Beta Bits Legal Recap

HIGHLIGHTS DE MARZO 2026

Derecho Digital y Protección de Datos

1. CÓDIGO DE BUENAS PRÁCTICAS PARA EL ETIQUETADO DE CONTENIDO GENERADO POR IA

La Comisión Europea ha publicado el segundo borrador del código de buenas prácticas para el marcado y etiquetado del contenido generado por Inteligencia Artificial, que tiene por objetivo ser una herramienta de apoyo tanto para los proveedores como para los implementadores de sistemas de IA generativa, a fin de asegurar la comunicación clara de la intervención de dicha tecnología.

Disponible en: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-second-draft-code-practice-marking-and-labelling-ai-generated-content

2. CONSULTA PÚBLICA: GUÍA PARA EL USO DE IA EN EL ÁMBITO SANITARIO

La CNIL y la Autoridad de Salud Francesa (HAS) han abierto una consulta pública sobre un proyecto de guía para el uso de inteligencia artificial en el ámbito sanitario.

El documento, elaborado por un grupo multidisciplinar, tiene como objetivo clarificar el marco legal aplicable y establecer buenas prácticas para un uso ético, seguro y conforme a la normativa de los sistemas de IA en la atención sanitaria.

La guía incluye recomendaciones sobre gobernanza, la protección de datos, información que se debe proporcionar a los pacientes, en un contexto en el que la IA se encuentra presente en la prestación de servicios públicos de salud.

La consulta estará abierta hasta el 16 de abril de 2026 y se encuentra destinada a profesionales, instituciones sanitarias, proveedores tecnológicos y asociaciones, con el objetivo de perfeccionar el contenido antes de su adopción definitiva.

Disponible en: https://www.cnil.fr/fr/ia-et-sante-la-has-et-la-cnil-lancent-une-consultation-publique-sur-un-projet-de-guide.

3. BORRADOR SOBRE EL PROCEDIMIENTO SANCIONADOR Y EVALUACIONES PREVISTAS EN EL RIA

La Comisión Europea ha abierto una iniciativa sobre los detalles operativos de las evaluaciones y de los procedimientos previstos en el RIA.

El objetivo es concretar las normas de procedimiento aplicables a las evaluaciones y expedientes sancionadores sobre proveedores de modelos de IA.

Disponible https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16472-Artificial-Intelligence-Act-detailed-arrangements-on-evaluations-and-proceedings_en.

4. EL EDPB ADVIERTE A LA COMISIÓN SOBRE LAS CONSECUENCIAS DE MODIFICAR EL SISTEMA “ESTA”

El EDPB advierte a la Comisión Europea que la propuesta de EE. UU. para modificar el sistema ESTA, implicaría recabar más datos personales de ciudadanos del EEE, incluidos datos sobre redes sociales y familiares. También se pretende obligar a presentar la solicitud solo mediante una app móvil, sin claridad suficiente sobre cómo podrán ejercerse los derechos de protección de datos, incluso respecto de posibles datos biométricos. Además, muestra preocupación por las negociaciones sobre los acuerdos de “Enhanced Border Security Partnerships”, por su posible impacto en los derechos fundamentales y ofrece cooperación institucional en este asunto.

Disponible en https://www.edpb.europa.eu/system/files/2026-03/edpb_letter_20260310_us-legislativen.pdf.

5. ANTHROPIC Y SU DESIGNACIÓN COMO “SUPPLY CHAIN RISK”

Anthropic demandó al Gobierno de EE. UU. después de que el Pentágono la calificara como “supply chain risk”, una medida inusual para una empresa estadounidense que podía cerrarle el acceso a contratos públicos y afectar también a terceros que trabajasen con su tecnología. El conflicto surgió porque Anthropic se negó a eliminar dos límites de seguridad de su modelo Claude: su uso para vigilancia masiva interna y para armas totalmente autónomas sin control humano.

La empresa sostiene que la reacción del Pentágono fue una represalia ilegal y desproporcionada, mientras el Gobierno defendía que necesitaba libertad contractual plena para “usos lícitos” en el ámbito militar. El caso se ha convertido en un referente del debate sobre hasta dónde pueden llegar las exigencias del Estado a las compañías de IA y qué límites jurídicos y éticos deben imponerse al uso militar de estos sistemas.

