N.º 22

GA_P
Gómez-Acebo & Pombo

Boletín

DERECHO DIGITAL

2026

G A _ P
Gómez-Acebo & Pombo

CONTENIDO

PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO DIGITAL

Dictámenes 14/2026 y 15/2026 del Comité Europeo de Protección de Datos (EDPB) sobre los criterios de certificación de Europrivacy

La certificación es uno de los mecanismos de rendición de cuentas a los que hace referencia el Reglamento General de Protección de Datos (RGPD) y uno de los menos utilizados en la práctica. Los artículos 42 y 43 permiten a los responsables y encargados del tratamiento demostrar el cumplimiento mediante sistemas voluntarios y auditados de forma independiente, y el artículo 42, apartado 5, prevé un sello europeo de protección de datos cuyos criterios deben ser aprobados por el Comité Europeo de Protección de Datos (EDPB o el «Comité»).

Hasta hace poco, esa vía sólo se había materializado en una ocasión: en el Dictamen 28/2022, de 10 de octubre, el Comité aprobó los criterios de Europrivacy como el primer (y único) sello europeo de protección de datos, concebido como una herramienta para demostrar el cumplimiento y no para las transferencias internacionales.

Una segunda posibilidad se había quedado en el papel. En virtud del artículo 46, apartado 2, letra *f*, del Reglamento General de Protección de Datos, una certificación aprobada con arreglo al artículo 42 puede constituir por sí misma una garantía adecuada para las transferencias a terceros países, siempre que vaya acompañada de compromisos vinculantes y exigibles por parte del importador de datos. El Comité había explicado cómo debían evaluarse dichos sistemas en sus Directrices 07/2022 sobre la certificación como herramienta para las transferencias (directrices adoptadas el 14 de febrero del 2023), pero nunca se había aprobado ni aplicado ninguna certificación sobre esa base.

Ambas lagunas se abordan en los dos dictámenes adoptados el 15 de abril del 2026, a raíz de las observaciones presentadas por la autoridad de control de Luxemburgo (LU SA) el 29 de enero del 2026.

El Dictamen 14/2026 aprueba los criterios actualizados de Europrivacy (versión 82) como

sello europeo de protección de datos con arreglo al artículo 42, apartado 5, del Reglamento General de Protección de Datos. El principal cambio con respecto al del 2022 es la ampliación del ámbito de aplicación del sistema a los responsables y encargados del tratamiento establecidos fuera del Espacio Económico Europeo, pero sujetos al mencionado reglamento en virtud del artículo 3, apartado 2; va acompañada, además, de un nuevo criterio que aborda los posibles conflictos con la legislación de terceros países: cuando no exista una decisión de adecuación que cubra el objeto de la evaluación, el solicitante deberá presentar un dictamen de un experto jurídico en el que se confirme que la legislación y la práctica del tercer país no impiden el cumplimiento de los requisitos de certificación. Asimismo, se han perfeccionado los criterios en lo que respecta a la designación de un representante en el Espacio Económico Europeo, al Informe de Evaluación del Cumplimiento de las Obligaciones Nacionales (NOCAR), al tratamiento posterior, a las categorías especiales de datos, a los derechos de los interesados, a la contratación de subencargados del tratamiento, a la gestión de las violaciones de datos, a la evaluación de riesgos y a la política y requisitos de seguridad. Se aplica un régimen transitorio: las certificaciones en curso deben finalizarse antes de que acabe el 2026; los certificados expedidos con arreglo a la versión 60 seguirán siendo válidos hasta que llegue a término su plazo de tres años, y la versión 60 quedará totalmente derogada antes de que concluya el 2029.

El Dictamen 15/2026 es el más novedoso de los dos. Por primera vez, el Comité aprueba un sello europeo de protección de datos que se utilizará como herramienta para las transferencias en virtud de los artículos 42, apartado 2, y 46, apartado 2, letra *f*, del Reglamento General de Protección de Datos, mediante una extensión independiente que certifica a los importadores de datos establecidos fuera del Espacio Económico Europeo que no están sujetos a dicho reglamento. Los criterios requieren, entre otras garantías, compromisos vinculantes y exigibles por parte del importador frente al exportador del Espacio Económico Europeo, una evaluación de impacto de la transferencia con medidas complementarias cuando sea necesario, el reconocimiento de los interesados como terceros beneficiarios con derecho a hacer valer las normas, la cooperación con la autoridad de control competente para el exportador y la exclusión del ámbito de aplicación del tratamiento conjunto; las transferencias no podrán comenzar antes de que se haya expedido el certificado.

