DURÁNSINDREU

Newsletter
Protección de datos y Derecho Digital

JULIO 2025

En este nuevo número de la **Newsletter de protección de datos y Derecho Digital de julio 2025** incluimos:

- **Reformas normativas:** La Comisión Europea propone elevar el umbral del Registro de Actividades de Tratamiento de 250 a 750 empleados para reducir cargas administrativas. La AEPD presenta su Plan Estratégico 2025-2030 enfocado en supervisión de tecnologías emergentes. En materia de transferencias, el CEPD clarifica aplicación del artículo 48 RGPD sobre solicitudes de autoridades de terceros países. La CNIL francesa establece condiciones para usar interés legítimo en desarrollo de IA y web scraping
- **Jurisprudencia destacada:** La Audiencia Nacional reduce una sanción de 6 a 2 millones de euros por concurso medial entre infracciones. Nuevas sanciones destacan violaciones del principio de minimización de datos en sectores hotelero y de ocio, así como graves brechas de seguridad en distribución minorista..
- **Novedades en regulación de sistemas de IA:**. El 2 de agosto entra en vigor el régimen supervisor del Reglamento de IA europeo con obligaciones para modelos de propósito general.

Novedades normativas destacadas

Propuesta de reforma RGPD

El pasado 21 de mayo del corriente la Comisión Europea propuso una reforma del Reglamento General de Protección de Datos (RGPD) que se enmarca en un "paquete ómnibus" de simplificación regulatoria para empresas, especialmente pequeñas y medianas empresas (en adelante, la "Reforma").

El objetivo principal de la Reforma es reducir la burocracia y las cargas administrativas, fomentando así la innovación y el crecimiento del ámbito empresarial. Con posterioridad, el Comité Europeo de Protección de Datos (CEPD) y el Supervisor Europeo de Protección de Datos (SEPD) han emitido el pasado 8 de julio un dictamen (en adelante, el "Dictamen") sobre la anterior propuesta de la Comisión Europea.

Si bien es importante destacar que la propuesta de la Comisión busca un equilibrio entre la necesidad de simplificar el cumplimiento para las empresas y la importancia de mantener los altos estándares de privacidad establecidos por el RGPD, la propuesta puede generar controversia ya que dicha flexibilización podría debilitar la protección de datos en esta tipología de empresas, si no se aborda de forma adecuada.

Propuesta de reforma del RGPD

La principal novedad de la propuesta de Reforma se refiere a **cambios en el umbral número y exenciones sobre la obligación de disponer de un Registro de Actividades del Tratamiento** regulado en el artículo 30 del RGPD.

En particular, la propuesta recoge **ampliar el umbral de excepciones** aplicables a la obligación de disponer de un RAT de forma que un mayor número de empresas puedan decidir no confeccionar este registro.

Al respecto, se propone **ampliar el umbral numérico** de empleados de una empresa para delimitar si es obligatorio disponer de un RAT y, además, hay cambios en las exenciones.

En este sentido, actualmente, aquellas empresas que empleen al menos a 250 **trabajadores deben disponer de un RAT** y con la propuesta se propone que dicho umbral **pase a al menos 750 empleados**, salvo que la empresa realice tratamientos de datos que supongan un alto riesgo para los derechos y libertades de los interesados en los términos del artículo 35 del RGPD. Esta propuesta de excepción sustituye las que están actualmente reguladas en el artículo 30.5 del RGPD las cuales establecen que, aun no alcanzando el umbral número de empleados, la empresa debe disponer de un RAT si se da alguna de estas tres circunstancias: (i) que el tratamiento entrañe riesgo, (ii) que no sea ocasional o (iii) que incluya categorías especiales de datos o antecedentes penales.

Otras propuestas de la Reforma serían las siguientes:

- **Nuevas Definiciones en el Artículo 4 RGPD:** Se incluye una definición de las PYMES en línea con el artículo 2 del Anexo de la Recomendación 2003/361/CE de la Comisión y una definición para las SMCs (*Smal Mid-Caps*) que se definirían como aquellas empresas que no son PYMES, emplean a menos de 750 personas y tienen una facturación anual que no excede los 150 millones de euros o un balance anual que no excede los 129 millones de euros, según la Recomendación de la Comisión de 21 de mayo de 2025.
- **Extensión del Ámbito de los Artículos 40.1 y 42.1 RGPD a las SMCs**: La propuesta extendería el alcance de los artículos 40.1 (códigos de conducta) y 42.1 (mecanismos de certificación) del RGPD a las SMCs.

