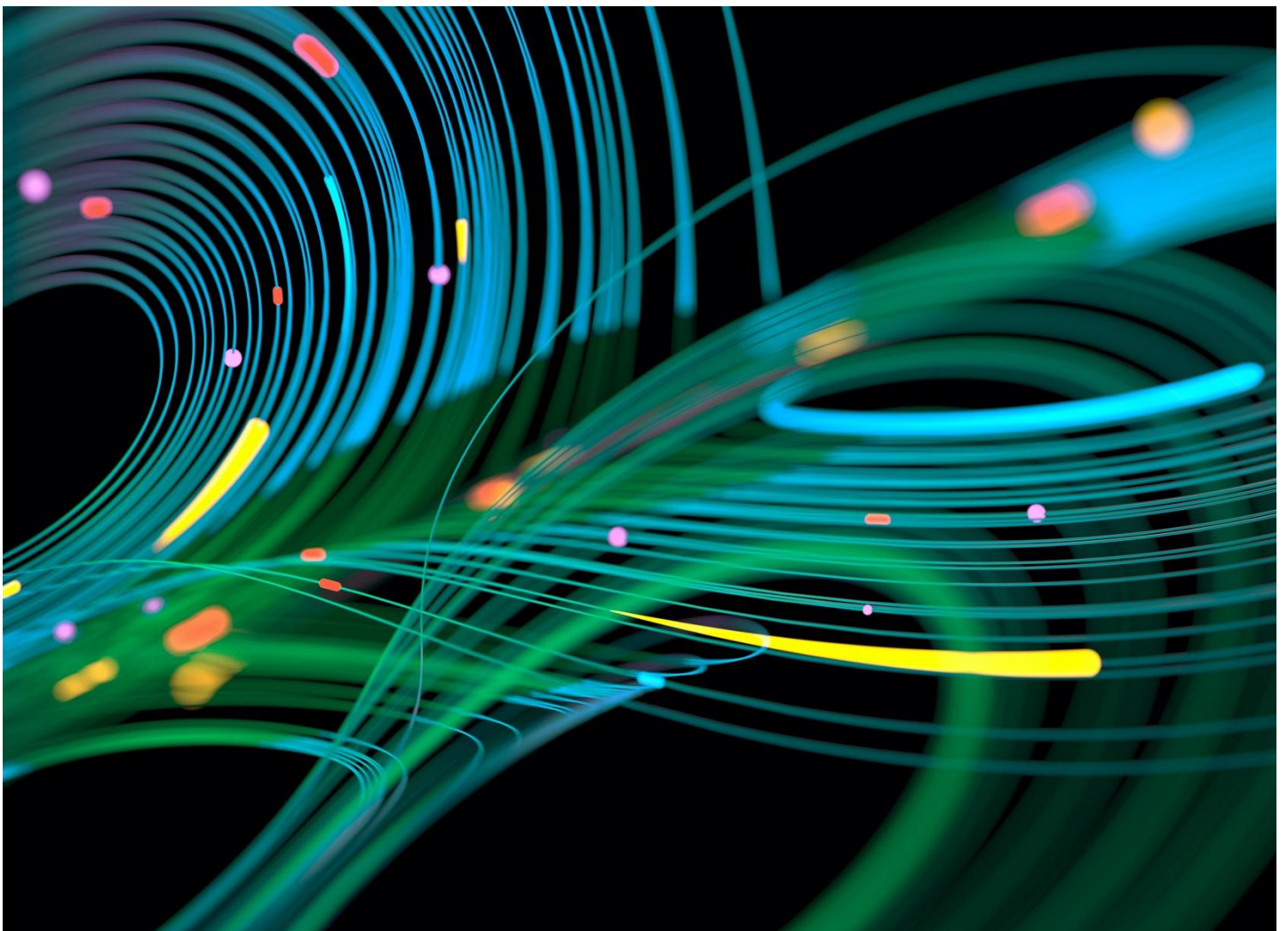


GARRIGUES

Newsletter de Economía del Dato, Privacidad y Ciberseguridad

Febrero de 2026

Últimas novedades en derecho digital e innovación tecnológica, con resoluciones recientes y sentencias clave sobre IA, *e-commerce* y normativa tecnológica



La UE impulsa en 2026 una profunda reconfiguración de la economía digital proponiendo modificaciones en la normativa de IA, datos y plataformas



[Alejandro Padín Vidal](#)

2026 llega cargado de reformas que redefinirán la IA, la privacidad y los mercados digitales en la UE. La agenda regulatoria avanza hacia más transparencia, mayor supervisión y nuevas obligaciones para plataformas, proveedores tecnológicos y empresas que traten datos o dependan de servicios digitales. Un año clave para anticipar riesgos, adaptar procesos y reforzar la estrategia digital corporativa.

En el ámbito de la economía digital, 2026 se presenta, una vez más, como un año de novedades y retos normativos de calado trascendental.

Inteligencia artificial

En lo referente a la inteligencia artificial, 2026 será el año en el que veremos o bien la consolidación definitiva o bien un aplazamiento de la aplicación del Reglamento de Inteligencia Artificial (RIA). Así, la Comisión Europea ha publicado [una propuesta de reglamento](#) que, de aprobarse, introduciría diversas modificaciones relevantes en el RIA, incluyendo una que afectaría al plazo de aplicación obligatoria de toda la normativa referida a las obligaciones aplicables a los proveedores y responsables del despliegue de sistemas de alto riesgo. En [este enlace](#) puede consultar la publicación al respecto.

Simplificación del acervo digital europeo

En este próximo año 2026 también se verán debates intensos relativos a algunos de los conceptos estructurales de la regulación de la economía digital, como el concepto mismo de “dato personal” o el concepto de “pseudonimización”. Esto es consecuencia de otra [propuesta de reglamento](#) de la Comisión Europea, esta vez bajo el nombre genérico de “simplificación del acervo digital europeo”, que propone la modificación de normas tan importantes como el Reglamento General de Protección de Datos, la Directiva NIS 2 o el Reglamento de Datos (*Data Act*), en los que se integrarían, derogando otras normas relacionadas como son el Reglamento de Gobernanza de Datos (*Data Governance Act*) o la Directiva de datos abiertos y reutilización de información del sector público.

Privacidad

Los principios básicos recogidos en la normativa de protección de datos en la Unión Europea están siendo objeto de revisión, tanto como consecuencia de los avances jurisprudenciales (por ejemplo, poniendo en cuestión la tradicional doctrina absoluta del concepto de dato personal, como ha ocurrido con la sentencia del TJUE en el caso [SRB vs EDPS](#)) como por las propuestas de modificación legislativa que se incluyen en las dos normas Ómnibus comentadas y en otros movimientos regulatorios. Aunque se pretende simplificar y racionalizar la aplicación de la norma, existen resistencias en el ámbito de la defensa de los derechos fundamentales, lo que nos llevará a presenciar intensos debates doctrinales y regulatorios cuyo resultado, en este momento, es difícil de prever.

Desde una perspectiva internacional y haciendo foco en las jurisdicciones donde Garrigues tiene presencia, Chile se afronta todo el proceso de cumplimiento de la nueva ley de protección de datos, por lo que las compañías chilenas o con negocios en este país están obligadas a realizar los trabajos necesarios para dar cumplimiento a la norma antes de su aplicación obligatoria.

Reglamento de Servicios Digitales (DSA)

En 2026 continuará intensificándose la aplicación efectiva del Reglamento de Servicios Digitales (DSA), que está consolidando un marco homogéneo en la UE para la responsabilidad y las obligaciones de diligencia de los prestadores de servicios intermediarios (alojamiento, redes sociales, *marketplaces*, motores de búsqueda, etc.). El año estará marcado por el incremento de actuaciones supervisoras, criterios interpretativos y resolución de procedimientos (incluidas medidas correctivas), especialmente sobre obligaciones de transparencia, gestión de contenidos ilícitos, trazabilidad de comerciantes en *marketplaces*, sistemas de notificación y actuación, y mecanismos de reclamación y *redress*. En el caso de las plataformas y motores de búsqueda de muy gran tamaño, será particularmente relevante la exigencia de evaluaciones y mitigación de riesgos sistémicos (por ejemplo, protección de menores, efectos algorítmicos, desinformación, riesgos para la seguridad y la salud pública), así como la transparencia publicitaria y la supervisión de prácticas como patrones de diseño engañosos.

En España, la supervisión del DSA se articula en torno a la CNMC como coordinador de servicios digitales. No obstante, el despliegue efectivo del marco nacional (incluido el régimen sancionador y la operativa completa de supervisión) continúa muy ligado a la tramitación normativa interna y a la dotación de medios, por lo que 2026 previsiblemente será un año de consolidación institucional y de incremento gradual de actuaciones supervisoras y de coordinación con la Comisión Europea.

Reglamento de Mercados Digitales (DMA)

En paralelo, en 2026 se consolidará la aplicación práctica del Reglamento de Mercados Digitales (DMA), orientado a garantizar mercados digitales abiertos y en competencia efectiva mediante obligaciones específicas para los *gatekeepers*. El foco se desplazará desde la mera designación de estos operadores hacia la evaluación de sus medidas de cumplimiento y la adopción de decisiones sobre prácticas clave que afectan a la estructura del mercado, como la autopreferencia, las restricciones a la libertad comercial de los usuarios empresariales, la interoperabilidad y las condiciones de acceso a ecosistemas cerrados (*app stores* y sistemas operativos) y el uso de datos. Este proceso previsiblemente vendrá acompañado de un incremento de la litigiosidad y de la necesidad de coordinar el análisis regulatorio con los ámbitos de competencia, consumo y protección de datos.

A más tardar en mayo de 2026, la Comisión Europea presentará a las demás instituciones de la Unión Europea su primer informe sobre la aplicación del Reglamento de Mercados Digitales (DMA). Una de las cuestiones centrales que deberá abordar la Comisión Europea en dicho informe será si, y en qué medida, la normativa resulta aplicable a la inteligencia artificial (IA).

En particular, la Comisión Europea podrá plantear la inclusión de la IA dentro de las categorías existentes de “servicios básicos de plataforma” (*core platform services*) o, en su caso, proponer definiciones nuevas o modificadas con el fin de abarcar herramientas y servicios de IA. Del mismo

modo, la Comisión Europea analizará la forma en que las obligaciones sustantivas previstas en el DMA resultan aplicables a la IA y si es necesaria una modificación legislativa a tal efecto.