En conjunto, ambos dictámenes hacen que la certificación del Reglamento General de Protección de Datos pase de ser un mecanismo en gran medida teórico a uno operativo y añaden una vía certificada al conjunto de las herramientas ya existentes (las decisiones de adecuación, las cláusulas contractuales tipo y las normas corporativas vinculantes para la transferencia de datos personales a terceros países).

Inês Dias Pinheiro

Comité Europeo de Protección de Datos: Directrices 1/2026 sobre el tratamiento de datos personales con fines de investigación científica

Las Directrices 1/2026 sobre el tratamiento de datos personales con fines de investigación

científica establecen un marco interpretativo completo sobre la aplicación del Reglamento General de Protección de Datos al uso de datos personales en el ámbito de la investigación. El documento parte de una premisa esencial: la investigación científica constituye un objetivo de especial relevancia para la Unión Europea, pero su desarrollo debe conciliarse con la protección de los derechos fundamentales de las personas, en particular, la privacidad y la protección de datos.

En este contexto, las directrices precisan que no cualquier actividad puede acogerse al régimen específico previsto por el citado reglamento para la investigación científica. Para ello, la investigación debe tener una naturaleza genuinamente científica, lo que exige, entre otros elementos, un enfoque metódico y sistemático, el respeto de los estándares éticos, la transparencia y verificabilidad de los resultados, la independencia de los investigadores y una contribución real al conocimiento o al interés social.

El documento aborda también las bases jurídicas que pueden legitimar el tratamiento de datos personales, incluidos el consentimiento, el interés público, el cumplimiento de obligaciones legales y el interés legítimo. En particular, presta especial atención al consentimiento, que puede adoptar fórmulas flexibles como el consentimiento amplio, referido a un área de investigación determinada, o el consentimiento dinámico, mediante el cual los participantes autorizan proyectos concretos a medida que éstos se plantean. En ambos casos, se exige información clara y garantías adicionales para los interesados.

Otra cuestión relevante es la conservación de los datos. Aunque el reglamento general permite conservar datos personales durante periodos más prolongados cuando sea necesario para fines de investigación, los responsables deben justificar dicha duración, revisar periódicamente su necesidad y evitar una conservación indefinida sin una finalidad concreta.

Por último, las directrices subrayan la importancia de la transparencia, el respeto de los derechos de los interesados y la adopción de garantías adecuadas como la anonimización o seudonimización, la supervisión ética, los entornos seguros de tratamiento y las evaluaciones de impacto relativas a la protección de datos. En definitiva, el documento busca equilibrar el impulso de la innovación científica con una protección sólida de los datos personales, exigiendo responsabilidad proactiva, transparencia y garantías robustas durante todo el ciclo de la investigación.

Claudia Pérez Moneu

Recomendación (UE) 2026/1035 de la Comisión, de 29 de abril, sobre el establecimiento de un marco común para las tecnologías de verificación de la edad a escala de la Unión

La Comisión Europea ha adoptado la Recomendación (UE) 2026/1035, que establece un régimen jurídico común para el desarrollo de tecnologías de verificación de la edad en la Unión Europea. El objetivo principal es reforzar la protección de los menores en entornos digitales garantizando al mismo tiempo el respeto de la privacidad y la seguridad de los datos personales.

El creciente uso por los menores de servicios en línea, como redes sociales, videojuegos o plataformas de contenido, genera importantes oportunidades, pero también riesgos, como la exposición a contenidos nocivos o el ciberacoso. Por ello, la Comisión considera esencial disponer de métodos fiables de verificación de la edad que permitan limitar el acceso a determinados servicios y contenidos sensibles.

La recomendación propone el desarrollo de una solución europea armonizada basada en tecnologías seguras, interoperables y respetuosas con la privacidad. Estas herramientas deben permitir únicamente confirmar si una persona supera una determinada edad (por ejemplo, los dieciocho años), evitando la recopilación innecesaria de datos y el seguimiento de la actividad en línea de los usuarios.

Para ello, la Comisión impulsa un sistema europeo de verificación de la edad apoyado en un plan director técnico de código abierto y en su integración con las futuras carteras europeas de identidad digital. Asimismo, se prevé la creación de listas de proveedores y de soluciones de confianza para garantizar que cumplan los requisitos de fiabilidad, seguridad y protección de datos.

La recomendación insta a los Estados miembros a facilitar el despliegue de estas soluciones antes de finales del 2026 y a coordinar sus actuaciones para evitar la fragmentación del mercado interior. En definitiva, se trata de avanzar hacia un entorno digital más seguro, especialmente para los menores, sin comprometer los derechos fundamentales de todos los ciudadanos.