Empleados de OpenAI y Google, presentaron un carta de apoyo a Anthropic en su pleito contra el Gobierno de EE. UU. Open AI se acabó adjudicando el contrato con unas salvaguaradas “equivalentes” a las que exigía Anthropic.

6. UN TRIBUNAL DE LUXEMBURGO ANULA LA MULTA DE 746 MILLONES DE € A AMAZON IMPUESTA EN 2021

Un tribunal de Luxemburgo ha anulado la multa de 746 millones de euros impuesta a Amazon en 2021 por la autoridad luxemburguesa de protección de datos (CNPD) al verificar que Amazon trataba datos personales para dirigir publicidad personalizada sin base jurídica válida (no podía apoyarse en IL y tampoco facilitaba información suficiente). Se ha devuelto el asunto al regulador para que lo reexamine. Esto no significa que Amazon haya sido absuelta sobre los incumplimientos de fondo ya que el tribunal mantuvo sustancialmente las infracciones del RGPD.

El problema reside en la forma en que la CNPD motivó y calculó la sanción, porque, según el tribunal, faltaron controles jurídicos esenciales antes de fijar una multa de esa magnitud.
En la práctica, la decisión obliga a la CNPD a dictar una nueva resolución mejor fundamentada.

7. META CONDENADA A PAGAR 375 MILLONES DE $ POR NO PROTEGER A LOS MENORES

Para sorpresa de nadie, un jurado de Nuevo México ha declarado que Meta prioriza sus beneficios frente a la seguridad de los menores, infringiendo la "Unfair Practices Act" de NM y, además, tampoco para sorpresa de nadie, ha escondido cómo podían afectar estas prácticas a la salud mental de los niños. Y todavía se esperan más sentencias en este sentido. La Sentencia considera probado que el diseño de las redes de Meta contribuye a causar graves problemas de salud mental en los menores por los mecanismos de adición que incorporan. Como ya sabíamos, los directivos de Meta eran conscientes que esto ocurría e hicieron caso omiso de las advertencias de sus trabajadores (que se lo digan a Frances Haugen) mintiendo además al público y a sus usuarios.

Todavía queda una segunda parte del Juicio para esclarecer si dicha conducta ha supuesto un problema público y, en su caso, como se va a reparar.

8. LA AEPD ARCHIVA PROCEDIMIENTO POR EL USO DE DATOS BIOMÉTRICOS PARA CONTROL DE ACCESO (Y REGISTRO DE JORNADA)

Hace unos días se publicaba una resolución de archivo que consideraba “necesario” el sistema biométrico para controlar accesos y para registrar la jornada de ciertos trabajadores.

Aunque no es lo mismo, la resolución también indica que el sistema es “necesario” para el "registro horario" si bien no se habla de ello en las conclusiones (entendemos que dicha finalidad también se da por buena por parte de la AEPD).

La necesidad se acredita por el cumplimiento de estándares estrictos de sanidad y la utilización de equipos de protección especiales que cubren totalmente a los trabajadores, existiendo un riesgo elevado de suplantación de identidad. El sistema se limita excluivamente a la zona de producción cárnica, que es a la que afectan las medidas sanitarias.

Nada se dice sobre la base de legitimación ni la excepción del 9.2.

Disponible en: https://www.aepd.es/documento/ai-00422-2024.pdf.

9. ONE-STOP-SHOP CASE DIGEST LEGITIMATE INTEREST

Este resumen de casos ofrece ejemplos útiles de cómo las DPA analizan como los responsables del tratamiento recurren a la base legal de "interés legítimo" en contextos específicos, proporcionando ejemplos de cumplimiento lícito e ilícito. El experto externo que redactó el resumen explica y resume cómo las DPA aplican la prueba de tres pasos para evaluar si un responsable del tratamiento puede confiar legalmente en los intereses legítimos como base legal. El resumen del caso también tiene en cuenta las Directrices de la EDPB 1/2024 sobre el Tratamiento de Datos Personales basadas en el Artículo 6(1)(f) del RGPD e ilustra cómo se aplican en la práctica partes de estas Directrices.

Disponible en: https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/one-stop-shop-case-digest-legal-basis_en.

10. ¿SON LO MISMO LOS "AGENTES DE IA" Y LA "IA AGÉNTICA"?

