DURÁNSINDREU

Newsletter
Protección de datos

FEBRERO 2025

www.duransindreu.com

Esta Newsletter de febrero 2025 destaca avances normativos en ciberseguridad y protección de datos en España y la Unión Europea. Se menciona la aprobación del anteproyecto de Ley que transpondrá la Directiva NIS2 y la entrada en vigor de determinadas disposiciones del Reglamento de Inteligencia Artificial (RIA), mediante las que se prohíben, en el marco de la IA, prácticas como técnicas subliminales, manipulación, explotación de vulnerabilidades y sistemas de reconocimiento facial masivo, entre otras.

Se detallan resoluciones recientes de la AEPD, como una sanción de 60.000€ a una empresa de alquiler de vehículos por infracciones relacionadas con plazos de conservación de datos, información al interesado y gestión del derecho de acceso. También se recuerda la postura adoptada por la AEPD en relación con el tratamiento del DNI, considerándolo dato sensible cuyo uso debe limitarse a lo legalmente requerido.

En cuanto a jurisprudencia reciente, se destaca una sentencia del TJUE que permite calcular sanciones por infracciones del RGPD sobre el volumen de negocio global de grupos empresariales, no solo sobre la filial infractora. Finalmente, se analiza una sentencia del TSJPV que declaró nulo un despido basado en grabaciones de videovigilancia que no habían sido debidamente informadas a los trabajadores para fines de control laboral.

Novedades destacables

El Gobierno aprueba el Anteproyecto de Ley que transpondrá la Directiva NIS2

El pasado 14 de enero, el Consejo de Ministros aprobó el anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, mediante el cual se inicia el proceso de transposición de la Directiva NIS2 al ordenamiento jurídico español.

Para tener más información sobre a qué entidades afecta, obligaciones y próximos pasos consulta nuestra Nota Legal.

Entrada en vigor de los capítulos I y II del Reglamento de Inteligencia Artificial (RIA)

El Parlamento Europeo aprobó el Reglamento (UE) 2024/1689, también conocido como Reglamento de Inteligencia Artificial (RIA), que establece normas armonizadas en la UE para garantizar un desarrollo de la IA ético y respetuoso con los derechos fundamentales.

Calendario de aplicación del RIA

1 de agosto de 2024
Entrada en vigor del RIA

2 de febrero de 2025
Son aplicables Las prácticas prohibidas de los capítulos I y II del RIA.

2 de mayo de 2025
Oficina de IA elaborará Códigos de buenas prácticas por uso de la IA.

2 de agosto de 2025
Serán aplicables determinadas normas de gobernanza.

2 de febrero de 2026
La Comisión facilitará directrices de aplicación el RIA y lista exhaustiva de casos de uso de alto riesgo y de no alto riesgo.

2 de agosto de 2026
Aplicación del RIA con excepción del artículo 6.1 y obligaciones sobre los sistemas de IA de alto riesgo.

2 de agosto de 2027
Las disposiciones relativas a los sistemas de alto riesgo vinculadas a la legislación de armonización de la UE sobre seguridad de los productos serán aplicables a partir del 2 de agosto de 2027.

Puedes consultar toda la información sobre las novedades del RIA en nuestra Nota Legal.

Resoluciones de la AEPD

Empresa de alquiler de vehículos sancionada por la AEPD ante varias infracciones en materia de protección de datos

La Agencia Española de Protección de Datos (AEPD) ha sancionado a una entidad de alquiler de vehículos con 60.000€ por vulneraciones del RGPD en relación con el derecho de acceso y la transparencia en la gestión de datos personales.

Infracciones detectadas

- Plazo de conservación de datos: No se especificaron períodos de conservación según la finalidad del tratamiento, incumpliendo el artículo 5.1.e del RGPD. A pesar de que la empresa indicó un plazo genérico de 5 años, no detallaron criterios específicos vinculados para cada finalidad. Ello constituye un claro incumplimiento de la normativa, puesto que la misma exige definir plazos de conservación específicos y coherentes con las finalidades establecidas.
- Información al interesado: La identidad del responsable del tratamiento era confusa en la política de privacidad, infringiendo el artículo 13 del RGPD. Así, la AEPD detectó una discrepancia entre la razón social y el NIF del responsable, lo que generaba falta de claridad sobre quién trataba los datos.
- Derecho de acceso: la AEPD también concluyó que la entidad había incumplido los artículos 12 y 15 del RGPD, en relación con el derecho de acceso. Ello responde al hecho que la entidad no atendió a una solicitud en alemán alegando barreras lingüísticas y falta de acreditación, a pesar de que la entidad ofrecía servicios en Alemania en ese mismo idioma. En cuanto a la supuesta falta de acreditación, la AEPD entendió que la empresa no informó al interesado sobre la necesidad de documentación adicional ni ofreció alternativas para atender su solicitud.