Recomendaciones del dictamen

Respecto los cambios en la obligación de disponer del RAT, el Dictamen dictado por el CEPD y el SEPD recoge que, aunque no se mantenga el RAT en ciertos supuestos, **las obligaciones fundamentales del RGPD se mantienen inalteradas**, y se recalca la necesidad de que las empresas mantengan mecanismos internos de control de cumplimiento para garantizar el principio de responsabilidad proactiva en el tratamiento de datos personales.

En este punto, recuerdan que, aunque la exención se amplíe, **los registros de actividades de tratamiento son una herramienta muy útil para apoyar el cumplimiento** de diversos requisitos del RGPD, más allá de la simple demostración ex-post.

En este sentido, el CEPD y el SEPD apoyan el objetivo de reducir la carga administrativa para PYMES siempre que no se reduzca el nivel de protección de los derechos fundamentales de las personas, en particular el derecho fundamental a la protección de datos personales.

El Dictamen **enfatiza la importancia de que la propuesta final de reforma del RGPD** establezca claramente que los responsables y encargados del tratamiento deben realizar una evaluación de riesgos preliminar. Esta evaluación es crucial para determinar si una operación de tratamiento de datos entraña un "alto riesgo" y, por consiguiente, requiere la elaboración de una evaluación de impacto y su recogida en un registro a colación de la obligación del RAT recogida anteriormente. Se subraya por el CEPD y el SEPD la necesidad de un análisis individualizado para asegurar que los tratamientos que implican datos sensibles o el uso de métodos intensivos de tratamiento estén sujetos a las garantías adecuadas.

En definitiva, la reforma **no pretende eliminar obligaciones, sino adaptarlas a la realidad** de determinada tipología de empresas buscando, a su vez, reforzar la confianza en un modelo europeo de protección de datos que siga siendo un referente sin frenar la innovación.

Plan estratégico 2025-2030 de la AEPD

El pasado 3 de julio la Agencia Española de Protección de Datos (AEPD) presentó su Plan Estratégico 2025–2030. Un documento que regula las líneas esenciales de actuación de la AEPD para los próximos cinco años. Seguidamente analizamos los aspectos clave de este Plan centrado en la innovación responsable y en la defensa de la dignidad en la era digital.

Propósito y misión

- El Plan Estratégico 2025-2030 busca **proporcionar una estrategia estructurada** para la AEPD en un contexto de transformación digital continua.
- La misión de la AEPD es **garantizar de manera efectiva y proactiva el derecho fundamental a la protección de datos personales de la ciudadanía**, con especial atención a colectivos vulnerables. Se prioriza la privacidad desde el diseño y por defecto, y se fomenta la prevención y cooperación para alcanzar el máximo nivel de privacidad y protección de datos.

La AEPD se regirá por ocho principios clave

- **Independencia:** Actuar con plena autonomía orgánica, funcional y decisoria, libre de influencias externas.
- **Innovación y adaptabilidad:** Reforzar la agilidad y capacidad de adaptación a los cambios tecnológicos y sociales, promoviendo una cultura proactiva de innovación que integre la protección de datos desde el diseño y por defecto.
- **Internacionalización e influencia:** Mejorar su posicionamiento y capacidad de influencia en organizaciones internacionales.
- **Cooperación:** Generar nuevas alianzas y fortalecer las existentes a nivel nacional e internacional, promoviendo la colaboración y la creación conjunta de soluciones innovadoras.

- **Proactividad y prevención:** Anticiparse a los riesgos y desafíos en protección de datos, desarrollando actuaciones con una perspectiva preventiva basada en la sensibilización, el asesoramiento y la supervisión.
- **Excelencia y calidad técnica:** Mantener el rigor técnico en todas sus actuaciones, potenciando la formación del personal y la mejora de procesos.
- **Defensa del interés general:** Salvaguardar los derechos fundamentales y las libertades públicas vinculadas a la privacidad y el tratamiento de datos personales, promoviendo la confianza ciudadana y la equidad social.
- **Agencia abierta:** Caracterizarse por su apertura, transparencia, rendición de cuentas, participación e interacción con la ciudadanía, profesionales y la sociedad civil.

El plan se estructura en **siete ejes de actuación** entre los que destacamos su **compromiso con la innovación tecnológica responsable,** priorizando la supervisión de tecnologías emergentes como la IA, sistemas biométricos o neuro tecnologías. Al respecto fomentará la generación de conocimiento a través del Laboratorio de Privacidad y se reforzará el papel de la AEPD en la aplicación coordinada de normativas europeas.

