Beta Bits Legal Recap

HIGHLIGHTS DE ENERO 2026

Derecho Digital y Protección de Datos

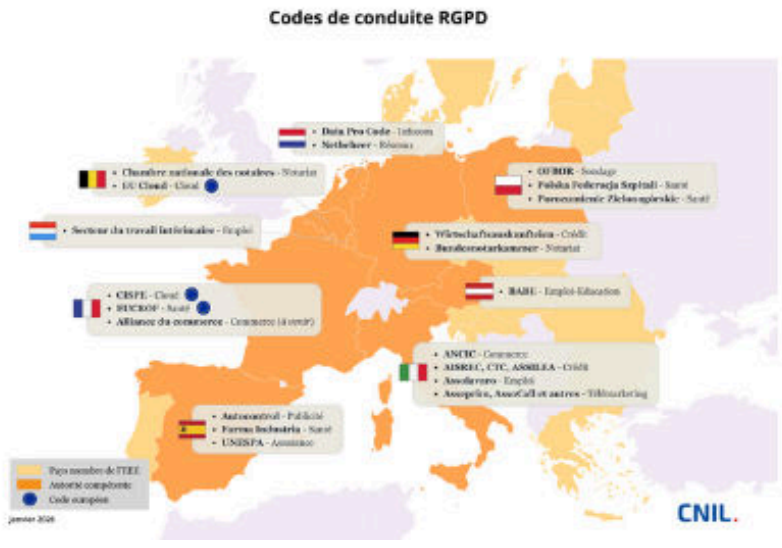
1. ACTUALIZACIÓN DE PREGUNTAS FRECUENTES DE LA AEPD

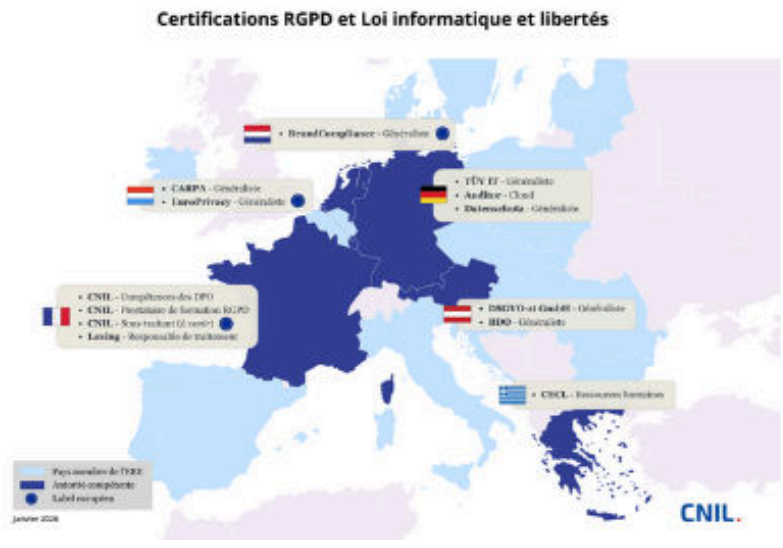
La AEPD ha renovado su catálogo de preguntas frecuentes publicado en su sitio web, reorganizando y ampliando las secciones, con el objetivo de ofrecer un recurso más práctico y accesible para los profesionales encargados de garantizar el cumplimiento de la normativa de protección de datos así como para los responsables del tratamiento de pequeñas y medianas empresas. Esta actualización se encuentra alineada con los objetivos contemplados en el Plan Estratégico 2025-2030 de la AEPD.

Acceso a las preguntas frecuentes actualizadas en https://www.aepd.es/preguntas-frecuentes.

2. MAPEO DE CÓDIGOS DE CONDUCTA Y CERTIFICACIONES RGPD

Para facilitar la identificación de las herramientas de cumplimiento disponibles, la CNIL pone en línea dos tarjetas que enumeran las certificaciones y códigos de conducta aprobados por las autoridades nacionales o por el Consejo Europeo de Protección de Datos (EDPS) desde la entrada en vigor del GDPR:





Disponible en: https://www.cnil.fr/fr/la-cnil-cartographie-le-deploiement-des-outils-rgpd-en-europe.