Este caso resalta la importancia del **establecimiento de plazos concretos de conservación**, la transparencia y el cumplimiento de los derechos de los ciudadanos en materia de protección de datos. Las empresas deben asegurarse de que sus políticas sean claras y accesibles, y de que los procedimientos internos permitan a los usuarios ejercer sus derechos de manera efectiva.

La AEPD refuerza su postura sobre el tratamiento del DNI: requisitos y limitaciones

En los últimos meses, la Agencia Española de Protección de Datos (AEPD) ha emitido varias **resoluciones limitando la recogida, uso y conservación del Documento Nacional de Identidad (DNI).** En ese sentido, la AEPD ha venido exigiendo mayores medidas de seguridad y considerando el DNI un dato especialmente sensible debido a los riesgos asociados a su uso indebido.

Así, en su Informe 7/2023 la AEPD ya establecía que "*Sobre el uso del DNI, el criterio de esta Agencia es que únicamente se ha de someter a tratamiento cuando la norma así lo establezca, resultando excesivo el mismo cuando se pretende únicamente identificar a las personas, ya que el número del DNI es una información especialmente sensible pues su uso indebido o sin las garantías suficientes puede tener múltiples efectos desfavorables para el titular de los datos.*"

Mediante este enfoque, la AEPD refuerza la necesidad de que las organizaciones adopten **prácticas seguras y garanticen** el respeto a los principios de proporcionalidad y minimización de datos en el tratamiento de información personal.

Casos recientes

1. La AEPD sanciona a una entidad con 50.000€ por solicitar una copia del DNI mediante un canal que no ofrecía suficientes medidas de seguridad

Antecedentes del caso: Un inversor denunció a la empresa por exigir una copia de su **DNI** para acceder a información sobre los proyectos en los que participaba, sin ofrecer detalles sobre el tratamiento de sus datos personales.

Infracción detectada: Falta de medidas de seguridad adecuadas para la solicitud de información (Artículo 32.1 del RGPD). La infracción se basa en la **falta de medidas técnicas y organizativas adecuadas** al solicitar copia escaneada del DNI por correo electrónico. Aunque la empresa no especificó este medio de envío, se sobreentiende que era el canal utilizado para la comunicación. Si la empresa hubiera considerado que este no era un método seguro, debería haber ofrecido un canal alternativo.

Según el RGPD, los datos personales, en particular los documentos de identidad requieren **protecciones adicionales**, ya que pueden ser utilizados para **suplantaciones de identidad y fraudes**. En este caso, la empresa no realizó un **análisis de riesgos** ni implementó medidas de seguridad adecuadas para mitigar los peligros asociados a la transmisión del DNI por correo electrónico.

2. Sanción a un establecimiento de hospedajes por la recopilación excesiva de datos personales

En este supuesto, la AEPD sanciona a un establecimiento de hospedajes por la recopilación excesiva de información de los huéspedes sin una base legal suficiente. Así, aunque la normativa de seguridad ciudadana exige el registro de ciertos datos, la **exigencia de una imagen del DNI completa** no está justificada y excede los requisitos legales. La normativa únicamente exige la recopilación de datos específicos, como nombre, apellidos y número de documento, pero no la conservación de una copia o imagen del DNI, que contiene información adicional sensible, como la fotografía del titular y otros datos personales irrelevantes para el registro.

Además, el almacenamiento de imágenes completas del DNI supone un **riesgo innecesario** para la privacidad de los huéspedes, ya que facilita posibles casos de **suplantación de identidad y fraude**. En este caso, la entidad debería haber ofrecido alternativas menos invasivas, como la exhibición del documento sin necesidad de escanearlo o fotocopiarlo.

Recomendaciones para empresas

- Implementar **medios seguros** para la transmisión de documentos sensibles, como portales cifrados o firmas electrónicas.
- Realizar un **análisis de riesgos** antes de solicitar documentación personal.

- Evitar la recolección de documentos de identidad sin un protocolo de seguridad adecuado.
- Informar **de manera clara y detallada** a los usuarios sobre el tratamiento de sus datos personales, cumpliendo con el **artículo 13 del RGPD**.
- Asegurar que sólo se recojan **los datos estrictamente necesarios** para cumplir con las obligaciones legales.