El plan regula otros ejes de actuación centrados en la **promoción y en el acompañamiento** a las micropymes, startups, pymes, autónomos y administraciones públicas. en el **cumplimiento normativo** en protección de datos; el impulso de alianzas y colaboración con entidades y profesionales del sector y el liderazgo e **influencia estratégica internacional y nacional** incrementando la participación de la AEPD n foros nacionales e internacionales, especialmente en la Unión Europea y el Comité Europeo de Protección de Datos (CEPD), con proyección a Iberoamérica.

Evaluación y revisión continua

El Plan Estratégico se instrumenta en un **documento operativo interno con más de 200 medidas** concretas, responsables, plazos e indicadores de seguimiento.

Se realizará un seguimiento y evaluación continua, con la posibilidad de revisiones y actualizaciones dinámicas para incorporar nuevas normativas, tecnologías emergentes o transformaciones del entorno. Se ofrecerá información pública sobre el desarrollo y avance del citado Plan.

Recomendaciones de la CNIL sobre el uso del interés legítimo en el desarrollo de sistemas de inteligencia artificial

El 19 de junio de 2025, la **CNIL** (“***Commission Nationale de l'Informatique et des Libertés***”), la **autoridad de control francesa de protección de datos** publicó recomendaciones sobre el uso del interés legítimo como base jurídica para el desarrollo de sistemas de inteligencia artificial (**IA**).

Estas recomendaciones surgen de una consulta pública previa y buscan equilibrar la innovación en IA con la protección de los derechos fundamentales de las personas.

Los aspectos claves de las recomendaciones son los siguientes:

Interés Legítimo como base jurídica

- **Aplicabilidad:** La CNIL confirma que el interés legítimo puede ser una base adecuada para el desarrollo de IA, siempre que se cumplan ciertas condiciones. Es importante que el interés sea:
  - **Manifiestamente lícito** según la ley aplicable.
  - **Suficientemente específico y bien definido**.
  - **Real y presente** para la organización.

Asimismo, se enfatiza la necesidad de un "*balance de intereses*" riguroso, demostrando que el interés legítimo del desarrollador de IA no prevalece sobre los derechos y libertades de los interesados. Esto implica considerar los riesgos para los derechos fundamentales y las expectativas razonables de los afectados.

Adicionalmente, destacar que el tratamiento debe ser necesario para perseguir el interés legítimo, y no debe haber medios menos intrusivos disponibles.

Recopilación de Datos (*Web Scraping*)

- **Condiciones para el Web Scraping:** La CNIL establece condiciones para que el web scraping sea permisible bajo el interés legítimo:
  - **Exclusión de sitios con oposición explícita:** No se debe hacer scraping de sitios que lo prohíben activamente (por ejemplo, a través de archivos robots.txt).
  - **Datos libremente accesibles:** La recopilación debe limitarse a datos que sean libremente accesibles y que no requieran autenticación o registro.
  - **Exclusión de datos sensibles:** Se deben evitar la recopilación de datos sensibles o de categorías especiales (origen racial o étnico, opiniones políticas, creencias religiosas, datos de salud, etc.).
  - **Expectativas de privacidad:** Se debe respetar las expectativas de privacidad contextuales. Por ejemplo, se desaconseja el scraping de blogs personales, foros o sitios relacionados con la salud, donde las expectativas de privacidad son más altas.

Asimismo, se debe proporcionar información clara a los interesados sobre la recopilación y el uso de sus datos.

Medidas de salvaguardia y reducción de riesgos

- **Principio de minimización y técnicas de anonimización o cifrado:** Se recomienda la minimización de datos y, cuando sea posible, la anonimización o pseudonimización rápida de los datos recopilados. Se debe priorizar el uso de datos sintéticos si no afecta el rendimiento del modelo.
- **Derechos de los Interesados:** Es crucial garantizar que las personas puedan ejercer sus derechos sobre los datos utilizados en los conjuntos de entrenamiento y, en la medida de lo posible, en los modelos de IA. Se contempla la implementación de mecanismos de oposición efectivos.

