DURÁNSINDREU

Newsletter Derecho Digital, IT y protección de datos

Novedades en materia de Inteligencia Artificial

En los últimos meses, el marco europeo y nacional en materia de inteligencia artificial y protección de datos ha experimentado avances relevantes, con iniciativas como el Ómnibus Digital que ajusta el Reglamento de IA mediante nuevas obligaciones, plazos y mecanismos de gobernanza, así como la publicación de directrices que concretan las exigencias de transparencia en el uso de estos sistemas; en paralelo, España impulsa su propio modelo de regulación a través de un proyecto de ley de gobernanza de la IA, mientras que la jurisprudencia y las resoluciones de autoridades como la AEPD continúan precisando el alcance práctico de los derechos y obligaciones en ámbitos como el acceso a datos, el entorno laboral o el uso de tecnologías biométricas.

Índice de contenidos

Novedades en materia de Inteligencia Artificial

Ómnibus Digital en Inteligencia Artificial: nuevas obligaciones, plazos y ajustes regulatorios

El pasado **7 de mayo de 2026** la Unión Europea alcanzó un acuerdo provisional sobre el denominado Ómnibus Digital en Inteligencia Artificial, una iniciativa destinada a ajustar y flexibilizar determinados elementos del Reglamento de IA (AI Act). Este paquete normativo tiene como objetivo principal reducir cargas administrativas y facilitar la adaptación de empresas y operadores al nuevo marco europeo, introduciendo modificaciones relevantes en materia de plazos, obligaciones y gobernanza.

Entre sus principales novedades, el Acuerdo prevé una ampliación de los plazos de aplicación para sistemas de alto riesgo, trasladando su entrada en vigor efectiva hasta finales de 2027 o incluso 2028 en determinados supuestos. Asimismo, incorpora nuevas prohibiciones —como la relativa a la generación de contenido íntimo no consentido— y refuerza las obligaciones de transparencia, reduciendo el plazo para implementar medidas como el etiquetado de contenido generado por IA. Junto a ello, introduce ajustes relevantes en materia de sandbox regulatorios, registro de sistemas y tratamiento de datos para la detección de sesgos, configurando un marco más flexible pero también más exigente en términos de cumplimiento.

Para más información sobre el Ómnibus Digital puede consultar nuestra Nota informativa.

Directrices sobre la implementación de las obligaciones de transparencia para ciertos sistemas de IA conforme al Artículo 50 del Reglamento de IA

El pasado 1 de agosto de 2024 entró en vigor el Reglamento (UE) 2024/1689, conocido como la Ley de IA (en adelante "**AI Act**") o el Reglamento de IA (en adelante "**RIA**"). Dentro de su enfoque basado en el riesgo, uno de los pilares fundamentales para garantizar la confianza de la ciudadanía es la transparencia. Para clarificar cómo deben aplicarse estas obligaciones, la Comisión Europea publicó el pasado **8 de mayo** el borrador de las *"Directrices sobre la aplicación de las obligaciones de transparencia para determinados sistemas de IA en virtud del artículo 50 del Reglamento de IA".*

Estas directrices, aunque de carácter no vinculante, proporcionan la interpretación necesaria para implementar las cuatro obligaciones de transparencia del Artículo 50 del RIA, plenamente aplicables a partir del 2 de agosto de 2026. De ese modo, el documento se define como la hoja de ruta esencial para dos actores principales:

- Los **proveedores de sistemas de IA** en toda la Unión Europea: quienes desarrollan el sistema y lo introducen en el mercado.

- Los **implementadores o desplegadores de sistemas de IA** en toda la Unión Europea: quienes utilizan el sistema bajo su autoridad (empresas, autoridades públicas, etc.). Estos usan los sistemas de IA en contextos profesionales o públicos.

Sin embargo, se establecen exclusiones importantes: la normativa no se aplica a actividades puramente personales y no profesionales, ni a sistemas dedicados exclusivamente a la investigación y desarrollo científico antes de su puesta en servicio.