Por razones de eficiencia y celeridad, cabe prever que la Comisión Europea se incline por soluciones que no requieran una reforma legislativa.

e-IDAS e identidad digital

Otro ámbito en el que se presentan novedades muy importantes durante el año 2026 es el relacionado con la identidad digital. En este ejercicio se prevé que se terminen de desarrollar las especificaciones técnicas para la puesta en marcha real y efectiva de la Cartera de Identidad Digital Europea (*EU ID Digital Wallet*), que supondrá un hito en los mecanismos de identificación oficial de las personas en la Unión, al permitir disponer de una cartera digital en forma de una aplicación móvil en la que tendremos todas nuestras credenciales oficiales (DNI, carnet de conducir, tarjetas de salud, biblioteca o universidad, títulos académicos, etc.).

Ciberseguridad

Esperamos también que 2026 suponga el año en que veamos aprobada y publicada la ley de transposición de la Directiva NIS 2 en España, no solo por el retraso que ya arrastramos con respecto a la fecha obligatoria de promulgación de esta importantísima norma (que tenía que haber sido aprobada antes de octubre de 2024), sino por la importancia extraordinaria que tiene para conseguir un mayor nivel de seguridad en las redes y sistemas de un grandísimo número de empresas en España que pertenecen a diversos sectores de la economía. El trabajo de adaptación que se requiere en muchas empresas es todo un reto operativo que será necesario afrontar sin dilación.



Actualidad

La Comisión Europea impone a X la primera multa en aplicación del 'Digital Services Act' (DSA) a una VLOP

La Comisión Europea investigó a la plataforma X (antes Twitter), calificada como "very large online platform" (VLOP), por posibles incumplimientos de las obligaciones reforzadas que le impone el Reglamento de Servicios Digitales (DSA), en particular en materia de diseño de interfaces, transparencia publicitaria y acceso a datos para investigadores.

La Comisión [concluye](#) que X infringió varias disposiciones del DSA y le impone una multa de 120 millones de euros, la primera sanción adoptada en aplicación del nuevo régimen sancionador del citado reglamento.

En primer lugar, considera engañoso el diseño del sistema de "verificación azul", al permitir obtener el distintivo de cuenta verificada mediante el pago de una suscripción sin una verificación real de la identidad, lo que dificulta evaluar la autenticidad de las cuentas y aumenta los riesgos de suplantación y fraude.

Asimismo, la Comisión aprecia incumplimientos de las obligaciones de transparencia publicitaria por no disponer de un repositorio de anuncios conforme al DSA, y por el incumplimiento del deber de facilitar acceso a datos públicos a investigadores acreditados, al imponer restricciones contractuales indebidas.

La decisión confirma que el DSA no solo regula en relación con contenidos ilícitos, sino también lo relativo al diseño de las plataformas, la transparencia y la rendición de cuentas de las grandes plataformas digitales.

El CEPD somete a consulta pública las recomendaciones 2/2025 sobre la base jurídica para exigir la creación de cuentas de usuario en sitios de comercio electrónico

El Comité Europeo de Protección de Datos (CEPD) ha publicado las [recomendaciones 2/2025](#) sobre la base jurídica para exigir la creación de cuentas de usuario en sitios de comercio electrónico para someterlas a consulta pública. El documento analiza la práctica, cada vez más extendida, de obligar a los usuarios a registrarse para poder acceder a ofertas o completar compras *online* y concluye que, con carácter general, esta exigencia no es conforme con el RGPD si no existe una base legal clara y suficiente.

Como principio general, el CEPD señala que los usuarios deberían poder comprar o interactuar con una plataforma de comercio electrónico sin necesidad de crear una cuenta obligatoria, recomendando opciones como la compra como invitado o la creación voluntaria de cuentas, en aplicación de los principios de protección de datos desde el diseño y por defecto (artículo 25 del RGPD).

En relación con las bases legales del artículo 6 del RGPD, el CEPD aclara que:

- i. La ejecución de un contrato solo puede justificar la cuenta obligatoria cuando esta sea estrictamente necesaria para la prestación del servicio, como en servicios de suscripción o relaciones continuadas, pero no en ventas puntuales simples.
- ii. La existencia de una obligación legal solo permitiría exigir una cuenta cuando una

norma lo imponga de forma expresa, supuesto poco habitual actualmente en el comercio electrónico.

- iii. El interés legítimo, por lo general, no resulta suficiente para imponer la creación de cuentas obligatorias cuando existen alternativas menos intrusivas para los derechos y libertades de los usuarios.

El CEPD identifica, además, riesgos relevantes asociados a la imposición de cuentas obligatorias, como el tratamiento excesivo de datos personales, una mayor conservación de la información en el tiempo y un incremento de los riesgos de seguridad y accesos no autorizados.

En conclusión, el CEPD afirma que la creación obligatoria de cuentas debe ser la excepción y no la regla, y solo será compatible con el RGPD cuando supere un análisis estricto de necesidad y proporcionalidad, debiendo los responsables ofrecer, siempre que sea posible, alternativas más respetuosas con la privacidad del usuario.

La Agencia Nacional de Ciberseguridad de Chile aprueba nómina definitiva del primer proceso de calificación de operadores de importancia vital

La Agencia Nacional de Ciberseguridad de Chile (ANCI) aprobó mediante la Resolución exenta n° 87 la nómina definitiva del primer proceso de calificación de operadores de importancia vital (OIV) conforme al procedimiento de la Ley N°21.663 Marco de Ciberseguridad y su Reglamento, tras consulta pública y evaluación técnica multisectorial, consolidando un hito fundamental del nuevo marco chileno de ciberseguridad.

La calificación consistió en una evaluación de dos fases: dependencia de redes y sistemas informáticos, e impacto significativo sobre seguridad, orden público, continuidad de servicios esenciales y funciones del Estado, ponderado con criterios del reglamento. La nómina abarca electricidad, telecomunicaciones, infraestructura y servicios digitales, banca/servicios financieros/medios de pago, prestadores institucionales de salud, empresas del Estado y organismos de la

Administración, tras informes sectoriales y consulta pública.

La resolución da paso a obligaciones reforzadas de gestión de riesgos, continuidad y resiliencia para los OIV, y anticipa próximas fases para sectores remanentes, consolidando un enfoque sistémico y escalonado de protección de infraestructura crítica digital.

La nómina puede consultarse en el siguiente [enlace](#).

La AESIA publica guías prácticas para facilitar el cumplimiento del Reglamento Europeo de Inteligencia Artificial (RIA)

La Agencia Española de Supervisión de la Inteligencia Artificial (AESIA), organismo público dependiente del Ministerio para la Transformación Digital y la Función Pública, ha publicado un conjunto de [16 guías prácticas](#) destinadas a apoyar a organizaciones públicas y privadas en la comprensión, implementación y cumplimiento del Reglamento Europeo de Inteligencia Artificial (RIA / AI Act).

Estas guías, fruto del *sandbox* regulatorio español de IA, están dirigidas tanto a pymes y *start-ups* como a grandes empresas que desarrollan o implementan sistemas de IA de alto riesgo, con recomendaciones alineadas con los requisitos regulatorios europeos y en espera de normas armonizadas.

Las publicaciones no son vinculantes ni sustituyen a la normativa aplicable, pero proporcionan orientación operativa detallada sobre obligaciones complejas, ayudando a las entidades a organizar sus estrategias de cumplimiento antes de la entrada en vigor progresiva de exigencias del *AI Act*, especialmente de cara a agosto de 2026.

Listado de guías publicadas:

1. Guía introductoria al reglamento de IA
2. Guía práctica y ejemplos para entender el Reglamento de IA
3. Guía de Evaluación de conformidad
4. Guía del sistema de gestión de la calidad

5. Guía de gestión de riesgos
6. Guía de Vigilancia humana
7. Guía de datos y gobernanza de datos
8. Guía de Transparencia
9. Guía de Precisión
10. Guía de Solidez
11. Guía de Ciberseguridad
12. Guía de registros
13. Guía de Vigilancia poscomercialización
14. Guía de Gestión de Incidentes
15. Guía de Documentación Técnica
16. Manual de *checklist* de guías de requisitos (*checklists* y ejemplos)

Estas guías están estructuradas en tres bloques (introdutorias, técnicas y *checklist*) y constituyen una herramienta práctica para facilitar que las organizaciones españolas y del resto de la UE adapten sus sistemas de IA al marco europeo con un enfoque de innovación responsable y respeto a los derechos fundamentales.

Publicada la actualización de la norma ISO 27701:2025 sobre gestión de la información de privacidad

La Organización Internacional de Normalización (ISO) ha [publicado](#) la nueva ISO 27701:2025, una actualización del estándar internacional que amplía los requisitos y orientaciones para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la información de privacidad (PIMS).

La norma, que complementa a la ISO 27001 en materia de seguridad de la información, refuerza la integración entre seguridad y protección de datos personales, estableciendo directrices adaptadas al contexto del Reglamento General de Protección de Datos (RGPD) y a otros marcos internacionales.

La publicación de la versión 2025 actualiza los controles, la terminología y las referencias normativas, alineándolos con las últimas versiones de los estándares ISO/IEC 27001:2022 e ISO/IEC 27002:2022, consolidando así su papel como referencia para las organizaciones que buscan certificar la gestión de la privacidad dentro de sus sistemas de seguridad.

Entrada en el blog de la AEPD: equilibrio entre derechos fundamentales cuando entra en juego la protección del menor

La AEPD ha publicado una [entrada en su blog](#) en la que refuerza el concepto del "interés superior del menor", recogido en el artículo 24.2 de la Carta de los Derechos Fundamentales de la Unión Europea y alegado en distintas sentencias del Tribunal de Justicia de la Unión Europea, como la del caso [C-230/21](#).

En el ámbito de la protección de la infancia en Internet, se suele abogar por un equilibrio entre el interés superior del menor y el derecho a la protección de datos. Sin embargo, la AEPD concluye que "esta falsa dicotomía realmente quiere expresar que los derechos fundamentales deberían equilibrarse en relación con los intereses comerciales de los actores que operan en el ecosistema digital", y añade que "esta es una falsa elección que no debe hacerse, de la misma manera que no se debe admitir la falsa elección entre seguridad y privacidad, expresada en el pasado en diferentes escenarios".

A la hora de realizar ponderaciones en la que están en juego los intereses de menores, la AEPD indica que "el interés superior del menor y el derecho a la protección de datos están en el mismo plato de la balanza; son complementarios y, por lo tanto, no deben ser equilibrados, ni se debe comprometer uno a favor del otro". Por tanto, con esta entrada de la AEPD, se concluye que la ponderación que busca el equilibrio entre derechos fundamentales (como el derecho a la intimidad), utilizando los conceptos de idoneidad, necesidad y proporcionalidad, no tiene cabida en el marco de la protección del menor.