Iratze
Arrigain García

La Agencia Española de Protección de Datos y la transcripción de voz con IA: responsabilidad, derechos y transparencia

En su publicación de 20 de abril del 2026, la Agencia Española de Protección de Datos (AEPD) continúa su análisis sobre la transcripción de voz mediante inteligencia artificial (IA) y su impacto en la protección de datos, particularmente la exigencia de aplicar plenamente las obligaciones del Reglamento General de Protección de Datos (RGPD) en relación con este tipo de operaciones que constituyen tratamientos de datos personales.

En este sentido, la agencia subraya que, al recurrir a este tipo de productos, servicios y aplicaciones de inteligencia artificial, el responsable y el encargado del tratamiento deben garantizar, con medidas adecuadas, el cumplimiento de las garantías del referido reglamento.

El regulador incide en el principio de exactitud del artículo 5 del Reglamento General de Protección de Datos, en la medida en que una transcripción atribuye una información a una persona identificada o identificable, lo que implica la necesidad de prever mecanismos eficaces para su acceso y rectificación, adaptados a las particularidades técnicas de estos sistemas, pero sin que puedan verse condicionados por las posibles limitaciones técnicas o por los datos de terceros cuando éstos puedan ser protegidos.

Por último, la Agencia Española de Protección de Datos insiste en las exigencias de transparencia: los interesados deben ser conscientes en todo momento de que están siendo grabados gracias a indicativos visibles o auditivos activos

durante toda la sesión; el responsable debe garantizar que la información sobre la grabación y sus fines se comunique de forma efectiva con carácter previo, sin ampararse en fórmulas genéricas de consentimiento (como advertencias implícitas al acceder a una sesión); el consentimiento debe ser específico para cada grabación y limitado temporalmente, lo que exige mecanismos que aseguren la finalización automática de la captación de voz una vez concluida la sesión.

En definitiva, la adopción de soluciones de transcripción de voz con inteligencia artificial no exime del cumplimiento normativo, sino que, por el contrario, exige un enfoque proactivo y reforzado de cumplimiento en materia de protección de datos.

Camino Bustinduy de la Guerra

La mera solicitud de datos personales implica su tratamiento

La Sala de lo Contencioso-Administrativo del Tribunal Supremo español, en su Sentencia 390/2026, de 26 de marzo (ECLI:ES:TS:2026::1590), ha examinado si puede entenderse que se ha producido un tratamiento de datos personales en los términos recogidos en el artículo 4 del Reglamento General de Protección de Datos por el solo requerimiento de aportación de documentación con datos protegidos de carácter personal.

Tras recordar que el *tratamiento de datos de carácter personal* se define en el artículo 4 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos (RGPD), como «cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjunto de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción», el alto tribunal declara lo siguiente:

> … la adecuada salvaguarda de los derechos fundamentales de la persona, singularmente el derecho a la protección de datos de carácter personal, reconocido en el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, así como el derecho a la intimidad personal, proclamado en el artículo 18, párrafos 1 y 4, de la Constitución española, exige una interpretación amplia y no restrictiva del concepto del tratamiento de datos de carácter personal […], de lo que se infiere que el responsable del tratamiento de datos de carácter personal quede sujeto al cumplimiento de los principios reguladores del tratamiento de datos de carácter personal, entre ellos, el principio de minimización de datos, contenidos en el artículo 5 del citado Reglamento (UE), desde el mismo momento en que solicita a una persona física la aportación de datos de carácter personal, con independencia de que los mencionados datos lleguen o no a ser efectivamente facilitados y ulteriormente recogidos por el responsable del tratamiento de datos, todo ello con la finalidad de prevenir la

> generación de riesgos relevantes para los derechos fundamentales de las personas afectadas».

En efecto, según el Tribunal Supremo, el tratamiento responsable de los datos personales comienza con la mera solicitud al interesado de la aportación de datos de carácter personal, por cuanto, en ese momento, el responsable del tratamiento de los datos está obligado a examinar si los datos personales cuya aportación y entrega solicita cumplen efectivamente los principios relativos al tratamiento de datos mencionados en el artículo 5 del Reglamento General de Protección de Datos y, entre ellos, si los datos que se solicitan son adecuados y pertinentes y están limitados a lo necesario en relación con los fines para los que van a ser tratados.