Las obligaciones de transparencia se pueden resumirse en los siguientes puntos:

1. Los proveedores deben desarrollar y diseñar el sistema de IA de tal manera que las personas implicadas sean informadas de que están interactuando con un sistema de IA. Excepción: Esta obligación no será aplicable si el uso de la herramienta de IA es evidente, o el sistema está autorizado por ley para detectar, prevenir, investigar o procesar delitos penales, salvo que el sistema esté disponible para que el público pueda denunciar un delito.
2. Los proveedores deben asegurarse de que los resultados del sistema de IA estén identificados como generados o manipulados por sistemas de IA. Excepción: Esta obligación no aplicará si el sistema de IA realiza una función meramente de asistencia para la edición o no altera sustancialmente los datos de entrada, o el sistema está autorizado por ley detectar, prevenir e investigar o procesar delitos.
3. Si se usa IA para reconocer emociones o clasificar rasgos biométricos, las personas deben ser informadas y sus datos deben protegerse según leyes de protección de datos, con la excepción de si el uso de la IA se debe a un uso autorizado para seguridad o investigación de delitos.
4. Si se crean o difunden imágenes, vídeos o audios falsos, se debe informar de que han sido generados mediante IA. También aplica a textos informativos generados por IA (por ejemplo, noticias). Son excepciones el uso legal con fines policiales, las obras artísticas o creativas (en estos casos se permite una transparencia "atenuada" para no romper el disfrute de la obra) o los textos revisados por humanos con responsabilidad editorial.

Además, toda la información proporcionada sobre las obligaciones mencionadas debe ser:

- Clara y visible
- Proporcionada desde el primer contacto
- Accesible

Asimismo, cabe destacar que la vigilancia corresponde a las autoridades designadas por los Estados miembros, la Oficina Europea de Inteligencia Artificial y el Supervisor Europeo de Protección de Datos, que pueden actuar de oficio o tras denuncia; asimismo, el incumplimiento puede conllevar multas de hasta 15 millones de euros o el 3 % del volumen de negocios anual mundial, y hasta 750.000 euros para organismos de la UE.

Proyecto de Ley Orgánica para el buen uso y la gobernanza de la IA

El Consejo de Ministros aprobó el pasado **26 de mayo** el Proyecto de Ley Orgánica para el buen uso y la gobernanza de la inteligencia artificial, una normativa que adapta el ordenamiento español al

Reglamento europeo de IA (en adelante, "AI Act") y establece un marco orientado a garantizar un uso confiable, supervisado y respetuoso de los sistemas de IA con los derechos fundamentales.

Desde el punto de vista normativo, la propuesta de ley actúa como instrumento de desarrollo del AI Act, integrando su enfoque basado en riesgos y trasladándolo al ordenamiento jurídico español. Concretamente, introduce un modelo de gobernanza reforzado en el que la Agencia Española de Supervisión de Inteligencia Artificial (AESIA) asume un importante papel en coordinación con otras autoridades como la AEPD o el CGPJ, según el ámbito de aplicación.

- **Límites al uso de la IA:** el proyecto incorpora y desarrolla las prohibiciones ya previstas en el AI Act para los sistemas de riesgo inaceptable. Entre ellos destacan los que utilizan técnicas subliminales para manipular decisiones, los que explotan vulnerabilidades de colectivos especialmente protegidos o los sistemas de clasificación biométrica por ideología, religión u orientación.

Asimismo, introduce una propuesta de **régimen sancionador** que clasifica las infracciones en leves, graves y muy graves y estableciendo unas sanciones que pueden alcanzar hasta **35 millones de euros o el 7% del volumen de negocio global**.

- **Especial atención al sector público:** una de las principales aportaciones del proyecto es la regulación específica del uso de la IA en la Administración. En este ámbito se prevé la creación de un inventario de sistemas de IA utilizados en procedimientos administrativos, con el objetivo de reforzar la transparencia, así como la introducción de la figura del delegado de IA, encargado de coordinar la aplicación normativa y asesorar en el uso de estos sistemas.

