Beta Bits Legal Recap

HIGHLIGHTS DE FEBRERO 2026

Derecho Digital y Protección de Datos

1. OPINIÓN CONJUNTA EDPB-EDPS SOBRE EL DIGITAL OMNIBUS

Se ha publicado la opinión conjunta EDPB-EDPS sobre el tan cacareado “Digital Omnibus”. Aquí van los puntos principales:

- **Modificar** el RGPD en el sentido indicado por el TJUE puede generar inseguridad jurídica y vías de elusión del RGPD si se “negativiza” el concepto.

- **IA + interés legítimo:** No es necesaria una regla especial. Ya existe marco suficiente y una cláusula específica puede crear confusión. La opinión recomienda incluir un "derecho incondicional de oposición". Si se recurre al interés legítimo, habrá que blindar ponderación, transparencia y mecanismos de oposición.

- **Derecho de acceso:** No limitar el “abuso” del derecho de acceso con finalidad distinta de obtener información sobre el tratamiento.

- **Decisiones automatizadas (art. 22 RGPD):** mantener la prohibición general. Debe evitarse que la ejecución de contrato se convierta en una habilitación general. El hecho de que la decisión pueda ser tomada por una persona, no obstante, no debe evitar a que se recurra a la decisión automatizada per se.

- **Biometría**: la opinión acoge que se pretenda permitir la autenticación biométrica (1:1) solo si los medios de verificación están bajo control exclusivo de la persona. OJO, aun así, el tratamiento deberá ser proporcional y necesario.

- **Brechas de seguridad:** más margen temporal. A favor de ampliar el plazo de notificación (de 72 a 96h) y centrar notificación en supuestos relevantes, sin perder trazabilidad interna y de notificar a la DPA solo las brechas con afectación sustancial a los interesados.

- **ePrivacy/cookies:** ok a solucionar "la fatiga del consentimiento" y a reducir banners con excepciones limitadas. Sobre las nuevas excepciones al consentimiento para medición de audiencia y seguridad deben establecerse condiciones (funcionalidad limitada, anonimidad, finalidad limitada y uso propio, etc.). Se sugieren plazos máximos para solicitar el consentimiento cuando se ha rechazado (6 meses). Ok a las Indicaciones automatizadas y legibles por máquina sobre las elecciones del interesado, pero indicando quién debe aplicarlos.

Opinión disponible en: https://www.edpb.europa.eu/news/news/2026/digital-omnibus-edpb-and-edps-support-simplification-and-competitiveness-while_es.

2. GUÍA DE LA AEPD SOBRE “IA AGÉNTICA”

La AEPD ha emitido una recomendaciones sobre IA agéntica. Estos sistemas, que no solo generan contenido sino que también ejecutan tareas, están en boga.

Las orientaciones analizan los aspectos de cumplimiento de la normativa de protección de datos, las posibles vulnerabilidades, que no son pocas, y las amenazas específicas que pueden aprovecharse de esas vulnerabilidades. Se enumeran un conjunto de posibles medidas que podría adoptar un responsable o encargado para garantizar el cumplimiento de la normativa y reducir o eliminar los impactos que presenta la IA agéntica en relación con los derechos y libertades de las personas.

La OECD también ha contribuido a clarificar los conceptos de “IA agéntica” y “agentes de IA”, que no son lo mismo.

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

3. “CONVERSIÓN” DE ENCARGADO A RESPONSABLE EN CASO DE QUIEBRA DEL RESPONSABLE INICIAL

Cuando el responsable, que proporcionaba un sistema de registro de jornada, se declaró en quiebra, algunos de los trabajadores necesitaron acceso a sus registros de tiempo para documentar reclamaciones de cantidad por salarios no pagados. Un interesado solicitó directamente los registros al encargado, pero la compañía se negó a proporcionar los datos, argumentando que era eso, encargado, y que, tras la quiebra del responsable, no recibía indicaciones respecto del tratamiento, por lo que no tenía ningún deber de revelar los datos personales sin compensación por parte del responsable (en quiebra).

La DPA sostuvo que siempre debe haber un responsable del tratamiento. No puede existir sólo encargado (sin responsable), considerando que Timegrip era el responsable al conservarlos tras la quiebra, determinando quién podía acceder a ellos, estableció el período de almacenamiento y rechazó las solicitudes de acceso de forma independiente. Como responsable, Timegrip tenía la obligación legal de cumplir con el derecho de acceso de los interesados en virtud del artículo 15.1 y 3 del RGPD.

La resolución: https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/?y=2026.

