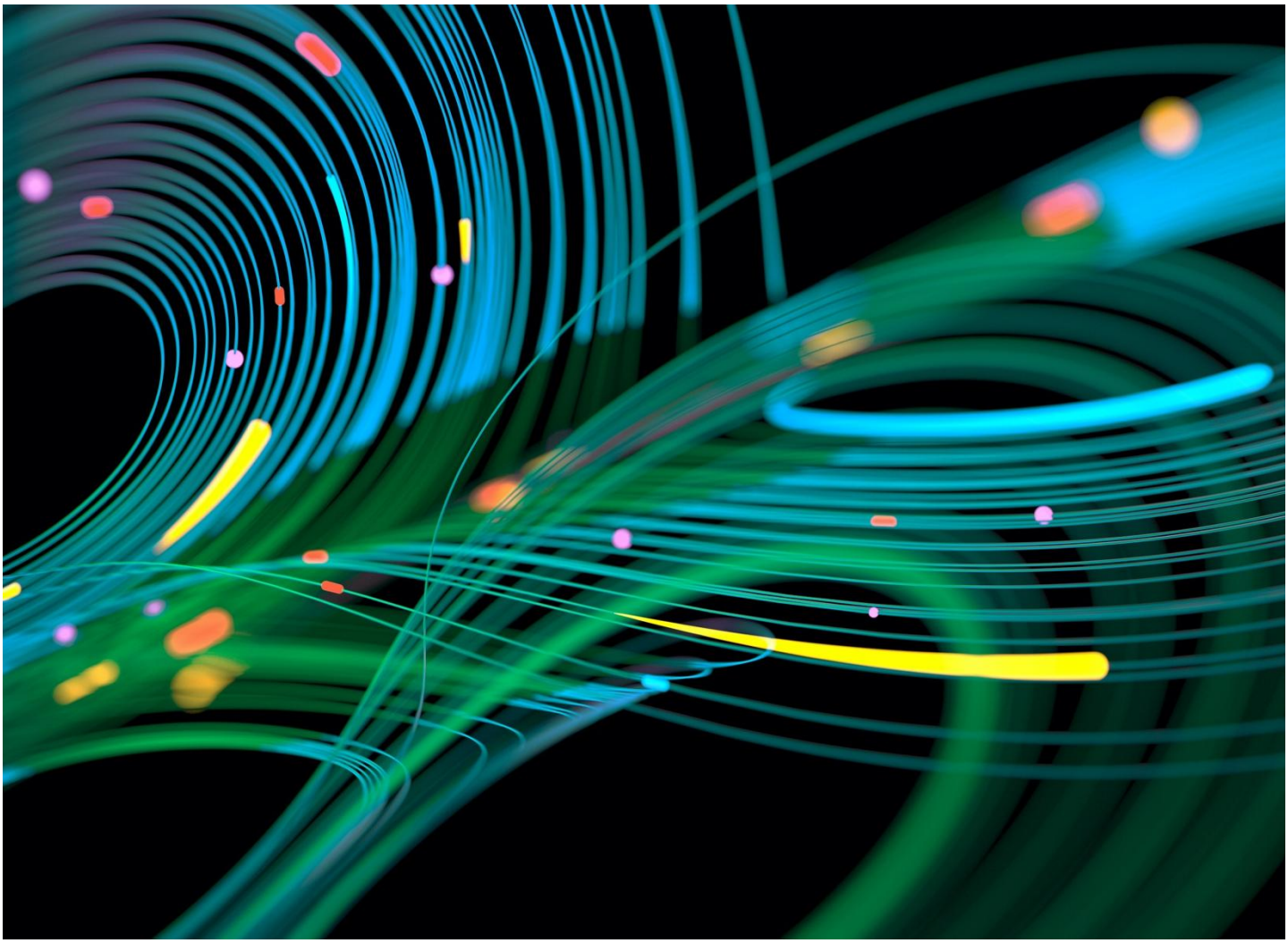
GARRIGUES

Newsletter de Economía del Dato, Privacidad y Ciberseguridad

Octubre de 2026

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



El deber de diligencia digital: la responsabilidad personal de los consejos y sus miembros vinculada a los riesgos tecnológicos



Alejandro Padín

La ciberseguridad ha dejado de ser una cuestión exclusivamente técnica para convertirse en una responsabilidad esencial de gobierno corporativo. La convergencia de la normativa europea en materia de ciberseguridad, resiliencia digital e inteligencia artificial está configurando un nuevo deber de diligencia para los administradores, que exige una implicación directa y continuada en la gestión de los riesgos tecnológicos y puede tener consecuencias sobre su responsabilidad personal.

Hasta hace muy poco, la ciberseguridad formaba parte del ámbito de responsabilidad funcional del director de sistemas de información o del responsable de seguridad informática. Los consejos de administración solo la trataban, cuando lo hacían, tras un incidente relevante y para gestionar sus consecuencias económicas o reputacionales. Era una cuestión técnica, ajena al gobierno corporativo, que no figuraba de forma estable en su agenda ni generaba una preocupación personal entre los administradores. Hoy, esa delegación despreocupada se ha convertido en un riesgo jurídico para cada consejero.

En la Unión Europea existe ya un conjunto denso de normas relevantes -NIS 2, DORA, el Reglamento de Ciberresiliencia, el RGPD y el Reglamento de Inteligencia Artificial-. Este artículo no pretende analizar exhaustivamente ninguna de ellas, sino plantear una tesis de especial importancia para la alta dirección: su convergencia está generando, de facto, un nuevo estándar de diligencia exigible a administradores y altos directivos en materia de ciberseguridad y riesgo tecnológico. Lo denominaremos deber de diligencia digital.

La convergencia regulatoria: una malla de obligaciones dirigidas al órgano de administración

El legislador europeo ha adoptado en pocos años normas con objetos y ámbitos distintos, pero con un rasgo común: imponen obligaciones directas -y no meramente delegables- al máximo órgano de gobierno de las organizaciones afectadas. No es una coincidencia, sino una decisión de política legislativa. Estas son las piezas principales de esa malla regulatoria.

Directiva NIS 2

La Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión es probablemente la norma más explícita al atribuir responsabilidades directas a los órganos de dirección. Su artículo 20 exige que aprueben las medidas de gestión de riesgos de ciberseguridad, supervisen su aplicación y puedan ser considerados responsables de las infracciones cometidas por la entidad. También exige que sus miembros reciban formación específica en ciberseguridad y fomenta una formación periódica para los empleados.

En España, el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad transpone esta directiva mediante la creación del Centro Nacional de Ciberseguridad y el establecimiento del marco institucional y de obligaciones que hará operativas las exigencias de NIS 2.

Reglamento DORA

El Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero, aplicable desde el 17 de enero de 2025, sigue la misma lógica con mayor detalle. Su artículo 5 atribuye al órgano de dirección la responsabilidad última de definir y aprobar la estrategia de resiliencia operativa digital, fijar las funciones y responsabilidades en materia de TIC, determinar la tolerancia al riesgo tecnológico, y aprobar, supervisar y revisar la continuidad del negocio y los planes de recuperación. Las directrices de la EBA adaptadas a DORA refuerzan la implicación del órgano de administración. Además, la obligación de mantener información actualizada sobre los proveedores TIC convierte la supervisión de la cadena de suministro digital en una función de gobernanza.

Reglamento de Inteligencia Artificial

El Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial resulta especialmente relevante por sus exigencias de gestión de riesgos y ciberseguridad. El artículo 9 exige a los proveedores de sistemas de alto riesgo un sistema de gestión continuo e iterativo durante todo el ciclo de vida. El artículo 15 establece que esos sistemas deben ser resilientes frente a intentos de manipulación no autorizados. Para los modelos de IA de uso general con riesgo sistémico se imponen obligaciones reforzadas, incluida la protección frente a ciberamenazas.

Reglamento de Ciberresiliencia

El Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales cierra la malla desde la perspectiva del producto. Impone obligaciones para los productos con elementos digitales durante todo su ciclo de vida: seguridad desde el diseño y por defecto, gestión activa de vulnerabilidades y notificación de incidentes. Su ámbito alcanza a cualquier empresa que fabrique o comercialice productos conectados, por lo que afecta a un espectro muy amplio de la industria europea.

La lectura conjunta de estas normas -y de otras conexas, como el RGPD- conduce a una conclusión inequívoca: la ciberseguridad no puede seguir siendo un asunto meramente delegado. Es una responsabilidad de gobierno corporativo, y quien gobierna responde.

El deber de diligencia digital: un nuevo estándar fiduciario

La acumulación de obligaciones no es una mera superposición de normas sectoriales. En su conjunto, estas disposiciones están cristalizando en un deber de diligencia digital: un estándar fiduciario exigible a los administradores en materia de ciberseguridad, resiliencia digital y gestión del riesgo tecnológico. Es la consecuencia lógica de la convergencia normativa descrita.

El deber general de diligencia de los administradores ha experimentado una progresiva concreción sectorial. Así ocurrió con el *compliance* penal: la responsabilidad de las personas jurídicas obligó a los consejos a implicarse en la prevención de riesgos, aprobar modelos de organización y gestión, establecer órganos de supervisión y dotar de recursos a la función de cumplimiento. Un proceso semejante se produjo en la prevención del blanqueo de capitales, hasta convertir la supervisión del sistema de prevención en un deber personal de los órganos de administración.

La ciberseguridad recorre el mismo camino, pero con una particularidad: la velocidad. El tránsito desde obligaciones genéricas de seguridad, como las del RGPD, hasta un marco detallado de responsabilidades directas se ha producido en apenas unos años. Las empresas y sus consejeros disponen de un margen de adaptación mucho más estrecho.

Este deber presenta cuatro características que lo diferencian de otros estándares de diligencia:

a) Es **continuo**, no puntual. La naturaleza dinámica de las amenazas exige vigilancia permanente. No basta con aprobar una política y archivarla: el consejo debe verificar su adecuación a un entorno de amenazas que cambia por definición y mantenerse informado sobre los riesgos TIC.

b) Es **transversal**. La ciberseguridad afecta a toda la organización: cadena de suministro, datos de clientes, sistemas productivos y propiedad intelectual. El órgano de administración necesita una visión integrada, no fragmentada por departamentos o líneas de negocio.

c) Es **técnicamente exigente**. NIS 2 exige formación específica a los miembros del órgano de dirección. No se puede supervisar eficazmente lo que no se comprende, y la complejidad técnica no puede justificar la pasividad del consejo. La ignorancia tecnológica deja de ser una defensa razonable.

d) Es **personalmente irrenunciable**. El consejero puede y debe apoyarse en expertos internos y externos, pero la responsabilidad de supervisión no se transfiere. NIS 2 y DORA atribuyen la responsabilidad al órgano de dirección y prevén consecuencias personales, incluida, en determinados casos, la inhabilitación temporal de quienes desempeñen funciones directivas.

La convergencia de estas notas configura un estándar que va más allá de la diligencia genérica del ordenado empresario. A medida que la jurisprudencia y la práctica regulatoria le doten de contenido, se consolidará como un parámetro autónomo para enjuiciar la conducta de los administradores.

La inteligencia artificial como factor multiplicador del riesgo de ciberseguridad para el consejo

Si el panorama regulatorio ya impone exigencias significativas, la inteligencia artificial actúa como un factor multiplicador del riesgo y, por tanto, de la responsabilidad en materia de ciberseguridad.

La IA tiene una naturaleza dual. Es una herramienta poderosa para la defensa -detección de amenazas, análisis de anomalías, automatización de respuestas e identificación predictiva de vulnerabilidades-,

pero también un vector de ataque sofisticado: envenenamiento de datos, ataques adversarios, *deepfakes* para ingeniería social, generación automatizada de código malicioso o instrucciones ocultas en documentos de trabajo.

El Reglamento de IA aborda esta dualidad. Los sistemas de alto riesgo deben alcanzar un nivel adecuado de ciberseguridad y ser resilientes frente a manipulaciones no autorizadas. Su sistema de gestión de riesgos debe identificar los riesgos conocidos y razonablemente previsibles, incluidos los cibernéticos, durante todo el ciclo de vida. Para los modelos de uso general con riesgo sistémico las obligaciones son aún más intensas.

La relevancia para los consejos reside en la convergencia de estas obligaciones con las de NIS 2, DORA, el CRA y el RGPD. Una empresa que despliegue IA debe supervisar simultáneamente las exigencias aplicables al sistema, a los datos, a la infraestructura TIC y, en su caso, al producto conectado. Todas esas normas pueden converger sobre un mismo activo tecnológico.

Se crea así una zona de responsabilidad reforzada: la adopción de IA multiplica las obligaciones de ciberseguridad y eleva el estándar de diligencia del órgano de administración. Implementar IA no es solo una decisión de negocio o innovación; tiene implicaciones directas en la responsabilidad personal de los administradores.

Además, la evolución de la IA supera la actualización normativa. El legislador ha optado por principios y gestión de riesgos, en lugar de prescripciones técnicas rápidamente obsoletas. Esa flexibilidad traslada al consejo una responsabilidad interpretativa: determinar qué nivel de ciberseguridad es adecuado para un sistema de IA en cada momento.

Consecuencias prácticas para los órganos de administración

El marco descrito tiene consecuencias inmediatas para la organización de los consejos. Sin pretensión de exhaustividad, pueden destacarse las siguientes:

- En primer lugar, la ciberseguridad debe ser un punto recurrente del orden del día. El consejo debe recibir información estructurada sobre el estado de la seguridad, los incidentes, las vulnerabilidades, las amenazas emergentes y el grado de cumplimiento normativo, con una frecuencia proporcional al perfil de riesgo de la entidad.
- En segundo lugar, la formación de los consejeros no es opcional. Deben adquirir y mantener conocimientos suficientes para comprender los riesgos de su organización y evaluar críticamente las medidas adoptadas. No se trata de convertirlos en expertos técnicos, sino de proporcionarles una interlocución informada que les permita supervisar efectivamente.
- En tercer lugar, deben revisarse las pólizas de responsabilidad de administradores y directivos. Es necesario comprobar que cubren adecuadamente los escenarios derivados de incidentes de ciberseguridad y que la cobertura es coherente con las sanciones y responsabilidades personales previstas por NIS 2. Una cobertura inadecuada puede revelar, además, un déficit de diligencia.
- En cuarto lugar, las organizaciones de cierta dimensión deberán crear o reforzar comités especializados de riesgo tecnológico. Estas estructuras permiten al consejo cumplir sus obligaciones con la profundidad técnica necesaria, sin diluir su responsabilidad final.
- En quinto lugar, la cadena de suministro digital adquiere una dimensión de gobernanza. DORA y el CRA exigen visibilidad sobre los riesgos derivados de la dependencia tecnológica respecto de terceros. Externalizar servicios TIC no externaliza la responsabilidad.
- Finalmente, toda decisión de adopción de IA debe incorporar una evaluación específica de ciberseguridad, tanto desde el cumplimiento normativo como desde el riesgo operativo que el sistema introduce en la organización.