Además, el texto incorpora medidas destinadas a mediar entre el control regulatorio y el impulso a la innovación. En este sentido, se regula el funcionamiento de los entornos de prueba o Sandbox de IA, incluyendo un Sandbox nacional gestionado por la AESIA y la posibilidad de desarrollar entornos sectoriales adicionales. Estos espacios permiten testar soluciones tecnológicas en un entorno controlado, facilitando el cumplimiento normativo sin frenar el desarrollo.

Jurisprudencia y Doctrina destacada

El TJUE se pronuncia sobre el ejercicio de derechos en el marco del RGPD y el derecho a indemnización de los interesados

La sentencia del Tribunal de Justicia de la Unión Europea (en adelante, "**TJUE**") de **19 de marzo de 2026** analiza cómo deben interpretarse tanto el derecho de acceso a los datos personales y el derecho a indemnización previsto en el Reglamento General de Protección de Datos (en adelante, "**RGPD**")

El caso que se analiza surge a raíz de una solicitud de acceso a sus datos personales de un interesado y, tras la negativa de la empresa, reclama una indemnización. La empresa sostiene que esa solicitud no era genuina, sino parte de una estrategia para obtener compensaciones económicas.

Por ello, el TJUE analiza varias cuestiones:

- En primer lugar, una solicitud de acceso a datos personales puede considerarse "excesiva" o abusiva. Aunque el RGPD reconoce este derecho de acceso como fundamental, no es ilimitado.

Si se demuestra que la solicitud no tiene como objetivo conocer o verificar el uso de los datos, sino que se ha presentado con una finalidad fraudulenta o estratégica (provocar un incumplimiento para reclamar dinero), la empresa puede negarse a atenderla.

La carga de la prueba recae en la empresa, que debe demostrar claramente la intención abusiva teniendo en cuenta todas las circunstancias del caso, como el comportamiento del solicitante o la repetición de este tipo de prácticas con otras empresas.

- En segundo lugar, la sentencia reconoce que el derecho a indemnización previsto en el RGPD no se limita a los casos en los que haya un tratamiento ilícito de datos. También puede existir indemnización cuando se vulnera un derecho del interesado, como el derecho de acceso, aunque no haya habido un uso indebido de los datos en sí.

Asimismo, el TJUE concluye que no toda infracción genera automáticamente un derecho a indemnización, sino que para que exista ese derecho, deben cumplirse tres requisitos acumulativos:

- Que haya una infracción del RGPD.
- Que la persona haya sufrido un daño (material o inmaterial).
- Que exista una relación de causalidad entre ambos; no basta con que se haya vulnerado el derecho, sino que hay que demostrar un perjuicio real.

En cuanto a los daños inmateriales, el alto tribunal acepta que pueden incluir situaciones como la pérdida de control sobre los datos personales o la incertidumbre sobre su tratamiento, pero no son daños que se puedan presumir, sino que la persona afectada debe probarlos. Además, si el propio interesado ha provocado la situación, puede romperse la relación causal y perder el derecho a indemnización.

El Tribunal Supremo obliga a las empresas a publicar el nombre de los trabajadores en los listados de antigüedad si así lo exige el convenio

El Tribunal Supremo ha dictado una sentencia que clarifica los límites entre la transparencia laboral y la protección de datos personales. En su reciente resolución STS 1215/2026, la Sala de lo Social ha dado la razón a un sindicato frente a una aerolínea, determinando que la empresa no puede ocultar la identidad de los empleados en los escalafones de antigüedad bajo el pretexto de cumplir con el Reglamento General de Protección de Datos (en adelante “RGPD”).

La disputa se inició cuando la aerolínea, en base al principio de minimización de datos personales establecido en el RGP, decidió sustituir los nombres y apellidos de sus tripulantes de cabina por códigos numéricos de 12 cifras en los listados de antigüedad publicados en su intranet. El sindicato demandante alegó que esta práctica hacía imposible que los trabajadores verificaran su posición real para optar a promociones o traslados, incumpliendo lo pactado en el Convenio Colectivo de la compañía.

Aunque la Audiencia Nacional rechazó inicialmente la demanda, el Tribunal Supremo ha corregido esta decisión estableciendo que el convenio colectivo es una norma vinculante y el Artículo 88 del RGPD faculta expresamente a la negociación colectiva para regular el tratamiento de datos en el entorno de trabajo. También argumenta que conocer la identidad de los compañeros en un escalafón es un "interés

legítimo" y una necesidad para la ejecución del contrato de trabajo. Sin embargo, la sentencia no otorga una carta blanca para la difusión indiscriminada de datos.