- **Evaluación de Impacto en la Protección de Datos (EIPD):** La realización de una EIPD es fundamental, especialmente para tratamientos innovadores o de alto riesgo. Esta evaluación debe integrar el análisis de riesgos desde las fases iniciales de desarrollo del sistema de IA, considerando la calidad de los datos, los procesos de anotación, la trazabilidad de versiones y la gobernanza de los modelos.
- **Mitigación de Riesgos:** En el caso de la IA generativa, se debe abordar el riesgo de que el modelo "memorice" y reproduzca datos personales del conjunto de entrenamiento. La CNIL no exige la eliminación total de este riesgo, pero sí medidas de mitigación como el filtrado de entradas, la exclusión de entradas de alto riesgo (como nombres de usuario o publicaciones de foros) y pruebas internas para detectar la memorización o la fuga de datos.
- **Colaboración en Estándares Técnicos:** La CNIL recomienda que los desarrolladores de IA colaboren en la creación de estándares técnicos que permitan a los titulares de derechos oponerse de manera efectiva al uso de sus datos para el entrenamiento de IA.
- **Seguridad del Desarrollo de IA:** Se deben implementar medidas de seguridad durante el desarrollo del sistema de IA para proteger los datos y garantizar un entorno seguro.
- **Licencias y Restricciones de Uso:** Para sistemas de IA de propósito general, se recomienda limitar el riesgo de reutilización ilegal mediante medidas técnicas (como marcas de agua digitales) y/o legales (cláusulas contractuales que prohíban usos poco éticos o inesperados). También se contempla el uso de licencias que restrinjan los usos destinados a reidentificar a las personas.

En resumen, las recomendaciones de la CNIL buscan proporcionar un marco claro para el desarrollo de la IA, permitiendo la innovación, pero siempre con un fuerte énfasis en la protección de la privacidad y los derechos fundamentales.

El CEPD publica la versión final de las directrices sobre transferencias de datos a autoridades de terceros países

Por último, queremos destacar la publicación de la versión final de las Directrices sobre transferencias de datos a autoridades de terceros países

Las Directrices 02/2024 del Comité Europeo de Protección de Datos (CEPD) clarifican la aplicación del **Artículo 48 del Reglamento General de Protección de Datos**, el cual establece que las sentencias o decisiones de autoridades de terceros países que requieran la transferencia o divulgación de datos personales solo podrán ser reconocidas o ejecutables en la Unión Europea si se basan en un acuerdo internacional, como un tratado de asistencia legal mutua, en vigor entre el tercer país solicitante y la Unión o un Estado miembro. El objetivo principal de este artículo es reafirmar la soberanía legal de la UE frente a las leyes de terceros países y proteger los datos personales de la aplicación extraterritorial de dichas leyes. Estas directrices ofrecen recomendaciones prácticas para los responsables y encargados del tratamiento de datos en la UE que reciban este tipo de solicitudes.

Sentencias y resoluciones

Sentencia de la Audiencia Nacional, Sala de lo Contencioso Administrativo 1448/2021 de 8 de mayo de 2025, resaltando la eliminación de agravantes de la sanción administrativa de la que deriva

Hace pocos meses la Audiencia Nacional ha resuelto un recurso interpuesto por una entidad bancaria contra la resolución de la Agencia Española de Protección de Datos que le había impuesto una sanción total de 6 millones de euros por la comisión de varias infracciones del Reglamento General de Protección de Datos.

Los hechos que originaron dicha sanción se remontan a 2018 y 2019, cuando un particular, así como la asociación FACUA presentaron reclamaciones contra una entidad bancaria por el modo en que obtenía el consentimiento de sus clientes para el tratamiento de datos personales y por la cesión de dichos datos a terceras empresas del grupo sin proporcionar información clara ni mecanismos sencillos para revocar el consentimiento. A raíz de estas reclamaciones, la AEPD inició un procedimiento sancionador que terminó con una resolución de enero de 2021, confirmada posteriormente en marzo del mismo año, imponiendo dos sanciones: (a) Sanción de dos millones de euros por incumplir el deber de información (arts. 13 y 14 RGPD); y (b) Sanción de cuatro millones por tratar datos personales sin una base jurídica válida (art. 6 RGPD).

La entidad bancaria recurrió dicha resolución alegando, entre otros motivos, la caducidad del procedimiento, la falta de imparcialidad de la directora de la AEPD, la ausencia de pruebas que acreditasen el daño, la desproporcionalidad de las sanciones y la existencia de un concurso medial entre ambas infracciones, es decir, que una infracción fue medio para cometer la otra.

Si bien la Audiencia Nacional desestimó la mayoría de los argumentos planteados por la entidad bancaria, considerando probado que la información ofrecida a los clientes no cumplía con los estándares exigidos por el RGPD, y que el consentimiento recabado no era libre ni suficientemente informado, entendió procedente estimar uno de los argumentos empleados por la demandante.

