DURÁNSINDREU

Newsletter Derecho Digital, IT y protección de datos

Novedades recientes

En esta nueva Newsletter sobre novedades más recientes en Derecho Digital, IT y protección de datos destacamos: nuevas sanciones de la AEPD por brechas de seguridad —incluyendo multas de 186.000 €, 3,2 millones € y 18.000 €—, además de casos por envíos comerciales sin consentimiento; la entrada en vigor de la Ley SAC; los avances en la reforma de la LO 1/1982 para abordar deepfakes y reforzar la protección de menores; y la primera sentencia europea que considera ilícito que modelos de IA memoricen obras protegidas.

DURÁNSINDREU

Índice de contenidos

Brechas de seguridad en 2025: riesgos reales y consecuencias para las organizaciones

Según informó la Agencia Española de Protección de Datos (en adelante, "**AEPD**") el pasado 23 de enero del presente, durante el año 2025 se recibieron un total de **2.765 notificaciones de brechas de seguridad**, con un impacto que superó los **200 millones de personas afectadas**. Ello pone de manifiesto que los incidentes de seguridad de los datos personales no son hechos aislados, sino un riesgo recurrente par organizaciones de todo tipo y sector.

Cabe recordar que se entiende por brecha de seguridad de los datos personales en los términos del artículo 33 del Reglamento General de Protección de Datos (en adelante, "**RGPD**") cualquier incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de cualquier otra forma, así como la comunicación o acceso no autorizado a dichos datos. Al respecto, su detección temprana, correcta evaluación y gestión diligente, incluida la notificación a la autoridad de control y, en su caso, a los interesados es especialmente

Incidente de seguridad en un E-Commerce deriva en una sanción de 186.000€

Una empresa comercial sufrió una brecha de seguridad en su tienda online que permitió el posible robo de datos de tarjetas de crédito de clientes mediante la inserción de código malicioso en el formulario de pago de la web. El ataque, de origen externo e intencionado, comprometió la confidencialidad de los datos de pago, como el número de tarjeta, fecha de caducidad y CVV, aunque no afectó al resto de datos personales almacenados en bases separadas.

La empresa tuvo indicios previos de problemas de seguridad desde 2023, pero dio los incidentes por resueltos. En febrero de 2024, tras la notificación de cargos fraudulentos por parte de un cliente y el aviso de terceros, confirmó la brecha, cambió el sistema de pago por una pasarela externa y notificó el incidente a la AEPD el 20 de febrero de 2024.

La AEPD inició actuaciones de oficio y requirió información en varias ocasiones. Los informes forenses revelaron que el sitio web estaba gravemente comprometido, con más de 140 archivos maliciosos, uso de herramientas sospechosas y numerosas vulnerabilidades críticas y altas, muchas de ellas conocidas desde años anteriores y no corregidas. Los atacantes aprovecharon vulnerabilidades de la plataforma para interceptar la información de las tarjetas de pago y transmitirla a sistemas ajenos a la empresa, sin que haya sido posible conocer con exactitud cuántos datos fueron sustraídos ni hasta dónde llegó el incidente.

Además, se constató que no se había realizado un análisis de riesgos específico, que existían deficiencias en las medidas de seguridad, inconsistencias en el número de afectados comunicados, y falta de contratos de encargo de tratamiento con algunos proveedores. Todo ello se produjo en una empresa con un elevado volumen de negocio, lo que agrava la relevancia del incidente.

La AEPD acordó iniciar un procedimiento sancionador contra la empresa por vulnerar el principio de seguridad y confidencialidad de los datos (art. 5.1.f del Reglamento General de Protección de Datos, en

adelante "RGPD") y por dos infracciones relacionadas con la falta de control y formalización adecuada de los encargados del tratamiento (art. 28 del RGPD).

La Agencia fijó como sanción posible una multa total de 310.000 €, desglosada en 150.000 € por la infracción del artículo 5.1.f del RGPD y 80.000 € por cada una de las dos infracciones del artículo 28 del RGPD.