3. EL EDPB ACTUALIZA LAS FAQS SOBRE EU-US DATA TRANSFERS

Pocas novedades. El documento, sobre todo, repasa las acciones de reclamación y ejercicio de derechos que puede llevar a cabo el interesado.


EU-U.S. Data Privacy Framework
F.A.Q. for European individuals[1]

Version 2.0

Adopted on 15 January 2026

Disponible en: https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals-0_en

4. SANCIÓN DE 42 MILLONES DE EUROS A FREE MOBILE POR FALTA DE MEDIDAS DE SEGURIDAD

La CNIL sancionó a la empresa FREE MOBILE con una multa de 27 millones de euros y a la empresa FREE con una multa de 15 millones de euros, debido a la falta de medidas de seguridad, según el artículo 32 RGPD, para garantizar la seguridad de los datos personales. La sanción es el resultado de un procedimiento de inspección realizado tras una brecha de datos personales relacionados con 24 millones de abonados de ambas empresas.

Entre los incumplimientos detectados, la falta de medidas de seguridad suficientes (art. 32 RGPD), la obligación de informar a las personas afectadas (art. 34.2 RGPD) y la obligación de conservar los datos personales durante un tiempo limitado (art. 5.1.e RGPD).

Las sanciones se encuentran disponibles en los siguientes enlaces: https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000053352664 y https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000053352643.

5. GUÍA PARA LA EVALUACIÓN DEL INTERÉS LEGÍTIMO DE LA DPA DE HAMBURGO

El 8 de enero de 2026, la autoridad de protección de datos de Hamburgo publicó una guía basada en las Directrices 1/2024 sobre el tratamiento de datos basado en interés legítimo del EDPB, como recurso de apoyo para evaluar y documentar el interés legítimo. Este documento contiene una lista detallada de preguntas destinadas a ayudar a los responsables del tratamiento a determinar la existencia de un interés legítimo como base jurídica para el tratamiento de datos personales según el artículo 6.1.f. RGPD.

La guía se encuentra disponible y traducida al inglés en el siguiente enlace: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/260108_Fragenkatalog_LIA__English.pdf?

The Hamburg Commissioner for Data Protection and Freedom of Information

6. NUEVO PROTOCOLO DE GOOGLE PARA “AGENTES DE COMPRA CON IA”

Un organismo de defensa de los consumidores ha alertado sobre el nuevo protocolo de Google para agentes de compra basados en IA, advirtiendo de posibles riesgos de precios personalizados a partir del análisis de datos de interacción de los usuarios (“surveillance pricing”). Google ha negado estas afirmaciones, asegurando que el sistema no permite fijar precios superiores ni dinámicos individualizados y que su objetivo es mejorar recomendaciones y descuentos. El debate pone de relieve los riesgos regulatorios del comercio impulsado por IA, especialmente en materia de transparencia, uso de datos personales y protección de los consumidores.

Disponible en: https://techcrunch.com/2026/01/13/a-consumer-watchdog-issued-a-warning-about-googles-ai-agent-shopping-protocol-google-says-shes-wrong/?utm_campaign=daily_pm

7. ¿SE PUEDEN EXTRAER TEXTOS COMPLETOS DE OBRAS USADAS PARA ENTRENAR UN LLM?

Sí, se puede.

El paper "*Extracting books from production language models*" analiza si es posible extraer texto (casi) literal de libros desde LLMs, pese a sus salvaguardas.

Y lo hace con dos mecanismos (i) un extracto breve y real del libro y (ii) peticiones iterativas de continuación para extender la extracción.