Reflexiones finales

Estamos ante un cambio de paradigma: la ciberseguridad ha dejado de ser un gasto técnico para convertirse en un deber fiduciario. La regulación europea ha trazado un camino hacia la responsabilización personal de los órganos de gobierno en materia de ciberseguridad y resiliencia digital.

El deber de diligencia digital no es una posibilidad teórica. Es el resultado de la lectura conjunta de NIS 2, DORA, el Reglamento de IA, el RGPD y el CRA. Cualquier consejero de una empresa sujeta a estas normas debe saber que su responsabilidad personal está normativamente definida, es supervisada por reguladores con potestades sancionadoras y puede ser exigida judicialmente.

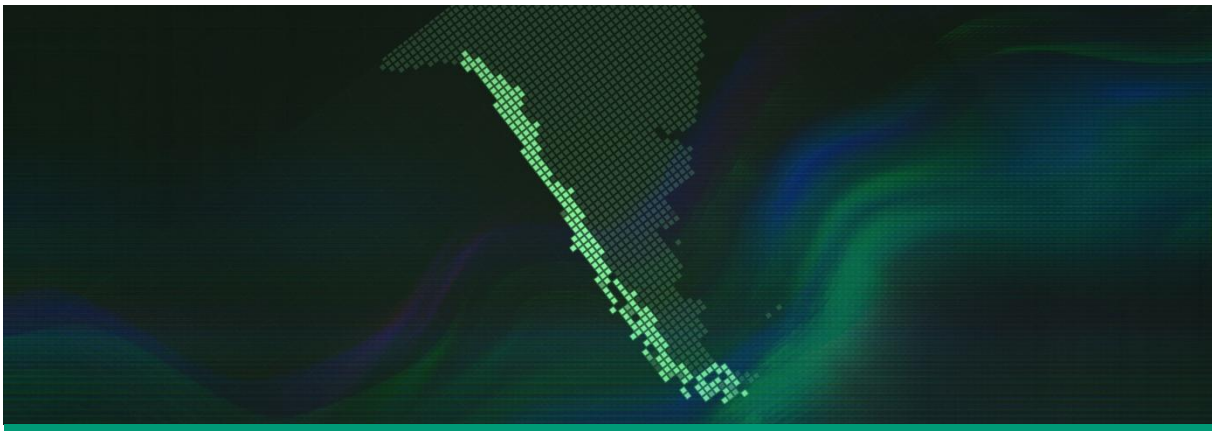
La pregunta ya no es si un consejero debe ocuparse de la ciberseguridad. La pregunta es cuánto riesgo personal está dispuesto a asumir si no lo hace.

La evolución recuerda a la transformación de los factores ESG: de cuestión marginal y voluntaria a pilar de la gobernanza corporativa. La ciberseguridad y la resiliencia digital recorren un camino similar, pero a mayor velocidad y con consecuencias más inmediatas y personales: sanciones directas, responsabilidad de los administradores e incluso inhabilitación temporal en los casos más graves.

La sofisticación creciente de las pólizas de ciberriesgo y de D&O, con coberturas y exclusiones específicas, confirma que no estamos ante una cuestión académica, sino ante una realidad de mercado que los consejos deben integrar en su estrategia y evaluación de riesgos.

En definitiva, la ciberseguridad ha entrado en la sala de consejo para quedarse. Los consejos que comprendan esta realidad no solo cumplirán la ley: protegerán a sus organizaciones, accionistas y a sí mismos. La delegación despreocupada en el departamento de IT ha dejado de ser una opción jurídicamente sostenible.

Chile redefine su marco de privacidad y ciberseguridad con nuevas reglas de cumplimiento y cambios regulatorios en tramitación



Sebastián Barros y Sebastián Hassi

Chile acelera la transformación de su marco de privacidad y ciberseguridad, con posibles cambios en los plazos de adaptación, nuevas pautas de cumplimiento y futuras exigencias para el sector eléctrico. Las empresas deben seguir preparándose ante un escenario regulatorio aún en evolución.

El segundo semestre de 2026 ha sido especialmente relevante para el marco chileno de protección de datos personales y ciberseguridad. Tres desarrollos concentran la atención: (i) el proyecto de ley aprobado por el Senado, y que ahora pasa a la Cámara de Diputadas y Diputados, que posterga al 15 de octubre de 2027 la entrada en vigencia de la ley Nº 21.719; (ii) la publicación del reglamento sobre modelos de prevención de infracciones; y (iii) el texto preliminar de la norma técnica de ciberseguridad para el sector eléctrico de la Comisión Nacional de Energía (CNE). La Agencia Nacional de Ciberseguridad (ANCI), por su parte, dictó un ajuste procedimental relativo a la calificación de operadores de importancia vital y desarrolló iniciativas de implementación que no crean nuevas obligaciones.

Protección de datos personales

Proyecto de ley que propone postergar la entrada en vigencia de la Ley N.º 21.719

Con fecha 28 de octubre de 2026, el Senado aprobó, en primer trámite constitucional, el proyecto de ley que modifica la ley Nº 21.719, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (Boletín N.º 18.623-07), iniciado por mensaje presidencial de 31 de agosto de 2026. El proyecto, que tuvo urgencia de discusión inmediata y fue informado por las comisiones de Constitución y de Hacienda, pasa ahora a la Cámara de Diputadas y Diputados para su segundo trámite constitucional. Sus principales contenidos, en los términos aprobados por el Senado, son:

- **Postergación entrada en vigencia de la ley.** La ley comenzaría a regir el 15 de octubre de 2027, en lugar del 1 de diciembre de 2026. El mensaje proponía originalmente el 1 de

diciembre de 2027; la nueva fecha fue incorporada por la Comisión de Constitución Legislación, Justicia y Reglamento del Senado, y la Comisión de Hacienda no introdujo modificaciones.

- **Consejo Directivo de la Agencia.** Se aumenta de tres a cinco el número de consejeros, que durarán seis años en sus cargos, sin posibilidad de nueva designación y con renovación parcial cada dos años, y se eleva el quórum de funcionamiento de dos a tres.

- **Designación del primer Consejo.** Deberá efectuarse a más tardar nueve meses antes de la entrada en vigencia de la ley (actualmente, seis meses). El presidente de la República propondrá en un solo acto a dos consejeros por seis años, dos por cuatro años y uno por dos años; el Senado se pronunciará sobre la propuesta como una unidad, con el voto favorable de dos tercios de sus miembros en ejercicio. Desde su nombramiento, los consejeros quedarán sujetos a remuneración y dedicación exclusiva.

- **Disposiciones transitorias.** El mayor gasto fiscal del primer año se financiará con el presupuesto del Ministerio de Economía, Fomento y Turismo y, en lo que faltare, con cargo al Tesoro Público. Si al publicarse la ley faltaran menos de doce meses para la entrada en vigencia de la ley Nº 21.719, la primera designación deberá proponerse al Senado dentro de los diez días siguientes. El texto aprobado por el Senado (un artículo único con tres numerales y dos disposiciones transitorias) no contempla la extensión del régimen de amonestación por escrito a todos los responsables de datos.

Es fundamental distinguir entre lo aprobado por el Senado y lo vigente. Mientras el proyecto no concluya su tramitación en el Congreso y sea publicado como ley, la ley Nº 21.719 entrará en vigencia el 1 de diciembre de 2026, conforme a su artículo primero transitorio, y la Agencia mantendrá la composición actualmente prevista. Además, la Cámara de Diputadas y Diputados podría introducir modificaciones al texto.

Para las empresas, la incertidumbre sobre la fecha de inicio no justifica suspender los programas de adecuación. A menos de un mes de la fecha legal, lo prudente es mantener el calendario de cumplimiento, priorizando el inventario de actividades de tratamiento, la determinación de bases de licitud, la revisión de contratos con encargados, los procedimientos para el ejercicio de derechos y la gestión de vulneraciones de seguridad.

Reglamento sobre modelos de prevención de infracciones

El 9 de septiembre de 2026 se publicó en el Diario Oficial el Decreto Supremo Nº 662, de 2025, del Ministerio de Hacienda, que aprueba el Reglamento que regula los requisitos, modalidades y procedimientos para la implementación, certificación, registro y supervisión de los modelos de prevención de infracciones a que se refiere el artículo 49 que la ley Nº 21.719 incorpora a la ley Nº 19.628 (Decreto supremo Nº 662, de 2025, del Ministerio de Hacienda, publicado en el Diario Oficial el 9 de septiembre de 2026).

El modelo de prevención es voluntario: puede ser adoptado por cualquier responsable de datos, persona natural o jurídica, pública o privada, y consiste en un programa de cumplimiento. El reglamento aclara que su adopción no altera el deber general de todo responsable de prevenir infracciones y cumplir la ley. Sus aspectos más relevantes son:

- **Contenido mínimo del programa.** Debe incluir, entre otros elementos, la caracterización de los datos y operaciones de tratamiento (finalidades, bases de licitud, transferencias internacionales, plazos de supresión y decisiones automatizadas); una matriz de riesgos que identifique los procesos con mayor riesgo de infracción, considerando la graduación de sanciones; protocolos específicos de prevención; mecanismos de reporte; sanciones internas, y un canal de denuncia que asegure la reserva de identidad del denunciante.

- **Integración laboral y contractual.** La regulación interna derivada del programa debe incorporarse expresamente como obligación en los contratos de trabajo y de prestación de servicios, incluidos los de los máximos cargos ejecutivos y, cuando corresponda, en el reglamento interno de orden, higiene y seguridad.

- **Delegado de protección de datos.** Su designación es obligatoria en el marco de la adopción y certificación del programa, pero no constituye una exigencia general para todo responsable. Debe ser designado por la máxima autoridad (por ejemplo, el directorio), contar con autonomía respecto de la administración, conocimientos especializados y recursos suficientes, y rendir cuenta directamente ante quien lo designó. Puede ser interno o externo, y un grupo empresarial puede designar un único delegado si opera bajo estándares comunes.

- **Certificación, registro y supervisión.** La certificación se inicia a solicitud del interesado ante la Agencia, tiene una vigencia de tres años renovable y da lugar a la inscripción en el Registro Nacional de Sanciones y Cumplimiento, de acceso público. La Agencia puede supervisar los modelos certificados, requerir información y revocar la certificación, entre otras causales, si el responsable deja de cumplir los requisitos.

El principal efecto jurídico del modelo certificado es su consideración como circunstancia atenuante de las sanciones que imponga la Agencia. Dado que la Agencia aún no se encuentra en funcionamiento, la certificación no es todavía operativa. Sin embargo, el reglamento permite iniciar la implementación con anterioridad a la inscripción en el registro.

Ciberseguridad

Proyecto de Norma Técnica de Seguridad de la Información y Ciberseguridad Industrial para el sector eléctrico

La CNE sometió a consulta pública el texto preliminar de la Norma Técnica de Seguridad de la Información y Ciberseguridad Industrial, entre 28 agosto y el 2 de octubre de 2026. Se trata de una propuesta: sus disposiciones no son exigibles y podrían modificarse antes de su dictación definitiva.

Ámbito de aplicación y relación con la Ley Marco de Ciberseguridad. La norma se aplicaría a las empresas eléctricas, esto es, los coordinados del sistema eléctrico nacional (generadoras, transmisoras, distribuidoras, sistemas de almacenamiento, clientes libres y PMGD, entre otros), las empresas de sistemas medianos y los centros de control común, y al Coordinador Eléctrico Nacional. En seguridad de la información, sus exigencias serían complementarias y aplicables a las empresas que no hayan sido calificadas como operadores de importancia vital (OIV) por la ANCI; las calificadas como OIV se regirían, además, por la ley Nº 21.663 y su normativa complementaria. En ciberseguridad industrial, en cambio, las exigencias alcanzarían a todas las empresas eléctricas y al Coordinador. En todo caso, la Ley Marco prevalecería ante cualquier incompatibilidad, y la fiscalización correspondería a la ANCI en coordinación con la Superintendencia de Electricidad y Combustibles.

Seguridad de la información. Las empresas no OIV se clasificarían en niveles de impacto alto, medio o bajo según criterios objetivos (por ejemplo, más de 100.000 clientes regulados para distribuidoras). Las de impacto alto deberían implementar y certificar un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001, con una declaración de aplicabilidad registrada ante el Coordinador; las de impacto medio o bajo deberían implementar 36 controles mínimos tomados de las normas ISO/IEC 27001 e ISO/IEC 27002. Todas deberían contar con una política de seguridad de la información aprobada por la alta dirección y con una Unidad de Seguridad de la Información y Ciberseguridad Industrial, con un encargado titular y uno suplente, que actúe como contraparte técnica del Coordinador y de las autoridades.

Ciberseguridad industrial. Las empresas deberían proteger sus entornos de tecnologías de la operación conforme al estándar de ciberseguridad para el sector eléctrico publicado por el Coordinador en octubre de 2022, basado en el estándar NERC-CIP. Los requerimientos dependerían del nivel de impacto asignado a cada cibersistema según las instalaciones en que se ubica, como centros de control

o centrales de 300 MW o más. Se admite implementar estándares complementarios, como ISA/IEC 62443 o ISO/IEC 27019, y el Coordinador evaluaría anualmente el nivel de madurez, con una primera medición en 2028.

Plazos propuestos. Desde la publicación, las primeras obligaciones tendrían plazos de uno a cuatro meses (designación de la Unidad, política de seguridad y alcance del SGSI). El SGSI debería implementarse dentro de dos años desde la aprobación de la declaración de aplicabilidad y certificarse dentro de los ocho meses siguientes, mientras que los controles mínimos tendrían plazos de tres o cuatro años según el nivel de impacto. El estándar de ciberseguridad debería implementarse por las empresas en operación en plazos de entre seis meses y un año, según el nivel de impacto del cibersistema.