4. EL GARANTE ITALIANO ORDENA A AMAZON LA DETENCIÓN DEL TRATAMIENTO DE DATOS DE TRABAJADORES

Parece que la filial italiana se ha extralimitado, digamos, “ligeramente” en el tratamiento de los datos de trabajadores que volvían al trabajo tras periodos de baja o ausencia.

Después de su regreso les solicitaban y trataban información sobre patologías específicas, adhesión a huelgas y participación en actividades sindicales, así como datos personales de tipo familiar y privado.

Además, tendrá que detener el procesamiento de los datos recopilados a través de cuatro cámaras ubicadas cerca de baños y áreas de refresco reservadas para los trabajadores.

El comunicado está disponible aquí: https://gpdp.it/home/docweb/-/docweb-display/docweb/10224050.

5. SANCIÓN A REDDIT

La Information Commissioner’s Office (ICO) ha multado a Reddit, Inc. con 14, 47 millones de libras por utilizar información personal de menores de 13 años sin una base legítima para el tratamiento. Con la investigación realizada por la ICO, se concluyó que Reddit no había implementado medidas robustas de verificación de edad para acceder a contenido de adultos y, por tanto, no contó con una base legal para tratar la información personal de menores de 13 años. Asimismo, Reddit no había realizado una Evaluación de Impacto centrada en los riesgos de utilizar datos personales de menores.

Disponible en: https://cy.ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/02/reddit-issued-with-1447m-fine-for-children-s-privacy-failures/.

6. ANTHROPIC ACUSA A TRES EMPRESAS CHINAS DE “DESTILAR” A CLAUDE AI

Anthropic, mediante un comunicado, ha acusado a tres empresas chinas: Deepseek, Minimax y Moonshot AI, de hacer un uso indebido de su modelo de IA Claude para intentar mejorar sus propios productos. Según Anthropic, este uso indebido incluye la implicación de más de 24.000 cuentas fraudulentas, el uso de servicios de proxy y más de 16 millones de intercambios con Claude, en concreto: Deepseek sobre 150,000, Minimax sobre 13 millones y Moonshot AI sobre 3.4 millones.

Dichas interacciones están destinadas a extraer capacidades específicas del modelo de Claude. De esta forma pueden entrenar a un modelo menos avanzado a partir de las salidas generadas por otro más avanzado. Si bien, Anthropic indica que “destilar” un modelo es una práctica legítima en determinados casos, los modelos destilados ilícitamente carecen de las salvaguardias necesarias, cuestión que genera importantes riesgos.

Comunicado disponible en: https://www.anthropic.com/news/detecting-and-preventing-distillation-attacks.

7. OPENCLAW Y LAS ADVERTENCIAS DE LA *DUTCH* DPA

Ni que decir tiene del lanzamiento de OpenClaw ha roto los esquemas de la IA Agéntica. OpenAI ha corrido en “fichar” a su creador. La Dutch DPA también ha alertado de los más que evidentes riesgos del uso de estos sistemas, que podemos resumir en los siguientes:

Riesgo	En qué consiste	¿Afecta en uso local?	Impacto típico
Prompt injection	Instrucciones “ocultas” en webs, emails, mensajes o adjuntos que fuerzan al agente a ejecutar acciones o revelar datos.	Sí, si consume contenido externo o interno “infectado”.	Exfiltración de “secretos”; acciones destructivas; acceso indebido a correo/servicios.
Gestión de “secretos” (tokens, logs, etc.)	Claves API/OAuth en ficheros, directorios del agente o logs; fuga por mala praxis o por el propio agente.	Sí	Compromiso de correo, mensajería, repositorios, APIs, etc.
Permisos excesivos	El agente hereda privilegios del usuario (lectura/escritura/ejecución). Si es manipulado, el daño es “local” pero total.	Sí	Borrado/cifrado de ficheros, extracción de documentos, etc.
Supply chain	Paquetes o extensiones maliciosas, “skills” envenenados; typosquatting, etc.	Sí	Robo de credenciales, descarga de malware.
Instancia/panel expuesto (puertos abiertos)	Consolas o APIs accesibles públicamente por mala configuración	Reducido en local si no hay exposición	RCE/compromiso remoto.
Privacidad y datos personales	Tratamiento de mensajes/adjuntos/PII; posible envío a terceros (APIs)	Sí	Brecha de datos incumplimiento RGPD y del secreto profesional.
Acciones autónomas con efecto económico/operativo	Llamadas a APIs con coste; automatizaciones que ejecutan acciones sin revisión.	Sí	Costes inesperados o errores operativos.
Telemetría/envío involuntario de datos	Subida de logs, prompts o trazas a servicios externos por defecto.	Depende de la configuración	Fuga de información sensible y/o datos personales.

