Beta Bits Legal Recap

HIGHLIGHTS DE MAYO 2026

Derecho Digital y Protección de Datos

1. LA COMISIÓN EUROPEA PUBLICA EL BORRADOR DE DIRECTRICES SOBRE TRANSPARENCIA EN IA

La Oficina de IA de la Comisión Europea ha publicado el borrador de las directrices para la implementación de las obligaciones de transparencia previstas en el Artículo 50 del Reglamento de Inteligencia Artificial (AI Act). El objetivo de estas directrices es servir de guía práctica para ayudar a las autoridades competentes, así como a los proveedores y usuarios de sistemas de IA, a garantizar el cumplimiento de dichas obligaciones de forma coherente, eficaz y uniforme.

El borrador se ha elaborado en paralelo al Código de Buenas Prácticas para el etiquetado de contenido generado por IA.

Disponible en: https://digital-strategy.ec.europa.eu/en/library/draft-guidelines-implementation-transparency-obligations-certain-ai-systems-under-article-50-ai-act.

2. LA COMISIÓN EUROPEA PUBLICA EL BORRADOR DE DIRECTRICES PARA CLASIFICAR LOS SISTEMAS DE IA DE ALTO RIESGO

El 19 de mayo de 2026, la Comisión Europea publicó el borrador de directrices sobre la clasificación de sistemas de IA de alto riesgo, con el objetivo de ayudar a proveedores, usuarios y autoridades de vigilancia del mercado a determinar cuándo un sistema de IA debe considerarse de alto riesgo, facilitando así la aplicación uniforme y la ejecución efectiva del Artículo 6 del RIA.

Disponible en: https://digital-strategy.ec.europa.eu/en/library/draft-commission-guidelines-classification-high-risk-ai-systems.

3. ESTUDIO DE ORIENTACIÓN SOBRE LAS PROHIBICIONES DE IDENTIFICACIÓN BIOMÉTRICA REMOTA EN EL RIA

La Dirección General de Redes de Comunicación, Contenido y Tecnología de la Comisión Europea (CNECT) ha publicado un estudio que analiza en profundidad las prácticas prohibidas recogidas en el Artículo 5 del AI Act, con el objetivo de ayudar a proveedores, usuarios y autoridades competentes a comprender el alcance de dichas prohibiciones, sus excepciones expresamente previstas y su aplicación práctica.

El documento se centra en las prohibiciones del artículo 5.1.h RIA, sobre el uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público y la del artículo 5.1.e, que prohíbe crear o ampliar bases de datos de reconocimiento facial mediante la recopilación masiva e indiscriminada de imágenes de Internet o de circuitos cerrados de televisión. Respecto a la primera prohibición, el estudio también analiza sus tres excepciones: la búsqueda dirigida de víctimas de determinados delitos o personas desaparecidas, la prevención de amenazas inminentes a la vida o la seguridad física, incluidos los ataques terroristas, y la identificación de sospechosos de delitos graves contemplados en el Anexo II del RIA.

Disponible en: https://op.europa.eu/en/publication-detail/-/publication/24b979fc-4829-11f1-8095-01aa75ed71a1/language-en.

4. INFORME PARA EVALUAR LA MODIFICACIÓN DE LA LISTA DE PRÁCTICAS PROHIBIDAS DEL RIA

La Comisión ha adoptado, según lo establecido en el artículo 112.1. del RIA, un informe para evaluar si es necesario modificar la lista de prácticas de IA prohibidas y los casos de uso de alto riesgo establecidos en el Anexo III del RIA.

Disponible en: https://digital-strategy.ec.europa.eu/en/library/report-review-prohibitions-and-high-risk-ai.

5. LISTA DE EJEMPLOS PARA DISTINGUIR ENTRE RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

La Autoridad Holandesa de Protección de Datos (Autoriteit Persoonsgegevens) ha publicado una lista de ejemplos prácticos para ayudar a las organizaciones a determinar cuándo se encuentran ante un responsable del tratamiento y cuándo ante un encargado.