Evalúa cuatro modelos de producción: Claude 3.7 Sonnet, GPT-4.1, Gemini 2.5 Pro y Grok 3.
En el conjunto de experimentos (11 libros con copyright), la mayoría de ejecuciones arrojan nv-recall ≤ 10%, aunque en Claude se alcanzan casos de extracción casi total en algunos títulos. Traducido: en la mayoría de intentos solo consiguieron reconstruir como máximo alrededor del 10% del libro en fragmentos suficientemente largos y contiguos (no frases sueltas), pero en Claude, en algunos libros y bajo ciertas condiciones, llegaron a poder extraer casi todo el libro.
Incluso con salvaguardas de modelo y sistema, la extracción de datos de entrenamiento con copyright sigue siendo un riesgo real en LLMs de producción, con implicaciones técnicas y jurídicas.

Paper disponible en: https://arxiv.org/pdf/2601.02671.

8. INFORME SOBRE AGENTIC AI DEL ICO

La Information Commissioner's Office (ICO) ha publicado un informe dedicado a la "Agentic AI", una tecnología emergente que combina la IA generativa con herramientas adicionales para poder ejecutar tareas más complejas y que puede utilizarse en el ámbito del comercio, el entorno laboral, la ciberseguridad o la medicina. En el informe, la ICO analiza los riesgos que esta tecnología puede suponer en la protección de datos personales.

https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/tech-horizons-and-ico-tech-futures/ico-tech-futures-agentic-ai/.

9. GOOGLE Y CHARACTER.AI BUSCAN CERRAR ACUERDOS CON DEMANDANTES QUE LES ACUSABAN DE CAUSAR DAÑOS A MENORES

Las demandas alegaban que los chatbots de Character.AI (con la que Google mantiene vinculación empresarial) contribuyeron a daños graves, incluidos casos de suicidio o autolesiones en adolescentes. El caso más conocido es el de Florida, impulsado por la madre de un menor de 14 años fallecido en febrero de 2024, que atribuía un papel causal a un bot temático. Según los escritos judiciales, las partes han solicitado pausar o suspender trámites mientras se finalizan los términos del acuerdo. Los términos económicos y condiciones concretas no se han hecho públicos y, en algunos casos, quedarían sujetos a aprobación judicial.

10. ANTEPROYECTO DE L.O. DE PROTECCIÓN CIVIL AL D° AL HONOR, INTIMIDAD Y PROPIA IMAGEN

Se ha aprobado el Anteproyecto de L.O. de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Se incluye, como principal novedad, el uso de deepfakes como intromisión ilícita, ya sea utilizando IA o otra tecnología similar. Se incluye, asimismo, como intromisión ilícita, la utilización de un delito por parte de su autor, que cause un daño a la víctima (con los true crimes, por ejemplo). A pesar de la dificultad que la propuesta va a tener para pasar el trámite parlamentario, por las mayorías existentes, aquí van las principales novedades:

Novedad	Qué incorpora	Observaciones (fricciones con p.e. RGPD/LOPDGDD)
***Deepfakes* comerciales/publicitarios como intromisión ilegítima (con IA o sin)**	Se considera ilegítimo **usar voz o imagen sin autorización con fines publicitarios o comerciales** empleando IA o tecnologías similares (ultrasuplantaciones).	Esto ya venía siendo así al tratarse la imagen de un dato personal. El uso de la misma precisaba de una base de licitud, normalmente el consentimiento. Se solaparán dos consentimientos.
Compartir imágenes en RRSS no habilita su reutilización en otros canales.	Se explicita que compartir imágenes personales en redes **no autoriza** a terceros a reutilizarlas en otras redes o canales.	Esto está conectado con el **principio de limitación de finalidad** RGPD (art. 5) y con que el consentimiento debe cubrir **fines específicos** (art. 6).
Menores: consentimiento desde los 16 años con limitaciones.	Se fija **16 años** como edad para consentir uso de imagen. Incluso si existe consentimiento, si se menoscaba dignidad/reputación del menor, será intromisión ilegítima.	En la LOPDyGDD se fija en 14 años la edad para el tratamiento de datos personales basado en consentimiento (art. 7). De nuevo, se solaparán dos consentimientos.
Víctimas de delitos y "*true crime*".	Considera intromisión ilegítima cualquier utilización del delito por el victimario que pueda causar daño (por ejemplo, en "*true crimes*").	-
Personas fallecidas: prohibición "post mortem" por testamento/designación	Se incorpora la posibilidad de prohibir por testamento (o por persona designada) el uso de imagen/voz del fallecido con fines comerciales o similares.	Algo similar se prevé en la LOPDyGDD con el (mal)llamado "testamento digital".
Excepciones: libertad de expresión/información y nueva excepción "IA creativa"	Mantiene excepciones previas (p.ej. interés general en difusión de comunicaciones privadas) y añade una excepción: si el afectado es persona con proyección pública, se protege libertad de expresión si el uso de IA o tecnología similar es creativo/satírico/ficción y se indica el uso de esa tecnología.	Relacionado con el art. art. 50 de la **IA Act** (sin que dificulte, el etiquetado, la exhibición de la obra)
Indemnización por daño moral: criterios y veto a indemnizaciones simbólicas	Se regulan criterios de gravedad (reincidencia, repercusión social, etc.) y se afirma que la indemnización por daño moral no podrá ser simbólica, que es lo que venía ocurriendo.	-