Para el sector, el proyecto confirma que la determinación de la calidad de OIV será clave para identificar el régimen aplicable y que las exigencias de ciberseguridad industrial alcanzarían igualmente a los OIV. Atendidos los plazos propuestos, es recomendable efectuar desde ya un análisis de brechas.

Modificación de la delegación de firma en la ANCI

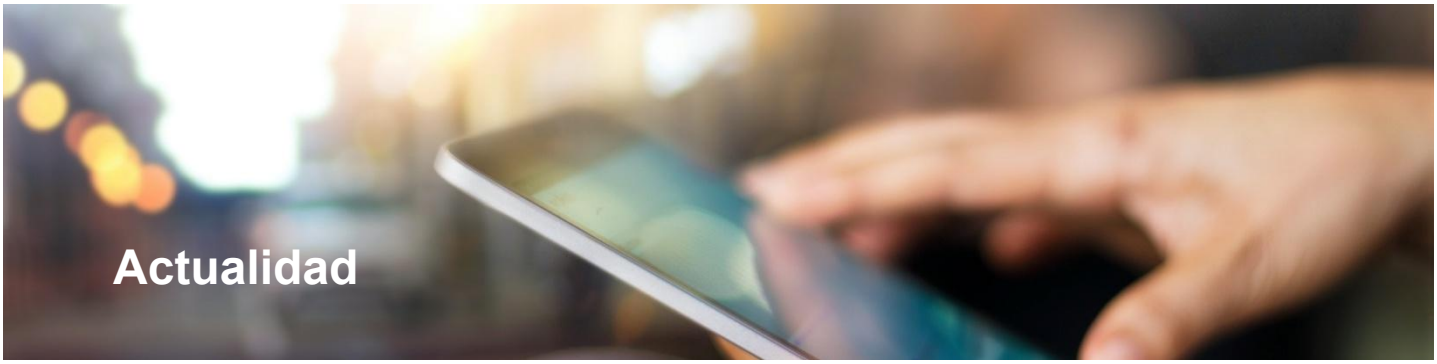
El 9 de octubre de 2026 se publicó la Resolución Exenta Nº 250, de 7 de octubre de 2026, de la ANCI, que modifica la Resolución Exenta Nº 77, de 2025, sobre delegación de la facultad de firmar por orden del director nacional. Junto con ajustes en compras y personal, incorpora, entre los actos delegados, las resoluciones que resuelvan recursos administrativos interpuestos contra actos dictados en el procedimiento de calificación de OIV. La resolución no altera los criterios ni las obligaciones aplicables a los OIV, pero es relevante para las entidades que impugnen su calificación, al determinar quién firma la decisión de sus recursos.

Otras medidas de implementación de la Ley Marco de Ciberseguridad

En el marco del mes de la ciberseguridad, la ANCI informó que en el primer semestre de 2026 recibió 324 reportes de incidentes de efecto significativo de prestadores de servicios esenciales y OIV, y habilitó un portal de reporte ciudadano para comunicar incidentes y vulnerabilidades, de forma identificada o anónima y con una modalidad de puerto seguro. Este canal no sustituye los deberes legales de notificación de las entidades reguladas. La Agencia anunció, además, el primer Ejercicio Nacional de Ciberseguridad, de carácter anual, que se realizará el 29 de octubre de 2026, e incorporó el mecanismo ASPA (del inglés *Autonomous System Provider Authorization*) a la red de conectividad segura del Estado, lo que hace más difícil que terceros la suplanten o puedan desviar su tráfico hacia sitios maliciosos.

Principales implicancias para las empresas

En protección de datos, la fecha legal de entrada en vigencia de la ley Nº 21.719 sigue siendo el 1 de diciembre de 2026, de modo que la postergación propuesta debe tratarse como una contingencia y no como un supuesto de planificación. El Decreto Supremo Nº 662, ya vigente, ofrece un parámetro concreto para organizar la gobernanza interna, la matriz de riesgos y el rol del delegado. En ciberseguridad, las empresas del sector eléctrico deberían confirmar su situación frente a la calificación de OIV y evaluar anticipadamente el impacto del proyecto de la CNE. Las entidades sujetas a la Ley Marco deben, por su parte, mantener sus procedimientos de notificación de incidentes conforme a la normativa vigente.



Actualidad

Recibida la primera notificación en España de una brecha de datos personales ejecutada mediante un agente de inteligencia artificial

La Agencia Española de Protección de Datos ha informado en su blog de la recepción de la primera notificación de una brecha de datos personales en la que el ataque habría sido ejecutado mediante un agente de inteligencia artificial basado en un modelo de lenguaje. Según la información facilitada por la organización afectada, el agente realizó de forma autónoma distintas fases del ataque: identificó vulnerabilidades, accedió correctamente al sistema, analizó la aplicación en busca de nuevas debilidades y consiguió modificar datos personales y acceder a facturas. No obstante, la Agencia aclara que la información disponible es todavía preliminar y que no puede concluirse ni que el modelo de IA estuviera comprometido ni que hubiera sido diseñado con fines maliciosos.

Lo relevante para la autoridad de control es que la inteligencia artificial habría sido utilizada como herramienta para automatizar y encadenar con éxito distintas etapas del ataque. A diferencia de los usos ya conocidos de la IA en campañas de *phishing*, análisis de código o búsqueda de vulnerabilidades, los agentes pueden planificar tareas, utilizar herramientas, interpretar resultados y adaptar su comportamiento de forma autónoma para alcanzar un objetivo concreto.

La AEPD destaca que esta notificación no permite identificar aún una tendencia estadística, pero sí constituye una señal relevante de que los ataques apoyados en agentes de IA han dejado de ser un escenario teórico. Desde la perspectiva de la protección de datos, el incidente pone de manifiesto la necesidad de incorporar expresamente este tipo de amenazas a los análisis de riesgos, reforzar la gestión de vulnerabilidades, proteger credenciales e identidades digitales, y disponer de mecanismos de detección y respuesta capaces de operar a la velocidad que permiten estas tecnologías.

La AEPD publica una nota aclaratoria sobre los conceptos de exactitud, idoneidad y calidad de los datos en tratamientos de datos personales con IA

En esta nota técnica, la Agencia parte de la idea de que la calidad de los datos, que aplica tanto a datos personales como no personales, es un concepto más amplio que el de exactitud previsto en el RGPD.

En este sentido, la Agencia rechaza una visión estricta de la exactitud basada únicamente en que los datos sean verdaderos o estén permanentemente actualizados. Lo relevante es que los datos sean adecuados para cumplir el objetivo del tratamiento. Dependiendo del caso, ello puede exigir atributos como precisión, granularidad, frecuencia de actualización, representatividad o ausencia de sesgos, mientras que en otros contextos la correspondencia exacta con la realidad de cada individuo puede no ser determinante.

En sistemas de IA basados en aprendizaje automático, la AEPD destaca que la calidad debe evaluarse también a nivel del conjunto de datos (*dataset*), ya que factores como la representatividad o los sesgos pueden resultar determinantes para la finalidad perseguida, sin perjuicio de la calidad exigible a los datos individuales cuando estos produzcan efectos sobre las personas. Así, un conjunto de datos

puede contener información individualmente correcta y, sin embargo, resultar inadecuado por falta de representatividad o por incorporar sesgos que afecten al funcionamiento y resultados del sistema.

Asimismo, la AEPD reconoce que determinadas técnicas habituales en el desarrollo de IA, como la anonimización, la generación de datos sintéticos, la corrección de sesgos o la imputación estadística de valores faltantes, pueden introducir datos que no reflejan exactamente la realidad de una persona concreta. Ello no implica necesariamente una infracción del principio de exactitud, siempre que el conjunto de datos siga siendo adecuado para la finalidad perseguida y no genere efectos perjudiciales para los derechos de las personas afectadas.

Finalmente, la Agencia subraya que los requisitos de calidad deben definirse mediante criterios objetivos y revisarse de forma continua durante todo el ciclo de vida de los sistemas de IA. Además, advierte de que exigir niveles de calidad superiores a los realmente necesarios puede entrar en conflicto con el principio de minimización de datos, incrementar costes y dificultar injustificadamente el acceso a datos necesarios para la innovación y la investigación.

La AEPD advierte a una empresa sobre las garantías necesarias antes de implantar una herramienta de inteligencia artificial para analizar currículums

La Agencia Española de Protección de Datos ha remitido una advertencia a una empresa que planeaba implantar una herramienta de inteligencia artificial para analizar currículums, puntuarlos y priorizar candidaturas, tanto en procesos de selección como de promoción interna, si bien la herramienta todavía no se había puesto en marcha.

La Agencia reconoce que la inteligencia artificial puede mejorar estos procesos, pero recuerda varias obligaciones. La empresa debe aplicar la protección de datos desde el diseño, evaluar los riesgos del tratamiento y, si estos son altos, realizar una evaluación de impacto antes de empezar. También debe explicar de forma clara a los candidatos qué papel desempeña la herramienta en su evaluación.

Aunque la empresa había puntualizado que la decisión final la tomaría una persona, la AEPD advierte que esa intervención humana solo es efectiva si quien decide valora la puntuación de forma crítica y no se limita a aceptar el resultado de la herramienta; de lo contrario, podría resultar aplicable el derecho a no ser objeto de decisiones basadas únicamente en un tratamiento automatizado. La propia Agencia aclara que la advertencia, prevista en el artículo 58.2.a) del RGPD, es una medida preventiva y no supone que la empresa haya cometido infracción alguna.

La AEPD analiza los riesgos de exclusión y las amenazas para la protección de datos en la cartera europea de identidad digital

La Agencia Española de Protección de Datos ha publicado en su blog la quinta y la sexta entrega de su serie sobre el Reglamento (UE) 2024/1183 (eIDAS2), dedicadas a los riesgos que plantean las carteras europeas de identidad digital para la inclusión y para la protección de los datos personales de sus usuarios.

En la quinta entrega, la Agencia advierte del riesgo de exclusión. Condicionar el acceso a la cartera a la autenticación biométrica o a determinados documentos de identidad, exigir dispositivos recientes o diseñar procesos de registro complejos y sin soporte humano puede dejar fuera a personas con discapacidad, personas mayores, migrantes o personas con baja alfabetización digital. Además, aunque eIDAS2 prohíbe denegar servicios por no disponer de la cartera, podrían producirse discriminaciones indirectas, como procesos más lentos o solicitudes adicionales de información para quienes no la utilicen.

La sexta entrega analiza tres amenazas: la detección, por la que distintos actores del ecosistema podrían inferir información sensible a partir del comportamiento de las aplicaciones, las respuestas de las API o los registros de actividad, aun sin acceder a los datos; las brechas de datos, cuyo impacto puede ser muy elevado cuando documentos identificativos o datos biométricos se almacenan de forma centralizada o durante periodos prolongados; y

la divulgación excesiva de datos personales más allá de lo estrictamente necesario.

Para mitigar estos riesgos, la AEPD propone aplicar la privacidad desde el diseño mediante la divulgación selectiva de atributos, el tratamiento local de la información, el uso de seudónimos y mecanismos criptográficos avanzados.

La AEPD publica recomendaciones sobre buenas prácticas en el uso de gafas de sol inteligentes con cámara y micrófono integrados

La Agencia Española de Protección de Datos ha publicado un artículo en el que analiza las implicaciones en materia de privacidad derivadas del uso de gafas de sol inteligentes equipadas con cámara y micrófono, dispositivos cuya comercialización se ha extendido notablemente en los últimos meses y que permiten captar imágenes, sonido y otros datos personales de forma poco perceptible para las personas del entorno, a diferencia de lo que ocurre con una cámara o un teléfono móvil convencionales.

En su publicación, la Agencia recomienda utilizar estas gafas con los mismos criterios de prudencia que una cámara o un teléfono móvil, informar de forma transparente cuando se vaya a grabar, prestar especial atención a la captación de audio y limitar las grabaciones a lo estrictamente necesario. También aconseja configurar adecuadamente las opciones de privacidad y seguridad del dispositivo, revisar qué datos adicionales recopilan estos aparatos, como la ubicación o los metadatos asociados a las grabaciones, respetar las restricciones legales existentes en determinados lugares y eliminar las grabaciones cuando ya no sean necesarias.

La publicación resulta de interés en un contexto de creciente popularización de estos dispositivos, en la medida en que su uso por particulares puede implicar tratamientos de datos personales sujetos al RGPD y plantea cuestiones relativas a la captación de imágenes en espacios públicos y privados, la grabación de conversaciones y la eventual aplicación de las normas sobre videovigilancia.

Compatibilidad entre 'blockchain' y protección de datos personales en el marco del RGPD

El Comité Europeo de Protección de Datos (CEPD) ha aprobado las nuevas directrices sobre el tratamiento de datos personales mediante tecnologías *blockchain*, documento cuya elaboración fue liderada por la Agencia Española de Protección de Datos (AEPD). Las directrices tienen como finalidad proporcionar seguridad jurídica a las organizaciones que utilizan esta tecnología y aclarar cómo pueden compatibilizar sus características técnicas con las exigencias del RGPD.

El CEPD reconoce que la principal tensión jurídica deriva de la propia naturaleza de la tecnología *blockchain*, basada en registros distribuidos e inmutables, lo que puede entrar en conflicto con principios fundamentales de protección de datos como la limitación del plazo de conservación, la minimización de datos o el derecho de supresión. No obstante, las directrices concluyen que la utilización de esta tecnología puede ser compatible con el RGPD siempre que se adopte una arquitectura adecuada y una gobernanza orientada a la protección de la privacidad.

Entre los criterios más relevantes, el CEPD desaconseja almacenar datos personales directamente en la cadena de bloques y recomienda que los datos identificativos permanezcan fuera de la *blockchain* (*off-chain*), limitando la información registrada en la cadena a pruebas criptográficas o referencias técnicas que reduzcan el riesgo de identificación de las personas. Asimismo, insiste en la necesidad de aplicar medidas de privacidad desde el diseño y por defecto, incorporando mecanismos de minimización, seudonimización y cifrado desde las fases iniciales del proyecto.