En ese sentido, la Audiencia Nacional reconoció que se había producido un concurso medial entre las dos infracciones, dado que el incumplimiento del deber de información fue el medio necesario para que se produjera el tratamiento ilícito de datos. Por tanto, en lugar de imponerse dos sanciones independientes, procedía impuesto una sola sanción por la infracción más grave.

Asimismo, en cuanto a la apreciación de las agravantes, la Sala entendió que, en cuanto a la prevista en el artículo 83.2.a RGPD, relativa a la naturaleza, gravedad y duración de la infracción, esta circunstancia es inherente a la propia tipicidad del hecho sancionado, es decir, que la vaguedad e imprecisión de la información —origen del consentimiento inválido— forma parte del núcleo del tipo infractor y no puede operar adicionalmente como agravante. Del mismo modo, respecto a la agravante recogida en el artículo 83.2.h RGPD, referida a la ausencia de procedimientos adecuados de tratamiento de datos, el tribunal señala que dicha carencia es igualmente consustancial a la infracción y no debe ser apreciada como elemento agravante autónomo.

En consecuencia, la Audiencia **Nacional estimó parcialmente el recurso y anuló la resolución impugnada** en cuanto a la acumulación de sanciones, estableciendo una única multa de 2 millones de euros (reduciendo por tanto la inicial de 6 millones) al apreciarse la existencia de un concurso medial.

Nueva sanción para empresa hotelera sancionada por escanear el DNI de sus clientes

La Agencia Española de Protección de Datos ha **sancionado a una empresa hotelera con una multa de 9.000 euros por vulnerar el principio de minimización de datos** recogido en el Reglamento General de Protección de Datos.

El origen de la sanción recae en una reclamación presentada por un cliente, quien denunció que, durante el proceso de registro en el hotel, se le solicitó el escaneo de su DNI. Ante su negativa, el personal copió sus datos manualmente.

Ante dicha reclamación, la entidad hotelera justificó esta práctica alegando que estaba cumpliendo con las obligaciones del Real Decreto 933/2021, que regula la comunicación de datos de huéspedes a las Fuerzas y Cuerpos de Seguridad del Estado. Sin embargo, la AEPD aclaró que esta normativa **no exige el escaneo ni la copia completa del documento de identidad,** sino únicamente la recogida de determinados datos (nombre, apellidos, número de documento, etc.).

Así, la AEPD concluyó que el escaneo del DNI supone un tratamiento de datos excesivo, **al incluir información innecesaria como la fotografía, el número CAN o datos de familiares, lo que vulnera el principio de minimización de datos del RGPD**. Además, este tipo de prácticas aumenta el riesgo de suplantación de identidad.

Finalmente, la entidad hotelera reconoció su responsabilidad y se acogió al pago voluntario, lo que le permitió beneficiarse de dos reducciones del 20% sobre la sanción inicial (9.000 euros), asumiendo finalmente, una sanción de 5.400 euros.

Entidad sancionada por solicitar más datos de aquellos estrictamente necesarios para la compra de entradas vía web

La Agencia Española de Protección de Datos ha resuelto que **una fundación pública del sector del ocio ha vulnerado el Reglamento General de Protección de Datos** y, concretamente, el principio de minimización de datos al **exigir demasiada información personal para comprar entradas a través de su página web**.

La reclamación fue presentada por un ciudadano que se encontró con un proceso de compra que obligaba a facilitar datos como nombre, apellidos, email, teléfono móvil, dirección postal, fecha de nacimiento, pasaporte o DNI, país y código postal. Ante ello, la AEPD ha considerado **que esta práctica incumple el principio de minimización de datos**, ya que muchos de estos datos no eran necesarios para gestionar la venta de entradas.

Durante el proceso, **la fundación introdujo mejoras**: hizo opcionales algunos campos (como la fecha de nacimiento o el número de documento), revisó su política de privacidad y justificó parte de la recogida de datos por motivos fiscales, de seguridad o de atención al cliente. Sin embargo, la AEPD concluyó que estos argumentos no justificaban la obligatoriedad inicial de datos como el teléfono, el código postal o el DNI.

Aunque la infracción fue calificada como muy grave, la AEPD **no impuso sanción económica al tratarse de una fundación pública**.

Sin perjuicio de lo anterior, se le ha ordenado como obligación de hacer modificar su sistema de recogida de datos en el plazo de tres meses para adaptarlo a la normativa.