Por el contrario, no existiría una eficaz protección si se aceptara que la autoridad, una vez que tuviera en su poder y conoce los datos personales, pudiera entonces determinar si esos datos «recogidos» son adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que hubieran sido recogidos. Es decir, una interpretación del tratamiento de datos de carácter personal que dependiera del éxito del intento de acceso a los datos personales generaría una incertidumbre incompatible con el principio de seguridad jurídica y con la protección de los derechos fundamentales de las personas físicas.

Ángel García Vidal

El concepto amplio de *responsable del tratamiento de datos personales*

La Sala de lo Civil del Tribunal Supremo, en su Sentencia 620/2026, de 20 de abril (ECLI:ES:TS:2026:1704), ha reiterado su jurisprudencia previa sobre el responsable del tratamiento de datos personales. Como es sabido, el artículo 4.7 del Reglamento General de Protección de Datos define al *responsable del tratamiento* como «la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento». Pues bien, según el Tribunal Supremo, cuando los actos son realizados por diferentes sociedades de un mismo grupo empresarial, debe seguirse un concepto amplio de responsable del tratamiento, de modo que las distintas sociedades sean responsables, y añade que una interpretación restrictiva del concepto de *responsable del tratamiento* supondría, en la práctica, un serio obstáculo, cuando no un impedimento, para la efectividad de los derechos fundamentales que el ordenamiento jurídico de la Unión Europea, las normas convencionales internacionales y las propias normas internas, constitucionales y de rango legal y reglamentario protegen frente al tratamiento automatizado de datos personales de carácter ilícito.

Ángel García Vidal

PROPIEDAD INTELECTUAL

Copias sin conexión en los servicios de *streaming:* no son copias privadas

Como es notorio, el modo *offline* de las plataformas de *streaming* permite a los usuarios acceder a obras previamente almacenadas en sus dispositivos sin necesidad de conexión a la red. Esta posibilidad se integra en los servicios de suscripción ofrecidos por los proveedores con fines comerciales, mejorando así la accesibilidad y la experiencia de uso del servicio.

La cuestión, no obstante, es si estas copias *offline* encajan en el concepto de *copia privada* que maneja la Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información, y que se refiere a reproducciones en cualquier soporte efectuadas por una persona física para uso privado y sin fines directa o indirectamente comerciales. Dicha directiva permite a los Estados miembros introducir una excepción o limitación al derecho de reproducción, de modo que se permitan las copia privadas, pero siempre que los titulares de los derechos reciban una compensación equitativa.

Pues bien, el Tribunal de Justicia, en su Sentencia de 16 de abril del 2026, *Stichting de Thuiskopie*, C-496/24 (ECLI:EU:C:2026:296), ha declarado que «la puesta a disposición, mediante una copia en *streaming offline*, de una obra protegida, efectuada por el proveedor de un servicio de *streaming* en el dispositivo del usuario final, a petición de dicho usuario, sin que éste pueda disponer técnicamente de ella fuera de ese servicio y garantizando, al mismo tiempo, que el titular de los derechos de autor sobre la obra conserve un control sobre ésta que le permita, en su caso, bloquear el acceso a la copia, no está comprendida en la excepción de copia privada».

En consecuencia, esas copias *offline* no son copias privadas, sino reproducciones por las que el titular del derecho puede obtener una remuneración pactada con el proveedor del servicio de *streaming*. Como afirma el Tribunal de Justicia, el titular de los derechos está

en condiciones de supervisar la utilización de sus obras protegidas por las personas que acceden legalmente a ellas, y la autorización de copias en *streaming offline* forma parte de la explotación normal por dicho titular, respecto de la cual puede negociar una compensación ejerciendo su derecho de autor.

Ángel
García Vidal

INTELIGENCIA ARTIFICIAL

Directrices de la Comisión Europea sobre el cumplimiento de las obligaciones de transparencia

El artículo 50 de la ley de inteligencia artificial —Reglamento de Inteligencia Artificial (IA)— impone obligaciones de transparencia para determinados sistemas de IA:

AI Act	Sistema de IA	Responsable	Obligación de transparencia
50.1	Sistemas de IA que interactúan directamente con personas físicas	Proveedor	Diseñar el sistema de modo que las personas sepan que están interactuando con una IA
50.2	Sistemas de IA que generan o manipulan audio, imágenes, vídeo o texto sintéticos	Proveedor	Marcar los resultados en un formato legible por máquina y garantizar que sean detectables como generados o manipulados por IA
50.3	Sistemas de reconocimiento de emociones y de categorización biométrica	Responsables del despliegue	Informar a las personas afectadas de que el sistema está en funcionamiento
50.4	*Deep fakes* y determinados textos de interés público generados o manipulados por IA	Responsable del despliegue	Revelar que el contenido ha sido generado o manipulado artificialmente

La Comisión Europea ha elaborado unas directrices que contienen orientaciones prácticas para ayudar a las autoridades competentes, así como a los proveedores y a quienes implementan sistemas de inteligencia artificial, a garantizar el cumplimiento de estas obligaciones de transparencia.