Enlace al texto del anteproyecto aquí: https://www.mpr.gob.es/servicios/participacion/audienciapublica/Paginas/2026/2025-1206%20APLO%20Honor/anteproyecto-de-ley-org-nica-de-protecci-n-civil-d.aspx.

11. OPINIÓN CONJUNTA EDPB-EDPS SOBRE EL *"DIGITAL OMNIBUS ON IA"*

El objetivo general de reducir cargas y resolver fricciones de implementación, pero advierten que la simplificación no debe rebajar la protección de derechos fundamentales. Bravo.
Sobre el uso de categorías especiales de datos para detección/corrección de sesgos, respaldan la ampliación de base jurídica "excepcional", pero piden acotar estrictamente cuándo podría usarse en sistemas/modelos de no-alto riesgo y mantener el estándar de estricta necesidad en alto riesgo. En relación la *AI literacy* recomiendan mantenerla tal y como está ahora, así como mantener la obligación de registrar en la base de datos UE el sistema de IA, incluso cuando el proveedor concluya que un sistema del Anexo III no es de alto riesgo, para evitar incentivos a "autoeximirse" y perder trazabilidad.

Disponible en: https://www.edpb.europa.eu/system/files/2026-01/edpb_edps_jointopinion_202601_proposal_ai-omnibus_en.pdf.

12. LA AEPD PUBLICA LA GUIA PARA USO DE IMÁGENES DE TERCEROS EN SISTEMAS DE IA Y SUS RIESGOS VISIBLES E INVISIBLES

La Agencia Española de Protección de Datos (AEPD) ha publicado una guía centrada en los riesgos del uso de imágenes o vídeos de terceros en sistemas de inteligencia artificial y sus implicaciones desde la perspectiva de la protección de datos. La guía parte de la premisa de que cualquier imagen o vídeo que permita identificar a una persona constituye un dato personal, ya sea un contenido real o generado/modificado por IA, lo que implica un tratamiento sujeto al RGPD y a la LOPDGDD.

El documento analiza tanto los riesgos visibles, esto es, lo que otras personas pueden ver, interpretar o difundir cuando una imagen o un vídeo generado con IA se comparte como los riesgos no visibles que corresponden al impacto que estas acciones pueden ocasionar pero que no son visibles, es decir, lo que sucede por el simple hecho de subir una imagen o un vídeo a un sistema de IA, aunque el resultado no llegue a publicarse ni a compartirse posteriormente.

Disponible en: https://www.aepd.es/guias/guia-aepd-uso-de-imagenes-de-terceros-en-sistemas-ia.pdf

13. LA CNIL PUBLICA, EN INGLÉS, SUS DIRECTRICES PARA EL DESARROLLO DE MODELOS DE IA

La DPA francesa ha publicado, en inglés, sus directrices sobre desarrollo de modelos de IA cuando la información utilizada para el entrenamiento incluye datos personales. Se abordan asuntos como el recurso al interés legítimo, medidas en el caso de que la recopilación se realice a través de raspado web, cómo informar a los interesados y facilitar el ejercicio de sus derechos y seguridad, en general, de los modelos de IA.