Las directrices subrayan igualmente que los derechos de los interesados previstos en el RGPD -incluidos los derechos de acceso, rectificación, oposición y supresión- siguen siendo plenamente aplicables en entornos *blockchain*. Para ello, se contemplan distintas soluciones técnicas destinadas a garantizar la efectiva anonimización o inutilización irreversible de la información cuando resulte necesario atender dichos derechos.

Por último, el CEPD considera que los tratamientos realizados mediante *blockchain* presentan habitualmente riesgos elevados asociados a la replicación de la información, la descentralización de la red y las posibles transferencias internacionales de datos. Por esta razón, las entidades deberán llevar a cabo una evaluación de impacto relativa a la protección de datos (EIPD) antes de implantar este tipo de soluciones cuando concurran riesgos significativos para los derechos y libertades de las personas.

La aprobación de estas directrices constituye un hito relevante en la aplicación del RGPD en materia de tecnologías descentralizadas.

Publicado el Reglamento Ómnibus de IA que simplifica requisitos y aplaza determinadas obligaciones previstas en la normativa europea de IA

Se ha publicado en el Diario Oficial de la Unión Europea (DOUE) el Reglamento (UE) 2026/1744 del Parlamento Europeo y del Consejo, de 8 de julio de 2026, por el que se modifican los Reglamentos (UE) 2024/1689, (UE) 2018/1139 y (UE) 2023/1230 en lo que respecta a la simplificación de la aplicación de normas armonizadas en materia de inteligencia artificial (Reglamento Ómnibus Digital de IA). Se trata de una iniciativa legislativa europea destinada a simplificar determinadas obligaciones regulatorias que emanan del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de IA), para reforzar la competitividad europea en el ámbito de la inteligencia artificial. La medida forma parte de una estrategia más amplia de simplificación normativa impulsada por las instituciones europeas para reducir cargas administrativas y facilitar la adopción de tecnologías digitales.

Una de las principales novedades consiste en la prórroga de determinados plazos de aplicación y en la revisión de varias obligaciones documentales previstas inicialmente para proveedores y desarrolladores de sistemas de IA. El objetivo es permitir una adaptación más gradual al nuevo marco regulatorio, especialmente para pequeñas y medianas empresas y *start-ups*.

El reglamento introduce asimismo medidas dirigidas a proteger los intereses de menores y la protección de la intimidad, simplificar determinadas exigencias de reporte y suprimir la obligación general de alfabetización en materia de IA que se imponía a todos los operadores, entre otras medidas. La Comisión considera que estas modificaciones permitirán mantener los objetivos de seguridad, transparencia y protección de derechos fundamentales del Reglamento de IA sin generar cargas desproporcionadas para los operadores económicos. Puede consultar más información en este artículo.

La Comisión Europea impone a Google una multa de 890 millones de euros por incumplir la Ley de Mercados Digitales

La Comisión Europea ha impuesto multas por un total de 890 millones de euros a Google, en su rol de guardián de acceso o *gatekeeper*, por incumplir el Reglamento (UE) 2022/1925, de Mercados Digitales (DMA). Las infracciones se refieren al favorecimiento de servicios propios en los resultados de búsqueda y a las restricciones impuestas a los desarrolladores de aplicaciones para informar a los usuarios sobre ofertas disponibles fuera de la plataforma.

En relación con la primera infracción, la Comisión concluyó que el operador otorgaba un trato preferente a sus propios servicios, como compras, hoteles, transporte o resultados deportivos, frente a servicios competidores. Según la autoridad europea, dichos resultados recibían una posición más destacada, con elementos visuales y funcionalidades que no estaban disponibles para terceros, incumpliendo así la obligación de aplicar criterios transparentes, justos y no discriminatorios exigida por la DMA. Por esta conducta, la Comisión impuso una multa de 460 millones de euros.

La segunda decisión se refiere a las restricciones de *anti-steering* aplicadas a través de una tienda de aplicaciones. La Comisión consideró que el operador impedía a los desarrolladores comunicar libremente a los usuarios la existencia de ofertas alternativas o más económicas fuera de la plataforma y limitaba su capacidad para contratar directamente con ellos a través de otros

canales. Asimismo, entendió que las tarifas exigidas para determinadas conversiones de clientes excedían lo permitido por la DMA. Por esta infracción se impuso una multa adicional de 430 millones de euros.

La decisión refuerza el criterio de que los guardianes de acceso no pueden utilizar su posición para favorecer sus propios servicios ni restringir el acceso de empresas y consumidores a alternativas competitivas.

El CEPD publica sus Directrices 04/2026 sobre la imposición de multas administrativas en relación con las demás facultades correctivas del RGPD

El Comité Europeo de Protección de Datos (CEPD) ha publicado las Directrices 04/2026 sobre la aplicación de la facultad de imponer multas administrativas en relación con otras facultades correctivas previstas en el RGPD, junto con la versión final de sus directrices sobre la interacción entre el Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales (Reglamento de Servicios Digitales), y el RGPD.

Según las Directrices 04/2026, las autoridades de protección de datos deben seguir una metodología de cinco pasos a la hora de decidir si imponen una multa administrativa. El documento recapitula las facultades correctivas de las autoridades nacionales y explica su propósito, su alcance y la relación entre ellas. Entre estas medidas correctivas se incluyen las advertencias, las amonestaciones, las órdenes, las limitaciones del tratamiento (incluidas las prohibiciones) y la retirada de la certificación.

Las directrices resultan de interés para responsables y encargados del tratamiento, en la medida en que contribuyen a anticipar cómo razonarán las autoridades de control al elegir entre una sanción económica y otras medidas correctivas, y refuerzan la coherencia en la aplicación del RGPD en los distintos Estados miembros.

Nuevos criterios europeos sobre anonimización de datos y extracción masiva de información para el entrenamiento de modelos de inteligencia artificial

El Comité Europeo de Protección de Datos (CEPD) ha aprobado Directrices sobre anonimización de datos y sobre *web scraping* en el contexto de la IA generativa.

En materia de anonimización, el CEPD aclara cuándo un conjunto de datos puede considerarse realmente anónimo a efectos del RGPD. Un dato será anónimo únicamente cuando ya no permita identificar, directa o indirectamente, a una persona física. Para evaluar la eficacia de la anonimización, propone tres criterios fundamentales: imposibilidad de aislar registros individuales, imposibilidad de vincular datos entre distintas fuentes e imposibilidad de inferir la identidad de una persona. Si los tres requisitos se cumplen, los datos podrán considerarse anónimos.

Respecto al *web scraping* para IA generativa, el CEPD recuerda que la extracción automatizada de datos de internet constituye un tratamiento sujeto al RGPD cuando implica datos personales. Las organizaciones deberán contar con una base jurídica válida, respetar los principios de transparencia, limitación de finalidad, minimización y exactitud, y utilizar preferentemente fuentes fiables y verificadas para el entrenamiento de modelos de IA. Asimismo, se insiste en que el tratamiento de categorías especiales de datos sigue estando, con carácter general, prohibido salvo que concurra una excepción específica prevista en el RGPD.

En conjunto, estas iniciativas refuerzan la posición europea de que el desarrollo de tecnologías emergentes -IA, anonimización avanzada y *blockchain*- debe realizarse garantizando la protección efectiva de los derechos fundamentales y la privacidad de las personas.

La autoridad francesa de protección de datos publica recomendaciones sobre el tratamiento de datos de ubicación de vehículos conectados

La *Commission nationale de l'informatique et des libertés (CNIL),* la autoridad francesa de protección de datos, publicó el 30 de junio de 2026 unas recomendaciones sobre el uso de datos personales de localización en vehículos conectados, dirigidas a fabricantes, gestores de flotas, proveedores de telemática y agregadores de datos.

La guía califica los datos de ubicación como datos altamente personales, sujetos al RGPD y a la Directiva 2002/58/CE, porque revelan desplazamientos, lugares frecuentados y centros de interés. Todo tratamiento debe perseguir una finalidad determinada, explícita y legítima. Cada actor debe identificar su rol: responsable, corresponsable o encargado. Cuando se requiera consentimiento, debe obtenerse antes del tratamiento y ser libre, específico, informado e inequívoco. Además, debe poder retirarse con la misma facilidad con que se otorgó.

En el plano técnico, la CNIL recomienda:

1. minimizar los datos, por ejemplo, conservando solo la última posición cuando sea suficiente;
2. limitar los plazos de conservación;
3. seudonimizar y, cuando sea posible, anonimizar lo antes posible, preferiblemente en el propio vehículo;
4. cifrar los datos en tránsito y en reposo;
5. gestionar las habilitaciones con revisión periódica y registrar los accesos;
6. separar los datos por cliente y por finalidad;
7. realizar una evaluación de impacto cuando exista un riesgo elevado.

La guía exige también informar de forma transparente por varios canales (contrato, pantalla del vehículo, códigos QR y política de privacidad). Además, debe facilitarse el ejercicio de los derechos de acceso, rectificación, supresión y portabilidad.

ENISA activa la plataforma única de notificación del 'Cyber Resilience Act' para vulnerabilidades e incidentes graves

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) ha puesto en funcionamiento la capacidad operativa inicial de la *Single Reporting Platform*, la plataforma única de notificación prevista en el Reglamento (UE) 2024/2847, conocido como *Cyber Resilience Act*. Esta herramienta tiene como objetivo simplificar el cumplimiento de las obligaciones de notificación establecidas por la norma, permitiendo que fabricantes de productos con elementos digitales y responsables de proyectos de *software* de código abierto presenten una única comunicación que será posteriormente trasladada a las autoridades competentes correspondientes.

La puesta en marcha de esta plataforma marca el inicio de la aplicación de una de las obligaciones más relevantes del *Cyber Resilience Act*: la notificación de vulnerabilidades explotadas activamente e incidentes graves de seguridad que afecten a productos digitales. Con ello, la Unión Europea busca mejorar la coordinación entre autoridades y reforzar la capacidad de respuesta frente a amenazas que puedan comprometer la seguridad de productos conectados y servicios digitales.

La creación de un mecanismo único de reporte pretende, además, reducir cargas administrativas para los sujetos obligados y favorecer una gestión más eficiente y homogénea de la información sobre ciberincidentes en el mercado europeo. Esta iniciativa constituye uno de los primeros hitos operativos del *Cyber Resilience Act*, una norma que introduce requisitos de ciberseguridad a lo largo de todo el ciclo de vida de los productos digitales y que persigue elevar los estándares de seguridad de los dispositivos y programas comercializados en la Unión Europea.

El CEPD solicita a la Comisión Europea una base jurídica que permita el intercambio de información entre autoridades reguladoras con competencias distintas

El Comité Europeo de Protección de Datos ha solicitado a la Comisión Europea la creación de una base jurídica específica que habilite el intercambio de información entre autoridades reguladoras con competencias distintas pero complementarias, lo que se conoce como intercambio de información de regulación cruzada. Su objetivo es facilitar la transmisión de información relevante, incluida información confidencial, y mejorar la aplicación coordinada de la normativa de la Unión Europea en un entorno regulatorio cada vez más interconectado.

Según la publicación del CEPD, esta petición responde a la creciente interacción entre los distintos marcos normativos europeos que inciden sobre el entorno digital, entre ellos la protección de datos, la regulación de la inteligencia artificial, los servicios digitales, la resiliencia operativa digital del sector financiero y la ciberseguridad, ámbitos en los que la supervisión eficaz exige con frecuencia la colaboración entre autoridades que operan bajo regímenes normativos diferenciados y que, en ocasiones, carecen de un cauce legal claro para compartir información obtenida en el ejercicio de sus funciones de control.

Asimismo, el CEPD destacó la necesidad de reforzar la cooperación entre las propias autoridades de protección de datos ante el aumento del volumen y la complejidad de los casos, especialmente los relacionados con la inteligencia artificial, impulsando el uso compartido de recursos y las actuaciones conjuntas para garantizar una aplicación más eficaz y coherente del RGPD.

Publicadas las conclusiones de un grupo de más de 100 expertos sobre competitividad, soberanía y seguridad en el ámbito de la IA de frontera

La Oficina Europea de Inteligencia Artificial, organismo adscrito a la Comisión Europea con competencias en materia de supervisión del Reglamento de Inteligencia Artificial, ha publicado un informe que recoge las conclusiones de más de 100 expertos sobre cómo reforzar la posición de la Unión Europea en el desarrollo de la denominada IA de frontera, es decir, los modelos de inteligencia artificial más avanzados del mercado.

Entre las principales recomendaciones figura la necesidad de mejorar las condiciones para atraer inversión y talento, aumentando especialmente la capacidad de computación y la infraestructura energética necesaria para desarrollar y entrenar sistemas avanzados de inteligencia artificial. Los expertos también señalan la importancia de proporcionar mayor seguridad jurídica en ámbitos como la protección de datos y los derechos de autor, cuestión especialmente relevante en la medida en que el entrenamiento de modelos de IA avanzados plantea interrogantes sobre las bases de legitimación del tratamiento de datos personales y la reutilización de contenidos protegidos.

Asimismo, el informe pone el foco en la soberanía tecnológica europea, subrayando que la Unión Europea debe ser capaz de acceder, utilizar y beneficiarse de los modelos de IA más avanzados, incluso cuando estos se desarrollen fuera de sus fronteras. Para ello, considera fundamental aprovechar activos como el tamaño del mercado europeo, su capacidad regulatoria y su fortaleza industrial, así como reforzar la colaboración con socios internacionales de confianza.

Resoluciones

Uber, multado por desactivar automáticamente las cuentas de sus conductores a través de decisiones totalmente automatizadas

El 21 de agosto de 2026, la autoridad neerlandesa de protección de datos (*Autoriteit Persoonsgegevens*) impuso a Uber una multa de 824.990.000 euros por adoptar decisiones totalmente automatizadas sobre sus conductores. Entre los años 2018 y 2022, la compañía utilizó un *software* que controlaba la forma de conducir de los conductores y las valoraciones de los clientes. Cuando el sistema detectaba una sospecha de fraude o valoraciones demasiado bajas, desactivaba automáticamente la cuenta del conductor, de forma temporal o, si las valoraciones bajas persistían, definitiva. Mientras duraba la desactivación, el conductor dejaba de obtener ingresos a través de la plataforma, y en ningún momento intervenía una persona.