Estas directrices se sometieron a consulta pública hasta el 3 de junio. Se espera que su adopción definitiva tenga lugar antes de que el artículo 50 entre en vigor el 2 de agosto del 2026.

Las directrices incluyen numerosos ejemplos y aclaran las excepciones. A continuación, señalamos algunos que consideramos especialmente relevantes:

— *Artículo 50, apartado 1: sistemas de IA interactivos*

Las directrices contienen un catálogo negativo explícito: la divulgación en los términos y condiciones, las señales legibles por máquina por sí solas, las referencias genéricas a un «asistente» y declaraciones como «este sistema utiliza modelos de lenguaje a gran escala (LLM)» incumplen lo dispuesto en el artículo 50, apartado 1.

— *Artículo 50, apartado 2: identificación y detección de contenidos generados por IA*

El artículo 50, apartado 2, no es específico de la GPAI (sigla de *general-purpose artificial intelligence* —inteligencia artificial de propósito general—): comprende cualquier sistema de inteligencia artificial que genere o manipule contenidos sintéticos de audio, imagen, vídeo o texto, incluidas las herramientas de uso único, como un motor de traducción, un clonador de voz o un generador de imágenes de un único dominio.

— *Artículo 50, apartado 3: reconocimiento de emociones y categorización biométrica*

El artículo 50, apartado 3, abarca todos los sistemas de categorización biométrica, incluidos los que no entran en la clasificación de alto riesgo. Los sistemas que deducen el rango de edad, el género o el origen étnico con fines publicitarios; los de análisis de tiendas o de adaptación de contenidos, incluso cuando los proveedores los hayan excluido del catálogo de alto riesgo, siguen estando sujetos a la obligación de incluir un aviso conforme al artículo 50, apartado 3.

— *Artículo 50, apartado 4: «Deepfakes» y textos de interés público generados por IA*

La forma de divulgación difiere de la del artículo 50, apartado 2: mientras que este apartado 2 exige una marca legible por máquina y detectable mediante herramientas, el apartado 4 exige una divulgación que sea directamente perceptible por el ser humano: una etiqueta visible, una superposición en pantalla, una señal de audio o un método análogo adaptado a la modalidad. El público debe reconocer el origen artificial sin necesidad de utilizar ninguna herramienta técnica. En consecuencia, para los responsables del despliegue, una marca de agua *(watermark)* conforme al artículo 50.2 e incorporada previamente no cumple por sí sola con la obligación establecida en el artículo 50.4.

Daniel Reis

Proyecto de directrices de la Comisión sobre la clasificación de los sistemas de inteligencia artificial de alto riesgo

En mayo del 2026, la Comisión Europea ha publicado el borrador de las directrices sobre la clasificación de los sistemas de alto riesgo en el marco del Reglamento de Inteligencia Artificial, con el objetivo de aportar criterios interpretativos que faciliten una aplicación uniforme por parte de los diversos operadores. Aunque se trata de un instrumento no vinculante, constituye una referencia práctica relevante para anticipar cómo se valorará si a un sistema le será aplicable el régimen más exigente del citado reglamento.

El borrador confirma el enfoque basado en el riesgo del Reglamento de Inteligencia Artificialy aclara que la calificación como de alto riesgo depende, en primer lugar, de que el sistema encaje en la definición de *inteligencia artificial* y, en segundo lugar, de su finalidad prevista. En este sentido, se incide en la importancia de la documentación técnica, contractual y comercial del proveedor para determinar el uso que se haya propuesto darle. Asimismo, las directrices estructuran el análisis en torno a dos principales clasificaciones:

1) sistemas que constituyen productos o componentes de seguridad sujetos a normativa sectorial (anexo I);

2) sistemas utilizados en determinados ámbitos sensibles (anexo III), como empleo, educación, biometría o acceso a servicios esenciales.

El borrador aborda la clasificación mediante ejemplos prácticos y criterios técnicos adicionales, incluidos mecanismos que permiten descartar determinados sistemas cuando no influyen materialmente en la toma de decisiones. En este sentido, la Comisión insiste en que la evaluación debe realizarse atendiendo a los riesgos reales para la salud, la seguridad o los derechos fundamentales.