Advertencia de la DPA disponible en: https://www.autoriteitpersoonsgegevens.nl/en/current/ap-warns-of-major-security-risks-with-ai-agents-like-openclaw.

8. LOS DIPUTADOS DE LA COMISIÓN DE ASUNTOS JURÍDICOS DEL PARLAMENTO EUROPEO APRUEBAN PROPUESTAS SOBRE DERECHOS DE AUTOR Y USO DE LA IA GENERATIVA

Los diputados de la Comisión de Asuntos Jurídicos adoptaron una serie de propuestas para garantizar la transparencia y la remuneración justa a los autores por el uso de sus obras protegidas en inteligencia artificial generativa. En particular:

- Se solicita que la Ley de derechos de autor de la UE se aplique a todos los sistemas de IA generativa disponibles en el mercado de la UE, independientemente de dónde se lleve a cabo les entrenamiento.

- Se cumplan las obligaciones de transparencia mediante aportaciones de información detallada sobre contenidos protegidos usados para entrenar y disponer de registros detallados de las actividades de rastreo.

- Se exige una remuneración adecuada para los titulares de los derechos por el uso de sus contenidos y, además, se pide a la Comisión que analice si la remuneración podría extenderse también a usos pasados.

- Se solicita proteger el pluralismo de los medios frente a la IA que agrega noticias y desvía ingresos, garantizando control y remuneración por el uso de contenidos para entrenar sistemas de IA.

- Se sostiene que el contenido totalmente generado por IA no debe tener protección por la normativa de derechos de autor y reclaman medidas contra la difusión de contenidos manipulados o ilegales generados por IA.

- Se reclama un marco claro de licencias para el uso de obras por la IA generativa, con acuerdos colectivos accesibles a todos, y herramientas que permitan a los autores excluir sus contenidos del entrenamiento de IA.

Disponible en: https://www.europarl.europa.eu/news/en/press-room/20260126IPR32636/protect-copyrighted-work-used-by-generative-ai-say-legal-affairs-meps.

9. SANCIÓN DE LA CNMC A UN PROVEEDOR DE TV BAJO DEMANDA POR OFRECER CONTENIDO PORNOGRÁFICO

La CNMC ha sancionado a una empresa prestadora de servicios de televisión bajo demanda (una web de contenido pornográfico) por ofrecer contenidos pornográficos para adultos, sin contar con mecanismos eficaces de verificación de edad que impidieran el acceso a menores, tal y como exige el artículo 99.4 de Ley General de Comunicación Audiovisual.

En la resolución, la CNMC indica que según las Directrices de la Comisión Europea sobre medidas para garantizar un elevado nivel de privacidad, seguridad y protección de los menores en línea (C/2025/5519), al tratarse de un supuesto de alto riesgo como es el acceso a contenido pornográfico, deben implementarse sistemas de verificación de edad apropiados y proporcionados para garantizar la protección de los menores. En el presente caso, la empresa no había implementado estos mecanismos técnicos y solamente tenía implementado un banner de autodeclaración de edad.

La sanción ha sido de 1.300€. Resolución disponible en: https://www.cnmc.es/sites/default/files/6391670.pdf.

10. ¿SE PUEDE CONSIDERAR A UN TRABAJADOR RESPONSABLE DEL TRATAMIENTO?

Resolución curiosa esta de la AEPD que hace una interpretación muy extensiva del concepto de responsable del tratamiento.

Trabajadoras de centro médico que acceden a historia clínica de otra compañera sin relación asistencial mediante. La persona afectada presenta denuncia ante la AEPD contra una de ellas, no contra el centro médico. La AEPD, ojo, interpreta que ello es posible, y la reclamada puede ser considerada, por tanto, Responsable del Tratamiento, si se dan dos condiciones:

1) Si no existe relación asistencial alguna entre quien realiza los accesos indebidos y el interesado.

2) Se contravienen las indicaciones del centro (responsable del tratamiento).

Lo anterior, entendemos amplía de manera forzada el concepto de Responsable del Tratamiento. Las directrices del EDPB están pensando en supuestos en que, efectivamente, hay un uso de los datos por parte de un trabajador con fines propios, por ejemplo, alguien que extrae bases de datos de clientes para su propia empresa. Otro supuesto sería el de la extensión del tratamiento, por ejemplo, en casos de difusión de datos de terceros en redes sociales.