Desde la perspectiva de protección de datos, la sentencia resulta especialmente relevante porque delimita el alcance de la seudonimización. El Tribunal recuerda que los datos seudonimizados no dejan automáticamente de ser datos personales, sino que su consideración depende de la posibilidad real de identificar a las personas a partir de ellos o mediante información adicional. En este caso, la seudonimización no servía para cumplir con la finalidad del tratamiento, que exigía precisamente identificar a los trabajadores para garantizar la transparencia y el control en procesos como promociones o cambios de base.

Asimismo, el Supremo subraya que el RGPD no prohíbe el tratamiento de datos personales cuando este se apoya en una base jurídica válida. En ese sentido, el Tribunal Supremo concluyó que la protección de datos no puede servir de "escudo" para vaciar de contenido los derechos de información y control que los trabajadores tienen a través de la negociación colectiva. En definitiva, se establece que la seudonimización era un incumplimiento claro de lo pactado en el convenio.

De esta forma, se obliga a la aerolínea a incluir los nombres y apellidos, pero le exige implementar medidas técnicas de seguridad. De este modo, el acceso a estos datos completos dentro de la intranet corporativa debe quedar restringido exclusivamente a los propios trabajadores afectados, a sus representantes sindicales y a cualquier persona que acredite un interés legítimo en el proceso.

Resoluciones recientes de la AEPD

La AEPD delimita la compatibilidad del DPD: el riesgo de conflicto de intereses con el canal de denuncias

La Agencia Española de Protección de Datos se ha pronunciado de nuevo sobre los límites de compatibilidad del Delegado de Protección de Datos (en adelante, "**DPD**") al considerar que su designación como responsable del Sistema Interno de Información (canal de denuncias) puede generar conflictos de interés si no se analiza adecuadamente.

El supuesto surge en el marco de un procedimiento sancionador contra una entidad pública en el que, además de una brecha de seguridad, se evaluó la independencia del DPD, quien había sido designado también como responsable del canal de denuncias previsto en la Ley 2/2023.

Aunque el RGPD permite que el DPD asuma otras funciones, tal y como establece art. 38.6 del RGPD, la AEPD recuerda que el responsable del tratamiento debe garantizar que estas no den lugar a conflictos de interés. En este caso, la AEPD concluye que la entidad no realizó un análisis adecuado de compatibilidad entre ambas funciones y mantuvo la designación pese a la existencia de dudas internas, incluso planteadas por la propia DPD.

Desde la perspectiva de protección de datos, el problema reside en que la gestión del canal de denuncias implica la toma de decisiones sobre el tratamiento de datos personales, mientras que el DPD debe supervisar precisamente la licitud de esos tratamientos. Esta doble función sitúa al delegado en una posición en la que podría verse obligado a evaluar sus propias decisiones, comprometiendo su independencia.

La AEPD concluye que, en este caso concreto, se vulneró el artículo 38 del RGPD, no por la mera acumulación de funciones, sino por la falta de evaluación efectiva del conflicto de intereses y por haber mantenido una designación potencialmente incompatible.

En definitiva, en base a la citada resolución cabe extraer la siguiente conclusión: la compatibilidad del DPD con otras funciones no está prohibida, pero exige un análisis riguroso del riesgo de conflicto de intereses, especialmente cuando dichas funciones implican decisiones sobre tratamientos de datos que el propio DPD debe supervisar.

Sanción de 500.000€ a un club de fútbol por el uso de biometría

La AEPD ha impuesto una sanción de 500.000 € una entidad deportiva por la implementación de un sistema de identificación basado en reconocimiento facial y de voz en la actualización del censo de sus socios, afectando a más de 140.000 socios sin haber realizado una Evaluación de Impacto relativa a la Protección de Datos (en adelante "**EIPD**") que cumpliera con los estándares legales exigibles.