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 por el CEPD y la Comisión Europea para facilitar una aplicación coherente de la DMA y el RGPD, aportar mayor seguridad jurídica y simplificar el cumplimiento para usuarios, beneficiarios e individuos en general.

En esta primera guía se busca armonizar interpretaciones y reducir fricciones de cumplimiento. Entre otros aspectos básicos, las directrices publicadas clarifican los elementos que deben considerarse para cumplir los requisitos de “elección específica” y “consentimiento válido” del artículo 5.2 de la DMA y del RGPD, permitiendo la combinación o el uso cruzado lícito de datos personales en servicios de plataforma esenciales. También se abordan aspectos relativos a la distribución de aplicaciones y tiendas de terceros, la portabilidad de datos, las solicitudes de acceso a datos y la interoperabilidad de los servicios de mensajería.

El texto final, que incorporará las aportaciones recibidas durante la consulta pública lanzada por el CEPD y la Comisión, será preparado conjuntamente por ambas.

El sistema de entradas y salidas (SES) de la UE entra en funcionamiento

Con motivo de la entrada en funcionamiento del sistema de entradas y salidas de la UE (SES) el pasado 12 de octubre de 2025, el Comité de Supervisión Coordinada (CSC) lo ha [incluido](#) en su ámbito de aplicación.

El SES es un sistema informático a gran escala desarrollado por la UE para prevenir la migración irregular y mejorar la seguridad en el espacio Schengen, y se prevé que sustituya gradualmente el sistema de sellado de pasaportes en las fronteras exteriores del

espacio Schengen, con el objetivo de optimizar el proceso fronterizo.

Este sistema registra a los nacionales de países no pertenecientes al espacio Schengen que viajan con un visado de corta duración o a los viajeros exentos de visado, incluyendo de todos estos viajeros los datos personales de los documentos de viaje, como el nombre, la fecha y el lugar de nacimiento. También registra las fechas de entrada y salida de los viajeros, así como datos biométricos como la imagen facial y las huellas dactilares. Las autoridades que traten datos personales en el SES -como la autoridad fronteriza, los servicios de migración y, en determinadas circunstancias, las fuerzas de seguridad- deberán garantizar que las personas puedan solicitar fácilmente el acceso a sus datos, así como ejercitar sus derechos en el marco del RGPD.

Se prevé que el SES esté plenamente operativo el próximo 10 de abril de 2026, fecha en la que el sistema se utilizará en todos los pasos fronterizos para todos los nacionales de terceros países que cumplan los requisitos y dispongan de pasaportes biométricos.

El Comité Europeo de Protección de Datos centrará su quinta acción coordinada en el cumplimiento de las obligaciones de transparencia

El CEPD ha [anunciado](#) que su quinta acción coordinada de control se centrará en verificar el cumplimiento de las obligaciones de transparencia e información establecidas en los artículos 12, 13 y 14 del RGPD, que garantizan el derecho de las personas a ser informadas sobre el tratamiento de sus datos personales.

En este tipo de acciones, el CEPD selecciona un tema prioritario y las autoridades nacionales de protección de datos realizan investigaciones paralelas y coordinadas. Posteriormente, el comité agrupa los resultados y formula recomendaciones o medidas de seguimiento comunes, tanto a nivel nacional como europeo.

Las acciones anteriores se han centrado en ámbitos clave como el uso de servicios en la nube en el sector público (2023), la figura del delegado de protección de datos (2024) y el derecho de acceso (2025). La nueva iniciativa se desarrollará a lo largo de 2026, y se suma a

la acción actualmente en curso sobre el derecho de supresión (artículo 17 del RGPD), cuyo informe final se publicará en los próximos meses.

Las transferencias de datos UE-Reino Unido podrán mantenerse sin garantías adicionales, aunque con vigilancia por posibles riesgos futuros

Según informa la AEPD en su [comunicado del 23 de octubre](#), el Comité Europeo de Protección de Datos (CEPD) ha emitido dictamen favorable a la propuesta de la Comisión Europea de prorrogar hasta diciembre de 2031 la decisión de adecuación del Reino Unido. Esta extensión permitirá que las organizaciones europeas sigan transfiriendo datos personales a territorio británico sin necesidad de garantías adicionales, al considerar que su marco de protección mantiene un nivel esencialmente equivalente al europeo.

El CEPD valora positivamente la continuidad y estabilidad de los flujos internacionales de datos, así como la persistente armonización entre el régimen británico y el europeo, incluso tras las recientes reformas legislativas del Reino Unido. No obstante, advierte a la Comisión de varios riesgos que requieren supervisión activa, entre ellos los efectos de la Ley de Revocación del Derecho de la UE (REUL) y su posible impacto sobre la coherencia normativa, la ampliación de facultades del Gobierno británico que podría reducir el control parlamentario en áreas clave, y las implicaciones en materia de acceso gubernamental a datos, cifrado y exenciones por seguridad nacional.

En conclusión, aunque el CEPD respalda la prórroga, insiste en la necesidad de que la Comisión Europea mantenga una vigilancia continua sobre los cambios legislativos británicos para garantizar que el nivel de protección siga siendo equivalente durante toda la vigencia de la decisión de adecuación.

Se imponen medidas correctivas a Microsoft por el tratamiento de datos personales de menores de edad en Austria

La autoridad de protección de datos de Austria dictaminó el pasado miércoles 8 de octubre que Microsoft rastreó ilegalmente a estudiantes que usaban su *software* educativo al no darles acceso a sus datos y utilizar *cookies* sin consentimiento.

La [decisión](#) de la autoridad austriaca (DSB) se produjo en respuesta a una reclamación presentada en 2024. El denunciante en el caso, el padre de un menor cuya escuela utiliza el *software* de Microsoft, informó a la autoridad austriaca de que no se había consentido ni por su parte, ni por la del menor, la instalación de *cookies*, y que no pudo obtener información sobre cómo se estaban utilizando los datos de su hijo.

Se constata por parte de la DSB la existencia de infracciones del derecho de acceso e información y dicta la obligación de incorporar determinadas medidas correctivas. En concreto, entre otras cuestiones, ordena que se complete la información facilitada a los usuarios conforme al artículo 13 del RGPD y que se revisen y, en su caso, se eliminen en diez semanas los datos tratados de menores procedentes de *cookies* no técnicas.

La 'Global Privacy Assembly' aprueba tres nuevas resoluciones centradas en la inteligencia artificial y la educación digital

La *Global Privacy Assembly (GPA)*, que agrupa a las autoridades de protección de datos de todo el mundo, ha adoptado tres nuevas [resoluciones](#) clave en su 47ª sesión anual celebrada recientemente en Corea del Sur, dos de las cuales se centran directamente en la inteligencia artificial.

La primera aborda el uso de datos personales en el entrenamiento de modelos de IA, subrayando que solo pueden emplearse si han sido obtenidos de forma lícita y conforme a los principios del RGPD, recordando que la

disponibilidad pública no equivale a un uso legítimo.

La segunda se centra en la supervisión humana significativa de decisiones automatizadas, definiendo los roles de supervisión, los requisitos de formación y la obligación de documentar las decisiones tomadas con apoyo de sistemas de IA.

Por último, la tercera resolución trata sobre educación digital y ciudadanía responsable, recomendando la creación de contenidos educativos sobre los derechos en protección de datos y de protocolos accesibles para entidades educativas, con el fin de promover una cultura digital inclusiva y segura.

La Agencia pone en marcha la revista científica “Privacidad, Innovación y Tecnología” y hace un llamamiento a autores para publicar en el primer número

La AEPD ha lanzado la [revista científica “Privacidad, Innovación y Tecnología” \(PIT\)](#), un nuevo espacio académico dedicado a la reflexión, análisis y difusión de conocimiento especializado en privacidad, protección de datos y el impacto de las tecnologías

disruptivas -especialmente la inteligencia artificial- en los derechos fundamentales.

La creación de la revista refuerza la misión institucional de la Agencia y busca consolidar un ecosistema de investigación riguroso y útil para todos los sectores implicados. PIT se inspira en los valores de independencia, innovación, cooperación y excelencia, y está concebida para fortalecer la colaboración entre la Agencia, la academia, la empresa y la sociedad, promoviendo la transferencia de conocimiento y el análisis interdisciplinar.

La AEPD irá abriendo el plazo de recepción de artículos para los sucesivos números de la revista, aceptando contribuciones originales en español o inglés que serán evaluadas mediante revisión doble ciego por pares externos. La publicación del primer número está prevista para abril de 2026 bajo licencia CC BY-NC, garantizando acceso abierto y transparencia.

La revista PIT también se plantea como un observatorio de buenas prácticas casos de uso y propuestas regulatorias, con el objetivo de demostrar que la innovación tecnológica y el cumplimiento normativo son compatibles y necesarios para un desarrollo ético y sostenible.

Resoluciones

La AEPD impone una sanción a AENA en relación con un sistema de reconocimiento biométrico

En este caso, AENA había lanzado un proyecto piloto de reconocimiento biométrico de pasajeros para controlar su flujo por los aeropuertos. Esta medida, tal como se desprende de la [resolución](#) emitida por la AEPD, era opcional, de modo que los pasajeros podían seguir llevando a cabo su identificación por medios tradicionales.

En el proceso de lanzamiento de este proyecto, AENA remitió consultas previas a la AEPD tras realizar las correspondientes evaluaciones de impacto del tratamiento pretendido.

Esta resolución es importante, ya que contiene una síntesis de los criterios de la AEPD al respecto del tratamiento de datos biométricos por parte de los responsables, cuya viabilidad, con carácter general, se ha visto puesta en tela de juicio conforme a los últimos criterios del supervisor. En este sentido, cabe destacar el análisis de la AEPD sobre los criterios de necesidad y proporcionalidad del tratamiento, en relación con los cuales vuelve a incidir en cómo: (i) la utilidad o conveniencia de un tratamiento no legitima la elección de un sistema “agresivo” para los derechos y libertades de las personas; y (ii) los datos biométricos son datos especialmente protegidos, por lo que cualquier tratamiento de esta clase de datos debe venir precedido de análisis exhaustivos sobre el impacto del tratamiento, así como acompañado de la implementación de suficientes garantías.

Es en relación con las citadas evaluaciones de impacto por lo que la AEPD impone la sanción económica (10.043.002 euros) a AENA, ya que considera que estas no eran lo suficientemente

completas ni detalladas, precisando un mayor nivel de exhaustividad especialmente en relación con el análisis de necesidad y proporcionalidad del tratamiento.