3,2 millones de euros de sanción por múltiples brechas de seguridad

La AEPD ha impuesto una sanción de 3,2 millones de euros a una empresa de consumo tras constatar varias brechas de seguridad de datos personales sufridas entre 2022 y 2023. Según la resolución, los incidentes afectaron a un total de 118.895 cuentas únicas de clientes, en las que terceros accedieron de manera no autorizada mediante técnicas de "credential stuffing", obteniendo credenciales válidas y accediendo a datos personales como nombres, apellidos, fecha de nacimiento, documentos de identidad parcialmente enmascarados, correos electrónicos, teléfonos, direcciones y, en algunos casos, información económica.

La AEPD concluye que estos accesos ilegítimos constituyen una infracción muy grave del artículo 5.1.f del RGPD, por la pérdida de integridad y confidencialidad de los datos, y una infracción grave del artículo 32 del RGPD, al no haberse adoptado medidas técnicas y organizativas adecuadas pese a contar con auditorías, pruebas de penetración y evaluaciones de impacto de protección de datos previas. Entre las deficiencias señaladas se incluyen la detección insuficiente de accesos anómalos, la implementación tardía del doble factor de autenticación y el retraso en aplicar recomendaciones de seguridad.

La sanción incluye también una infracción leve del artículo 34 del RGPD por la gestión inadecuada de la comunicación de las brechas a los afectados. La empresa notificó solo la cuarta y quinta brecha, afectando a más de 20.000 clientes, mientras que las tres primeras no fueron comunicadas, aunque esta posible omisión se consideró prescrita. La AEPD obliga a la compañía a notificar correctamente todas las brechas a los afectados en el plazo de un mes y advierte que el incumplimiento de esta orden podría acarrear nuevas sanciones.

Las multas se desglosan en 2 millones de euros por la infracción del artículo 5.1.f RGPD, 1 millón por la infracción del artículo 32 RGPD y 200.000 euros por la infracción del artículo 34 RGPD.

En su defensa, la empresa sancionada había alegado que los accesos fraudulentos fueron limitados y que se habían adoptado medidas de seguridad, argumentos que la AEPD desestimó, ya que la pérdida de control sobre los datos y el riesgo para los derechos de los clientes se produce desde el primer acceso no autorizado. La Agencia concluye que los hechos acreditan una reiterada falta de diligencia en la protección de datos a gran escala.

Sanción de 18.000€ a una empresa de servicios tecnológicos por una brecha de datos que afectó a trabajadores de varias compañías

La AEPD sancionó a una compañía de servicios tecnológicos tras detectarse una brecha de seguridad que comprometió datos personales de empleados y exempleados de varias empresas vinculadas contractual y operativamente. El incidente fue notificado inicialmente el 6 de octubre de 2023, cuando se descubrió que los servidores de la empresa habían sido cifrados y se exigía un rescate para evitar la

divulgación de información. Posteriormente, se recibieron informes complementarios, así como notificaciones de otras entidades afectadas.

La investigación de la Subdirección General de Inspección de Datos, iniciada el 14 de diciembre de 2023 conforme a la normativa de protección de datos, determinó que un total de 976 personas resultaron afectadas. Los datos comprometidos incluían información identificativa, como nombre, apellidos, DNI, NIE, pasaporte, correo electrónico, teléfono y dirección postal, así como datos financieros de nóminas en algunos casos. Algunos archivos estaban protegidos con contraseña, aunque la protección resultó insuficiente ante el acceso no autorizado.

El fallo se originó a partir de deficiencias graves en la seguridad informática de la empresa, como la existencia de un usuario genérico de VPN con credenciales desactualizadas, ausencia de límite de intentos de autenticación, equipos obsoletos y falta de autenticación reforzada para accesos remotos. Estas vulnerabilidades permitieron el acceso indebido y la exfiltración de datos de empleados de varias empresas para las que la compañía actuaba como encargado de tratamiento de información.

La AEPD concluyó que la empresa vulneró el artículo 5.1.f) del RGPD, que obliga a garantizar la integridad y confidencialidad de los datos mediante medidas técnicas y organizativas adecuadas. La sanción inicial ascendía a 30.000 €, desglosada en 10.000 € por los datos propios de sus trabajadores y 20.000 € por los de empleados de terceros.