Disponible en: https://www.cnil.fr/fr/ai-how-to-sheets

14. LA AEPD ANALIZA EL USO DE SISTEMAS DE IA PARA SERVICIOS DE TRANSCRIPCIÓN

La AEPD analiza en su blog las implicaciones en protección de datos del uso de servicios de transcripción de voz mediante IA, recordando que con carácter general la voz es un dato personal debido a que permite identificar a una persona, lo que activa plenamente la aplicación del RGPD. El tratamiento no se limita a la conversión de audio a texto, sino que puede incluir tratamientos adicionales, como el reentrenamiento de los sistemas, con finalidades propias y responsabilidades diferenciadas.

La Agencia subraya la obligación de diligencia del responsable al elegir estos servicios: verificar bases legitimadoras, transparencia, uso de terceros, conservación de datos, así como posibles inferencias (emociones u otros datos sensibles), que podrían implicar mayores riesgos e incluso encajar en supuestos de IA prohibida por el RIA.

Disponible en: https://www.aepd.es/prensa-y-comunicacion/blog/transcripcion-de-voz-con-ai

15. ANUNCIOS EN CHAT GPT

OpenAI ha presentado ChatGPT Health, una nueva sección orientada al análisis de datos de salud, además, permite la conexión con aplicaciones de salud y registros electrónicos de salud. Esta funcionalidad implica el acceso potencial a una cantidad ingente de datos especialmente sensibles, lo que eleva de forma significativa los riesgos desde la perspectiva de la protección de datos.

Las implicaciones son relevantes: desde las consecuencias de una eventual brecha de seguridad, hasta los usos secundarios que OpenAI pueda realizar de esta información, con las obligaciones regulatorias que ello conlleva. Por el momento, el servicio no está disponible en la UE ni en el Reino Unido, pero será cuestión de tiempo.

Disponible en: https://openai.com/es-ES/index/introducing-chatgpt-health/?utm_source=substack&utm_medium=email.

16. LA IAPP HA PUBLICADO UN DIRECTORIO DESTINADO A OFRECER SOPORTE SOBRE LA REGULACIÓN DE LA IA

La IAPP ha actualizado su directorio normativo sobre la regulación de IA de la UE. Dicho directorio permite identificar a los organismos nacionales encargados de su aplicación, supervisión y ejecución en cada Estado miembro. El recurso aporta claridad sobre un marco institucional complejo y todavía en construcción, clave para entender quién controla qué en materia de IA en la UE.

Disponible en: https://iapp.org/resources/article/eu-ai-act-regulatory-directory?utm_source=substack&utm_medium=email

17. ANUNCIOS EN OPEN AI ESTADOS UNIDOS

Open AI ha comunicado que comenzará a realizar pruebas en la implementación de anuncios en Estados Unidos para los usuarios de los planes gratuitos y ChatGPTGo. En cuanto a los riesgos en la privacidad, Open AI indica que los datos y conversaciones no serán vendidos a los anunciantes, permitiendo, a su vez, que los usuarios puedan desactivar la personalización de los anuncios.