Por lo tanto, de esta resolución se pueden extraer no solo los criterios de la AEPD al respecto del tratamiento de datos biométricos, sino también la importancia de llevar a cabo evaluaciones de impacto detalladas y exhaustivas. La infracción de este deber puede, de por sí, acarrear importantes consecuencias.

Impuestas dos sanciones millonarias a una empresa de telefonía por un incidente de seguridad

En esta [resolución](#) de la AEPD se imponen dos sanciones millonarias a una empresa de telefonía móvil por infracciones del artículo 5.1.f) del RGPD, sobre el principio de confidencialidad de los datos (2.500.000 euros), y del artículo 32 del RGPD, sobre medidas de seguridad (1.500.000 euros).

En este caso, según se desprende de la resolución, tras recibir una comunicación del responsable del tratamiento informando de un incidente de seguridad que había resultado en la pérdida de confidencialidad de sus datos personales, varios clientes interpusieron reclamaciones ante la AEPD.

Más allá de la apreciación sobre las medidas concretas implementadas por el responsable del tratamiento, el punto de mayor interés en esta resolución es el análisis que se hace en la misma en relación con la concurrencia de las dos infracciones citadas anteriormente. La AEPD aprecia esta sin atender a las alegaciones del responsable acerca de cómo la imposición de multas por estos dos preceptos

relacionados entre sí podría estar incurriendo en una violación del principio de *non bis in idem*. Tampoco aprecia la AEPD la concurrencia de un concurso medial ni una violación del principio de especialidad, por lo que se reafirma en su posición ya reiterada en anteriores ocasiones de que ambas infracciones pueden sancionarse simultáneamente en relación con un mismo incidente.

Esta resolución contiene una recopilación actualizada de los argumentos esgrimidos a este respecto por parte de la AEPD, y es un claro recordatorio del nivel de diligencia exigible tanto de forma previa (en la adopción de medidas de seguridad, por ejemplo), como posterior al incidente acaecido (en la gestión del mismo) que los responsables han de adoptar.

Sancionada una entidad financiera por no garantizar la trazabilidad y seguridad de datos personales en el envío de documentación a través de su empresa de mensajería

La AEPD ha sancionado a una [entidad financiera](#) por infringir el artículo 32 del RGPD, al no implementar medidas técnicas y organizativas adecuadas para garantizar la seguridad en el tratamiento de datos personales durante la relación contractual con una empresa de mensajería encargada de la recogida de documentación de clientes. La resolución subraya que la entidad, como responsable del tratamiento, debía establecer mecanismos efectivos de trazabilidad y alerta temprana para detectar y gestionar posibles brechas de datos, más allá de la mera existencia formal de contratos o evaluaciones de impacto.

Se rechaza la alegación de la entidad financiera sobre la diligencia en la selección y control de su encargado, destacando que la ausencia de control efectivo y la falta de medidas específicas para la trazabilidad de los envíos constituyen una vulneración del deber de seguridad. Además, se recalca que la pérdida de datos personales supone una lesión al derecho fundamental de protección de datos, independientemente de que no se haya acreditado acceso por terceros no autorizados.

La sanción se gradúa considerando la gravedad, el volumen de afectados potenciales y la naturaleza de los datos extraviados (incluyendo DNI y datos bancarios), imponiendo una multa de 500.000 euros, reducida a 400.000 euros por pago voluntario. La resolución enfatiza la obligación proactiva y constante de adecuación de las medidas de seguridad al riesgo.

Sanción a una universidad por el uso de biometría en sistemas de 'proctoring'

La AEPD ha decidido [sancionar](#) a una universidad por el tratamiento de datos biométricos a través de un sistema de *proctoring* con reconocimiento facial impuesto a los estudiantes sin ofrecer alternativas.

La Agencia declara la infracción del artículo 9 del RGPD (tratamiento de categorías especiales de datos personales) al tratar datos biométricos sin base de legitimación ni excepción habilitante. En particular, determina que la autenticación 1:1 mediante patrones de geometría facial constituye tratamiento de datos biométricos. La universidad alegó que el reconocimiento facial respondía a exigencias de la Agencia Nacional de Evaluación de la Calidad y Acreditación (ANECA) para prevenir el fraude académico, pero la AEPD rechaza esta justificación al constatar que ninguna norma obliga a dicho tratamiento y que, en todo caso, las directrices de la ANECA carecen de rango legal suficiente para habilitarlo.

Respecto al consentimiento prestado por los estudiantes, la Agencia concluye que no constituye un consentimiento libre al no existir alternativas equivalentes y concurrir un desequilibrio de poder entre la institución y el alumnado, análogo al existente en el ámbito laboral. Se destaca, además, que la universidad descartó aplicaciones que no requerían datos biométricos. No obstante, la AEPD reconoce que, hasta la publicación de la Guía sobre Biometría en noviembre de 2023, existían dudas razonables sobre este tipo de tratamientos, por lo que reduce el período sancionable a partir de dicha fecha. Por esta infracción se impone una multa de 300.000 euros.

Adicionalmente, la Agencia sanciona la infracción del artículo 5.1.c) del RGPD

(principio de minimización), al considerar que el sistema utilizado era innecesariamente intrusivo existiendo alternativas operativas que no requerían biometría. La AEPD subraya que el tratamiento resulta desproporcionado, sin que el fin perseguido justifique el medio empleado, y que la elección del sistema respondió a criterios de utilidad organizativa y no de protección de datos. En este caso, no se reduce el período de infracción, considerándose continuada desde la entrada en vigor del RGPD, e imponiéndose una sanción de 350.000 euros.

Multa de 200.000 euros a una comercializadora energética por dar de baja al cliente incorrecto

La AEPD ha [sancionado](#) a una comercializadora energética con una multa de 200.000 euros por vulnerar el principio de exactitud recogido en el artículo 5.1.d) del RGPD durante la gestión de un cambio de comercializadora y titularidad en un contrato de suministro eléctrico y de gas.

El caso tiene su origen en la contratación por parte de un tercero de los servicios de luz y gas con la compañía sancionada en marzo de 2022. Durante esa contratación, la comercializadora asoció por error los códigos CUPS (que identifican el punto de suministro) del aquí reclamante con el contrato de ese tercero. Como consecuencia, cuando el tercero canceló su contrato, se cortó el suministro en la vivienda del reclamante, dejándole sin luz ni gas durante dos días.

La AEPD considera acreditado que la reclamada no aplicó las medidas necesarias para garantizar la exactitud de los datos, como la verificación del CUPS y la relación del contratante con el punto de suministro. La empresa alegó que el error se debió a la confusión en la dirección y a la información del DNI del contratante, invocando incluso la figura del “error invencible”. Sin embargo, la Agencia desestimó estas alegaciones, señalando que la comercializadora disponía de medios técnicos y jurídicos para evitar la confusión.

La Comisión de Protección de Datos irlandesa (DPC) impone una multa de 530 millones de euros a Tik Tok y suspende las transferencias de datos a China

La Comisión de Protección de Datos irlandesa (DPC) ha impuesto una sanción de 530 millones de euros a Tik Tok por realizar transferencias internacionales de datos mediante acceso remoto desde China sin aplicar las garantías adecuadas exigidas por el RGPD ni cumplir con los deberes de información hacia los usuarios. Si bien la noticia se hizo pública en mayo de 2025, la [resolución](#) no se publicó hasta octubre.

La DPC concluyó que la reclamada no evaluó correctamente la legislación china en el contexto del acceso remoto, partiendo de la suposición errónea de que las autoridades chinas no podían acceder legalmente a los datos almacenados fuera del país. Además, no logró demostrar que leyes como la Ley de Inteligencia Nacional, la Ley de Contraespionaje y la Ley de Ciberseguridad no fueran aplicables a los datos durante su procesamiento en China.

Asimismo, la DPC examinó las medidas complementarias adoptadas por la red social para reforzar las cláusulas contractuales tipo (CCT), incluyendo medidas técnicas, contractuales y organizativas. Aunque estas medidas eran pertinentes, se consideraron insuficientes para compensar las deficiencias legales del marco normativo chino, especialmente porque no se realizó un análisis adecuado del mismo que permitiera conocer el nivel de riesgo inicial.

Respecto a las excepciones del artículo 49 del RGPD, la DPC determinó que no eran aplicables, ya que las transferencias no eran ocasionales, sino sistemáticas y continuas.

Por último, en cuanto a la transparencia, la política de privacidad de la red social omitía mencionar a China como país de destino y no explicaba la naturaleza del acceso remoto. Aunque posteriormente se corrigieron estas omisiones, la DPC consideró que se había incumplido el artículo 13.1.f) del RGPD durante más de dos años.

Al hilo de la publicación de esta resolución, la AEPD ha lanzado una serie de [recomendaciones](#) a los usuarios, especialmente a los más jóvenes, animándolos a que:

- Lean detenidamente las notificaciones y políticas de privacidad.
- Revisen la configuración de privacidad y los permisos concedidos en las aplicaciones.
- Valoren si desean seguir usando servicios que transfieren datos a países sin garantías equivalentes a las europeas.
- Actúen con prudencia al compartir información sensible en redes sociales.

Publicadas múltiples sanciones a distintas farmacias catalanas por irregularidades en el tratamiento de datos personales

La AEPD ha publicado 18 resoluciones sancionadoras contra varias farmacias catalanas por irregularidades en el tratamiento de datos personales de residentes en centros geriátricos (una de ellas se puede consultar en [este enlace](#)), incluyendo accesos indebidos y el envío de datos de salud por medios no seguros.

Las farmacias sancionadas elaboraban lo que se denomina “Sistemas Personalizados de Dosificación” (SPD) para centros residenciales, lo que implicaba la gestión de categorías especiales de datos, como las pautas médicas de los pacientes. Sin embargo, la transmisión de esta información se realizaba por correo electrónico sin cifrado, lo que constituye una grave vulneración de la seguridad. Aunque las farmacias alegaron corresponsabilidad con las residencias, la AEPD determinó que actuaban como responsables del tratamiento.

Entre los incumplimientos más relevantes se encuentra la infracción del artículo 6 del RGPD, al preparar los SPD sin contar con un consentimiento informado válido. La normativa sectorial y la guía SPD de Cataluña exigen autorización expresa y documentada, requisito que no se cumplió. También se vulneró el artículo 14 del RGPD, relativo al deber de informar cuando los datos se obtienen de terceros, ya que no se proporcionó a los

interesados información sobre la identidad del responsable, los fines del tratamiento, los derechos y demás extremos exigidos. Aunque algunas farmacias exhibían carteles informativos, la naturaleza de los datos tratados y las circunstancias de los pacientes - residentes en centros geriátricos- evidencian que esta información no llegó efectivamente a los afectados.