En definitiva, estas directrices proporcionan información para evaluar los sistemas de inteligencia artificial y anticipar si quedarán sujetos a las obligaciones reforzadas aplicables a los sistemas de alto riesgo (incluidos los requisitos de gobernanza, control humano o gestión de riesgos).

Camino Bustinduy de la Guerra

Simplificación de las normas de inteligencia artificial

La Comisión Europea ha acogido favorablemente el acuerdo político alcanzado entre el Parlamento Europeo y el Consejo para simplificar la aplicación de las normas de la Unión Europea sobre inteligencia artificial manteniendo al mismo tiempo sólidas garantías para los ciudadanos. La reforma forma parte del denominado *ómnibus digital sobre la IA*, orientado a impulsar la innovación y la competitividad en toda la Unión Europea.

El acuerdo introduce un calendario de aplicación más claro y gradual para los sistemas de inteligencia artificial de alto riesgo. Las normas aplicables a sectores sensibles, como la biometría, la educación, el empleo o el control fronterizo, comenzarán a aplicarse en diciembre del 2027, mientras que los sistemas integrados en productos de consumo lo harán en el 2028.

Este enfoque progresivo pretende ofrecer a las empresas tiempo suficiente para adaptarse y alinearse con los estándares técnicos.

Al mismo tiempo, el marco refuerza la protección de los derechos fundamentales. En particular, prohíbe expresamente las aplicaciones de inteligencia artificial que generen contenido íntimo no consentido o material de abuso sexual infantil, en respuesta a la creciente preocupación por el uso indebido de las tecnologías de inteligencia artificial generativa.

Para las empresas, especialmente las de menor tamaño, las nuevas normas buscan reducir la carga administrativa y mejorar la claridad jurídica. Entre las medidas previstas se cuentan la extensión de determinados beneficios a las pequeñas empresas de mediana capitalización, una mayor coherencia con la legislación sobre seguridad de los productos y la ampliación del acceso a espacios controlados de pruebas o *regulatory sandboxes*, incluido un nuevo entorno de pruebas a escala de la Unión Europea para probar soluciones innovadoras de inteligencia artificial.

El acuerdo también refuerza los mecanismos de supervisión, en particular mediante el fortalecimiento del papel de ejecución de la Oficina de Inteligencia Artificial de la Comisión, especialmente en relación con los sistemas de inteligencia artificial de propósito general y las grandes plataformas en línea.

En resumen, la reforma busca alcanzar un equilibrio entre el fomento de la innovación y la garantía de la seguridad, ofreciendo a las empresas un entorno regulatorio más accesible, sin rebajar los elevados estándares de protección de los ciudadanos europeos

Claudia Pérez Moneu

Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho

El Consejo de Europa ha adoptado un nuevo Convenio Marco sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho, llamado a convertirse en una referencia internacional para la gobernanza de los sistemas de inteligencia artificial. El texto parte de una idea central: el desarrollo y uso de ésta debe quedar alineado, durante todo su ciclo de vida, con los derechos fundamentales, la democracia y el Estado de derecho.

La aprobación del convenio se produce en un contexto de rápida expansión de las tecnologías de inteligencia artificial. Estas herramientas ofrecen oportunidades relevantes para la innovación y el progreso social, pero también plantean riesgos significativos, como la discriminación, la pérdida de privacidad o su utilización con fines de vigilancia o manipulación.

Frente a estos desafíos, el convenio articula una serie de principios que los Estados signatarios deberán promover. Entre ellos, destacan el respeto de la dignidad humana y de la autonomía individual, la transparencia y supervisión de los sistemas de inteligencia artificial, la responsabilidad por los impactos adversos, y la protección de la igualdad y de la no discriminación. El texto refuerza, además, las garantías de privacidad y de protección de datos, así como las exigencias de fiabilidad y seguridad de estas tecnologías.

Su ámbito de aplicación se dirige principalmente a las autoridades y a los actores privados que actúen por cuenta de aquéllas, aunque

también exige a los Estados abordar los riesgos que puedan derivarse de la actividad del sector privado en sentido amplio. El convenio prevé igualmente la existencia de recursos efectivos para las personas cuyos derechos puedan verse afectados por sistemas de inteligencia artificial y fomenta la creación de entornos controlados que permitan impulsar una innovación segura.