Pero es que en el presente supuesto, la finalidad del acceso ilícito es presentar una denuncia contra la reclamante (si bien no por ello se vuelve dicho acceso legítimo), lo que no la convierte en RT.

¿Dónde queda la excepción doméstica?

Existen otras vías sancionatorias para quien ha accedido a la HC de manera ilícita: la laboral, pudiendo ser causa de despido o, más severa aun, la penal.

La reclamada se libra de la sanción, parece, por no haberse podido acreditar que se encontrara en el lugar del que procedía la IP desde la que se produjeron los accesos, en otro caso, según indica la AEPD podría haber sido considerada responsable.

Resolución disponible en: https://www.aepd.es/documento/ps-00491-2024.pdf.

11. LA COMISIÓN EUROPEA INICIA INVESTIGACIÓN SOBRE SHEIN

De conformidad con la DSA, la Comisión Europea ha iniciado una investigación sobre SHEIN con la finalidad de realizar un análisis sobre el diseño adictivo de la plataforma (puntos y recompensas a los usuarios) y los riesgos que estos suponen para los consumidores, los mecanismos que tienen implantados para limitar la venta de productos ilegales en la UE, la transparencia de sus algoritmos de recomendación para proponer contenido y productos a los usuarios y la elaboración de perfiles para cada sistema de recomendación.

La Comisión ha iniciado la investigación tras analizar preliminarmente los informes de evaluación de riesgos de SHEIN, sus respuestas a las solicitudes formales de información (28 de junio de 2024, 6 de febrero de 2025 y 26 de noviembre de 2025) y la información aportada por terceros.

12.

SANCIÓN DE LA AUTORIDAD ITALIANA POR USO DE SISTEMAS DE GEOLOCALIZACIÓN CON PERFILADO EN VEHÍCULOS CORPORATIVOS

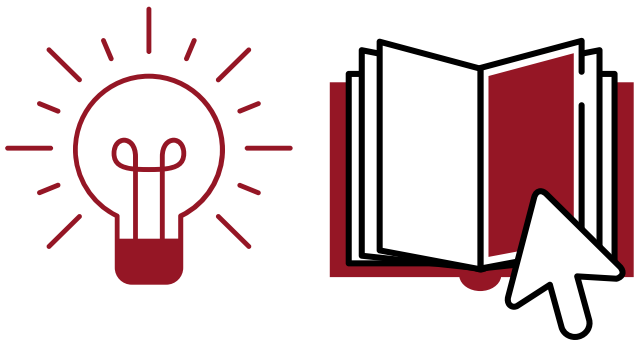
El Garante para la protección de datos sancionó con 120.000 € a una empresa por instalar en vehículos corporativos dispositivos telemáticos por satélite capaces de monitorizar de forma detallada la conducción de los empleados y asignarles puntuaciones según su estilo de conducción.