Asimismo, se sancionó la infracción del artículo 32 del RGPD por la ausencia de medidas técnicas y organizativas adecuadas, como el cifrado en el envío de correos electrónicos. En algunas resoluciones se destacó, además, la falta de adhesión al convenio obligatorio con la Administración y el Colegio de Farmacéuticos de Cataluña, condición previa para prestar el servicio SPD. Esta omisión implicó que el tratamiento de datos de salud careciera de base legal conforme al artículo 9 del RGPD, que regula el tratamiento de categorías especiales de datos.

Se desestima el recurso de reposición interpuesto por una empresa de telecomunicaciones para no aplicar las medidas correctivas hasta que finalice el proceso contencioso ante la Audiencia Nacional

La AEPD [desestima](#) el recurso de reposición interpuesto por una reconocida empresa de telecomunicaciones que opera en España contra una resolución en la que se constataban dos infracciones relevantes, sancionadas con una multa de elevada cuantía y la imposición de una medida correctiva.

La AEPD suspendió cautelarmente la ejecutividad de la obligación de pago de las sanciones cuando la sociedad anunció recurso contencioso, pero denegó la suspensión de la medida correctiva por prevalecer el interés general en la protección de los datos y la necesidad de evitar perjuicios graves e irreparables a los titulares. En este sentido, la AEPD confirma en la resolución que los procedimientos que la sociedad sancionada aplicaba para la emisión de duplicados de SIM permitían, en la práctica, fallos y excepciones que facilitaban la suplantación de identidad de los interesados.

Se aprecia por la AEPD que el protocolo en casos de duplicidad de la tarjeta SIM priorizaba la operativa comercial sin atender de modo suficiente al riesgo cierto y alto de fraude y a la necesidad de medidas técnicas y organizativas eficaces, lo que vulnera el principio de protección de datos desde el diseño del artículo 25 RGPD. La resolución enfatiza que la falta de controles robustos puede producir perjuicios graves e irreparables a los titulares, y, en definitiva, aun confirmando la suspensión cautelar del pago de las multas por concurrir los requisitos legales, decide rechazar la suspensión de la medida correctiva por considerar que debe prevalecer el interés general en la protección de datos de un número muy significativo de afectados frente al interés económico de la entidad, alineándose así con la doctrina de la Audiencia Nacional que, en supuestos análogos, ha denegado la suspensión de medidas de adecuación al RGPD por no generar efectos irreversibles y ser resarcibles los eventuales perjuicios.

La ICO impone una multa de 14 millones de libras por deficiencias graves de seguridad que expusieron datos de 6,6 millones de personas

La *Information Commissioner's Office* (ICO) del Reino Unido ha [impuesto](#) una multa total de 14 millones de libras esterlinas a una empresa de consultoría y su filial tras una brecha de seguridad ocurrida en 2023 que afectó a aproximadamente 6,6 millones de personas. El incidente se originó por un ciberataque que permitió el acceso no autorizado a información personal y, en algunos casos, a datos sensibles, incluyendo registros de pensiones, información financiera, datos de empleados y antecedentes penales.

La investigación de la ICO identificó fallos graves en las medidas de seguridad, destacando un retraso de 58 horas en la respuesta a una alerta crítica, frente al objetivo interno de una hora. Asimismo, se constató la ausencia de pruebas de penetración periódicas y evaluaciones de riesgo actualizadas en sistemas que trataban millones de registros personales.

La autoridad concluyó que estas deficiencias constituían infracciones de los artículos 5.1.f), 32.1 y 32.2 del UK GDPR (Reglamento General

de Protección de Datos del Reino Unido), relativos al principio de integridad y confidencialidad y a la obligación de aplicar medidas técnicas y organizativas apropiadas.

La ICO subrayó que la magnitud del incidente y la falta de controles preventivos adecuados evidencian una gestión negligente del riesgo cibernético, especialmente grave en empresas que prestan servicios críticos de administración de pensiones y gestión de datos financieros.

Sancionada una operadora por no verificar la identidad en el cambio de titularidad y duplicado de SIM, facilitando un fraude con datos personales

La autoridad de protección de datos sanciona a una [operadora de telecomunicaciones](#) por vulnerar el artículo 6.1 del RGPD, al realizar un cambio de titularidad de una línea móvil y expedir un duplicado de tarjeta SIM sin el consentimiento del titular y sin aplicar los controles de verificación previstos en sus propios protocolos. La resolución subraya que la entidad, como responsable del tratamiento, debe garantizar la licitud del tratamiento de datos personales, lo que implica no solo disponer de medidas técnicas y organizativas, sino también asegurar su correcta aplicación en cada caso.

Se considera que la omisión de la doble verificación y la falta de comprobación de la identidad del interesado permitieron que un tercero suplantara al titular, accediendo a datos personales y posibilitando un fraude bancario. La AEPD rechaza los argumentos de la entidad sobre la existencia de una base legitimadora y la suficiencia de sus medidas, señalando que la responsabilidad no puede trasladarse a terceros ni eximirse por errores puntuales de agentes o proveedores. La conducta se califica como negligente, ya que la entidad no actuó con la diligencia exigible en el manejo de datos personales.

La sanción impuesta asciende a 300.000 euros, considerando la gravedad, el daño causado y la vinculación de la actividad con el tratamiento masivo de datos personales.

Declarada la existencia de una infracción de la seguridad del tratamiento por el hurto de un equipo informático sin contraseña con información policial sobre desapariciones y condenas

En mayo de 2022 se produjo el hurto de un ordenador y un *pendrive* que estaban en poder de un investigador colaborador del Centro Nacional de Desaparecidos, dependiente de la Dirección General de Coordinación y Estudios (DGCE). Ambos dispositivos contenían información altamente sensible, incluyendo atestados policiales de desapariciones, datos de salud y condenas penales, así como grabaciones de entrevistas a víctimas y familiares. El equipo no disponía de contraseña de acceso, lo que permitía acceder a su contenido directamente.

La DGCE alegó que el tratamiento debía regirse por la Ley Orgánica 7/2021, de 26 de mayo, que transpone la Directiva (UE) 2016/680 y regula los tratamientos efectuados por autoridades competentes con fines de prevención o detección de infracciones penales. Sin embargo, la Agencia consideró que los datos se utilizaban con una finalidad científica y estadística -el desarrollo de la herramienta predictiva SERDESVI- y no en el marco de una investigación penal concreta, por lo que resultaba aplicable el RGPD.

La AEPD [apreció](#) graves deficiencias estructurales en las medidas de seguridad, incluyendo la ausencia de cifrado, contraseñas, copias de respaldo y control de inventario. Además, rechazó que el suceso pudiera considerarse un “error humano aislado”, al evidenciar un fallo sistémico en la gestión de la seguridad del tratamiento y en los protocolos internos de notificación de brechas.

Por todo ello, la Agencia declaró la existencia de una infracción del artículo 32 RGPD, aunque, conforme al artículo 83.7 del RGPD y al artículo 77.2 de la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-gdd), no impuso sanción económica al tratarse de una entidad del sector público. El recurso de reposición interpuesto fue desestimado por la Agencia, que ratificó su resolución.

Multa de 100.000 euros a una empresa de alquiler de coches por denegar la contratación a clientes que aparecían en su lista de exclusión

La AEPD ha [impuesto](#) una sanción de 100.000 euros (reducida a 80.000 euros por pago voluntario) a una empresa de alquiler de vehículos por incluir los datos de un cliente en un sistema interno de alertas que le impedía realizar nuevas reservas, sin disponer de una base legitimadora válida conforme al artículo 6.1 del RGPD.

El caso se remonta a 2018, cuando el reclamante, cliente de la empresa, dejó las llaves del coche a un tercero, produciéndose la desaparición temporal del vehículo. La compañía registró el incidente y vinculó los datos del cliente a una alerta interna que, tres años después, motivó la denegación de un nuevo alquiler. La entidad alegó que el tratamiento se basaba inicialmente en la antigua Ley Orgánica 15/1999 y que, tras la aplicación del RGPD, se amparaba en su interés legítimo, habiendo realizado una ponderación y una evaluación de impacto.

La Agencia rechaza estos argumentos y concluye que las condiciones generales de contratación de 2018 no informaban de la posibilidad de conservar datos para excluir a clientes de futuras contrataciones, por lo que el tratamiento no podía considerarse necesario para la ejecución del contrato. Tampoco aprecia una ponderación válida del interés legítimo ni de la proporcionalidad, considerando desmesurada la creación de listas de exclusión sin prueba objetiva de fraude o impago.

La AEPD equipara el caso a la inclusión indebida en “listas negras” o ficheros de morosidad, al carecer de las garantías exigidas, y declara la infracción del artículo 6.1 RGPD, imponiendo la sanción mencionada.

El acceso al historial clínico de un trabajador para fines organizativos internos del centro de salud constituye una infracción del principio de integridad y confidencialidad

La AEPD ha [declarado](#) la existencia de una infracción del artículo 5.1.f) del RGPD por vulneración del principio de integridad y confidencialidad, imponiendo a la Conselleria de Sanidad de la Generalitat Valenciana un apercibimiento y ordenando la adopción de medidas correctivas en el plazo de tres meses.

El procedimiento se inició a raíz de la reclamación presentada por un profesional sanitario que, durante una situación de incapacidad temporal, detectó numerosos accesos injustificados a su historia clínica por parte de personal del centro de salud en el que trabajaba. Según la denuncia, los datos se comentaron, además, en un grupo de WhatsApp del propio centro.

Durante la tramitación del expediente, la Conselleria solicitó la suspensión del procedimiento por la existencia de diligencias penales paralelas por presunto descubrimiento y revelación de secretos, alegando el principio *non bis in idem*. La Agencia desestimó esta pretensión, señalando que pueden coexistir procedimientos penal y administrativo cuando tutelan bienes jurídicos distintos.

Aunque las diligencias penales concluyeron con un auto de sobreseimiento provisional al considerar que los accesos se realizaron por instrucciones del coordinador y no con ánimo de vulnerar la intimidad del interesado, la AEPD destacó que el derecho a la protección de datos es más amplio que el derecho a la intimidad. Constató que los accesos se efectuaron para comprobar la situación laboral del reclamante, finalidad que no se encuadra en la excepción sanitaria prevista en el artículo 9.2.h) y 9.3 del RGPD, reservada a tratamientos con finalidad asistencial.