El instrumento incorpora también mecanismos de cooperación internacional y de seguimiento de su aplicación, lo que confirma su vocación de servir como estándar global en materia de inteligencia artificial fiable. Su finalidad es clara: permitir el desarrollo tecnológico sin debilitar la protección de los derechos fundamentales, asegurando que la inteligencia artificial contribuya de forma positiva a las sociedades democráticas y que sus riesgos sean minimizados debidamente.

Iratze Arrigain García

Proyecto de Ley Orgánica para el buen uso y la gobernanza de la inteligencia artificial

El Congreso de los Diputados tramita actualmente el Proyecto de Ley Orgánica para el Buen Uso y la Gobernanza de la Inteligencia Artificial (exp. 121/000096), impulsado por el Gobierno para adaptar el ordenamiento jurídico a las exigencias del Reglamento de inteligencia Artificial desarrollando aquellos aspectos cuya concreción corresponde a los Estados miembros.

En particular, la iniciativa establece el sistema nacional de gobernanza y supervisión de la inteligencia artificial designando autoridades competentes y articulando un modelo descentralizado en función del sector afectado (incluyendo, entre otras, a la Agencia Española de Supervisión de Inteligencia Artificial —AESIA—, a la Agencia Española de Protección de Datos —AEPD— y a autoridades financieras). Asimismo, regula espacios controlados de pruebas para fomentar la innovación en entornos seguros y prevé medidas organizativas específicas, especialmente en el sector público.

Desde la perspectiva de cumplimiento, el texto incorpora un régimen sancionador por incumplimiento de las obligaciones del Reglamento de Inteligencia Artificial, así como mecanismos de coordinación y supervisión del mercado. Igualmente, refuerza la exigencia de transparencia, control y responsabilidad en el uso de sistemas de inteligencia artificial, con especial atención a la protección de los derechos fundamentales y a la prevención de sesgos o usos indebidos.

La iniciativa constituye un paso clave en la construcción del marco nacional de aplicación del Reglamento de Inteligencia Artificial y, más allá de su contenido técnico, anticipa un entorno regulatorio más exigente en el que las organizaciones deberán integrar la gobernanza de la inteligencia artificial en sus sistemas de cumplimiento, especialmente en lo relativo a supervisión, documentación, control de riesgos y transparencia en el despliegue de esta tecnología.

Camino
Bustinduy de la Guerra

SOBERANÍA TECNOLÓGICA

El paquete de soberanía tecnológica: la ley de chips 2.0 y la ley de desarrollo de la nube y la IA

1. *Refuerzo de la soberanía tecnológica europea*

La Comisión Europea ha situado la soberanía tecnológica en el centro de su nueva agenda de política digital. En un contexto marcado por el aumento de las tensiones geopolíticas, la creciente demanda de infraestructuras para inteligencia artificial y la persistente dependencia de proveedores tecnológicos no europeos, la Comisión pretende reforzar la capacidad de Europa para desarrollar, desplegar y controlar tecnologías digitales clave.

Este nuevo paquete sirve como marco introductorio para dos grandes iniciativas legislativas: El Reglamento de Chips 2.0, también conocido como *ley de chips 2.0 (Chips Act 2.0)* se centra en la base tecnológica de los semiconductores, fundamental para la competitividad digital e industrial europea, mientras que el Reglamento de Desarrollo de la Nube y de la IA *(Cloud and AI Development Act —CADA—)* aborda la capacidad de computación, la infraestructura *cloud* y los servicios soberanos necesarios para apoyar el despliegue de la inteligencia artificial a gran escala. En conjunto, ambas propuestas forman parte de una estrategia europea más amplia dirigida a reducir dependencias estratégicas, reforzar la resiliencia y asegurar que Europa desempeñe un papel más activo en la configuración de la próxima etapa de la economía digital.

2. *Reglamento de Chips 2.0 («Chips Act 2.0»)*

La propuesta del Reglamento de Chips 2.0 constituye el nuevo marco de la Comisión Europea para reforzar el ecosistema de semiconductores de la Unión tras la aprobación del primer Reglamento de Chips. Su punto de partida es la persistente vulnerabilidad estructural de Europa en este ámbito: la Unión Europea produce menos del 10 % de los semiconductores a escala mundial y mantiene una elevada dependencia de los Estados Unidos y Asia respecto de los

chips más avanzados, incluidos los destinados a inteligencia artificial.

Aunque el primer Reglamento de Chips permitió impulsar avances relevantes (como cinco líneas piloto, una plataforma europea de diseño, centros de competencia en los Estados miembros, líneas piloto de chips cuánticos e importantes inversiones públicas y privadas en instalaciones de producción), la Comisión considera que siguen existiendo dos grandes problemas: por un lado, la excesiva dependencia de terceros países en el diseño y fabricación de semiconductores; por otro, una preparación insuficiente ante posibles crisis o interrupciones de suministro.