En el documento se abordan situaciones habituales en el entorno empresarial como por ejemplo el uso de soluciones SaaS o servicios en la nube, la contratación de servicios de correo electrónico externos, la contratación de servicios jurídicos, la externalización del servicio de nóminas y el uso de chatbots en local o en la nube.

Disponible en: https://www.autoriteitpersoonsgegevens.nl/documenten/voorbeeldlijst-wie-is-hier-de-verwerker-en-wie-de-verantwoordelijke.

6. DEMANDAN A CHROME HOLDING CO. (23ANDME) POR UNA BRECHA DE SEGURIDAD

El Fiscal General de California ha presentado una demanda contra Chrome Holding Co., (anteriormente conocida como 23andMe), por no haber protegido adecuadamente la información personal y los datos genéticos de sus clientes, en concreto, datos relativos a su salud, predisposiciones genéticas, datos biológicos, ascendencia y etnia, tras la brecha de seguridad que sufrieron en 2023 y que afectó a casi 7 millones de usuarios.

La demanda alega además que la empresa realizó declaraciones engañosas antes y después de la brecha, llegando incluso a negar públicamente que hubiera habido un incidente de seguridad en sus sistemas mientras negociaba en paralelo el pago de un rescate al atacante.

Puedes encontrar la demanda en el siguiente enlace: https://oag.ca.gov/system/files/attachments/press-docs/People%20v%20Chrome%20Holding%20fka%2023andMe%20et%20al.%20-%20Stamped%20Complaint.pdf.

7. INVESTIGAN A SHEIN POR TRANSFERENCIAS INTERNACIONALES DE DATOS A CHINA

La Comisión de Protección de Datos irlandesa (DPC) ha abierto una investigación formal contra SHEIN por la transferencia internacional de datos de usuarios hacia China.

La investigación examinará el cumplimiento por parte de SHEIN Irlanda de los principios del Artículo 5 del RGPD en materia de tratamiento de datos personales, las obligaciones de transparencia del Artículo 13, y los requisitos del Capítulo V relativos a las transferencias internacionales a terceros países.

Nota de prensa disponible en el siguiente enlace: https://www.dataprotection.ie/en/news-media/dpc-opens-inquiry-infinite-styles-services-co-ltd-shein-ireland.

8. LA AEPD PONE A DISPOSICIÓN PÚBLICA MÁS DE 1.500 INFORMES JURÍDICOS EN ABIERTO

La Agencia Española de Protección de Datos (AEPD) ha publicado más de 1.500 informes jurídicos con el objetivo de facilitar su consulta, análisis y reutilización por parte de organizaciones y profesionales, promoviendo una cultura de cumplimiento basada en la prevención y la responsabilidad activa. La iniciativa se acompaña del lanzamiento de una nueva sección de Datos abiertos desde la que es posible descargar el conjunto de informes de forma agrupada, y que se ampliará progresivamente con más documentación y recursos.

Los informes, elaborados en respuesta a consultas planteadas por entidades y particulares, constituyen una fuente de referencia para la interpretación de la normativa de protección de datos en múltiples ámbitos, y van dirigidos especialmente a responsables y encargados del tratamiento, delegados de protección de datos, profesionales de la privacidad y el cumplimiento normativo, y personal investigador.

Puede acceder y descargar los informes en este enlace: https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/aepd-publica-mas-de-1500-informes-juridicos.

9. LA DPA DE HAMBURGO PUBLICA INDICACIONES PARA LA APLICACIÓN DE LS STJUE RUSSMEDIA EN RRSS

La obligación de proporcionar medidas de protección contra la publicación de datos sensibles, derivados de la sentencia Rusmedia, se aplica en principio a las plataformas de medios sociales.

La forma y el alcance específicos de esta obligación deben determinarse en una evaluación que tenga en cuenta el tipo de cuenta, la naturaleza del contenido de la publicación, los derechos fundamentales afectados y el alcance de las medidas necesarias. Las plataformas de redes sociales que actúan como controladores en el sentido del GDPR son responsables de adaptar los procesos internos y los sistemas técnicos a los requisitos establecidos por el CJEU.