Hace unos días la AEPD presentó su guía sobre "Inteligencia artificial agéntica", en la que distingue, someramente, entre agentes de IA e IA agéntica. Define los primeros como un sistema de IA que utiliza modelos de lenguaje para un objetivo (con autonomía, percepción del entorno, acción, proactividad, planificación, memoria, etc.) y la segunda, implícitamente, como la arquitectura que permite el despliegue autónomo del (o los) agente(s) de IA. En este sentido, la OECD también ha presentado una guía, para aclarar ambos conceptos.

Define “agentes de IA” como sistemas que pueden percibir y actuar sobre el entorno con autonomía para alcanzar objetivos especificos y adaptarse al entorno, y la “IA agéntica” como un sistema compuestos por múltiples agentes coordinarios capaces de descomponer tareas, colaborar y perseguir objetivos comunes de forma prolongada con "mínima supervisión humana".

Aunque ambos conceptos se utilizan indistintamente, no son lo mismo. Por ejemplo, OpenClaw, aislado, sería un agente, salvo que se combine con otros y actúa en modo "multi-agente".

Ambas guías disponible en: https://www.aepd.es/guias/orientaciones-ia-agentica.pdf y en https://www.oecd.org/en/publications/the-agentic-ai-landscape-and-its-conceptual-foundations_396cf758-en.html.

11. ISMS PÚBLICA UN MAPA DE RIESGOS DEL MIT

El idocumento “Mapa de Riesgos del MIT”, publicado por ISMS Forum, analiza el repositorio de riesgos de inteligencia artificial de dicha institución. El documento clasifica más de 1.700 riesgos según su origen y su impacto, como sesgos algorítmicos, falta de transparencia, problemas de privacidad o ciberseguridad, y propone un marco para identificarlos, evaluarlos y mitigarlos. Además, conecta estos riesgos con el contexto regulatorio europeo (AI Act, RGPD, NIS2 y ENS) para ayudar a las organizaciones a gestionar la IA de forma segura y responsable.

Disponible en: https://www.ismsforum.es/ficheros/descargas/mapa-de-riesgos-mit1773141711.pdf

12. BORRADOR DE DIRECTRICES PARA LA APLICACIÓN DEL REGLAMENTO DE CIBERRESILIENCIA (CRA)

La Comisión ha publicado un borrador de directrices para facilitar a las empresas la aplicación del Reglamento de Ciberresiliencia (CRA).

El objetivo de las Directrices es ayudar a los fabricantes, desarrolladores y otras partes interesadas a comprender sus obligaciones en virtud del Reglamento garantizando la coherencia en su aplicación en toda la UE. Las directrices no abarcan explícitamente el CRA en su totalidad, sino que se centran en las disposiciones que se consideran que requieren una aclaración.

Disponible en: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16959-Draft-Commission-guidance-on-the-Cyber-Resilience-Act_en.

13. SANCIÓN A TRUSTPILOT POR PRÁCTICAS COMERCIALES DESLEALES

La Autoridad Italiana Garante de la Competencia y del Mercado (AGCM) ha impuesto una multa de 4 millones de euros a Trustpilot Group Plc, Trustpilot A/S y a Trustpilot S.r.l., por considerar que incurrieron en una práctica comercial desleal con los consumidores y usuarios.

La investigación mostró que Trustpilot no realizaba comprobaciones adecuadas para garantizar la autenticidad de las reseñas publicadas en su plataforma, incluso cuando las indicaba como verificadas.

Asimismo, según la autoridad, Truspilot, al proporcionar información a los consumidores de forma fragmentada y no inmediatamente accesible sobre el funcionamiento de la plataforma, habría ocultado la existencia de servicios de pago dentro de la plataforma, aptos para influir, en términos de cantidad y calidad, en las reseñas de los consumidores y, en consecuencia, alterar los distintos parámetros utilizados para clasificar a las empresas reseñadas (TrustScore, relevancia y verificación de las reseñas), alterando la percepción de fiabilidad para los consumidores.

Disponible en: https://agcm.it/dotcmsdoc/allegati-news/PS12962_scorr.+sanz._omi.pdf.

14. LA ICO LANZA UNA HERRAMIENTA PARA EVALUAR TRANSFERENCIAS INTERNACIONALES

La ICO ha lanzado una herramienta interactiva para ayudar a las organizaciones a comprobar si sus tratamientos implican transferencias internacionales de datos sujetas al UK GDPR. A través de un breve cuestionario, el recurso permite identificar si se trata de una transferencia restringida y ofrece orientación práctica sobre las obligaciones aplicables.