Desde el punto de vista de la protección de datos, la autoridad neerlandesa aprecia dos incumplimientos. El primero es la vulneración de la prohibición de decisiones basadas únicamente en tratamientos automatizados que regula el artículo 22 del RGPD: una decisión con consecuencias tan graves como dejar a alguien sin ingresos no puede adoptarla un sistema informático por sí solo, sino que antes debe revisarla una persona. El segundo es que Uber no informó suficientemente a los conductores de la existencia de estas decisiones automatizadas.

La decisión pone de relieve la creciente atención de las autoridades de control al uso de algoritmos en la gestión de trabajadores de plataformas digitales, y la importancia de garantizar una intervención humana real y una información adecuada cuando las decisiones automatizadas producen efectos significativos sobre las personas.

Multa a Google por el tratamiento de datos de localización de sus usuarios sin base jurídica válida ni transparencia suficiente

El 21 de septiembre de 2026, la Comisión de Protección de Datos de Irlanda (*Data Protection Commission*, *DPC*), que actúa como autoridad principal de Google en la Unión Europea, dictó su decisión final contra Google Ireland Limited. La investigación se inició en 2020 por iniciativa de la propia autoridad, a raíz de las quejas de varias organizaciones de consumidores, entre ellas la Organización Europea de Consumidores (BEUC). Se centró en el tratamiento de los datos de localización en tres funciones de Google (Actividad web y de aplicaciones, Historial de ubicaciones y Precisión de la ubicación) entre mayo del año 2018 y febrero del año 2020.

La autoridad irlandesa aprecia cuatro incumplimientos: el primero afecta a los principios de licitud y lealtad, porque el tratamiento de la ubicación en la actividad web y en el historial carecía de base jurídica válida y no se realizaba de forma leal con el usuario. El segundo se refiere a la responsabilidad proactiva: en la función de precisión de la ubicación, Google no pudo demostrar que cumplía el RGPD, lo que recuerda que no basta con cumplir, sino que hay que poder acreditarlo. El tercero es de transparencia, ya que la información facilitada sobre las tres funciones no permitía al usuario entender qué se hacía con su ubicación. El cuarto afecta a la limitación del plazo de conservación, puesto que los datos se guardaban durante más tiempo del necesario.

Por todo ello, la autoridad irlandesa impone multas por un total de 403 millones de euros por la vulneración de los artículos 5, 6, 12 y 13 del RGPD, y ordena a Google adaptar el tratamiento en un plazo de seis meses.

La AEPD sanciona con 2,4 millones de euros a una empresa por una brecha de seguridad que comprometió datos genéticos y de salud

La resolución se enmarca en un procedimiento sancionador incoado frente a una empresa estadounidense dedicada a la realización de pruebas genéticas y análisis de datos genéticos, como consecuencia de una brecha de seguridad que afectó a 2.642 clientes residentes en España. Los hechos tienen su origen en un ciberataque mediante el cual terceros accedieron a cuentas de usuarios utilizando credenciales previamente comprometidas en otros servicios. Como consecuencia, quedó expuesta información especialmente sensible, incluyendo datos genéticos, de salud y datos que revelaban el origen étnico de los afectados; además, parte de la información fue publicada en foros de internet y puesta a la venta en la *dark web*.

La AEPD concluye en su resolución que la entidad vulneró el artículo 5.1.f) del RGPD al no implementar medidas de seguridad adecuadas al riesgo del tratamiento. La Agencia destaca que el acceso a las cuentas se realizaba únicamente mediante usuario y contraseña, que la autenticación multifactor era opcional y que no existían límites o controles suficientes para el acceso y descarga masiva de datos. Por esta infracción, la AEPD impone una multa de 2.000.000 euros.

Asimismo, la Agencia considera vulnerado el artículo 33 del RGPD por la notificación tardía de la brecha. Aunque la entidad tuvo constancia suficiente de que se había producido una violación de seguridad el 5 de octubre de 2023, no notificó la brecha a la AEPD hasta el 17 de octubre, excediendo ampliamente el plazo máximo de 72 horas previsto en el RGPD. Por esta infracción se impone una sanción adicional de 400.000 euros.

Multado un operador de telecomunicaciones por una brecha de seguridad sufrida por su proveedor

La AEPD ha sancionado a un operador de telecomunicaciones por una brecha de seguridad que se produjo en los sistemas de uno de sus proveedores. Ese proveedor había desarrollado la aplicación de un servicio de *wifi* del operador y, a través de ella, trataba datos de sus clientes. En noviembre del año 2023 sufrió un ciberataque en el que un tercero accedió a sus sistemas con credenciales legítimas, de manera que quedaron expuestos el correo electrónico y, en parte de los casos, el nombre y apellidos de miles de clientes, datos que acabaron a la venta en internet.

El operador alegó que la brecha se había producido en los sistemas del proveedor y que había firmado con él un contrato de encargo con instrucciones de seguridad. La AEPD rechaza este argumento en su resolución por dos razones: la primera es que el responsable del tratamiento responde de lo que hacen sus encargados, salvo que estos decidan los fines y los medios del tratamiento, lo que no ocurrió en este caso; además, es responsable de supervisar que el encargado cumpla y no limitarse a imponerle meras obligaciones formales. La segunda es que, cuando se produjo la brecha, no existía un contrato válido: se firmó en septiembre del año 2024, casi un año después del ataque, aunque indicaba que estaba en vigor desde diciembre del año 2022. Para la Agencia, esa vigencia retroactiva no sirve, pues el contrato de encargo debe estar firmado por escrito antes de que el encargado empiece a tratar datos.

En consecuencia, la AEPD impone tres multas: 500.000 euros por vulnerar el principio de integridad y confidencialidad del artículo 5.1.f) del RGPD; 150.000 euros por no aplicar medidas de seguridad adecuadas conforme al artículo 32 del RGPD; y 100.000 euros por no tener firmado el contrato de encargo exigido por el artículo 28 del RGPD cuando se produjo la brecha.

Sancionada una empresa de compraventa de vehículos por una brecha de datos personales, información insuficiente sobre plazos de conservación y falta de medidas de seguridad

La AEPD ha impuesto sanciones por un total de 680.000 euros a una empresa del sector de compraventa de vehículos de ocasión tras constatar tres infracciones del RGPD derivadas de una brecha de datos personales que provocó una pérdida de confidencialidad y afectó a un número significativo de interesados.

La AEPD apreció una infracción del artículo 5.1.f) del RGPD, relativo al principio de integridad y confidencialidad, al considerar que las medidas de seguridad existentes con anterioridad a la brecha resultaban insuficientes para evitarla o, al menos, mitigar sus efectos. Por esta infracción se impuso una multa de 400.000 euros. También se declaró la infracción del artículo 13 del RGPD, al constatarse que la información facilitada a los clientes no cualificados sobre el plazo de conservación de sus datos era insuficiente, ya que no detallaba adecuadamente dicho plazo. La sanción por este incumplimiento ascendió a 30.000 euros. Por último, la Agencia declaró la infracción del artículo 32 del RGPD, al apreciar que la empresa no había adoptado medidas adecuadas para garantizar un nivel de seguridad apropiado respecto de los datos personales bloqueados de antiguos potenciales clientes. Esta infracción fue sancionada con una multa de 250.000 euros.

Además de las sanciones económicas, la resolución ordena a la empresa acreditar, en el plazo de un mes desde su firmeza, que su política de privacidad ofrece información más detallada sobre el plazo de conservación, especialmente para los clientes no cualificados, y, en el plazo de cuatro meses, acreditar la adopción de medidas adecuadas para cumplir las exigencias de seguridad del RGPD respecto del bloqueo de datos.

Sancionada una comercializadora eléctrica por una configuración inadecuada de permisos y deficiencias en el control de accesos

La AEPD ha sancionado a una comercializadora eléctrica tras un incidente de seguridad en el que terceros utilizaron credenciales sustraídas a un proveedor autorizado para acceder a datos identificativos, de contacto, bancarios, contractuales y de facturación de clientes. Aunque el acceso inicial se produjo mediante credenciales legítimas, el usuario comprometido tenía asignados erróneamente permisos que le permitían consultar la cartera general de clientes, en lugar de limitarse a la información necesaria para la actividad comercial encomendada.

La Agencia consideró que la utilización ilícita de credenciales no eximía a la comercializadora de responsabilidad. La incorrecta configuración de los roles permitió que el incidente alcanzara información a la que el proveedor no debía acceder, lo que evidenciaba una falta grave de diligencia. Asimismo, constató deficiencias adicionales en la gestión de accesos, como la utilización compartida de una misma cuenta por aproximadamente 120 trabajadores, la falta de trazabilidad individual, la ausencia de caducidad de las credenciales y la exposición pública de las aplicaciones sin restricciones adicionales suficientes.

La AEPD distinguió entre la vulneración del principio de integridad y confidencialidad del artículo 5.1.f) del RGPD, derivada del acceso efectivo a los datos, y el incumplimiento autónomo del artículo 32, relativo a la ausencia de medidas de seguridad adecuadas al riesgo. También rechazó suspender el procedimiento por la investigación penal del ataque, al no existir identidad entre el responsable administrativo y el presunto autor del delito.

En consecuencia, impuso multas de 400.000 euros por la infracción del artículo 5.1.f) y de 275.000 euros por la infracción del artículo 32 del RGPD, además de ordenar la adopción y acreditación de medidas correctoras en el plazo de tres meses.

Sancionado el Servicio de Salud irlandés con 645.000 euros por deficiencias en el almacenamiento y conservación de registros médicos en papel

La Comisión de Protección de Datos de Irlanda ha impuesto una multa de 645.000 euros al Servicio de Salud irlandés tras una investigación sobre el almacenamiento y conservación de datos personales contenidos en registros en papel. La investigación se inició a raíz de varias brechas de seguridad relacionadas con accesos no autorizados a historiales médicos almacenados en antiguos hospitales psiquiátricos y se amplió con inspecciones a doce instalaciones de almacenamiento en todo el país.

La autoridad irlandesa constató que el Servicio de Salud incumplió sus obligaciones en varios ámbitos. En materia de seguridad, no se garantizaron controles adecuados de seguridad ni de gestión documental; los inspectores encontraron registros dañados por moho, agua y excrementos de animales, así como documentos almacenados en baños en desuso, contenedores marítimos y edificios en ruinas. En relación con la conservación, se retuvieron datos personales durante más tiempo del necesario, vulnerando el principio de limitación del plazo de conservación del RGPD. Además, no se notificaron algunas brechas dentro del plazo obligatorio de 72 horas ni se informó a determinados interesados sobre las brechas que les afectaban.

Además de la multa, la autoridad ordenó al Servicio de Salud auditar todas sus instalaciones de almacenamiento de registros en papel, mejorar los sistemas de seguimiento y gestión documental, destruir los registros que ya no sean necesarios y trasladar aquellos que se encuentren en ubicaciones inadecuadas. La decisión subraya que las obligaciones en materia de protección de datos se aplican con independencia de que la información se conserve en formato digital o en papel, y pone de relieve la importancia de la responsabilidad institucional y de los plazos de conservación.

Multa de 510.000 euros a una entidad bancaria por exigir documentación hereditaria excesiva y no informar adecuadamente del tratamiento de datos

La AEPD ha sancionado a una entidad del sector bancario por el diseño de su procedimiento de gestión de herencias, al considerar que obligaba a los herederos a aportar una escritura completa de aceptación, partición y adjudicación de herencia, lo que permitía acceder a información patrimonial ajena a los productos bancarios objeto de la tramitación.

La autoridad concluye que esta práctica vulnera el artículo 25 del RGPD (protección de datos desde el diseño y por defecto). Según la resolución, el procedimiento interno de la entidad no respetaba adecuadamente el principio de minimización de datos, ya que se configuró de manera que implicaba tratar información patrimonial del fallecido y de los herederos que no resultaba necesaria para gestionar los productos bancarios afectados por la sucesión. La AEPD destaca que la normativa y los criterios del Banco de España permiten, en determinados casos, acreditar la partición de la herencia mediante documentos privados firmados por los herederos, sin necesidad de aportar una escritura pública íntegra.

Además, la AEPD aprecia una infracción del artículo 13 del RGPD al no acreditar la entidad que hubiera facilitado a los interesados la información exigida sobre el tratamiento de sus datos personales en el momento de su recogida. Tampoco consideró suficiente la mera existencia de una política de privacidad publicada en la página web de la entidad, al no constar que dicha información hubiera sido efectivamente puesta a disposición de los afectados.

Por estos hechos se impusieron multas de 500.000 euros por la infracción del artículo 25 y de 10.000 euros por la infracción del artículo 13. La infracción inicialmente investigada del artículo 30 del RGPD, relativa al registro de actividades de tratamiento, fue finalmente archivada. Tras acogerse al pago voluntario, la sanción quedó reducida a 408.000 euros.

Sancionado un operador de telecomunicaciones con 900.000 euros por deficiencias de seguridad y de supervisión de sus encargados tras sendos ataques de 'ransomware'

La AEPD ha sancionado en dos procedimientos distintos a un operador de telecomunicaciones por sendas brechas de datos personales originadas en ataques de *ransomware* contra sistemas gestionados por proveedores externos que actuaban como encargados del tratamiento. En ambos casos, la Agencia concluyó que el operador no había implantado medidas de seguridad adecuadas al riesgo, en vulneración del artículo 32 del RGPD.

En el primer caso, analizado en esta resolución, el ataque se produjo en noviembre de 2023 sobre una plataforma mantenida por un proveedor tecnológico y afectó a la confidencialidad y disponibilidad de los datos de 724.733 clientes. El atacante accedió a través de una cuenta genérica con una contraseña débil y sin autenticación multifactor, en una red privada virtual (VPN) que formaba parte de la propia infraestructura del operador, por lo que la Agencia consideró que se trataba de una deficiencia estructural imputable al responsable. Aunque inicialmente imputó también una infracción del artículo 5.1.f) del RGPD, la AEPD calificó finalmente los hechos como una única infracción del artículo 32 e impuso una multa de 500.000 euros.