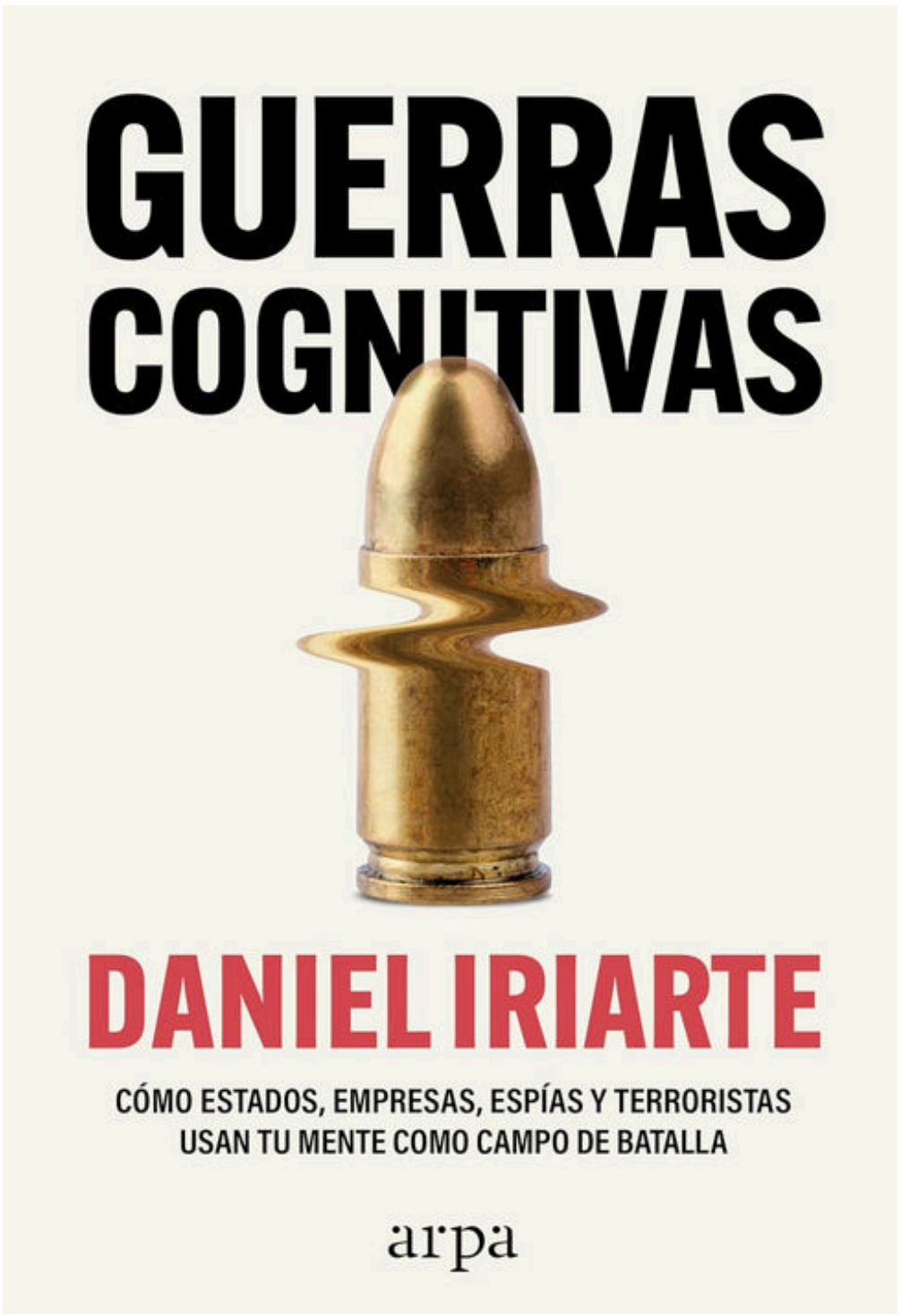
La autoridad identificó las siguientes infracciones:

- Control desproporcionado del trabajador: El sistema recopilaba información muy detallada (tiempos de uso, kilómetros recorridos, consumo y estilo de conducción), tanto durante los desplazamientos laborales como en los trayectos de uso privado, configurando un seguimiento continuo e invasivo.
- Falta de transparencia e información adecuada: La información facilitada era genérica para todas las sociedades del grupo (incluidas entidades fuera de la UE) y no especificaba con claridad las finalidades del tratamiento, la base jurídica, la identidad de los responsables, ni los destinatarios o sujetos autorizados a acceder a los datos.
- Justificación insuficiente: La empresa invocó el interés legítimo, pero el Garante consideró que no era válido para justificar un control permanente que afectaba también a la esfera privada de los empleados.
- Deficiente control de accesos: Los datos podían ser consultados por personal de distintas sociedades del grupo sin una adecuada limitación de perfiles y permisos.
- Conservación excesiva: La información se almacenaba durante 13 meses, un plazo considerado no proporcional ni alineado con las finalidades declaradas.

Puede consultar más información: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10213711.

EL LIBRO DEL MES





No puede ser más oportuno, en estos (malos) tiempos que corren para la geopolítica, el trabajazo que Daniel Iriarte ha tenido a bien plasmar en “Guerras Cognitivas: Cómo estados, empresas, espías y terroristas usan tu mente como campo de batalla”. Podrás descubrir en detalle como los Estados, desde USA, pasando por Rusia, Cuba, China, España, Taiwán o Rumanía, entre otros, en los conflictos actuales, ya no libran sus batallas solo con armas, sino también manipulando la mente de las sociedades utilizando internet, redes sociales, bots e inteligencia artificial para influir en la opinión pública y alterar comportamiento colectivo.

Iriarte analiza cómo campañas de desinformación, propaganda digital y manipulación algorítmica pueden influir en elecciones, conflictos internacionales o debates sociales. También muestra cómo estas estrategias buscan generar miedo, polarización o desconfianza para debilitar a los adversarios sin necesidad de iniciar una guerra militar directa. El libro combina análisis geopolítico con ejemplos reales, y advierte que estas tácticas ya forman parte de la competencia entre potencias globales.

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.