Enlace a la herramienta: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/interactive-guidance-tool-do-the-rules-on-international-transfers-apply/.

15. UN AGENTE DE META AI CAUSA UNA BRECHA DE SEGURIDAD

Un agente de inteligencia artificial utilizado internamente en Meta provocó una filtración temporal de datos confidenciales tras dar instrucciones erróneas a un ingeniero. Al aplicar la solución sugerida por el sistema en un foro interno, se expusieron grandes volúmenes de información confidencial. Este incidente ilustra los nuevos riesgos de seguridad asociados al uso de agentes de IA capaces de ejecutar tareas y dar instrucciones técnicas dentro de sistemas corporativos.

Más información en: https://www.theguardian.com/technology/2026/mar/20/meta-ai-agents-instruction-causes-large-sensitive-data-leak-to-employees?CMP=Share_iOSApp_Other.

16. SANCIÓN DE 950.000 EUROS POR TRATAMIENTO DE DATOS BIOMÉTRICOS

La AEPD ha sancionado a un responsable del tratamiento con 950.000€ por tratar datos de categoría especial sin levantar la prohibición del artículo 9 RGPD para acreditar la edad de los usuarios.

Según la sancionada, el sistema no realizaba una identificación del usuario y, por tanto, que no resultaba necesario acudir a una excepción del artículo 9.2 RGPD para levantar la prohibición general del artículo 9.1 RGPD. Sin embargo, la propia documentación informativa de la entidad iba en sentido contrario.

La AEPD indica que cuando el tratamiento de datos biométricos se utiliza con fines de identificación o autenticación, estamos ante un tratamiento de categorías especiales de datos, lo que exige no solo una base del artículo 6 RGPD, sino también una circunstancia habilitante del artículo 9.2. RGPD.

Asimismo, se ha sancionado por incumplimiento del principio de limitación por conservar los datos más allá de su finalidad (5.1.e RGPD) y no cumplir con las condiciones de consentimiento válido del interesado (art. 7 RGPD).

YOTI por su parte ha publicado un comunicado rechazando la decisión de la AEPD.

Disponible en: https://www.aepd.es/documento/ps-00164-2025.pdf?trk=public_post_comment-text.