En el segundo caso, recogido en esta otra resolución, la brecha tuvo su origen en los sistemas de un encargado que prestaba servicios de gestión de incidencias y afectó a más de 486.000 clientes particulares y a miles de autorizados de empresas. Aunque parte de la información estaba cifrada, los números de teléfono y otros identificadores seguían siendo accesibles. La Agencia apreció falta de diligencia en la supervisión del proveedor, porque existían antecedentes recientes de ciberataques y vulnerabilidades críticas conocidas que no se habían corregido, e impuso una multa de 400.000 euros, si bien valoró como atenuante las medidas correctoras adoptadas tras el incidente.

Ambas resoluciones aplican un mismo criterio: contratar a un encargado del tratamiento y fijarle por contrato obligaciones de seguridad no exime al responsable, que debe comprobar mediante auditorías y controles efectivos que esas medidas se aplican realmente. Solo cuando el encargado trata los datos para sus propios fines, conforme al artículo 28.10 del RGPD, puede trasladarse a él la responsabilidad.

Sancionada una empresa de seguridad por utilizar un número 902 para el ejercicio de derechos de protección de datos en carteles informativos

La AEPD ha sancionado a una empresa de seguridad privada por incluir en determinados carteles informativos de videovigilancia la indicación "derecho de acceso y oposición en el tel. indicado", remitiendo a los interesados a un número 902. La reclamación fue presentada por la asociación de consumidores FACUA-Consumidores en Acción, que consideraba que dicho sistema dificultaba el ejercicio de los derechos reconocidos por la normativa de protección de datos.

La Agencia recordó que el artículo 12 del RGPD obliga a los responsables del tratamiento a facilitar el ejercicio de los derechos de los interesados y que los medios ofrecidos deben ser fácilmente accesibles. Aunque la entidad disponía de canales alternativos gratuitos a través de su página web y de su delegado de protección de datos, la AEPD entendió que la existencia de otras vías no eliminaba la relevancia jurídica del mensaje incluido en el cartel, que dirigía expresamente a los afectados hacia un número de teléfono de tarificación especial para ejercer los derechos de acceso y oposición.

La resolución destaca que los números 902 implican para el usuario un coste superior al de una llamada ordinaria y, por regla general, no están incluidos en las tarifas planas de telefonía. Por ello, la Agencia concluyó que remitir a los interesados a este tipo de numeración no constituye un medio que facilite efectivamente el ejercicio de derechos en los términos exigidos por el RGPD. Asimismo, consideró especialmente relevante que la práctica se hubiera mantenido durante años y en un volumen muy elevado de dispositivos informativos instalados por la compañía.

En consecuencia, la AEPD declaró la infracción del artículo 12 del RGPD e impuso una multa de 100.000 euros, además de ordenar la sustitución de los carteles afectados por otros que respetaran las exigencias de la normativa de protección de datos en el plazo de doce meses.

La AEPD multa con 100.000 euros a la RFEF por recabar datos innecesarios para la inscripción de una menor

La AEPD ha sancionado a la Real Federación Española de Fútbol por exigir conjuntamente un certificado de empadronamiento y certificados escolares para inscribir a una menor nacida y residente en España, pero de nacionalidad extranjera. La documentación se solicitaba para acreditar que la jugadora había residido ininterrumpidamente en España durante al menos cinco años, requisito previsto en la normativa de la Federación Internacional de Fútbol Asociación (FIFA) sobre inscripción de menores.

La Real Federación Española de Fútbol (RFEF) defendió que ambos documentos eran necesarios para acreditar la residencia efectiva y prevenir situaciones de explotación o desarraigo de menores. Sin embargo, la Agencia observó que la guía oficial y vinculante de la FIFA contempla el certificado de residencia y los certificados escolares como medios alternativos, no acumulativos. Por tanto, si cualquiera de ellos resulta suficiente para acreditar la residencia continuada, exigir ambos implica recabar datos adicionales sin una finalidad distinta que justifique su tratamiento. La AEPD añadió que las comunicaciones aportadas sobre una supuesta práctica de la FIFA no acreditaban que ambos documentos debieran exigirse sistemáticamente.

En consecuencia, la Agencia declaró la infracción del artículo 5.1.c) del RGPD por vulneración del principio de minimización de datos e impuso una multa de 100.000 euros. Asimismo, ordenó a la RFEF adaptar, en el plazo de dos meses, el tratamiento realizado en estos procedimientos de inscripción para limitar los datos recabados a los estrictamente necesarios.

La AEPD recuerda que el bloqueo de los datos no exime de atender el derecho de acceso

En su resolución del caso PD-00073-2026, la AEPD da una serie de apuntes sobre el derecho de supresión y su interacción con la obligación de bloqueo prevista en la LOPD-gdd, así como sobre el derecho de acceso.

Si bien no supone un cambio radical del entendimiento de estos conceptos por parte del supervisor, es una resolución que conviene revisar, pues refresca una serie de conceptos que se prestan al debate, como son las implicaciones del bloqueo y su interacción con ambos derechos citados.

En relación con el derecho de supresión, la AEPD indica cómo la supresión de los datos debe llevarse a cabo a través del bloqueo, por lo que el ejercicio del derecho de supresión no conlleva, necesariamente, el borrado físico de los datos en ese preciso instante. Por su parte, en relación con el derecho de acceso, la AEPD recuerda que “cuando se ejercita el derecho de acceso, no cabe aceptar que, en caso de que los datos personales solicitados se encuentren bloqueados, se pretenda dejar sin respuesta el derecho de acceso ejercitado”. Es decir, ante un derecho de acceso se deberán consultar los datos bloqueados, procediendo en su caso a facilitarlos como parte del derecho ejercitado.

De nuevo, sin ser estas materias especialmente novedosas, dado el frecuente debate que suscitan estos conceptos, esta resolución es de elevado interés, pues contiene el criterio conocido más reciente de la AEPD al respecto.

Una universidad comete una infracción al divulgar la condición de víctima de violencia de género en un procedimiento selectivo

La AEPD ha declarado la comisión de una infracción por parte de una universidad española al incluir, en la resolución de una reclamación presentada en un proceso selectivo, información que permitía identificar a una candidata como víctima de violencia de género. La resolución fue notificada a otra aspirante interesada en el mismo

procedimiento tras la acumulación de ambas reclamaciones.

La Universidad defendió que la comunicación estaba amparada por el derecho de acceso al expediente y por la necesidad de motivar adecuadamente la decisión adoptada en el concurso público. No obstante, la Agencia consideró que la identificación de la candidata junto con la referencia expresa a su condición de víctima de violencia de género excedía de lo estrictamente necesario para garantizar el derecho de defensa de los demás interesados.

La AEPD recuerda que el derecho de acceso al expediente en procedimientos administrativos no es absoluto y debe compatibilizarse con los principios de protección de datos. En particular, destaca que el principio de minimización exige limitar la información comunicada a aquella que resulte adecuada, pertinente y necesaria para la finalidad perseguida, pudiendo emplearse técnicas de anonimización o seudonimización cuando concurran datos especialmente sensibles.

En consecuencia, la Agencia declaró la infracción del artículo 5.1.c) del RGPD por vulneración del principio de minimización de datos y ordenó a la Universidad adoptar, en el plazo de tres meses, las medidas necesarias para garantizar el cumplimiento de dicha obligación en sus procedimientos.

Sancionada una empresa por no tener suficientes medidas de seguridad en un tablón de anuncios sobre afectados por un despido colectivo

La AEPD ha sancionado a una compañía española por incumplir las obligaciones de seguridad previstas en el artículo 32 del RGPD al poner a disposición del comité de empresa un tablón de anuncios que carecía de medidas de protección adecuadas. La actuación se produjo tras comprobarse que, en dicho tablón, se había publicado el acta de un procedimiento de despido colectivo junto con un anexo que contenía datos personales de los trabajadores afectados, incluyendo nombres, DNI, datos de afiliación a la Seguridad Social, fechas de nacimiento y otros datos laborales.

La Agencia distinguió entre la responsabilidad derivada de la publicación concreta de la documentación -atribuible a la persona que la colocó materialmente en el tablón- y la responsabilidad de la empresa por no haber implantado medidas técnicas y organizativas adecuadas sobre el propio sistema de publicación. En particular, se constató que el tablón carecía de cerramiento o control de acceso, no existían medidas suficientes para limitar quién podía publicar o retirar documentos, y no se acreditó la formación o instrucciones adecuadas en materia de protección de datos para las personas autorizadas a utilizarlo.

La AEPD recuerda que el artículo 32 del RGPD exige realizar un análisis de riesgos y adoptar medidas de seguridad apropiadas atendiendo a la naturaleza y finalidad del tratamiento. En el ámbito laboral, ello implica garantizar que únicamente las personas legitimadas puedan gestionar los contenidos publicados y que el tratamiento de datos personales se realice conforme a los principios de protección de datos.

En consecuencia, la Agencia declaró la infracción del artículo 32 del RGPD por falta de adopción de medidas técnicas y organizativas adecuadas, y acordó imponer a la compañía una multa de 15.000 euros, reducida respecto de la inicialmente propuesta al apreciarse determinadas circunstancias atenuantes relacionadas con las condiciones de acceso al centro de trabajo y la situación de la empresa.

La AEPD sanciona a una entidad de diagnóstico médico por imagen por no contar con medidas adecuadas para detectar brechas de seguridad

La resolución se enmarca en un procedimiento sancionador incoado frente a una entidad dedicada a la realización de pruebas de diagnóstico por imagen, como consecuencia de una brecha de seguridad que comprometió los datos personales de 1.352 pacientes. Los hechos tienen su origen en un ciberataque sufrido en julio de 2024, mediante el cual terceros no autorizados accedieron a los sistemas de la entidad y exfiltraron información de pacientes, entre la que se encontraban datos relativos a la salud, categoría especialmente protegida conforme al artículo 9 del RGPD.

La AEPD concluye en su resolución que, con independencia de que no pudiera determinarse con exactitud el vector de entrada del ataque, la entidad no disponía de medidas técnicas y organizativas adecuadas al riesgo del tratamiento, tal y como exige el artículo 32 del RGPD. La Agencia destaca especialmente las deficiencias en los mecanismos de detección temprana de incidentes de seguridad, ya que la entidad no tuvo conocimiento de la brecha hasta recibir las comunicaciones de extorsión remitidas por el propio atacante, lo que evidencia una ausencia de sistemas de monitorización capaces de identificar accesos o exfiltraciones anómalas de forma proactiva.

En consecuencia, la AEPD considera vulnerado el artículo 32 del RGPD al no garantizarse un nivel de seguridad adecuado para unos tratamientos que implicaban categorías especiales de datos, cuya exposición conlleva un riesgo elevado para los derechos y libertades de los interesados afectados. Por esta infracción, la Agencia impone una sanción de 30.000 euros, conforme al artículo 83.4 del RGPD.

El CEPD rechaza que una reclamación en materia de 'banners' de 'cookies' pueda archivarse por formar parte de una campaña coordinada

El asunto tiene su origen en una reclamación presentada por *NOYB* (*None of Your Business*), una organización austriaca especializada en promover el cumplimiento del RGPD mediante reclamaciones estratégicas, dirigida contra la radiotelevisión pública belga por el funcionamiento de su *banner* de *cookies*. La autoridad belga de protección de datos propuso archivar la reclamación al considerar que existía un abuso del derecho de reclamación, ya que la denuncia formaba parte de una campaña organizada por *NOYB* y había sido preparada siguiendo una estrategia coordinada de impugnación de *banners* de *cookies*. La autoridad austriaca, sin embargo, se opuso a esta conclusión y defendió que la reclamación debía analizarse sobre el fondo del asunto.

El CEPD concluye en su decisión que no se ha acreditado ningún abuso de derecho. Recuerda que, según la jurisprudencia del TJUE, para apreciar dicho abuso deben concurrir tanto un elemento objetivo como un elemento subjetivo.

En este caso, aunque la organización desempeñó un papel activo en la identificación de posibles infracciones y en la preparación de las reclamaciones, el CEPD considera que esa actuación es compatible con la finalidad del artículo 80.1 del RGPD, que permite que organizaciones especializadas representen a los interesados en materia de protección de datos. Además, no existe evidencia de que el reclamante o la organización buscaran una ventaja indebida distinta de obtener el cumplimiento de la normativa.

En consecuencia, el CEPD ordena a la autoridad belga que no archive la reclamación y que examine el caso sobre su fondo, respaldando así la legitimidad de las reclamaciones presentadas por entidades especializadas en protección de datos y limitando la posibilidad de que las autoridades de control las rechacen por el mero hecho de formar parte de campañas coordinadas de cumplimiento del RGPD.

Sancionado el titular de una notaría por entregar a una clienta una certificación catastral con datos protegidos de un tercero sin base legitimadora

La AEPD ha impuesto una multa de 2.000 euros al titular de una notaría tras la reclamación de una persona que recibió de una clienta de la notaría una carta acompañada de una certificación catastral descriptiva y gráfica. La carta le proponía firmar un escrito reconociendo que no era propietaria de una finca para darla de baja en el Catastro y poder inscribirla a nombre de la clienta. La certificación identificaba a la persona reclamante como titular de la parcela e incluía su nombre, apellidos y domicilio, datos protegidos conforme a la normativa catastral.

Durante la investigación, la Dirección General del Catastro confirmó que la certificación había sido obtenida por la notaría con finalidad informativa. La notaría reconoció que la obtuvo a petición de su clienta, quien facilitó la referencia catastral para que su hijo negociara con la titular la compra o el arrendamiento de la finca, y que después le entregó la certificación, que contenía los datos protegidos de la persona reclamante.

La Agencia concluyó que, aunque la notaría podía acceder a información catastral protegida cuando concurriesen las condiciones legales, la entrega de la certificación a la clienta para una eventual operación inmobiliaria no estaba justificada ni contaba con una base legitimadora conforme al artículo 6.1 del RGPD. La clienta utilizó los datos para acudir al domicilio de la persona reclamante y remitirle una carta, lo que constituye una infracción del artículo 6.1 del RGPD, tipificada en el artículo 83.5.a) del mismo texto.

Además, se ordena al titular de la notaría acreditar, en el plazo máximo de tres meses, la adopción de las medidas necesarias para garantizar el cumplimiento del artículo 6.1 del RGPD en todas sus operaciones de tratamiento de datos personales.