Destacamos la importancia de que las entidades tanto públicas como privadas implanten medidas de seguridad técnicas y organizativas adecuadas al riesgo a los efectos de minimizar riesgos en la producción de una brecha de seguridad de datos; así como, implanten protocolos de gestión de brechas para que estén preparadas en el caso que la brecha llegase a producirse.

Sanciones a la AEPD por vulneración de la normativa de la Sociedad de la Información:

Tras los casos de brechas de seguridad que han afectado a grandes empresas, la AEPD también ha sancionado a compañías por incumplimientos en el envío de publicidad electrónica.

Se sanciona a empresas por el envío reiterado de correos comerciales a una empresa que había solicitado expresamente dejar de recibirlos, vulnerando la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (en adelante, "**LSSI**").

La AEPD sanciona a una empresa dedicada a la programación informática por el envío reiterado de correos publicitarios sin consentimiento

La AEPD ha sancionado a una empresa por el continuado envío de correos electrónicos comerciales sin atender las solicitudes de baja de otra empresa, en una actuación que vulnera la LSSI.

El procedimiento tiene su origen en una reclamación presentada por la empresa afectada en febrero de 2025, en la que denunciaba haber recibido comunicaciones publicitarias desde abril de 2024 hasta febrero de 2025 pese a haber solicitado en al menos cuatro ocasiones el cese de dichos envíos, incluso después de una solicitud expresa de baja remitida el 8 de enero de 2025.

En su respuesta, la empresa investigada atribuyó la falta de atención a las solicitudes de baja a un fallo técnico en su sistema de correo electrónico, asegurando que el problema fue detectado y corregido en marzo de 2025, aunque no pudieron aportar registros técnicos que acreditaran dicho incidente.

La reclamación fue admitida a trámite y en agosto del 2025, la AEPD inició formalmente un procedimiento sancionador al considerar que los hechos podían constituir una infracción leve del artículo 21 LSSI, que prohíbe el envío de comunicaciones comerciales por correo electrónico sin el consentimiento previo del destinatario o sin atender su derecho de oposición.

La Agencia propuso inicialmente una sanción de 1.400 €. Sin embargo, la empresa sancionada optó por el reconocimiento de responsabilidad y el pago voluntario de la multa, acogiéndose a las reducciones legales previstas, lo que redujo la cuantía final de la sanción a 840 €. El pago se realizó el 14 de agosto de 2025, lo que supuso la terminación del procedimiento y la firmeza de la sanción en vía administrativa.

Novedades legislativas: Ley SAC y Anteproyecto de reforma de la LO 1/1982

Ley 10/2025 de Servicios de Atención a la Clientela: principales obligaciones y plazos de adaptación

El pasado 28 de diciembre de 2025 entró en vigor la Ley 10/2025, de 26 de diciembre, por la que se regulan los Servicios de Atención a la Clientela (en adelante, "**Ley SAC**"). La norma establece un plazo de adaptación de doce (12) meses, que finalizará el 28 de diciembre de 2026, para que las empresas obligadas adecuen sus servicios de atención a la clientela a los nuevos estándares legales.

Ámbito de aplicación:

- Empresas que prestan servicios básicos de interés general, como suministro de agua, gas y electricidad, transporte de pasajeros, servicios postales, comunicaciones electrónicas y servicios financieros.

- Empresas y grupos de sociedades que operen con consumidores finales en España y que, en el ejercicio económico anterior, superen determinados umbrales de plantilla, volumen de negocio o balance.

Principios generales del servicio de atención a la clientela:

- El servicio debe ser gratuito, eficaz, accesible, inclusivo y evaluable.

- Obligación de permitir la presentación de consultas, quejas y reclamaciones, facilitando clave identificativa y justificante en soporte duradero.

- Resolución ágil y motivada de las incidencias y derecho al reembolso o compensación en caso de incumplimiento contractual.

- Prohibición de suspender servicios de tracto sucesivo por la mera presentación de una reclamación, salvo excepciones legales.

Para más información sobre la Ley SAC puede consultar nuestra Nota Legal.

Anteproyecto de reforma de la LO 1/1982: honor, intimidad e imagen

El Gobierno aprobó el pasado mes de enero del presente el Anteproyecto de la Ley Orgánica de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, que actualizará la normativa vigente en aras a adaptarla a la realidad tecnológica y digital actual.

