Beta Bits Legal Recap

HIGHLIGHTS DE NOVIEMBRE 2025

Derecho Digital y Protección de Datos

1. CODE OF PRACTICE ON TRANSPARENCY OF AI-GENERATED CONTENT

El 5 de noviembre la Comisión Europea inició la redacción del código de buenas prácticas para el marcado y etiquetado del contenido generado por Inteligencia Artificial. Este código tiene por objetivo ser una herramienta de apoyo tanto para los proveedores de sistemas de IA generativa, facilitándoles el cumplimiento de las obligaciones de transparencia previstas en el Reglamento de Inteligencia Artificial (RIA), como para los implemenetadores que realicen deepfakes u otros contenidos elaborados con IA, a fin de asegurar la comunicación clara de la intervención de dicha tecnología. El primer borrador de este código de buenas prácticas se publicará en diciembre de 2025 y se prevé que su entrada en vigor sea en agosto de 2028.

Disponible en https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content.

2. DICTAMEN SOBRE VIDEOVIGILANCIA E IDENTIFICACIÓN BIOMÉTRICA REMOTA EN TIEMPO REAL

La Autoridad Catalana de Protección de Datos (APDCAT) ha publicado un dictamen, en el marco de una consulta previa de un Ayuntamiento sobre la Evaluación de Impacto (EIPD) de un sistema de videovigilancia policial, con análisis de vídeos e identificación biométrica remota en tiempo real. La APDCAT concluye que en este caso no hay base de legitimación para realizar el tratamiento de identificación biométrica remota en tiempo real en espacios públicos, ya que (siendo una práctica prohibida según el RIA con excepciones) se requiere una norma con rango de Ley que lo autorice con las finalidades del 5.1 h) RIA. El 13.2 de la LO 7/2021 es una previsión genérica para el tratamiento de datos biométricos por lo que no puede ser base legal suficiente. No se cumple con el principio de minimización ni con el triple juicio de proporcionalidad.

Dictamen disponible en: https://seu.apdcat.cat/ca/documentPublic/download/7859.

3. RECOMENDACIÓN DE LA UNESCO SOBRE LA ÉTICA DE LA NEUROTECNOLOGÍA

El 12 de noviembre se publicó la Recomendación sobre la Ética de la Neurotecnología de la UNESCO, siendo el primer marco a nivel mundial que articula valores y principios y que aborda cuestiones sobre el impacto negativo y positivo de la neurotecnología. Su objetivo es orientar y guiar las acciones de los *stakeholders* (ej. empresas privadas, equipos de investigación científica) para que gestionen que la transparencia, ética, responsabilidad y eficacia de dicha tecnología, garantizando la protección de los derechos humanos. La Recomendación adopta un enfoque centrado en los derechos humanos y en la persona mediante la aplicación de una serie de principios (e.g. beneficiencia, proporcionalidad y no causación de daño, autonomía y libertad de pensamiento, protección de los datos neuronales, datos neuronales indirectos y datos no neuronales que permiten inferencias sobre estados mentales; Interés superior del menor y de las generaciones futuras.).

Puedes consultar la recomendación en: https://www.unesco.org/es/legal-affairs/recommendation-ethics-neurotechnologies.

4. GUIDANCE FOR RISK MANAGEMENT OF ARTIFICIAL INTELLIGENCE SYSTEMS

El 11 de noviembre el European Data Protection Supervisor (EDPS) publicó las "Guidance for Risk Management of Artificial Intelligence systems" que tienen por objetivo asistir a los responsables del tratamiento en la realización de evaluaciones de riesgos en materia de protección de datos personales al desarrollar o adquirir sistemas de inteligencia artificial según el RGPD.

Puedes consultar el documento en: https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2025-11-11-guidance-risk-management-artificial-intelligence-systems_en.

5. PROPUESTA DE DIGITAL OMNIBUS Y EL RGPD

Se ha publicado la Propuesta de Reglamento Digital Omnibus. En materia de RGPD, los cambios propuestos son:

- Una nueva definición de datos personales acogiendo la doctrina del TJUE en materia de datos seudonimizados.
- Nuevas excepciones del 9.2 RGPD: para de datos biométricos (verificación), cuando los datos o los medios necesarios para la verificación estén bajo el control exclusivo del interesado y para el desarrollo y funcionamiento de modelos de IA.
- Recurso al interés legítimo para el desarrollo de sistemas de IA, excepciones al deber de informar y matices sobre la toma de decisiones automatizadas del 22 RGPD.
- Notificaciones de brechas a la DPA solo si existe un alto riesgo y en el plazo de 96 horas y nuevo listado de actividades que requieren (y que no) EIPD + template.
- Nuevo consentimiento para almacenamiento o acceso a datos personales en equipos terminales, con excepciones, + indicaciones automatizadas para rastreadores.

