publicidad comportamental.

b. Vulneración del artículo 6.1.f) del RGPD (interés legítimo): entre abril y julio de 2023, Meta modificó su fundamento jurídico hacia el interés legítimo, sin que el tratamiento superase el preceptivo juicio de ponderación entre los intereses de la empresa y los derechos de los usuarios.

c. Infracción del principio de transparencia (arts. 5.1.a), 12.1 y 13.1.c) del RGPD): la compañía no informó de forma clara y accesible sobre las finalidades del tratamiento ni sobre la base jurídica empleada.

d. Infracción del principio de lealtad (art. 5.1.a) del RGPD): se generó una asimetría informativa estructural que situaba a los usuarios en una posición de desventaja, limitando su capacidad de control mediante un modelo de aceptación forzada ("tómalo o déjalo").

e. Infracción del principio de minimización (art. 5.1.c) del RGPD): se llevó a cabo una recogida masiva e indiscriminada de datos, incluyendo potencialmente categorías especiales de datos personales (art. 9.1 RGPD) sin el consentimiento explícito exigido.

A la vista de lo anterior, el juzgado considera acreditado que Meta obtuvo una ventaja competitiva significativa en el mercado de la publicidad digital mediante el tratamiento ilícito de los datos de usuarios de Facebook e Instagram, ventaja que no pudo ser replicada por los competidores demandantes, en particular los medios de comunicación.

En consecuencia, la resolución estima parcialmente la demanda y declara la existencia de un acto de competencia desleal por infracción de normas, en los términos del artículo 15.1 de la Ley de Competencia Desleal, condenando a Meta al pago de una indemnización total de 542.170.719,69 euros.

PUBLICACIONES EN RED

Como siempre, dedicamos este apartado a las nuevas publicaciones más notables en el campo de la privacidad y la protección de datos:

Fortalecimiento de la democracia y el Estado de Derecho a través de la Inteligencia Artificial. Instituto Vasco de Administraciones Públicas (IVAP), 2025.

Coords.: Bustos Gisbert, Rafael y García Roca, Francisco Javier.

La obra colectiva coordinada por Rafael Bustos Gisbert y Francisco Javier García Roca, Fortalecimiento de la democracia y el Estado de Derecho a través de la Inteligencia Artificial (2025), constituye una aportación particularmente valiosa al debate contemporáneo sobre la transformación tecnológica del poder público. El libro ofrece una combinación exhaustiva de trabajos, articulados a partir de unas jornadas académicas previas, que abordan de manera sistemática las principales cuestiones suscitadas por la aplicación de la inteligencia artificial en el ámbito institucional, tanto en su dimensión legislativa, como judicial y administrativa.

Asimismo, la obra concita la participación de autores de máximo prestigio, cuyos análisis, elaborados con gran rigor y profundidad, permiten al lector acceder a una perspectiva tan actualizada como omnicomprensiva de los retos, oportunidades y tensiones que la inteligencia artificial introduce en el Estado de Derecho.

Finalmente, y a diferencia de lo que suele ocurrir en estudios de esta naturaleza, el volumen propugna una aplicación decidida de estas tecnologías por los poderes públicos, sin renunciar por ello a la salvaguarda de los derechos y libertades, ni a la adecuada protección de los intereses legítimos concernidos.

Por todo ello, se trata de una obra más que recomendable para quien pueda estar interesado en esta temática.

Síganos en Linked

Visite nuestra web e infórmese de las novedades y actividades formativas que realizamos

www.rdu.es

2444-5762