Jurisprudencia destacada

Fallo del Tribunal de Justicia de la Unión Europea sobre las sanciones en materia de protección de datos a grupos empresariales

El **Tribunal de Justicia de la Unión Europea (TJUE)** ha emitido un fallo clave sobre la aplicación de sanciones en casos de infracción del Reglamento General de Protección de Datos (**RGPD**), en supuestos de grupos empresariales (STJUE 13 de febrero de 2025, C-383/23)

💼 **El caso**: Una empresa danesa, parte de un grupo empresarial, fue sancionada por almacenar indebidamente datos de 350.000 antiguos clientes. La cuestión central fue si la multa debía calcularse sobre el volumen de negocio de la entidad danesa o sobre el de todo el grupo empresarial.

⚖️ **El fallo**:

- El TJUE determinó que el término **"empresa"** en el artículo 83 del RGPD debe entenderse según la normativa de competencia de la UE (**artículos 101 y 102 TFUE**).
- Por lo tanto, en casos de sanción por incumplimiento del RGPD, la multa puede calcularse con base al **volumen de negocio global** del grupo empresarial, no sólo de la filial sancionada.
- Además, se ratificó que las multas deben ser **efectivas, proporcionadas y disuasorias**.

🔍 **Impacto en las empresas**:

- Mayor riesgo financiero para grupos empresariales que incumplan el RGPD.
- Mayor poder de las autoridades para imponer sanciones significativas.
- Necesidad de reforzar el cumplimiento normativo en toda la estructura del grupo.

📣 **Conclusión**: Con este fallo, la UE deja claro que el RGPD no sólo afecta a empresas individuales, sino a todo el ecosistema corporativo. Las multas podrán ser más severas si la empresa forma parte de un grupo con gran volumen de negocio.

Videovigilancia y control laboral: el TSJPV declara nulo un despido por uso indebido de cámaras

El **Tribunal Superior de Justicia del País Vasco** ha emitido una sentencia relevante sobre el uso de la videovigilancia en el ámbito laboral y su impacto en los derechos de los trabajadores.

💼 **El caso**: Un trabajador fue despedido tras ser captado por cámaras de seguridad en un presunto robo de material. La empresa utilizó las grabaciones como prueba clave para justificar el despido.

⚖️ **El fallo**:

- Aunque el sistema de cámaras estaba anunciado con **carteles visibles**, la empresa **no informó formalmente** a los trabajadores de que las imágenes podrían usarse para control laboral, incumpliendo la normativa.
- Las cámaras estaban destinadas a **fines de seguridad** en la empresa contratista principal, por lo que **no podían ser utilizadas** con otra finalidad sin previo aviso a los trabajadores.
- **Ambas empresas (contratista y principal) eran responsables** de garantizar la legalidad del uso de la videovigilancia.
- La empresa vulneró la **doctrina de los actos propios**, ya que había establecido previamente que las cámaras no se usarían para control laboral.
- El tribunal invalidó las pruebas obtenidas y declaró **nulo el despido**, obligando a la empresa a **readmitir al trabajador** y abonarle los **salarios de tramitación**.

🔍 **Lecciones clave para las empresas**:

- La videovigilancia debe cumplir estrictamente la **LOPDGDD** y el **RGPD**.
- No basta con instalar carteles informativos; los empleados deben ser notificados **explícitamente** de que las imágenes pueden ser utilizadas para control disciplinario.
- No se pueden cambiar las reglas de uso de las cámaras de forma arbitraria; si se han utilizado solo para seguridad, no pueden emplearse después para sancionar a trabajadores sin su conocimiento.
- El uso indebido de la videovigilancia puede llevar a la **nulidad del despido**, con las consecuentes indemnizaciones y salarios de tramitación.

📢 **Conclusión**: La sentencia refuerza la importancia de la **transparencia y legalidad** en el uso de la videovigilancia en el trabajo. Un mal uso de estos sistemas no solo puede resultar en la anulación de sanciones disciplinarias, sino que también puede generar responsabilidad legal para las empresas.

Contacto

Carme Setó
Socia | IP&IT y protección de datos
cseto@duransindreu.com
93 602 52 22

Cristina Miñana
Abogada | IP&IT y protección de datos
cminyana@duransindreu.com
93 602 52 22

Iván Roda
Abogado | IP&IT y protección de datos
iroda@duransindreu.com
93 602 52 22

Bàrbara Boguñá
Abogada | IP&IT y protección de datos
bboguna@duransindreu.com
93 602 52 22

Pere Puig
Área de IP&IT y protección de datos
ppuig@duransindreu.com
93 602 52 22