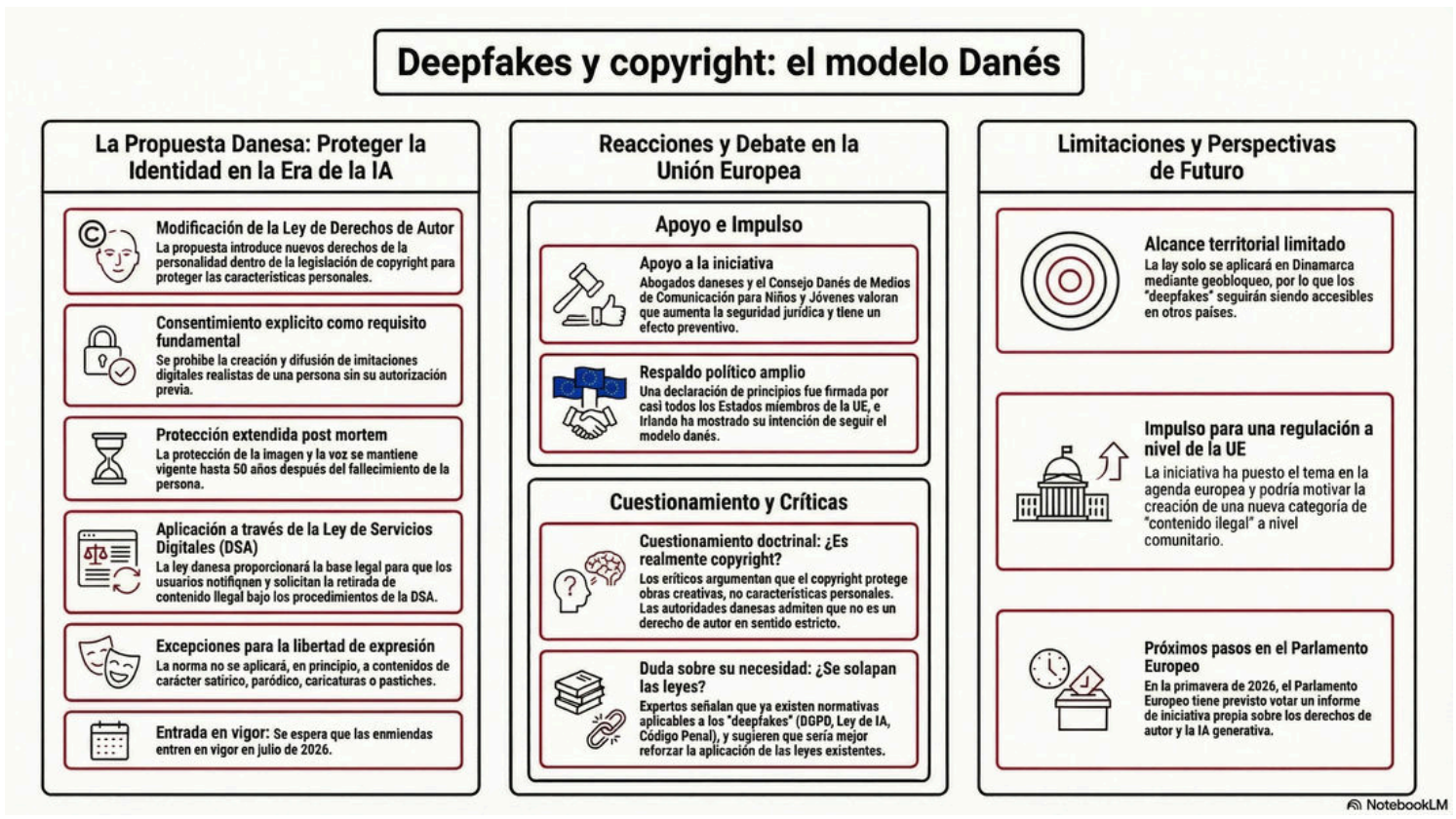
En relación con ello y, en un contexto en el que se deben generar ingresos, resulta interesante la lectura del artículo "Risky Business Advanced AI Companies' Race for Revenue" en el que se realiza un análisis de los principales modelos de negocios de las empresas líderes en IA. Disponible en: https://cdt.org/wp-content/uploads/2025/12/2026-01-07-CDT-Issue-Brief-Risky-Business-final.pdf.

18. DINAMARCA PROPONE MODIFICACIONES EN SU NORMATIVA DE COPYRIGHT PARA ABORDAR LOS DEEPFAKES

Dinamarca ha propuesto modificaciones en su Ley de Copyright para otorgar a las personas un mayor control sobre su voz e imagen para afrontar los deepfakes generados por IA a través del marco de copyright. El objetivo es ofrecer una protección general contra las imitaciones realistas generadas digitalmente de las características personales y la protección contra las imitaciones realistas generadas digitalmente de artistas, intérpretes o ejecutantes. La protección exigiría consentimiento previo y duraría hasta 50 años después de la muerte, aplicándose principalmente a contenidos no autorizados, mientras que caricaturas, sátira o parodias quedarían en principio excluidas. Se pretende facilitar la notificación y retirada de estos contenidos ilegales a través del mecanismo del Digital Services Act (DSA).