Una sociedad municipal de aparcamiento regulado es sancionada por grabar conversaciones de sus trabajadores mediante una aplicación de walkie-talkie sin informarles

La resolución sanciona a la sociedad municipal que gestiona en Palma el servicio de estacionamiento regulado en la vía pública (la denominada zona azul) por no tratar de forma leal y transparente los datos de sus trabajadores, en vulneración del artículo 5.1.a) del RGPD. En 2022, los controladores se quejaban de que el sistema para avisar de una emergencia era complicado, y la empresa decidió probar como alternativa una aplicación que funciona como un walkie-talkie en el teléfono móvil. La aplicación se instaló en los asistentes digitales personales (PDA) de los trabajadores y se activó en 92 de ellos. En noviembre del año 2022 se supo que había grabado una conversación de varios trabajadores durante su descanso, y que esa grabación era accesible para los responsables de zona. Tras la denuncia de los sindicatos, la empresa desinstaló la aplicación y borró las grabaciones pocos días después.

La entidad se defendió alegando que la aplicación estaba solo en pruebas y que no llegó a usar las grabaciones, que había informado verbalmente a los trabajadores al activarla y que no podía informar de los riesgos porque la aplicación carecía de manual técnico. La AEPD rechaza los tres argumentos en su resolución. En primer lugar, grabar una conversación ya constituye un tratamiento de datos, aunque la grabación no se utilice después. En segundo lugar, la empresa no acreditó qué información facilitó al activar la aplicación, no informó de nada a quienes la tenían instalada sin activar y su política de privacidad no mencionaba las grabaciones. En tercer lugar, precisamente porque la herramienta estaba en pruebas, la empresa debía extremar la transparencia y advertir de que podía fallar y afectar a los derechos de los trabajadores; al reconocer que desconocía los riesgos, admite que la instaló sin informar de ellos. La sanción impuesta asciende a 40.000 euros.

Multada una red de autoescuelas por una brecha de seguridad que expuso los datos de más de 264.000 personas tras ignorar los avisos de la Policía

La resolución se enmarca en un procedimiento sancionador incoado frente a una red de autoescuelas con franquicias en todo el territorio nacional, como consecuencia de una brecha de seguridad. El Grupo de Ciberataques de la Unidad Central de Ciberdelincuencia de la Policía Nacional localizó en internet la venta de una base de datos de la entidad con información de alumnos y empleados, como nombre y apellidos, DNI, teléfono, correo electrónico y domicilio. En total resultaron afectadas 264.435 personas, entre ellas algunos alumnos menores de edad. En un foro de ciberdelincuencia se publicó una muestra de los datos como prueba de que el robo era real.

La empresa desoyó las advertencias de una empresa de ciberseguridad y de la propia Policía Nacional, que intentó contactarla hasta en tres ocasiones. La entidad no les dio credibilidad porque le parecían intentos de fraude, y solo activó su protocolo de brechas en octubre de 2024, cuando su delegado de protección de datos accedió al foro y descargó la muestra.

La AEPD concluye en su resolución que la entidad vulneró el artículo 32 del RGPD por no disponer de medidas de seguridad adecuadas al riesgo, aunque no haya podido determinarse por dónde entró el atacante. La Agencia

destaca dos deficiencias: por un lado, los sistemas estaban obsoletos y la empresa lo sabía desde 2021, pero no los sustituyó hasta enero de 2025, cuando la brecha ya se había producido; por otro, no contaba con un procedimiento eficaz de gestión de incidentes. La Agencia recuerda que la capacidad de detectar una brecha y reaccionar a tiempo forma parte de la propia obligación de seguridad, e impone una multa de 30.000 euros.

Un ayuntamiento vulnera el RGPD al revelar a la prensa el motivo de la excedencia de una empleada identificable

La AEPD ha declarado que una entidad del sector público local vulneró el artículo 5.1.f) del RGPD, relativo al principio de integridad y confidencialidad, al comunicar a un medio de comunicación el motivo concreto por el que una empleada se encontraba en situación de excedencia.

El caso surgió tras la publicación de una noticia sobre las dificultades de funcionamiento de un servicio municipal. En ese contexto, la entidad pública informó no solo de que la empleada se encontraba en excedencia, sino también de la causa específica que la había motivado. La AEPD consideró que, aunque existía un interés legítimo en explicar la situación del servicio a la ciudadanía, la divulgación del motivo concreto de la excedencia no era necesaria para cumplir esa finalidad informativa. Además, la afectada resultaba fácilmente identificable al ocupar el único puesto de esas características dentro de la organización.

La resolución destaca que la transparencia administrativa no justifica la difusión de datos personales irrelevantes para la finalidad perseguida y recuerda que debe respetarse el principio de minimización de datos. La AEPD concluye que la comunicación realizada supuso una pérdida de confidencialidad de información personal y evidenció la ausencia de medidas organizativas adecuadas para evitar este tipo de divulgaciones.

Al tratarse de una administración pública, no se impuso una multa económica. No obstante, se declaró formalmente la infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) del mismo texto normativo, y se ordenó a la entidad adoptar, en un plazo de tres meses, medidas técnicas y organizativas destinadas a garantizar la seguridad y confidencialidad de los datos personales en futuras comunicaciones públicas e institucionales.

La AEPD declara infracciones por falta de información y evaluación de impacto insuficiente en controles biométricos fronterizos

La AEPD ha declarado la existencia de dos infracciones en relación con el sistema de control fronterizo utilizado por un organismo público encargado de la gestión de fronteras. El caso se originó tras la reclamación de una pasajera que denunció haber sido obligada a someterse a un control biométrico en un aeropuerto sin recibir información adecuada sobre el tratamiento de sus datos personales.

La resolución confirma que la utilización de datos biométricos para verificar la identidad de los viajeros cuenta con cobertura legal en la normativa europea sobre control de fronteras. No obstante, la AEPD considera que el responsable del tratamiento incumplió el artículo 21 de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (aplicable a la protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales por parte de autoridades competentes), al no facilitar a los interesados la información exigida sobre el tratamiento de sus datos, sus derechos, la identidad del responsable o las vías para ejercer dichos derechos.

Además, la AEPD concluye que también se vulneró el artículo 35 de la Ley Orgánica 7/2021, al no haber realizado una evaluación de impacto sobre protección de datos que cumpliera los requisitos legales. El documento aportado no analizaba adecuadamente los riesgos para los derechos y libertades de los afectados, el ciclo de vida de los datos biométricos ni las medidas previstas para mitigar dichos riesgos.

Al tratarse de una administración pública, la resolución no impone una multa económica. Sin embargo, declara la comisión de una infracción

muy grave por vulneración del artículo 21 y de una infracción grave por incumplimiento del artículo 35, ordenando la adopción de medidas correctoras. Entre ellas, facilitar información efectiva sobre protección de datos en los puestos fronterizos y elaborar una evaluación de impacto ajustada a las exigencias legales en el plazo de tres meses.

La AEPD declara una infracción por no realizar una evaluación de impacto en un proyecto de asistente virtual basado en inteligencia artificial

La AEPD ha declarado la existencia de una infracción del artículo 35 del RGPD por la ausencia de una evaluación de impacto relativa a la protección de datos (EIPD) en el diseño de un proyecto de asistente virtual basado en inteligencia artificial destinado a la atención ciudadana.

El proyecto contemplaba el uso de tecnologías avanzadas como procesamiento del lenguaje natural, reconocimiento de voz, aprendizaje automático, análisis emocional e interacción mediante avatares digitales. Además, preveía la recogida de datos identificativos de los usuarios a través de una aplicación móvil y el tratamiento de las interacciones mantenidas con el sistema para mejorar su funcionamiento mediante procesos de entrenamiento continuo de la inteligencia artificial.

La AEPD considera que estas características implicaban un tratamiento susceptible de generar un alto riesgo para los derechos y libertades de las personas, especialmente por el uso de nuevas tecnologías, la posibilidad de realizar inferencias sobre los usuarios a partir de sus interacciones y el despliegue del sistema a gran escala. Por ello, resultaba obligatoria la realización de una EIPD antes de iniciar el proyecto y durante sus fases de diseño y contratación.

La autoridad de control rechaza el argumento de que la ausencia de puesta en funcionamiento del sistema excluyera dicha obligación. Recuerda que la evaluación de impacto constituye una medida preventiva que debe realizarse desde las fases más tempranas de planificación, cuando todavía se están definiendo las características del tratamiento.

Al tratarse de una administración pública, no se impone multa económica. La resolución se limita a declarar la infracción del artículo 35 del RGPD y archiva la imputación inicial relativa al artículo 25 del mismo reglamento, tras considerar que la conducta quedaba absorbida por el incumplimiento específico de la obligación de realizar la evaluación de impacto.



Sentencias

El derecho de acceso del artículo 15 del RGPD no ampara, con carácter general, la identificación nominal del personal sanitario que ha accedido a una historia clínica

La sentencia resuelve un recurso de casación en el que se planteaba si el derecho de acceso reconocido en el artículo 15 del RGPD comprende la identificación concreta de los profesionales sanitarios que han consultado la historia clínica de un paciente. El asunto trae causa de la reclamación de un interesado que solicitó conocer la identidad del personal que había accedido a sus datos de salud, pretensión que fue desestimada por la AEPD y confirmada en vía judicial.

La Sala Tercera del Tribunal Supremo concluye en su sentencia que el concepto de "destinatario" del artículo 15.1.c) del RGPD no comprende a los empleados o profesionales que, integrados en la organización responsable del tratamiento, acceden a la información en el ejercicio de sus funciones y bajo las instrucciones del responsable. Por tanto, el derecho de acceso no incluye, con carácter general, la identificación nominal de médicos, personal sanitario o administrativo autorizado que haya consultado la historia clínica.

Apoyándose expresamente en la jurisprudencia del Tribunal de Justicia de la Unión Europea (asunto C-579/21), el Tribunal Supremo declara que el interesado sí puede conocer información relativa a los accesos realizados, como fechas, finalidades o categorías funcionales, para verificar la licitud del tratamiento, pero no la identidad de los empleados que actuaron legítimamente dentro de la organización sanitaria. Asimismo, establece que la identidad de estos profesionales únicamente podría facilitarse de manera excepcional cuando resultara indispensable para el ejercicio efectivo de los derechos reconocidos por el RGPD y previa ponderación con los derechos y libertades de dichos empleados. En consecuencia, desestima el recurso de casación y confirma la conformidad a derecho de la actuación de la AEPD.

Anulada la Guía de la AEPD sobre tratamientos de control de presencia mediante sistemas biométricos al tener naturaleza material de circular

La sentencia resuelve el recurso contencioso-administrativo interpuesto por la Asociación Española de Empresas de Seguridad contra la Guía sobre tratamientos de control de presencia mediante sistemas biométricos publicada por la AEPD el 23 de noviembre de 2023. La Sala concluye en su sentencia que el documento no podía calificarse como una mera guía orientativa, sino que, atendiendo a su contenido material, constituía una auténtica fijación de criterios de actuación y sanción de la Agencia. En particular, destaca que la guía determinaba los criterios que la propia AEPD aplicaría en materia de control de presencia mediante sistemas biométricos y que tales criterios estaban destinados a proyectar efectos sobre responsables y encargados del tratamiento, condicionando de forma relevante la implantación y comercialización de estas tecnologías.

Partiendo de la doctrina consolidada del Tribunal Supremo según la cual la naturaleza jurídica de una disposición depende de su contenido y efectos reales, y no de la denominación que reciba, la Audiencia Nacional entiende que la guía tenía naturaleza

material de circular en los términos del artículo 55 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). En consecuencia, debía haberse elaborado siguiendo el procedimiento específico previsto para este tipo de instrumentos regulatorios, incluyendo las garantías formales correspondientes. Al no haberse observado dicho procedimiento, la Sala declara su nulidad y deja sin efecto su aprobación y publicación. La sentencia no se pronuncia sobre la licitud o ilicitud de los sistemas biométricos de control horario o de presencia y control de accesos, sino exclusivamente sobre la invalidez formal del instrumento utilizado por la AEPD para fijar sus criterios interpretativos en esta materia.

La publicación en internet de sentencias penales no siempre puede acogerse a la excepción periodística del RGPD

El Tribunal de Justicia de la Unión Europea, en su sentencia de 9 de julio de 2026 dictada en el asunto C-199/24 (*Legal Newsdesk Sweden*), analiza si la difusión en internet, mediante pago, de sentencias penales condenatorias contenidas en una base de datos pública puede beneficiarse de las excepciones previstas en el artículo 85 del RGPD para los tratamientos realizados con fines periodísticos. El litigio surge tras la negativa de una plataforma sueca a suprimir los datos personales de una persona condenada penalmente que figuraban en su base de datos.

El Tribunal recuerda que los Estados miembros deben conciliar el derecho a la protección de los datos personales con la libertad de expresión e información, pero aclara que las excepciones previstas en el artículo 85.2 del RGPD solo pueden aplicarse a tratamientos realizados con fines periodísticos o de expresión académica, artística o literaria. En consecuencia, los Estados miembros no pueden extender dichas excepciones a otras actividades mediante legislación nacional.

Asimismo, el TJUE declara que los interesados deben conservar las vías de recurso reconocidas por el RGPD, por lo que una normativa nacional no puede limitar su tutela a acciones por difamación o reclamaciones indemnizatorias basadas exclusivamente en dicha figura. El derecho a presentar reclamaciones ante las autoridades de control y a ejercitar acciones judiciales derivadas del RGPD debe permanecer plenamente garantizado.

En relación con el concepto de fines periodísticos, el Tribunal adopta una interpretación amplia, pero exige que exista una verdadera actividad periodística. La mera puesta a disposición del público, previo pago, de sentencias penales sin labor de redacción, adaptación, verificación o sometimiento a una línea editorial no puede considerarse automáticamente una actividad periodística. Solo podrá beneficiarse de la excepción cuando la difusión de la información responda al ejercicio genuino de una actividad periodística desarrollada conforme a criterios editoriales y a las normas deontológicas de la profesión.

La sentencia refuerza así la protección de los datos relativos a condenas penales y limita el uso expansivo de las excepciones periodísticas previstas en el RGPD para bases de datos privadas que comercializan información judicial accesible al público.