Sanción por múltiples medidas de seguridad y falta de medidas de seguridad necesarias

La AEPD ha impuesto a una cadena multinacional de distribución minorista y mayorista una serie de **sanciones por múltiples violaciones de seguridad de datos personales**, detectadas y notificadas por la propia empresa entre 2023 y 2024.

Las infracciones principales se relacionan con **el acceso ilegítimo a cuentas de clientes mediante la técnica de "Credential Stuffing"** (uso de credenciales filtradas de otros orígenes), lo que resultó en la **exposición de datos** como nombre, apellidos, correo electrónico, dirección postal, DNI y contraseñas. La AEPD argumenta que la entidad no implementó medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos, como la implementación tardía del doble factor de autenticación (2FA) a pesar de haber sufrido múltiples brechas con el mismo vector de ataque.

La cadena de alimentación fue sancionada por **tres infracciones** distintas del RGPD. En particular, una infracción muy grave del artículo 5.1.f) por la **vulneración del principio de integridad y confidencialidad** (multa de 2.000.000 euros), una infracción grave del artículo 32 por la **falta de medidas de seguridad adecuadas** (multa de 1.000.000 euros), y una infracción leve del artículo 34 por la **comunicación incompleta de las brechas de seguridad** a los afectados (multa de 200.000 euros). La empresa alegó haber tomado medidas proactivas para mitigar los daños y haber cooperado con la AEPD, así como que el número de afectados por la pérdida de integridad y confidencialidad era menor al total de cuentas.

Sin embargo, la AEPD desestimó la mayoría de estas alegaciones, enfatizando que la pérdida de control sobre los datos personales se produce desde el momento del acceso no autorizado y que la actividad de la entidad, con un gran volumen de datos personales, exige una diligencia exquisita.

Como resultado, la AEPD impone una **multa total de 3.200.000 euros**. Adicionalmente, se ordena a la entidad comunicar de manera adecuada las brechas de datos personales a todos los afectados, en un plazo de un mes desde que la resolución sea firme y ejecutiva

Resolución sobre la denegación de un derecho de acceso de un usuario a direcciones IP

Un usuario solicitó a una entidad de telefonía el derecho de acceso a las direcciones IP que le habían sido asignadas como titular de una línea fija en un periodo determinado, y la misma denegó dicho

acceso. La AEPD admitió a trámite la reclamación el 21 de noviembre de 2024, tras constatar que la respuesta inicial de la entidad no satisfacía las pretensiones del reclamante.

La empresa de telefonía argumentó que, si bien una dirección IP es un dato personal, su divulgación, especialmente si es compartida por varios usuarios, podría comprometer la privacidad y la confidencialidad de las comunicaciones de terceros, en cumplimiento de su obligación como operador de telecomunicaciones. Para ello, basó su denegación en el artículo 15, apartado 4, del RGPD que establece que el derecho a obtener copia de los datos no debe afectar negativamente a los derechos y libertades de otros, un principio también respaldado por el Considerando 63 del RGPD. La empresa afirmó que la entrega de las direcciones IP podría permitir inferencias sobre actividades privadas de otros usuarios, vulnerando el secreto de las comunicaciones electrónicas y su deber de confidencialidad.

La AEPD concluyó que la denegación por parte de la empresa de telefonía fue motivada y ajustada a derecho. La Agencia reconoció que una dirección IP es un dato personal, pero enfatizó que no son únicas para un solo titular y pueden ser compartidas por varios usuarios, especialmente las dinámicas, que son las más comunes en conexiones residenciales. Por lo tanto, la AEPD determinó que la entidad no está obligada a proporcionar acceso a las direcciones IP solicitadas cuando su divulgación pueda afectar la privacidad y confidencialidad de las comunicaciones de terceros sin su consentimiento explícito. La resolución desestima la reclamación al considerar que el derecho de acceso se atendió de forma completa, denegando motivadamente lo que no se podía facilitar.

Novedades en materia de regulación de sistemas de Inteligencia Artificial

El próximo 2 de agosto, varias disposiciones clave del Reglamento (UE) 2024/1689 de Inteligencia Artificial ("RIA") de la Unión Europea serán de aplicación obligatoria.

Recordemos que el RIA tiene un calendario de aplicación gradual, con diferentes fechas para distintas obligaciones.