En consecuencia, la AEPD apercibe a la Conselleria e insta a implantar medidas técnicas y organizativas que garanticen la confidencialidad de las historias clínicas.

Sancionada una empresa por una brecha de datos en el directorio de usuarios que permitió la publicación de más de 2.600 números de teléfono y alias

La AEPD ha [sancionado](#) a Bizum, S.L. tras notificarse una brecha de datos personales que afectó a 2.634 usuarios del servicio. La entidad sancionada detectó en noviembre de 2023 que en una página web pública figuraban números de teléfono móvil y alias (nombres abreviados) extraídos de su "Directorio Bizum", base de datos que vincula cada número con la identidad del usuario.

La investigación interna reveló que dicho acceso indebido se produjo más de un año antes, en septiembre de 2022, cuando un usuario legítimo de una entidad bancaria, miembro del sistema "Bizum", realizó más de 20.000 consultas automáticas y secuenciales al servicio de validación de usuario, lo que permitió recopilar alias vinculados a múltiples números de teléfono. Aunque Bizum bloqueó ese mismo día al usuario responsable al detectar un volumen anómalo de consultas, no identificó entonces que se había producido una brecha de datos. La publicación posterior de parte de esos registros en Internet obligó a la compañía a comunicar formalmente el incidente y a retirar la información expuesta en la web afectada.

El RGPD exige adoptar medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales y prevenir accesos no autorizados. La AEPD consideró que Bizum vulneró el artículo 32 del RGPD al no haber limitado ni controlado suficientemente el acceso al "Directorio Bizum" ni evaluado adecuadamente los riesgos asociados a la función de consulta de alias. Asimismo, la ausencia de mecanismos eficaces de monitorización permitió que la brecha pasara inadvertida durante más de un año, evidenciando deficiencias en la detección temprana y la respuesta ante incidentes de seguridad. La infracción se calificó como grave conforme al artículo 73.f de la LOPD-gdd, relativo a la falta de medidas de seguridad apropiadas exigidas por el artículo 32.1 del RGPD, atribuyendo a Bizum la carga de probar que había aplicado un nivel de protección adecuado al riesgo, extremo que no consiguió justificar.

La infracción se sanciona con una multa de 100.000 euros, cuantía fijada atendiendo al volumen de negocio y a los criterios de proporcionalidad y efecto disuasorio. Además, la AEPD impuso una medida correctiva: Bizum deberá acreditar en un plazo máximo de seis meses la implantación de mecanismos reforzados de seguridad en su directorio, garantizando que los alias solo puedan consultarse cuando sea estrictamente necesario para la operación y evitando cualquier posibilidad de consultas masivas o automatizadas no autorizadas. Estas exigencias buscan prevenir la reiteración de incidentes y elevar el nivel de protección de los usuarios más allá de la sanción económica.

Multa de 150.000 euros una contratación 'online' fraudulenta de servicios de comunicaciones electrónicas

La [resolución](#) analiza un supuesto de contratación fraudulenta de una línea móvil a nombre de una persona que negó toda vinculación con la entidad sancionada, concluyendo la AEPD la existencia de un tratamiento sin base jurídica en vulneración del artículo 6.1 RGPD y, en consecuencia, imponiendo una multa de 150.000 euros. La investigación constató que el proceso de alta *online* permitido por el operador verificaba únicamente la estructura del DNI, basaba la firma en un PIN remitido por SMS a un número facilitado por el propio solicitante a través de un prestador de servicios de confianza y difería una comprobación visual del DNI a la fase de entrega de la SIM por mensajería, sin acreditación suficiente de su efectiva realización. La Agencia considera que dichas medidas no garantizan la identificación del verdadero titular ni la licitud del tratamiento, y que el contrato de hecho ya se ha formalizado cuando, en su caso, se produce la comprobación en la entrega.

La resolución enfatiza la responsabilidad proactiva del responsable (art. 5.2, 24 y 25 RGPD) y la necesidad de adoptar medidas técnicas y organizativas adecuadas al riesgo (arts. 25 y 32 RGPD) para prevenir suplantaciones. Reitera doctrina de la Audiencia Nacional y del Tribunal Supremo según la cual la intervención fraudulenta de un tercero no excluye la infracción si no se desplegó la diligencia exigible para verificar la

identidad. A efectos de graduación, se valoran la naturaleza y gravedad de la infracción, la negligencia apreciada, el tratamiento de datos de identificación -con especial referencia al DNI como dato particularmente sensible por su potencial lesivo-, el grado de responsabilidad por deficiencias en el diseño de controles, la vinculación de la actividad al tratamiento de datos, y los antecedentes sancionadores. Se rechazan las atenuantes invocadas (remediación posterior, cooperación, ausencia de beneficio y no tratamiento de categorías especiales) por no desvirtuar la necesidad de una sanción efectiva, proporcionada y disuasoria. Se confirma pues la infracción del art. 6.1 RGPD y la multa antes indicada.

Sanción por la difusión de imágenes manipuladas mediante herramientas de inteligencia artificial

El procedimiento sancionador se inició a raíz de una serie de noticias publicadas en medios de comunicación y de la presentación de una reclamación individual. En las actuaciones previas se constató la difusión de las imágenes manipuladas mediante herramientas de inteligencia artificial que asociaban rostros reales a cuerpos desnudos a través de servicios de mensajería y plataformas online.

La [resolución](#) de la AEPD señala que tal difusión constituye un tratamiento de datos personales sin base de legitimación conforme al artículo 6.1 RGPD, y califica a su autor como responsable del tratamiento (art. 4.7 RGPD), al determinar los fines y medios de la difusión. Se recuerda la doctrina sobre el poder de disposición del titular respecto de su imagen y la especial protección reforzada cuando los afectados son menores (art. 84 LOPD-gdd).

A efectos sancionadores, la infracción se encuadra en el artículo 83.5 RGPD (principios básicos y condiciones de licitud), con propuesta inicial de multa de 2.000 euros, valorando la naturaleza de los hechos, su alcance y la afectación a derechos fundamentales. En fase de tramitación, el presunto responsable se acoge al artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones (LPACAP), reconociendo responsabilidad y efectuando el pago voluntario, por lo que se aplican dos reducciones acumulables del 20% cada una,

quedando la sanción en 1.200 euros. La AEPD declara la comisión de la infracción, confirma la sanción resultante y acuerda la terminación del procedimiento, condicionando la eficacia de las reducciones al desistimiento de recursos en vía administrativa.

La resolución enfatiza la ilicitud de la difusión no consentida de imágenes (incluida su manipulación sintética) y la necesidad de prevenir estos tratamientos, advirtiendo de que, de confirmarse hechos similares, podrán imponerse medidas correctivas adicionales (art. 58.2 RGPD) para asegurar el cese de la conducta y la adecuada tutela de los afectados.

La AEPD sanciona a un encargado del tratamiento por la subcontratación en cadena sin autorización del responsable

En la resolución de este procedimiento sancionador, la AEPD [aborda](#) el régimen de responsabilidad en cadenas de subcontratación y los requisitos formales de los contratos de encargado del tratamiento.

Los hechos se originan cuando una interesada, para darse de alta como cotitular en una entidad bancaria, envía documentación sensible, incluyendo copia de su DNI, a través de un servicio de mensajería. La cadena de tratamiento implicaba a una primera empresa encargada del tratamiento por parte de la entidad bancaria, a una empresa de mensajería como subencargado de la primera, y a una tercera empresa como subencargado de la empresa de mensajería. Sin embargo, la documentación nunca llegó al destinatario final.

La investigación de la AEPD reveló que la entidad bancaria, como responsable del tratamiento, únicamente había aprobado la subcontratación de prestaciones de la primera empresa encargada a un proveedor distinto de la empresa de mensajería y la tercera empresa. Por tanto, ni la primera empresa encargada ni la de mensajería contaban con autorización previa y expresa del responsable para recurrir a estos subencargados adicionales.

La AEPD impone dos sanciones de 40.000 euros cada una. La primera, por infracción del artículo 28.2 del RGPD, al recurrir la empresa de mensajería a subencargados sin la preceptiva autorización del responsable del

tratamiento. La segunda, por infracción del artículo 28.4, dado que el contrato de encargado del tratamiento carecía de algunos de los elementos esenciales exigidos por el artículo 28: no identificaba al responsable, no contenía una descripción detallada del tratamiento, omitía la obligación de actuar exclusivamente según instrucciones documentadas del responsable, y las medidas de seguridad se describían de forma genérica e insuficiente.

La resolución subraya que la complejidad operativa de las cadenas de subcontratación no justifica el incumplimiento normativo, recordando que el RGPD exige la identificación del responsable en cada nivel de subencargo.

Sancionada una entidad financiera por una brecha de seguridad que expuso datos de millones de clientes

En noviembre de 2023, una entidad de crédito fue víctima de un ciberataque de tipo denegación de servicio (DDoS), que derivó en un acceso no autorizado a datos personales como nombre, DNI, domicilio fiscal y fecha de nacimiento. Estos datos eran tratados por la entidad tanto en calidad de responsable respecto a sus propios clientes como en calidad de encargado del tratamiento para otras entidades financieras y aseguradoras. El incidente afectó a aproximadamente dos millones de personas, comprometiendo información sensible como el nombre, el número de DNI, el domicilio fiscal y la fecha de nacimiento.

Tras la investigación, la AEPD concluyó en la [resolución](#) que las medidas técnicas y organizativas implementadas por la entidad no eran adecuadas para garantizar la integridad y confidencialidad de los datos personales. Además, la resolución destaca que la entidad financiera no solo falló en la implementación de medidas de seguridad adecuadas, sino que también prolongó la duración de la brecha, lo que incrementó el riesgo de uso indebido y fraude.

Por ello, se consideró vulnerado el principio de integridad y confidencialidad recogido en el artículo 5.1.f) del RGPD, imponiéndose una sanción de 10.000 euros, sin entrar a valorar si

las medidas de seguridad eran conformes con lo exigido por el artículo 32 del RGPD.

Impuesta una multa a una ciudad residencial por la captación de imágenes de sus residentes en el momento de recogida de paquetes

La AEPD [sanciona](#) a una sociedad civil particular que tenía implantado un sistema de recogida de paquetería de los residentes que utilizaba como medio de identificación de quien recogía un paquete la captación de una fotografía. La fotografía se almacenaba en un ordenador y los residentes no habían sido informados sobre este tratamiento de sus datos.