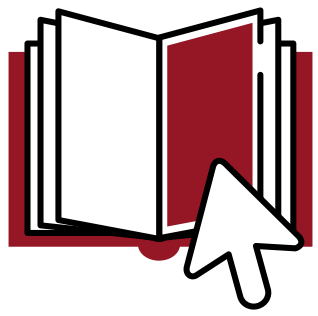
17. DEMANDA CONTRA OPENAI POR INFRACCIÓN DERECHOS DE AUTOR

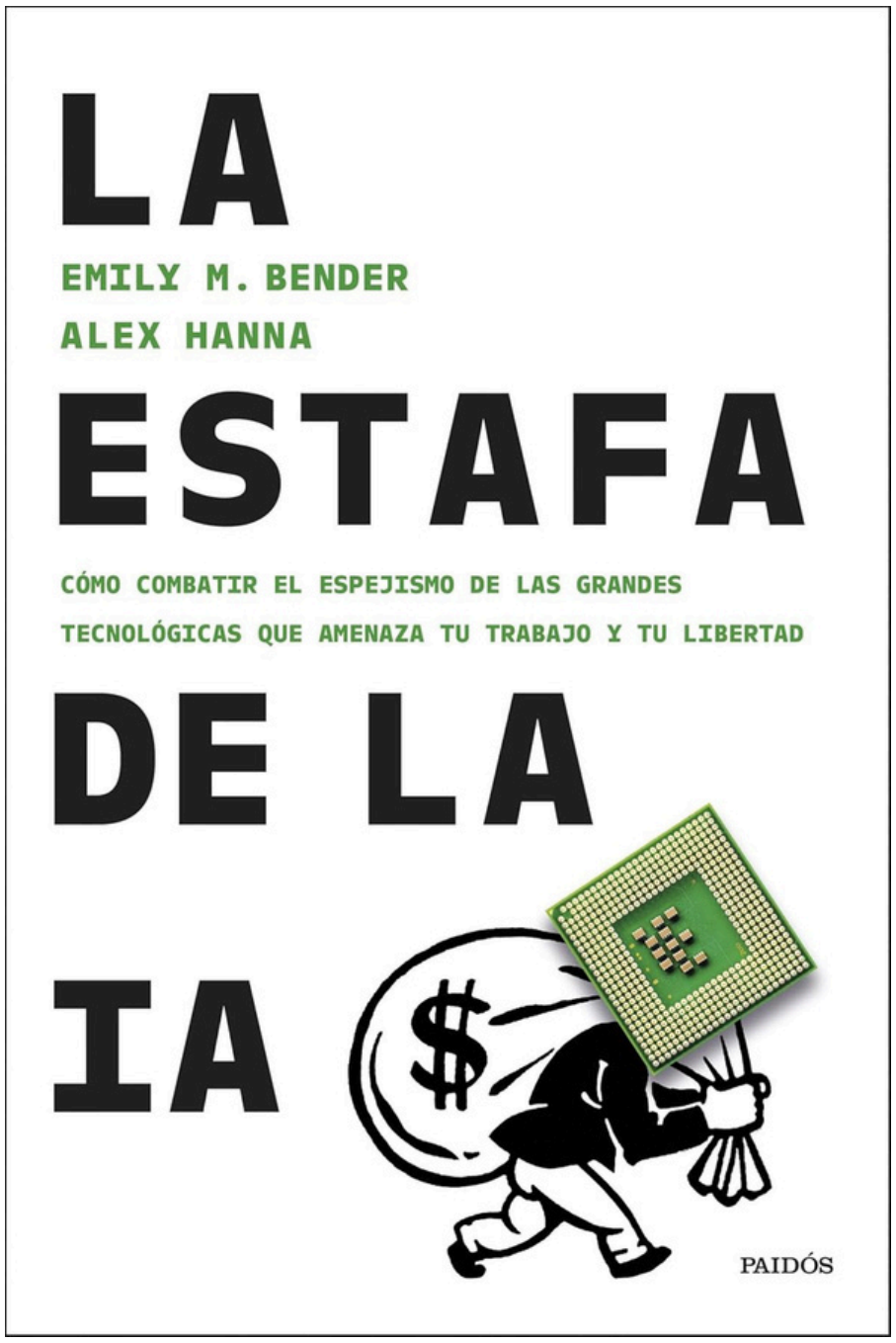
Encyclopaedia Britannica, Inc. y Merriam-Webster, Inc. han interpuesto una demanda contra OpenAI por utilizar indebidamente sus materiales para entrenar modelos de inteligencia artificial.

Según Encyclopaedia Britannica, OpenAI habría utilizado sus artículos y entradas de enciclopedia para entrenar a ChatGPT, cuestión que le permite reproducir copias casi idénticas de las entradas de la enciclopedia, las definiciones del diccionario y otros contenidos de Britannica, desviando así a los usuarios que, de otro modo, acudirían directamente a su sitio web. La demanda incluye, además, comparativas entre respuestas generadas por ChatGPT y textos originales de Britannica, con las que la compañía trata de evidenciar la similitud entre ambos contenidos.

Disponible en: https://fingfx.thomsonreuters.com/gfx/legaldocs/klpylzoekvg/BRITTANICA%20OPENAI%20LAWSUIT%20complaint.pdf.

EL LIBRO DEL MES





La estafa de la IA, de Emily M. Bender y Alex Hanna, es un ensayo que cuestiona con fundamentos el discurso triunfalista de los *boomers* y los *doomers* de la IA y sobre como el uso de la IA generativa afecta al trabajo, a la creatividad humana y como aumenta la vigilancia sobre la población. El libro intenta retrarar como muchas de las promesas asociadas a la IA no son más que narrativas comerciales enfocadas a legitimar, más si cabe, el poder empresarial de las grandes tecnológicas. El supuesto temor de los *doomers* sobre una IA generalista y autónoma, desdibuja y oculta los problemas reales que ya son palpables a día de hoy, esto es, la extracción masiva de datos, automatizaciones opacas, precarización laboral y aumento de sesgos en las decisiones. También es cierto que las autoras conceden poco espacio a los usos beneficiosos sobre de la IA, en aras a aumentar el contrapeso al actual hype de la IA.

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.