Las principales disposiciones que serán exigibles a partir de esta fecha son las siguientes:

- Modelos de IA de Propósito General: Este es uno de los puntos más relevantes que serán de aplicación. El RIA clasifica los modelos de IA según su potencial de riesgo. Los modelos de IA de Propósito General son aquellos que pueden ser utilizados para una amplia gama de propósitos y que pueden ser integrados en diversos sistemas de IA.

Las implicaciones prácticas para los proveedores de GPAI y para los que los desplieguen son las siguientes:

- Documentación Técnica y Transparencia: Los proveedores de estos sistemas deberán elaborar y mantener documentación técnica detallada sobre el modelo, sus capacidades y

limitaciones, para facilitar su uso responsable por parte de los desarrolladores posteriores. Esto incluye información sobre los datos utilizados para el entrenamiento.

- Gestión de Derechos de Autor: Deberán establecer guías y políticas para respetar los derechos de autor de los contenidos utilizados en el entrenamiento de los modelos y para los contenidos generados.
- Resumen de Contenidos de Entrenamiento: Deberán publicar un resumen de los contenidos utilizados para entrenar el modelo. Esto busca una mayor transparencia sobre la procedencia de los datos.
- Gestión del Riesgo Sistémico: Algunos sistemas podrían conllevar riesgos sistémicos (por ejemplo, para los derechos fundamentales o la seguridad pública). Los proveedores deberán evaluar y mitigar estos riesgos.

Otras implicaciones para los proveedores derivadas del marco legal serán supervisar, documentar e informar sobre incidentes graves; mantener un nivel adecuado de ciberseguridad y para proveedores no pertenecientes a la UE, designar un representante autorizado en la UE.

- Gobernanza y Autoridades Nacionales Competentes: A partir del 2 de agosto del corriente los Estados miembros de la UE deben designar a las autoridades nacionales competentes encargadas de supervisar la aplicación de las normas de IA y de realizar actividades de vigilancia del mercado. También deberán comunicar sus datos de contacto a la Comisión Europea.

Implicaciones prácticas

- Identificación de Autoridades: Las empresas y desarrolladores deberán conocer qué autoridades nacionales serán sus puntos de contacto para cuestiones relacionadas con el cumplimiento del Reglamento de IA en su país.
- Preparación para la Supervisión: Las autoridades nacionales comenzarán a ejercer sus funciones de supervisión y control, lo que implica que las empresas deberán estar preparadas para posibles inspecciones, solicitudes de información o auditorías de cumplimiento.
- Oficina de IA de la Comisión Europea: A nivel de la UE, la Oficina de IA de la Comisión será el principal organismo de implementación y encargado de hacer cumplir las reglas para los modelos de IA de propósito general.
- Sanciones del RIA: Aunque las multas específicas por infracción no se aplicarán en su totalidad hasta agosto de 2026, a partir del 2 de agosto de 2025, los Estados miembros tienen el plazo para establecer las normas sobre sanciones y multas, notificarlas a la Comisión y garantizar su correcta aplicación.

Al respecto, el pasado 11 de marzo se aprobó para su tramitación por la vía de urgencia el Anteproyecto de Ley para el buen uso y la gobernanza de la Inteligencia Artificial que desarrolla el régimen sancionador y de gobernanza previsto en el RIA. El Anteproyecto tiene como principal

misión adecuar la legislación española al RIA, en especial en cuanto a su régimen sancionador, así como, las autoridades de vigilancia del mercado competentes para el ejercicio de la citada potestad sancionadora. Estamos a la espera de su tramitación parlamentaria atendiendo la aplicación del marco sancionador.

Implicaciones prácticas

- Riesgo Financiero: Las multas pueden ser muy elevadas. Por ejemplo, por violaciones de las aplicaciones de IA prohibidas, las multas podrían ascender hasta el 7% de la facturación anual global de la empresa, hasta el 3% por otras violaciones y hasta el 1.5% por proporcionar información incorrecta.
- Refuerzo de la Debida Diligencia: La posibilidad de sanciones importantes exige que las empresas realicen una debida diligencia exhaustiva para asegurar el cumplimiento, especialmente en áreas de alto riesgo.