La reclamada, como responsable del tratamiento, estaba tratando la imagen de los residentes a pesar de no ser necesario para el fin perseguido. La AEPD no valida los argumentos relativos a que el tratamiento se limita al momento específico de la entrega, e indica que no consta se haya realizado ninguna valoración de los derechos, libertades e intereses de los afectados, haciendo únicamente referencia a las necesidades organizativas de la urbanización que la sociedad gestiona.

Por todo lo anterior, la AEPD determina que se ha infringido el principio de minimización del dato recogido en el artículo 5.1.c) del RGPD e impone a la reclamada una multa de 2.000 euros.

La AEPD valora positivamente la rapidez en la rectificación en el incumplimiento de la normativa de protección de datos

La reclamada estableció un sistema de registro de jornada consistente en una tableta que actuaba como videocámara de grabación de imágenes, activa en todo momento, y un teclado virtual alfanumérico al lado de la pantalla. El sistema se articula utilizando el número completo del DNI o descargándose un código QR en el propio dispositivo móvil del trabajador y colocándolo delante de la pantalla de la tableta.

La entidad detectó que, erróneamente, la aplicación estaba configurada para capturar imágenes en el momento del fichaje, por lo que solicitó al proveedor de la aplicación que desactivara dicha opción, puesto que la toma de fotos no era necesaria para la gestión del registro horario y no se estaba haciendo ningún tratamiento en ese sentido.

La AEPD [valoró](#) la reacción rápida de la compañía para corregir la configuración errónea, considerando que no hubo intención de utilizar datos de forma desproporcionada, sino que se trataba de un error técnico que fue subsanado en cuanto se detectó. Además, tampoco constaba que la entidad responsable hubiera accedido a las fotografías tomadas ni que estas hubieran sido utilizadas con ninguna finalidad.

Por todo lo anterior, la AEPD decidió no imponer sanción alguna por incumplimiento de la normativa de protección de datos.

Una clínica de estética crea un grupo de WhatsApp con varios de sus clientes sin su consentimiento para proporcionar sus servicios

La AEPD ha [sancionado](#) con 30.000 euros a una clínica de estética por vulnerar el principio de integridad y confidencialidad reconocido en el artículo 5.1.f del RGPD. La clínica creó un grupo de WhatsApp para promocionar sus servicios, incluyendo a varios clientes sin su consentimiento y haciendo visibles sus números de teléfono. Esta acción, dada la propia naturaleza del servicio prestado por la clínica, reveló indirectamente datos de salud de los participantes. Ante las quejas, la clínica abandonó el grupo sin cerrarlo de inmediato, permitiendo que la información siguiera expuesta.

Además de la multa, la AEPD ordenó a la clínica acreditar, en el plazo de un mes, la eliminación del grupo de WhatsApp y, en tres meses, la implementación de sistemas de comunicación que garanticen la confidencialidad de los integrantes, de modo que solo el administrador pueda ver los integrantes del grupo.

La AEPD declara que colocar información en el exterior de un sobre con avisos del tipo "diligencia de embargo" o "notificación providencia de apremio" vulnera el principio de confidencialidad

La AEPD inició un procedimiento sancionador contra un Ayuntamiento por una posible vulneración del principio de confidencialidad, recogido en el artículo 5.1.f del RGPD, tras una reclamación. El Departamento de Recaudación del Ayuntamiento envió dos notificaciones por correo postal certificado a la reclamante en cuyos sobres figuraban de forma visible, respectivamente, las leyendas "diligencia de embargo" y "notificación providencia de apremio", ambas seguidas de un número de referencia.

Aunque el Ayuntamiento corrigió esta práctica durante el procedimiento, sustituyendo las leyendas indicadas por "notificación administrativa", la AEPD [confirmó](#) la infracción del artículo 5.1.f) del RGPD. La AEPD consideró que las leyendas iniciales permitían que terceros conocieran la situación recaudatoria de la parte reclamante. Debido a que el Ayuntamiento había acreditado haber adoptado medidas correctoras, no se consideró necesaria su imposición.

Sanción por incumplimiento del principio de protección de datos desde el diseño y por defecto

El Instituto Nacional de Ciberseguridad de España (INCIBE) organizó un curso masivo *online* (MOOC) cuya plataforma permitió, por error de configuración, que determinados datos personales de los participantes, incluidos nombres, apellidos, correo electrónico, ciudad y país, fueran visibles para otros usuarios sin consentimiento ni información adecuada, lo que se denunció ante la AEPD.

La AEPD instruyó el procedimiento por presunta infracción del artículo 25 del RGPD (protección de datos desde el diseño y por defecto) y del artículo 5.1 f) del RGPD (integridad y confidencialidad del dato). El análisis de hechos probados confirmó que la configuración por defecto de la plataforma permitió la difusión no autorizada de datos personales entre los usuarios y que no se adoptaron adecuadamente las medidas técnicas y organizativas necesarias para protegerlos.

La [resolución](#) archiva el procedimiento por la presunta infracción del artículo 5.1 f) del RGPD, pero sí considera infringido el principio de privacidad desde el diseño y por defecto y, tras valorar las alegaciones y la conducta de la entidad, impone una sanción de 2.000 euros.



Sentencias

Meta, condenada al pago de más de 500 millones de euros por competencia desleal por infracción del RGPD

La [sentencia](#) del Juzgado de lo Mercantil nº 15 de Madrid, de 19 de noviembre de 2025, resuelve una demanda interpuesta por 87 empresas editoras de prensa, agencias de noticias y cadenas de radio españolas contra Meta Platforms Ireland Limited por competencia desleal derivada de infracciones en materia de protección de datos. El período analizado comprende desde el 25 de mayo de 2018 (entrada en vigor del RGPD) hasta el 31 de julio de 2023.

El juzgado determina que Meta infringió el RGPD en sus servicios Facebook e Instagram al realizar publicidad comportamental (publicidad basada en la observación continuada del comportamiento de los usuarios para crear perfiles específicos y ofrecer anuncios personalizados). Las principales infracciones detectadas son:

1. Infracción del artículo 6.1.b) del RGPD (base legal de ejecución contractual): Meta utilizó indebidamente la base legal de "necesidad para la ejecución del contrato" para justificar el tratamiento de datos con fines publicitarios, cuando dicha publicidad no era necesaria ni esencial para prestar el servicio de red social. El Comité Europeo de Protección de Datos (CEPD) concluyó que Meta no tenía derecho a invocar esta base legal para el tratamiento de datos con fines de publicidad comportamental.
2. Infracción del artículo 6.1.f) del RGPD (interés legítimo): entre abril y julio de 2023, Meta cambió su base legal al "interés legítimo", resultando igualmente

ilícito el tratamiento al no superar la ponderación de intereses exigida.

3. Infracción del principio de transparencia (arts. 5.1.a, 12.1 y 13.1.c del RGPD): Meta no informó claramente a los usuarios sobre los fines del tratamiento ni sobre la base jurídica utilizada.
4. Infracción del principio de lealtad (art. 5.1.a del RGPD): se creó una asimetría informativa que colocaba a los usuarios en situación de desventaja sistemática, limitando su control sobre sus datos personales mediante una política de "tómalo o déjalo".
5. Infracción del principio de minimización (art. 5.1.c del RGPD): Meta recopiló datos de forma generalizada e indiferenciada, incluyendo potencialmente categorías especiales de datos (art. 9.1 del RGPD) sin consentimiento explícito.

Se determinó que Meta obtuvo una ventaja competitiva significativa en el mercado publicitario *online* mediante el tratamiento ilícito de datos de usuarios de Instagram y Facebook para publicidad personalizada, infringiendo la normativa de protección de datos. Esta ventaja no pudo ser igualada por sus competidores, los medios de comunicación demandantes.

El juzgado estima parcialmente la demanda y condena a Meta al pago de indemnizaciones por competencia desleal según el artículo 15.1 de la Ley de Competencia Desleal por un importe total de 542.170.719,69 euros.

Conclusiones del TJUE en relación con la necesidad (o no) de autorización judicial previa para incautar correos electrónicos en inspecciones de competencia

El Tribunal de Justicia de la Unión Europea ha hecho públicas las [conclusiones de la abogada general Medina](#) en relación con las incautaciones de correos electrónicos corporativos realizadas por autoridades nacionales de competencia. Según estas conclusiones, el derecho fundamental a la protección de datos personales no exige la existencia de una autorización judicial previa para que una autoridad de competencia acceda a correos electrónicos profesionales en el marco de una investigación. Este acceso se considera compatible con el Derecho de la Unión porque su finalidad es estrictamente empresarial, orientada a la detección de prácticas contrarias a la competencia, y afecta a personas físicas únicamente de manera accesoria.

El caso se originó en Portugal, donde la autoridad nacional de competencia se incautó de correos electrónicos intercambiados entre empleados de varias sociedades investigadas. Estas alegaron que la actuación vulneraba su derecho al secreto de la correspondencia y que la incautación debía contar con autorización de un juez de instrucción y no solo del Ministerio Fiscal. El tribunal portugués elevó el asunto al Tribunal de Justicia preguntando si el hecho de tratarse de correos entre particulares, aun tratándose de direcciones profesionales, exigía un nivel de protección mayor, equiparable al de la correspondencia privada. Posteriormente, la Gran Sala del Tribunal solicitó conclusiones complementarias, especialmente tras la [sentencia Bezirkshauptmannschaft Landeck](#), que había establecido criterios más exigentes cuando la autoridad accede a datos altamente sensibles contenidos en un teléfono móvil.

La abogada general señala que esta jurisprudencia no es extrapolable porque los teléfonos móviles pueden contener información personal detallada sobre múltiples aspectos de la vida privada, mientras que los correos electrónicos corporativos se limitan a contenidos profesionales y no permiten reconstruir la esfera íntima de un individuo. Por ello, no se requiere un grado de protección reforzado ni un control previo judicial obligatorio. No obstante, indica que el acceso a correos electrónicos en una investigación de

competencia constituye una injerencia en la protección de datos que solo será legítima si se adoptan garantías adecuadas, como el respeto del principio de proporcionalidad, el cumplimiento de las obligaciones del RGPD, la existencia de procedimientos formalizados y el control jurisdiccional posterior sobre las actuaciones de inspección.

La intervención judicial previa únicamente sería necesaria cuando la incautación se realizase en un domicilio privado o tuviera por objeto incriminar penalmente a una persona física. Asimismo, recuerda que los Estados miembros pueden optar por exigir mecanismos de autorización previa -incluidos los emitidos por el Ministerio Fiscal- si desean reforzar las garantías en su normativa interna.