Si bien la reforma mantiene la estructura y principios intrínsecos de la citada normativa, introduce ajustes relevantes para una mayor protección de los derechos fundamentales. En ese sentido, entre las principales novedades cabe destacar:

Modificación del concepto de "intromisión ilegítima": se incorpora de forma expresa, como intromisión ilegítima a los mencionados derechos, la utilización o difusión de imágenes o voces creadas, simuladas o manipuladas tecnológicamente con una apariencia extremadamente realista, incluidas las denominadas ultrasuplantaciones o deepfakes.

- Refuerzo de la protección de los menores de edad: se introduce una presunción iuris tantum de madurez suficiente para otorgar el consentimiento a partir de los 16 años. No obstante, se establece como ilegítima, a pesar de existir el consentimiento del propio menor o de sus representantes, cualquier intromisión que pueda menoscabar su dignidad, reputación o intereses.

- Regulación específica del consentimiento de personas con discapacidad: en correlación con la Ley 8/2021, se permite que las personas con discapacidad presten su consentimiento por sí mismas, con los apoyos que, en su caso, precisen.

- Limitación del uso de la imagen o la voz tras el fallecimiento: se reconoce la posibilidad de que el testador pueda prohibir usos publicitarios, comerciales o análogos de su imagen o voz, así como de designar a un o varias personas para autorizar o denegar dichos usos.

- Criterios legales para la cuantificación del daño moral: el anteproyecto incorpora criterios como la gravedad de la lesión, la difusión o el alcance del contenido, la reiteración de la conducta, las repercusiones sociales, la prolongación en el tiempo de la intromisión o las circunstancias personales del afectado para cuantificar la indemnización relativa al daño moral. Asimismo, se establece que la indemnización no podrá tener un carácter simbólico.

En cualquier caso, se trata aún de un anteproyecto de ley, con lo que su contenido podría verse modificado a lo largo de su tramitación legislativa. Así, resulta oportuno seguir de cerca su evolución y esperar a su aprobación definitiva.

Inteligencia Artificial y Propiedad Intelectual

El Tribunal Regional de Múnich dictó la primera sentencia europea que considera ilícita la memorización de obras artísticas por inteligencia artificial. El fallo, que involucra a ChatGPT y canciones protegidas por la entidad GEMA, establece que entrenar un modelo con contenido protegido sin autorización constituye reproducción y comunicación pública, sentando un precedente clave en derechos de autor y tecnología.

Primera sentencia europea que reconoce la memorización de obras artísticas en IA como reproducción ilícita

El Tribunal Regional de Múnich falló el 11 de noviembre de 2025 a favor de la sociedad de autores alemana GEMA en un caso pionero sobre derechos de autor y uso de inteligencia artificial en Europa.

La disputa se originó porque ChatGPT entrenó sus modelos GPT-4 y GPT-4o con letras de canciones populares de artistas alemanes, que posteriormente podían reproducirse parcial o totalmente sin permiso.

El tribunal determinó que la memorización de obras protegidas en un modelo de lenguaje constituye una forma de reproducción, incluso si los textos no se almacenan de manera identificable, y que la excepción de minería de textos y datos solo cubre la extracción necesaria para preparar los datos, no la conservación ni reproducción de obras completas tras el entrenamiento. Además, los outputs del chatbot que reproducen las letras constituyen comunicación pública, y la responsabilidad recae directamente en OpenAI, no en los usuarios. También se descartó la existencia de consentimiento implícito por el hecho de que las obras estuvieran disponibles en Internet, ya que entrenar un modelo de IA con ellas requiere autorización expresa.

Como resultado, OpenAI deberá cesar la reproducción de las canciones, informar sobre los usos pasados y posibles ingresos obtenidos, y compensar los daños ocasionados, bajo riesgo de multas de hasta 250.000 €. La sentencia plantea retos técnicos, como la posible “desmemorización” de obras ya entrenadas, y abre la puerta a que entidades de gestión colectiva en otros países, como España, emprendan acciones similares.

La resolución marca un hito en Europa, consolidando la idea de que la innovación tecnológica no exime del respeto a los derechos de autor y podría influir en futuras decisiones del Tribunal de Justicia de la Unión Europea.

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