El Reglamento de Chips 2.0 propone, por ello, una estrategia más amplia basada en la combinación de oferta, demanda y resiliencia. La opción preferida, denominada *strategic sovereignty*, prevé reforzar el apoyo a la investigación, al desarrollo y a la innovación, aclarar las reglas aplicables a instalaciones pioneras, agilizar los procedimientos de autorización, invertir en capacidades profesionales y crear una nueva etiqueta «Regiones de Excelencia en Semiconductores» para atraer inversión hacia ecosistemas regionales sólidos.

La propuesta incorpora además medidas industriales específicas, como proyectos estratégicos a escala de la Unión, aceleradores para trasladar la innovación del laboratorio a la fábrica, contratación pública innovadora y posibles criterios vinculados a la seguridad del suministro. También refuerza la iniciativa *Chips for Europe 2.0* apoyando capacidades de diseño, líneas piloto, tecnologías avanzadas, chips cuánticos, centros de competencia y financiación para empresas emergentes y empresas en crecimiento.

En conjunto, el objetivo es hacer que Europa sea más competitiva, menos dependiente, mejor preparada frente a eventuales escaseces y más capaz de convertir su excelencia investigadora en capacidad industrial real.

3. *Propuesta de Reglamento de Desarrollo de la Nube y de la IA*

El 3 de junio del 2026, la Comisión Europea presentó su Propuesta de Reglamento de Desarrollo de la Nube y de la IA (CADA por sus siglas en inglés), un proyecto dirigido a reforzar el ecosistema europeo de la nube y de la inteligencia artificial. La iniciativa responde a dos debilidades estructurales identificadas por la Comisión: la disponibilidad limitada y geográficamente concentrada de capacidad de computación en la Unión Europea y la dependencia europea de servicios de nube e inteligencia artificial prestados por proveedores no europeos. Según la Comisión, tres hiperescaladores no pertenecientes a la Unión controlan actualmente más del 70 % del mercado europeo de servicios en la nube, mientras que la cuota de los proveedores europeos descendió del 29 % en el 2017 al 15 % en el 2022.

La propuesta de reglamento pretende aumentar la capacidad de computación ubicada en la Unión Europea, facilitar el despliegue de centros de datos sostenibles, reducir la dependencia de servicios en la nube y de inteligencia artificial no soberanos y reforzar la resiliencia de los servicios utilizados por el sector público. Uno de los elementos centrales de la propuesta es la creación de iniciativas de liderazgo en nube e inteligencia

artificial, que incluyen grandes retos a escala europea centrados en centros de datos sostenibles; infraestructuras en la nube europeas; inteligencia artificial de frontera, física, industrial y para el sector público; y agentes de inteligencia artificial.

La propuesta introduce también un marco para zonas de aceleración de centros de datos y proyectos estratégicos apoyado en procedimientos de autorización simplificados, puntos únicos de información y mecanismos de seguimiento de la brecha de capacidad de computación en la Unión Europea. Desde la perspectiva de la demanda, establece un marco europeo de soberanía en la nube con cuatro niveles de garantía que incorporan requisitos progresivamente más estrictos sobre establecimiento en la Unión, localización de datos, certificación de ciberseguridad, soporte operativo, controles de la cadena de suministro de *software* y exposición al control de terceros países.

En cuanto a la contratación pública, la propuesta exigiría a los poderes adjudicadores utilizar, como mínimo, servicios de nube con nivel de garantía de la Unión 1, elevando dicho nivel cuando las evaluaciones de riesgo identifiquen supuestos relevantes para el orden público. También promueve criterios de adjudicación de valor añadido europeo, contratación conjunta, una Federación EuroCloud y un mayor uso de soluciones de código abierto por parte de los organismos públicos.

Si se adopta, la propuesta de reglamento abrirá nuevas oportunidades para operadores europeos de nube, inteligencia artificial y centros de datos, aunque también introducirá importantes exigencias de cumplimiento, auditoría, contratación y transición para proveedores, autoridades públicas y determinadas entidades privadas críticas.

Claudia Pérez Moneu

G A _ P
Gómez-Acebo & Pombo

Para más información, contacte con las siguientes letradas del Grupo de Propiedad Intelectual:

Sofía Martínez-Almeida y Alejos-Pita

Socia
smartinez@ga-p.com

Rais Amils Arnal

Socia
ramils@ga-p.com