  En dicho ámbito es relevante que las empresas procedan a la revisión de sus seguros de responsabilidad civil en cuanto a las coberturas ante eventuales daños causados por sistemas de IA. Al respecto, recientemente durante este mes de julio de 2025 se ha completado un estudio solicitado por la Comisión de Asuntos Jurídicos del Parlamento Europeo que analiza la evolución del enfoque de la Unión Europea para regular la responsabilidad civil de los sistemas de IA. Al respecto, un marco de responsabilidad claro, eficiente y centrado en el ser humano es crucial para la competitividad de Europa en el sector de la IA.
- Sistemas de IA Prohibidos: Aunque la prohibición de los sistemas de IA de riesgo inaceptable fue de aplicación el pasado 2 de febrero de 2025, el próximo 2 de agosto será de aplicación el régimen supervisor y sancionador aplicable a estas prohibiciones. Esto significa que las autoridades nacionales ya podrán iniciar acciones contra el uso o comercialización de estos sistemas.

Implicaciones prácticas para empresas y desarrolladores:

- Reconfirmación de la Prohibición: Si bien ya estaban prohibidos, las empresas deben asegurarse de no estar utilizando ni comercializando sistemas de IA que caigan en las categorías de "riesgo inaceptable". Esto incluye, entre otros:

  – Sistemas de manipulación subliminal o engañosa que puedan causar daño físico o psicológico.

  – Sistemas que exploten vulnerabilidades de personas (edad, discapacidad, entre otros), para alterar su comportamiento de forma perjudicial.

  – Sistemas de "puntuación social" (social scoring) por parte de autoridades.

  – Sistemas de evaluación predictiva del riesgo penal basados únicamente en el perfilado de una persona.

- Sistemas de identificación biométrica remota "en tiempo real" en espacios de acceso público (con excepciones muy limitadas y estrictas).
- Creación o expansión de bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes de internet o videovigilancia.
- Sistemas de reconocimiento de emociones en entornos laborales y educativos (salvo por razones médicas o de seguridad justificadas).

Evaluación de Riesgos Continuada: Es fundamental que las organizaciones que desarrollan o implementan IA realicen evaluaciones continuas para identificar si alguno de sus sistemas podría encajar en estas categorías prohibidas y, de ser así, detener su uso o desarrollo.

Aprobación en Europa del Código de Buenas prácticas para la IA de propósito general

A raíz de la inminente aplicación de las disposiciones del RIA anteriormente citadas, el pasado 10 de julio del corriente se ha ultimado y aprobado en Europa un Código de Buenas Prácticas para IA de uso general. La **adhesión voluntaria** a este código puede ayudar a los proveedores a demostrar el cumplimiento de las obligaciones del RIA, beneficiándose de una menor carga administrativa y mayor seguridad jurídica.

Para los proveedores de modelos de IA de propósito general, el Código aborda y promueve las siguientes prácticas, cuyas obligaciones serán de aplicación a partir del 2 de agosto de 2025:

- **Documentación Técnica y Transparencia:** Los proveedores deben elaborar y mantener documentación técnica detallada sobre el modelo, sus capacidades, sus limitaciones y su funcionamiento. Esto incluye información sobre los datos utilizados para el entrenamiento, lo que facilita el uso responsable por parte de otros desarrolladores.
- **Gestión de Derechos de Autor:** Deben establecer directrices y políticas claras para respetar los derechos de autor de los contenidos utilizados en el entrenamiento de los modelos, así como para los contenidos generados por la IA.
- **Resumen de Contenidos de Entrenamiento:** Se exige a los proveedores que publiquen un resumen de los contenidos utilizados para entrenar el modelo. Esto es un paso hacia una mayor transparencia en la procedencia de los datos.
- **Gestión del Riesgo Sistémico:** Los proveedores deben evaluar y mitigar los riesgos sistémicos que sus modelos puedan generar, por ejemplo, aquellos que afecten a los derechos fundamentales o a la seguridad.
- **Transparencia:** El Código se alinea con los siete requisitos clave para una "*IA Confiable*" establecidos por el Grupo de Expertos de Alto Nivel en IA, entre los que se encuentra la transparencia.
- **Rendición de Cuentas:** Otro requisito fundamental es la rendición de cuentas, lo que implica que debe ser posible atribuir responsabilidades por las acciones de los sistemas de IA.

Implicaciones prácticas

- Para las empresas que desarrollan o utilizan sistemas de IA de propósito general, adherirse a este Código de Buenas Prácticas no solo es una señal de compromiso con la ética y la seguridad, sino también una estrategia proactiva para prepararse para las fases de aplicación más estrictas de la Ley de IA.
- Aunque es voluntario, el cumplimiento de estas directrices puede ser un factor atenuante en caso de litigios o investigaciones por parte de las autoridades competentes.
- Facilita la interoperabilidad y el entendimiento común sobre cómo deben operar los modelos de IA en el mercado europeo, reduciendo la incertidumbre regulatoria.

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