Se prevé su entrada en vigor en julio, aunque solo se aplicarían a los contenidos ilegales en su territorio a través del bloqueo geográfico por parte de las plataformas en línea y los motores de búsqueda de gran tamaño.

Disponible en: https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/782611/EPRS_ATA(2026)782611_EN.pdf



19. TIKTOK FINALIZA UN ACUERDO PARA CREAR UNA NUEVA ENTIDAD ESTADOUNIDENSE

TikTok ha cerrado un acuerdo para crear una entidad mayoritariamente estadounidense con el fin de evitar su prohibición en EE.UU., poniendo fin a seis años de disputas políticas por riesgos de "seguridad nacional". La nueva sociedad estará controlada por tres inversores, Oracle, Silver Lake y MGX. Según indica dicha sociedad, ésta "operará bajo salvaguardas definidas que protegen la seguridad nacional a través de protecciones integrales de datos, seguridad de algoritmos, moderación de contenido y garantías de software para los usuarios estadounidenses".

Disponible en: https://techcrunch.com/2026/01/23/tiktok-finalizes-deal-to-create-new-us-entity-and-avoid-ban/ .

20. NUBE "INDEPENDIENTE" PARA EUROPA: AWS SOVEREIGN CLOUD

Amazon Web Services (AWS) ha lanzado el servicio "AWS European Sovereign Cloud", una nube independiente para Europa situada íntegramente dentro de la UE, física y lógicamente separada de otras regiones de AWS.

La primera región de AWS se encuentra ubicada Brandeburgo, Alemania y planean establecer zonas locales en Bélgica, Países Bajos y Portugal. Con esta nube todos los datos permanecen dentro de la UE y cuentan con controles técnicos para impedir el acceso desde fuera de la UE. Según indican, todas las operaciones diarias, el soporte técnico y la atención al cliente se realizará exclusivamente por residentes en la UE.

Más información en: https://aws.eu/es/.

21. LA CNIL IMPONE UNA SANCIÓN DE 3,5 MILLONES DE EUROS POR TRANSMITIR DATOS A UNA RED SOCIAL CON FINES PUBLICITARIOS

La CNIL ha multado con 3,5 millones de euros a una empresa por compartir los datos de su programa de fidelidad con una red social con fines publicitarios, sin contar con un consentimiento válido de los usuarios. Entre 2018 y 2023, la compañía utilizó direcciones de correo electrónico y números de teléfono para mostrar anuncios personalizados, pero la información proporcionada fue insuficiente y poco clara, lo que impedía que los usuarios prestaran un consentimiento explícito e informado.

La sanción se adoptó en colaboración con 16 autoridades europeas y afecta a más de 10,5 millones de personas.

Disponible en: https://www.cnil.fr/fr/transmission-de-donnees-un-reseau-social-des-fins-publicitaires-sanction

EL LIBRO DEL MES

Ahora que los Deepfakes están al orden del día, este libro, de Beatriz Izquierdo, no puede parecernos más oportuno. No es que este asunto sea el eje central del libro, pero también se aborda. El libro plantea, de manera muy práctica, cómo el mundo digital ha cambiado el “patio del colegio”: lo que para unos es una broma, puede convertirse en conductas con calificación penal. Con un lenguaje directo (“bro”) pretende llegar a familias y adolescentes para explicar qué comportamientos son delito, cuáles son “zonas grises” y qué señales de alarma conviene detectar a tiempo. Su idea central es doble: proteger a los menores como posibles víctimas, pero también evitar que, por desconocimiento o presión de grupo, acaben actuando como autores (verdugos) de acoso, amenazas, sextorsión, difusión no consentida de imágenes, suplantaciones y humillaciones públicas. La edad atenúa y orienta la respuesta (vía menores, medidas educativas), pero no elimina consecuencias (responsabilidad penal del menor, civil de los progenitores en ciertos casos, huella digital etc.).

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.