Puedes encontrar el enlace aquí: https://datenschutz-hamburg.de/news/russmedia-urteil-des-eugh-neue-massstaebe-fuer-die-verantwortlichkeit-von-social-media-plattformen.

10. LA CNIL ADVIERTE SOBRE EL RIESGO DE LAS GAFAS CONECTADAS

La CNIL ha emitido un comunicado informando sobre los riesgos de las gafas conectadas, que pueden grabar a terceros, e indica un conjunto de buenas prácticas: informar a las personas cercanas cuando use gafas inteligentes, desactivar las funciones de captura tan pronto como ya no sean útiles., apagar las gafas inteligentes cada vez que se le solicite apagar su teléfono móvil, evitar usar gafas en lugares donde la gente no las espera., asegurarse de obtener su consentimiento si quieres usar fotos o vídeos donde aparecen, por ejemplo, para publicarlos en tus redes sociales, respetar el derecho a la propia imagen y pensarlo dos veces antes de comapartir las imágenes.

Nota de prensa accesible aquí: https://www.cnil.fr/fr/lunettes-connectees-appel-a-la-vigilance.

11. UN ATAQUE DE “INYECCIÓN SQL” LE CUESTA 120.000.-€ A DÉCIMAS

La AEPD multa a Décimas con 120.000 euros por una fuga masiva de datos de clientes. Los ciberdelincuentes aprovecharon un fallo en la web de la compañía para acceder a la base de datos y robar información sensible de usuarios. Entre los detalles filtrados había nombres y apellidos, correos electrónicos, fechas de nacimiento, género e incluso números de DNI.

La brecha se produjo a través de un ataque de inyección de SQL, un método que consiste en aprovechar errores en formularios o apartados de una web para colarse en la base de datos. En su escrito, la AEPD deja claro que se trata de un tipo de fallo muy conocido desde hace años y que existen medidas básicas para evitarlo que no se implementaron.

Fue el INCIBE quien avisó a la empresa de que los datos de sus clientes estaban ya en circulación por la red. DÉCIMAS no tenía ningún método de monitorización de ataques.

Resolución disponible aquí: https://www.aepd.es/documento/ps-00559-2025.pdf.

12. LA AUTORIDAD ITALIANA DE LA COMPETENCIA ABRE PROCEDIMIENTOS SOBRE LOS RIESGOS DE "ALUCINACIÓN" DE VARIOS MODELOS DE IA

La Autoridad cierra tres investigaciones con compromisos destinados a mejorar la transparencia en torno a los sistemas de IA, incluyendo los sitios web y aplicaciones a través de los cuales los usuarios acceden a los servicios y en las distintas etapas del proceso de toma de decisiones antes de la compra o el registro.

En particular, se ha centrado en el riesgo de las llamadas "alucinaciones": la generación de contenido inexacto o engañoso. En este ámbito, la Autoridad llevó a cabo tres investigaciones sobre Deepseek, Mistral y Scaleup.

Nota de prensa y enlace a los procedimientos aquí: https://en.agcm.it/en/media/press-releases/2024/4/PS12942-PS12968-PS12973.

EL LIBRO DEL MES

Para los que quieran huir del alarmismo y el entusiasmo exacerbado, este es su libro. *Co-Intelligence* es una obra práctica sobre cómo convivir y trabajar con la inteligencia artificial generativa. Ethan Mollick plantea que la IA no debe entenderse solo como una herramienta pasiva, sino como una especie de “copiloto” o colaborador intelectual que puede actuar como asistente, tutor, entrenador o compañero de trabajo. Mollick propone experimentar activamente con la IA, pero manteniendo siempre el criterio humano: revisar, contrastar y asumir la responsabilidad final sobre los resultados. El enfoque es especialmente útil para profesionales, docentes o directivos, porque traduce el impacto de la IA en tareas concretas: redacción, análisis, creatividad, formación, toma de decisiones y organización del trabajo.

Beta Legal
Advocats i economistes

info@betalegal.com
https://betalegal.com/
Beta Legal
@beta_legal

Si te han reenviado esta *newsletter*, puedes apuntarte aquí para recibirla mensualmente en tu correo electrónico.