El caso se centra en la campaña iniciada en 2023, en la que el club habilitó un proceso digital que requería la captura de una imagen facial (con movimientos para verificación) y, opcionalmente, la grabación de voz. Este sistema perseguía modernizar la gestión de socios y evitar fraudes como la cesión indebida de abonos.

Aunque inicialmente se investigó una posible infracción del artículo 9 del RGPD (tratamiento de categorías especiales de datos), esta cuestión fue finalmente archivada. La sanción se fundamenta exclusivamente en la vulneración del artículo 35 del RGPD, al no haber realizado una EIPD válida y completa antes de implantar el sistema.

La AEPD considera que el tratamiento presentaba un alto riesgo debido a varios factores: el uso de tecnologías biométricas, la afectación a gran escala, la inclusión de menores de edad y la utilización de procedimientos digitales complejos. En este contexto, la evaluación de riesgos realizada por el club fue calificada como insuficiente, ya que no analizaba adecuadamente la necesidad, proporcionalidad y riesgos reales del tratamiento ni justificaba las medidas adoptadas.

Asimismo, la Agencia subraya que la existencia de consentimiento o de medidas técnicas de seguridad no exonera del cumplimiento de la obligación de realizar una EIPD previa cuando el tratamiento es de alto riesgo.

La sanción final de 500.000 € supone una reducción significativa respecto de la propuesta inicial, que alcanzaba los 6 millones de euros, teniendo en cuenta factores atenuantes como la cooperación del club y la suspensión temporal del sistema.

La AEPD exige retirar el DNI de las firmas electrónicas por vulneración del principio de minimización

La Agencia Española de Protección de Datos ha declarado que la Comunidad Autónoma de Castilla-La Mancha (en adelante "CLM") ha vulnerado la normativa europea al incluir el número de DNI completo en las firmas electrónicas de sus empleados públicos.

El caso parte del funcionamiento de los sistemas de firma electrónica utilizados por la Junta, que permitían que cualquier ciudadano receptor de un documento firmado pudiera acceder al DNI del

funcionario. Aunque este dato podía no mostrarse directamente en la firma visible, resultaba siempre accesible a través de las propiedades del documento PDF, lo que facilitaba su consulta.

La AEPD considera que este tratamiento es desproporcionado y vulnera el principio de minimización de datos (artículo 5.1.c RGPD), ya que el DNI no es necesario para cumplir la finalidad de identificación del firmante en un acto administrativo. Además, la resolución subraya que el DNI constituye un dato de alta sensibilidad debido a su capacidad para identificar de forma directa e inequívoca a una persona y a los riesgos asociados, como la suplantación de identidad o los fraudes económicos.

Desde la perspectiva del artículo 25 RGPD, la AEPD aprecia también una falta de protección de datos desde el diseño, al no haberse implementado desde el inicio sistemas menos intrusivos ni revisado posteriormente el modelo para adaptarlo al principio de minimización.

En este sentido, la Agencia destaca que existen alternativas válidas y menos invasivas, como el uso de códigos de identificación profesional o certificados con seudónimo, que permiten cumplir la función de identificación sin exponer datos personales innecesarios.

Dado que se trata de una Administración pública, la resolución no impone una sanción económica, pero sí declara formalmente la infracción y ordena la adopción de medidas correctoras. En concreto, se concede un plazo de seis meses para que se elimine el DNI de las propiedades accesibles de los documentos firmados electrónicamente y se implanten soluciones técnicas que garanticen el cumplimiento del principio de minimización.

Contacto

Carme Setó

Socia | Derecho Digital, IT y protección de datos
cseto@duransindreu.com
93 602 52 22

Núria Galera

Abogada | Derecho Digital, IT y protección de datos
ngalera@duransindreu.com
93 602 52 22

Iván Roda

Abogado | Derecho Digital, IT y protección de datos
iroda@duransindreu.com
93 602 52 22

Bàrbara Boguñá

Abogada | Derecho Digital, IT y protección de datos
bboguna@duransindreu.com
93 602 52 22

Carlota Barreña

Área Derecho Digital, IT y protección de datos
cbarrena@duransindreu.com
93 602 52 22