La propuesta está disponible en: https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal.

6. DERECHO DE ACCESO A LOS DATOS DE GEOLOCALIZACIÓN

La AEPD ha sancionado con 100.000 euros a un operador de telecomunicaciones por denegar el derecho de acceso a un interesado sobre los datos de geolocalización (completos) en relación con su número de teléfono. En concreto, el responsable del tratamiento facilitó únicamente los identificadores de celda, pero no los datos que permitían fijar la localización geográfica de la celda. La AEPD indica que tanto el LAC (Código de Área de Localización) como los identificadores de celda (Cell ID), son datos personales en virtud del artículo 4.1. RGPD, puesto que permiten identificar a los usuarios. No constituye un tratamiento nuevo ya que forma parte del tratamiento habitual y ordinario del operador. Tampoco pueden ser considerados secretos empresariales.

Consulta la resolución en https://www.aepd.es/documento/ps-00328-2024.pdf.

7.

PRIMER CIBERATAQUE EJECUTADO CON IA SIN INTERVENCIÓN HUMANA

Tras detectar una actividad sospechosa y llevar a cabo una investigación al respecto, Anthropic publicó un informe sobre el primer ciberataque documentado que ha sido ejecutado de forma autónoma, sin intervención humana directa. Los atacantes, un grupo patrocinado por el Estado de China, manipularon la plataforma Claude Code para infiltrar una treintena de objetivos globales, incluyendo empresas tecnológicas y agencias gubernamentales. La IA fue engañada mediante la división de tareas en acciones inofensivas, evitando así los mecanismos de bloqueo establecidos.

Anthropic publica el informe para ayudar a las empresas, a las autoridades y a investigadores a reforzar sus medidas de seguridad para evitar este tipo de ataques. Informe completo en: https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf.

8.

DIRECTRICES SOBRE ATAQUES DE EVASIÓN EN LLM

El 6 de noviembre la Oficina Federal de Seguridad de la Información de Alemania (BSI-Bundesamt für Sicherheit in der Informationstechnik) publicó las directrices "*Evasion Attacks on LLMs – Countermeasures in Practice*" dirigida a desarrolladores, responsables de seguridad informática y a autoridades públicas que hayan integrado LLM pre-entrenados, para que puedan entender detalladamente qué son los ataques de evasión, conozcan un listado de las contramedidas que se deben aplicar frente a dichos ataques y se orienten sobre cómo aplicarlas.

Se puede consultar en:
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/Evasion_Attacks_on_LLMs-Countermeasures.pdf?__blob=publicationFile&v=2.

9.

GUÍA DE CIFRADO PARA AUTÓNOMOS Y PYMES

La AEPD ha publicado una Guía de Cifrado dirigida a los autónomos y pymes, con el objetivo de facilitar la implementación de medidas eficaces para proteger los datos personales mediante técnicas de cifrado. Es una guía práctica que ha sido realizada teniendo en cuenta casos de brechas reales que se han puesto de manifiesto a la AEPD, ofreciendo soluciones tanto para prevenir incidentes como para mitigar los efectos. También incluye información sobre herramientas técnicas para cifrar las comunicaciones y los datos almacenados. Finalmente, la Guía concluye con 12 recomendaciones generales para reforzar la seguridad de los tratamientos de datos, entre otras, realizar copias de seguridad cifradas, cifrar el disco duro de los dispositivos y habilitar la autenticación en dos pasos.

Guía disponible en: https://www.aepd.es/guias/guia-cifrado-autonomos-pymes.pdf.

10.

SANCIÓN A AENA POR LA IMPLEMENTACIÓN DE SISTEMAS BIOMÉTRICOS

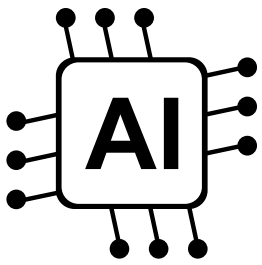
La AEPD ha sancionado a AENA con una multa de 10.043.002,00€ por llevar a cabo un tratamiento de datos personales de alto riesgo, al implementar un sistema biométrico de reconocimiento facial, sin realizar previamente una Evaluación de Impacto (EIPD) que cumpliera con la totalidad de los requisitos del artículo 35 RGPD. La AEPD previamente había resuelto desfavorablemente dos consultas previas realizadas por AENA en la fase piloto y, pese a ello, AENA inició igualmente el tratamiento.