La abogada general recomienda que las empresas sujetas a investigaciones de competencia revisen sus protocolos de gestión y acceso al correo corporativo, formen a sus empleados sobre las obligaciones aplicables y documenten adecuadamente la información a la que accedan las autoridades, asegurando que se respeta la minimización y el uso limitado de los datos. Mientras tanto, el Tribunal de Justicia continúa su deliberación, ya que las conclusiones no son vinculantes y la sentencia definitiva se dictará más adelante.

El TJUE niega la exención de responsabilidad a las plataformas que difunden datos personales y las considera responsables del tratamiento

Russmedia Digital SRL, empresa rumana, operaba un mercado en línea en el que los usuarios publicaban anuncios, algunos de ellos con datos personales y datos sensibles de terceros. El litigio dio lugar a una cuestión prejudicial sobre si el operador de la plataforma podía acogerse a la exención de responsabilidad de los prestadores de servicios de alojamiento o si debía considerarse responsable del tratamiento conforme al RGPD.

El Tribunal de Justicia de la Unión Europea (TJUE) [declara](#) que el operador de un mercado en línea que publica anuncios generados por usuarios no puede ser considerado un mero intermediario neutro cuando hace accesibles datos personales de terceros y obtiene un beneficio comercial de dicha difusión.

El Tribunal concluye que la empresa no se limitó a realizar un alojamiento pasivo del contenido, sino que determinó los fines y medios del tratamiento al organizar un mercado en línea con reglas propias, influyendo decisivamente en la difusión de los datos personales, por lo que actúa como responsable (o corresponsable) del tratamiento en el sentido del RGPD. En consecuencia, el TJUE establece que estas plataformas no pueden ampararse en la exención de responsabilidad de la Directiva 2000/31/CE (e-Commerce) para eludir las obligaciones del RGPD.

La sentencia impone a los operadores la obligación de identificar, antes de su publicación, los anuncios que contengan datos sensibles, verificar la legitimación del anunciante y denegar su publicación si no existe consentimiento explícito u otra excepción del artículo 9 RGPD, así como aplicar medidas técnicas y organizativas para evitar la copia y redistribución ilícita de dichos datos.

Sentencia de la Audiencia Nacional en relación con la infracción del artículo 6 del RGPD en actividades de videovigilancia con grabación de voz

La Audiencia Nacional resuelve un [recurso contencioso-administrativo](#) interpuesto contra una resolución de la AEPD de 23 de agosto de 2022 que impuso una multa de 6.000 euros por infracción del artículo 6 del RGPD en el marco de un sistema de videovigilancia instalado en un establecimiento abierto al público. La controversia surge a raíz de la captación no solo de imágenes sino también de sonido, habiéndose grabado una conversación de una trabajadora con una cliente que fue posteriormente referenciada en la carta de despido. Consta la entrega de documentación informativa general sobre cámaras y un "manual de videovigilancia", así como la admisión por la responsable de que el sistema disponía de grabación de audio.

La Sala parte de la premisa de que imagen y voz son datos personales, y realiza la ponderación entre las facultades de control empresarial del artículo 20.3 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores, y los derechos fundamentales de la persona trabajadora, con arreglo al artículo 89 LOPD-gdd y a la doctrina

del Tribunal Constitucional (entre otras, STC número 119/2022 y STC número 98/2000). En esa ponderación, distingue la captación de imágenes -que puede resultar idónea y necesaria en términos de seguridad y control si se cumple el deber de información previa y el principio de proporcionalidad- de la grabación de voz -que es sustancialmente más intrusiva y exige una justificación reforzada, basada en riesgos relevantes para la seguridad y respetando los principios de intervención mínima y proporcionalidad-.

Aplicando ese canon, el Tribunal concluye que, aunque la información previa sobre la existencia de cámaras fue proporcionada, no se informó de modo claro, expreso y específico de la activación de la grabación de sonido ni se acreditó que la misma fuera necesaria y proporcionada para la finalidad de control laboral. La captación de conversaciones permite acceder a contenidos íntimos o irrelevantes para el control de rendimiento, existiendo medios menos invasivos para los fines perseguidos. En consecuencia, el tratamiento de la grabación de audio careció de base jurídica lícita suficiente, vulnerando así lo dispuesto en el artículo 6 del RGPD.

Nuevas aclaraciones del TJUE sobre la interpretación de la Directiva 'ePrivacy' respecto al envío de comunicaciones comerciales por email

Esta [sentencia](#) aborda la relación entre la Directiva *ePrivacy* y el RGPD en el contexto de las comunicaciones comerciales. El litigio surge a raíz de una sanción de la autoridad de protección de datos rumana (ANSPDCP) a una editora rumana por infracción de los artículos 5, 6.1 y 7 del RGPD. La editora enviaba un boletín por *email* a usuarios con cuenta gratuita para incentivar la suscripción de pago y alegaba que no necesitaba consentimiento al amparo del artículo 13.2 de la Directiva *ePrivacy* (la excepción para clientes existentes).

El Tribunal de Justicia de la Unión Europea aclara tres puntos clave sobre la aplicación de la Directiva *ePrivacy*: (i) un boletín con contenido informativo que incentiva el consumo de contenido de pago constituye una comunicación con fines de venta directa en el sentido del artículo 13.1 de la Directiva *ePrivacy*; (ii) la obtención de una dirección de *email* a través de la creación de una cuenta

gratuita, estando además vinculada en este caso a una oferta de suscripción de pago y a un boletín que promueve el acceso *premium*, puede considerarse obtenida en el contexto de una "venta", ya que es una contraprestación indirecta; y (iii) en el caso de realizar comunicaciones comprendidas dentro del ámbito del artículo 13.2 de la Directiva *ePrivacy* (norma especial), la licitud del tratamiento se rige por esta norma especial sin necesidad de una base de legitimación del artículo 6 del RGPD (norma general).

El TJUE se pronuncia sobre los límites de recogida y conservación de datos biométricos y genéticos por parte de la Policía

El TJUE ha resuelto una cuestión prejudicial planteada por un tribunal checo sobre la toma y conservación por la Policía de huellas, fotografías y un perfil de ADN en un procedimiento penal por delitos dolosos. El tribunal remitente cuestionaba la compatibilidad de la normativa checa con la Directiva 2016/680 en tres planos: (i) si puede recogerse indiscriminadamente biometría/ADN de toda persona sospechosa o encausada por delito doloso, a la luz del principio de minimización (artículo 4.1.c del RGPD) y la estricta necesidad para datos relativos a condenas e infracciones penales (artículo 10 del RGPD); (ii) si es posible conservar sin plazo máximo dichos datos; y (iii) qué abarca el "Derecho del Estado miembro" (artículos 8 y 10 del RGPD) como base jurídica: ¿solo norma general o también jurisprudencia nacional?

El fallo de la [sentencia](#) indica que:

- El "Derecho del Estado miembro" comprende una norma de alcance general que establezca los requisitos mínimos de recogida, conservación y supresión, tal como la interprete la jurisprudencia nacional, siempre que esta sea accesible y previsible, por lo que puede utilizarse como base legal para un tratamiento.
- El derecho de la Unión no se opone a una normativa que permita la recogida de datos biométricos o de ADN respecto de sospechosos o encausados por delitos dolosos indistintamente, si (i) los fines específicos y concretos del tratamiento no exigen distinguir entre ambas categorías, y (ii) las autoridades aplican todos los principios (minimización) y el *test* de estricta necesidad con valoración del caso concreto (gravedad y naturaleza del delito, circunstancias, vínculos con otros procedimientos, antecedentes y perfil).

- Es compatible que no exista límite absoluto al plazo de conservación de dichos datos si la ley fija plazos apropiados de revisión periódica y, en cada revisión, se verifica la estricta necesidad de continuar conservando los datos. Las reglas internas policiales pueden usarse como guía, pero no sustituyen la obligación de justificar judicialmente el cumplimiento de la estricta necesidad.

El TJUE exige informar de inmediato al pasajero sobre el uso de cámaras corporales y el tratamiento de sus datos personales

El Tribunal de Justicia de la Unión Europea interpreta el RGPD respecto al [uso de cámaras corporales](#) por revisores en el transporte público, estableciendo que los datos personales obtenidos mediante grabación se consideran recogidos directamente del interesado, aunque este no realice ninguna acción consciente para facilitar los datos. Por tanto, el responsable del tratamiento debe proporcionar cierta información esencial al afectado de forma inmediata, conforme al artículo 13 del RGPD. Esta información incluye la identidad y datos de contacto del responsable, los fines y la base jurídica del tratamiento, los destinatarios, el plazo de conservación y los derechos de acceso y supresión.

El Tribunal aclara que la obtención indirecta de datos solo se da cuando el responsable no tiene contacto directo con el interesado y obtiene los datos de otra fuente. En el caso de obtención directa, la obligación de información puede cumplirse mediante un enfoque multinivel: la información más relevante puede indicarse en una señal de advertencia visible, mientras que el resto debe estar disponible de forma completa y accesible en otro lugar.

La sentencia subraya la importancia de la transparencia y la protección de los derechos de los interesados en el tratamiento de datos personales mediante dispositivos de vídeo, exigiendo que la información se facilite de manera clara y efectiva.

Contacta con nuestros profesionales

Alejandro Padín

Socio · Madrid

alejandro.padin@garrigues.com

Adrián León

Asociado sénior · Alicante

adrian.leon@garrigues.com

Carina Casadesús

Asociada · Barcelona

carina.casadesus@garrigues.com

Ignacio Suárez

Asociado · Madrid

ignacio.suarez@garrigues.com

Laia Llambrich

Asociada · Bilbao

laia.llambrich@garrigues.com

Sebastián Hassi

Asociado principal · Santiago de Chile

sebastian.hassi@garrigues.com

Antonio Durán

Asociado · Málaga

antonio.duran@garrigues.com

Iciar Velasco

Asociada · Madrid

iciar.velasco@garrigues.com

Javier Enebral

Asociado · Madrid

javier.enebral@garrigues.com

Marta Sabio

Asociada · Barcelona

marta.sabio@garrigues.com

Más información:

[Economía del Dato, Privacidad y Ciberseguridad](#)

GARRIGUES

Plaza de Colón, 2 - 28046 Madrid

T +34 91 514 52 00

Síguenos en:



info@garrigues.com

garrigues.com

Esta publicación contiene información de carácter general, sin que constituya opinión profesional ni asesoramiento jurídico

© J&A Garrigues, S.L.P., quedan reservados todos los derechos. Se prohíbe la explotación, reproducción, distribución, comunicación pública y transformación, total y parcial, de esta obra, sin autorización escrita de J&A Garrigues, S.L.P.