El TJUE declara que el RGPD se opone a la publicación indiscriminada de los datos personales de todos los accionistas de sociedades anónimas

El TJUE ha resuelto, en su sentencia de 3 de septiembre de 2026 dictada en el asunto C-798/24 (Jautiva), una cuestión prejudicial planteada por el Tribunal Constitucional de Letonia sobre la compatibilidad con el RGPD de una normativa nacional que obligaba a poner a disposición del público, incluida la descarga masiva en internet por usuarios no identificados, los datos personales de todos los accionistas de sociedades anónimas, incluyendo nombre, apellidos, número de identificación personal, dirección de contacto, correo electrónico, categoría y número de acciones y número de votos.

El Tribunal concluyó que el artículo 14, letra d), de la Directiva (UE) 2017/1132 del Parlamento Europeo y del Consejo, de 14 de junio de 2017, sobre determinados aspectos del Derecho de sociedades, no exige la publicación de

información sobre todos los accionistas, incluidos los minoritarios. También razonó que dicha disposición se refiere al nombramiento y cese de personas que, como órgano o miembros de un órgano, obligan a la sociedad frente a terceros o participan en su administración, vigilancia o control, y que los accionistas no son nombrados ni cesados, sino que su condición deriva de su participación en el capital.

Además, el Tribunal declaró que los artículos 5 y 6 del RGPD, interpretados a la luz de los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, se oponen a una normativa nacional que obliga a poner a disposición del público los datos personales de todos los accionistas sin exigir la acreditación de un interés legítimo, señalándose, además, que la publicación de datos de accionistas minoritarios no resulta ni idónea ni necesaria, que las dificultades prácticas de verificar el interés legítimo no justifican la injerencia, y que la normativa letona carecía de garantías suficientes al permitir la descarga masiva por usuarios no identificados.

La pérdida de independencia de la autoridad de consumo estadounidense, tras una sentencia del Tribunal Supremo de EE.UU., debilita uno de los pilares del 'EU-US Data Privacy Framework'

El Tribunal Supremo de Estados Unidos dictó el 29 de junio de 2026 sentencia en el asunto Trump v. Slaughter. La sentencia reconoce que el presidente puede destituir libremente a los miembros de la *Federal Trade Commission* (*FTC*), la Comisión Federal de Comercio de Estados Unidos. Así abandona un criterio aplicado desde 1935, según el cual sus comisionados solo podían ser cesados por causas tasadas. La *FTC* deja con ello de ser una agencia independiente y queda sometida al control político del presidente.

La *FTC* es la principal autoridad encargada de supervisar a las empresas adheridas al *EU-US Data Privacy Framework* (DPF): investiga incumplimientos, impone sanciones y exige el respeto de los compromisos de privacidad. La Comisión Europea destacó expresamente su independencia en la Decisión de Adecuación de julio de 2023. Esa independencia tiene peso porque el Derecho de la Unión exige que la supervisión en materia de protección de datos corresponda a autoridades independientes:

- artículo 8.3 de la Carta de los Derechos Fundamentales de la Unión Europea;
- artículo 16 del Tratado de Funcionamiento de la Unión Europea;
- artículo 52 del RGPD.

Los dos marcos anteriores, *Safe Harbor* y *Privacy Shield*, fueron anulados por el Tribunal de Justicia de la Unión Europea (TJUE) en las sentencias *Schrems I* (2015) y *Schrems II* (2020). En ambos casos los motivos fueron la vigilancia masiva y la falta de recursos efectivos, no la *FTC*. A ello se suma ahora que el *Privacy and Civil Liberties Oversight Board*, el órgano estadounidense de supervisión de la privacidad y las libertades civiles, quedó temporalmente sin quórum.

La organización *NOYB* ha remitido una carta a la Comisión Europea pidiendo la retirada ordenada de la Decisión de Adecuación. También ha anunciado acciones judiciales que podrían dar lugar a un *Schrems III*.

A la fecha de esta publicación, el DPF sigue plenamente vigente y las transferencias a empresas certificadas siguen siendo válidas.

El Tribunal Supremo refuerza el deber de verificar el consentimiento para fines publicitarios cuando la contratación se realiza mediante representante

El Tribunal Supremo ha confirmado la sanción impuesta a una empresa del sector energético por no haber adoptado medidas adecuadas para verificar que quienes actuaban como representantes de clientes estaban efectivamente autorizados para consentir tratamientos de datos con fines comerciales y publicitarios.

El caso se refería a la contratación de suministros energéticos a través de distintos canales, en los que se permitía la actuación de

representantes sin exigir, en muchos supuestos, una acreditación suficiente de sus poderes para autorizar tratamientos adicionales de datos personales. Entre dichos tratamientos se encontraban el envío de ofertas comerciales, la recepción de publicidad de productos y servicios ajenos al contrato, y la elaboración de perfiles comerciales mediante información procedente de terceros.

La AEPD consideró infringidos los artículos 25 y 13 del RGPD, imponiendo inicialmente multas de 500.000 euros y 1.000.000 euros, respectivamente. Posteriormente, la Audiencia Nacional redujo las sanciones a 250.000 euros por la infracción del artículo 25 y a 600.000 euros por la del artículo 13, cuantías que quedaron confirmadas tras el recurso de casación.

La sentencia aclara que la representación válida para celebrar un contrato no permite presumir automáticamente que el representante está facultado para prestar consentimientos relativos a tratamientos de datos con finalidades distintas de la ejecución contractual. En estos casos, el responsable del tratamiento debe aplicar medidas técnicas y organizativas que le permitan acreditar que el interesado ha consentido de forma libre, específica, expresa e inequívoca, o que el representante dispone de autorización suficiente para hacerlo en su nombre.

El TJUE declara que el RGPD no se opone a la publicación en internet de los nombres de deportistas sancionados por dopaje, pero exige una ponderación previa de proporcionalidad

La sentencia trae causa de la publicación por parte de la Agencia austriaca antidopaje y de la Comisión Jurídica Antidopaje de Austria en sus páginas web del nombre, deporte practicado, infracción cometida y sanción impuesta a deportistas sancionados por dopaje. Cuatro deportistas afectados impugnaron dicha publicación alegando que la información divulgada constituye datos relativos a la salud e información sobre condenas e infracciones penales, cuyo tratamiento está sujeto a un régimen reforzado de protección conforme al RGPD, y que el sistema austriaco de publicación generalizada e indiscriminada de dichos datos vulneraba la normativa de protección de datos.

El Tribunal de Justicia de la Unión Europea declara en su sentencia dictada en el asunto C-474/24 que el RGPD no se opone, en principio, a la publicación en internet del nombre del deportista, la sanción y sus motivos, al perseguir un objetivo de interés general vinculado a la lucha contra el dopaje, la igualdad de oportunidades en la competición deportiva y la disuasión. No obstante, el TJUE impone dos condiciones: en primer lugar, la entidad responsable de la publicación debe ponderar los intereses en juego antes de proceder a la publicación, respetando el principio de proporcionalidad, especialmente en lo que se refiere a la duración del mantenimiento de los datos en la página web. En segundo lugar, el deportista afectado debe poder reclamar de forma preventiva ante la autoridad de protección de datos cuando la publicación sea inminente, garantizándose así una tutela efectiva con carácter previo a la difusión de sus datos.

La Audiencia Nacional anula una sanción de la AEPD por el tratamiento de datos en la gestión de una herencia

La sentencia resuelve el recurso contencioso-administrativo interpuesto por una entidad financiera contra la resolución de la AEPD que le impuso una sanción de 100.000 euros por vulneración del artículo 6.1 del RGPD. El origen del procedimiento se encontraba en la apertura, por parte de la entidad, de cuentas vinculadas a la tramitación de una herencia y a la adjudicación de participaciones de un fondo de inversión a favor de menores de edad, sin que la madre hubiera prestado un consentimiento expreso para ello. La AEPD entendió que el tratamiento carecía de base legitimadora, al considerar que los datos facilitados para gestionar la herencia no podían emplearse para la apertura de dichas cuentas.

La Audiencia Nacional discrepa de este criterio en su sentencia y concluye que no existió una infracción del artículo 6 del RGPD. La Sala considera acreditado que los datos fueron utilizados en el contexto de la tramitación de la testamentaría solicitada por los herederos y que la apertura de las cuentas constituía un

paso necesario para ejecutar las operaciones inherentes al reparto de la herencia y a la adjudicación de las participaciones del fondo de inversión. Además, destaca que las cuentas se encontraban en un estado preliminar, no llegaron a estar operativas y requerían una posterior validación por parte de la representante legal de los menores. Sobre esta base, entiende que el tratamiento estaba amparado por una base de legitimación distinta del consentimiento, al resultar necesario para la ejecución de las actuaciones vinculadas a la gestión y adjudicación de los bienes hereditarios.

En consecuencia, la Audiencia Nacional estima el recurso, anula la sanción impuesta por la AEPD y ordena la devolución de la cantidad abonada por la entidad financiera junto con los intereses legales correspondientes.

El abogado general del TJUE considera insuficiente identificar como socios a los destinatarios de datos para comunicaciones comerciales

El TJUE ha celebrado la vista oral del asunto C-317/25, una cuestión prejudicial planteada por el Consejo de Estado francés. El origen es una multa de 600.000 euros impuesta por la *Commission nationale de l'informatique et des libertés (CNIL)*, la autoridad francesa de protección de datos, a un grupo audiovisual francés.

En 2021 el grupo envió campañas de *marketing* por correo electrónico a unos 3,9 millones de personas. Los datos procedían de dos proveedores de acceso a internet. Al contratar con ellos, los usuarios habían marcado una casilla autorizando su uso por los *partners* de esos operadores. Esos *partners* no estaban identificados ni había ninguna lista accesible. La *CNIL* consideró que ese consentimiento no amparaba las campañas.

El abogado general ha presentado sus conclusiones en este asunto, en el que diversos abonados prestaron consentimiento para que sus datos personales fueran utilizados con fines de prospección comercial por los "socios" de dos proveedores de acceso a internet, sin que se identificara concretamente quiénes eran dichos destinatarios. Posteriormente, Groupe Canal+ utilizó esos datos para realizar comunicaciones comerciales y fue sancionada por la autoridad francesa de protección de datos.

Según las conclusiones presentadas, el consentimiento solo puede considerarse válido si es libre, específico, informado e inequívoco. Para que exista un consentimiento informado, el interesado debe conocer la identidad del responsable del tratamiento que utilizará efectivamente sus datos. Por ello, el abogado general considera que una referencia genérica a los socios del proveedor no permite entender que el interesado haya consentido recibir comunicaciones comerciales de cualquier empresa integrada en esa categoría.

En consecuencia, cuando la identidad concreta de la empresa que pretende realizar la prospección comercial no era conocida en el momento de la recogida de los datos, debe recabarse un nuevo consentimiento antes de utilizar dichos datos con esa finalidad, como muy tarde en el momento de la primera comunicación comercial. Asimismo, rechaza que la posibilidad de oponerse o darse de baja tras recibir el primer mensaje pueda sustituir al consentimiento previo exigido por la normativa de protección de datos.

El abogado general concluye, por tanto, que la mera referencia a una categoría indeterminada de destinatarios no basta para legitimar actividades de *marketing* directo. No obstante, recuerda que sus conclusiones no vinculan al Tribunal de Justicia, que deberá pronunciarse posteriormente mediante sentencia.

El abogado general propone declarar incompatible con el Derecho de la Unión la normativa belga de conservación generalizada de datos de comunicaciones electrónicas

El abogado general Maciej Szpunar ha presentado el 3 de septiembre de 2026 sus conclusiones en el asunto C-661/24 en el marco de una remisión prejudicial planteada por el Tribunal Constitucional belga. En ellas propone al Tribunal de Justicia que declare que el Derecho de la Unión se opone a varias disposiciones de la Ley belga de 2022 relativa a la recogida y conservación de datos de

identificación, tráfico y localización en el sector de las comunicaciones electrónicas.

El abogado general recuerda que las medidas nacionales que imponen la conservación de datos de tráfico y de localización constituyen una injerencia en los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales, garantizados por la Carta de los Derechos Fundamentales de la Unión Europea, y que dicha injerencia solo puede admitirse si está establecida por ley, es estrictamente necesaria y respeta el principio de proporcionalidad.

En su análisis, el abogado general admite que, en determinadas condiciones técnicas estrictas, una conservación generalizada e indiferenciada de datos podría ser compatible con la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, siempre que se garantice una separación efectivamente estanca de las distintas categorías de datos, se impida su uso combinado y no puedan extraerse conclusiones precisas sobre la vida privada de los usuarios. Sin embargo, concluye que la normativa belga no satisface dichas condiciones: permite conservar datos excesivamente amplios, carece de separación técnica efectiva, otorga a los proveedores una discrecionalidad excesiva y no ofrece las garantías de claridad, precisión y proporcionalidad exigidas. Las conclusiones no son vinculantes y el Tribunal de Justicia dictará sentencia en fecha posterior.

Contacta con nuestros profesionales

Alejandro Padín
Socio · Madrid
alejandro.padin@garrigues.com

Sebastián Hassi
Asociado principal · Santiago de Chile
sebastian.hassi@garrigues.com

Andrea Ugalde
Asociada · Bilbao
andrea.ugalde@garrigues.com

Carina Casadesús
Asociada · Barcelona
carina.casadesus@garrigues.com

Javier Enebral
Asociado · Madrid
javier.enebral@garrigues.com

Sebastián Barros
Socio · Santiago de Chile
sebastian.barros@garrigues.com

Adrián León
Asociado sénior · Alicante
adrian.leon@garrigues.com

Antonio Durán
Asociado · Málaga
antonio.duran@garrigues.com

Ignacio Suárez
Asociado · Madrid
ignacio.suarez@garrigues.com

Más información:
Economía del Dato, Privacidad y Ciberseguridad

GARRIGUES

Plaza de Colón, 2 - 28046 Madrid
T +34 91 514 52 00

info@garrigues.com
garrigues.com

Síguenos en:

Esta publicación tiene carácter meramente informativo y no constituye asesoramiento jurídico, ni de ningún otro tipo. Tampoco pretende ofrecer un resumen exhaustivo de las normas y novedades a las que se refiere ni recoger todo lo publicado, sino únicamente ofrecer una selección, por lo que se recomienda consultar los textos oficiales y obtener asesoramiento profesional específico. Garrigues no asume responsabilidad alguna por el uso de esta información, ni la obligación de actualizarla tras su publicación.

© 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.