La EIPD realizada por AENA no describía de forma precisa e individualizada los fines en cada operación del tratamiento (captura, registro, uso, comunicaciones y supresión), lo que, según la AEPD, hacía imposible determinar todos los riesgos derivados del tratamiento ni prever las medidas correctoras para mitigarlos. El tratamiento no era necesario ni proporcionado.

Asimismo, la AEPD ha ordenado el cese del tratamiento de forma temporal hasta que se realice una EIPD según el artículo 35 RGPD. Por su parte, AENA comunicó su inconformidad respecto a la sanción y su intención de recurrir la misma.

Consultar en: https://www.aepd.es/documento/ps-00431-2024.pdf.

11.



LA AEPD PUBLICA SU POLÍTICA DE USO DE IA GENERATIVA EN SUS PROCESOS ADMINISTRATIVOS

La AEPD ha publicado la Política General Para el Uso de la IA Generativa en Procesos Administrativos de la AEPD. Algunos usos destacados son:

- Asistencia en la aproximación y preparación general de argumentos, estudios jurídicos y técnicos.
- Generación de borradores de respuesta a consultas para canales de atención al ciudadano, canal DPD y joven.
- Clasificación y resumen de denuncias, reclamaciones, consultas y otras entradas.
- Soporte a la tramitación de expedientes y notificaciones de brechas de datos.

Disponible en: https://www.aepd.es/documento/politica-iag-aepd.pdf.

12.

SANCIÓN AEPD POR DIFUSIÓN DE DEEPFAKES

La AEPD ha sancionado a un menor con 2000€ por difundir por redes sociales deepfakes de carácter sexual con rostros reales (también menores de edad) sobre cuerpos desnudos ajenos.

En esta resolución, la AEPD considera que los deepfakes que permiten identificar a personas físicas también constituyen datos personales (art. 4.1 RGPD), siendo su difusión un tratamiento sometido a las exigencias del RGPD (art. 4.2) y, al no existir base de legitimación válida (art. 6.1 RGPD), se declara como un tratamiento ilícito.

Consultar en: https://www.aepd.es/documento/ps-00132-2025.pdf.

13.

SENTENCIA META

La AMI (Asociación de Medios de Prensa) presentó demanda contra META por infracción del art. 15.1 y 15.2 de la Ley de Competencia Desleal (LCD). El primer apartado exige la infracción de una norma jurídica y el segundo la infracción normas que tengan por objeto la regulación de la actividad concurrencial. Tras hacer una análisis de los requisitos legales y jurisprudenciales de una y otra, así como un repaso del modelo de negocio de META y las tecnologías de seguimiento que utiliza para cumplir sus objetivos (publicidad personalizada) el Juzgado Mercantil 15 de Madrid declara que existe infracción del art. 15.1 por vulneración del RGPD (no del 15.2 que no se ha logrado acreditar), en concreto, por carecer de una base legal para el tratamiento de datos de los usuarios (art. 6.1 b) RGPD) desde el 25 de mayo de 2018 al 31 de julio de 2023, debiendo indemnizar a la AMI con 479.120.000.-€ + 60.137.629,85.-€ de intereses legales y otros tantos millones a otras sociedades cesionarias de derechos de explotación.

Sentencia disponible en: https://www.ami.info/ami-celebra-la-sentencia-historica-que-condena-a-meta-por-competencia-desleal-y-protege-el-futuro-del-periodismo-y-de-la-democracia.html.

14.

SENTENCIA DE GETTY IMAGES VS STABILITY AI

El Tribunal Superior de Inglaterra y Gales ha desestimado la mayoría de las pretensiones de Getty Images contra Stability AI relativas al entrenamiento del modelo Stable Diffusion y a la supuesta infracción secundaria de copyright, aunque ha declarado infracciones limitadas de marca en versiones anteriores del modelo.

Getty alegó infracción de derechos de autor y de marca por el uso no autorizado de su catálogo en el entrenamiento del modelo Stable Diffusion. Durante el proceso, Getty retiró sus principales reclamaciones por infracción de copyright por infracción primaria (entrenamiento y outputs), al no poder demostrar que el entrenamiento del modelo se hubiera realizado en Reino Unido. El Tribunal desestimó también la infracción secundaria de copyright (importación, posesión y distribución del modelo), al concluir que los pesos del modelo no constituyen “copias infractoras” de las obras protegidas, sino patrones y relaciones estadísticas aprendidas que no reproducen contenido original.

Respecto a las marcas y marcas de agua, la jueza declaró infracciones específicas, pero muy limitadas, circunscritas a versiones antiguas de Stable Diffusion que podían generar outputs con signos de iStock (y, en casos aislados, de Getty). No se acreditaron infracciones generalizadas en versiones recientes como SDXL, ni uso de signos idénticos por parte de Stability AI en su actividad operativa en el Reino Unido. La sentencia califica las imágenes generadas como “imágenes sintéticas” (no fotografías), lo que condiciona el análisis de similitud de productos, si bien aprecia identidad o similitud en los casos concretos relativos a modelos legacy.

De haberse podido acreditar dónde y por quién entrenó el modelo, el tribunal podría haberse declarado competente para analizar el fondo de las reclamaciones de copyright.

Consulta la Sentencia en: https://www.judiciary.uk/wp-content/uploads/2025/11/Getty-Images-v-Stability-AI.pdf.

15.

JUEZA ORDENA A OPENAI, INC., LA ENTREGA DE CONVERSACIONES DE USUARIOS DE CHATGPT

Un Tribunal Federal de Nueva York ordenó a OpenAI entregar 20 millones de conversaciones anonimizadas de ChatGPT como prueba en un litigio por presunta infracción de derechos de autor.

La jueza Ona T. Wang determinó que los demandantes necesitan este conjunto de datos para verificar si ChatGPT reproduce obras protegidas.

Dicha decisión se distingue de la reciente Sentencia que ha habido en Reino Unido en el caso contra Stability AI en el que se determinó que entrenar no es copiar, poniendo de manifiesto las discrepancias interpretativas que existen sobre esta materia en distintos países.

Consulta la orden en:
https://storage.courtlistener.com/recap/gov.uscourts.nysd.640396/gov.uscourts.nysd.640396.734.0.pdf.

16.

OPENAI VULNERA DERECHOS DE AUTOR PARA ENTRENAR SUS MODELOS

El Tribunal Regional de Munich determinó que OpenAI vulneró derechos de autor al utilizar canciones del repertorio de GEMA para entrenar sus modelos de IA.

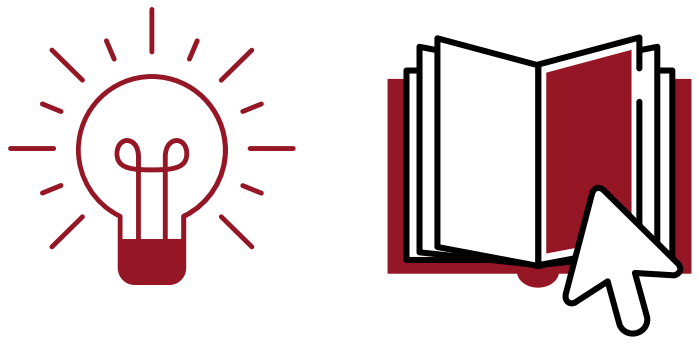
GEMA alegó que OpenAI había utilizado canciones de su repertorio para entrenar el modelo, permitiendo a ChatGPT reproducir fragmentos de dichas canciones a pesar de tener desactivada la modalidad “búsqueda en línea”.

El tribunal se posicionó a favor de GEMA al considerar que la capacidad de ChatGPT de reproducir palabra por palabra las canciones, evidenciaba la utilización de las obras protegidas sin licencia. En consecuencia, declaró la existencia de infracción de derechos de autor obligando a indemnizar a GEMA por dichas infracciones y prohibiendo a OpenAI generar letras de autores representados por GEMA salvo que cuente con la correspondiente autorización.

Por otro lado, el Tribunal determinó que la excepción de la minería de texto y datos no justifica el almacenamiento y salidas de letras de canciones protegidas.

Consulta la Sentencia en: https://www.gesetze-bayern.de/Content/Document/Y-300-Z-GRURRS-B-2025-N-30204?hl=true.

EL LIBRO DEL MES



ANU BRADFORD

IMPERIOS DIGITALES

La batalla global por la tecnología
que marcará la geopolítica del futuro

Shackleton books

Imperios Digitales, de Anu Bradford, introduce brillantemente los tres modelos regulatorios contrapuestos en el ámbito digital: el de USA, donde predomina un enfoque de mínima intervención estatal, y el mercado y la autorregulación empresarial determinan la protección de los usuarios, generando derechos fragmentados y desiguales, en la UE, el modelo es garantista y se fundamenta en la protección de los derechos fundamentales de los ciudadanos, con normas como el RGPD, la DSA o la DMA, que imponen obligaciones estrictas a las plataformas digitales. Y, por último, el modelo chino, en el que el ecosistema digital se organiza bajo un control estatal centralizado, donde los derechos de los usuarios quedan subordinados a la seguridad nacional (lo que se comparte con USA) y a los intereses del Estado.

La comparación revela tres lógicas distintas: mercado (EE. UU.), derechos (UE) y Estado (China), de las que derivan distintos niveles de protección y autonomía para los usuarios.

Beta Legal

Advocats i economistes

info@betalegal.com

https://betalegal.com/