Agencia Española de Protección de Datos
Premio Comunicación de Protección de Datos Personales

Título: El desafío de la privacidad en la era de la IA: Investigación, vigilancia tecnológica y defensa ciudadana
Autor: Carlos del Castillo
Medio de comunicación: elDiario.es

BLOQUE 1

Investigación y análisis: Riesgos visibles e invisibles de la IA Generativa

- Cuando la IA deja de ser privada: ¿qué implica que sus conversaciones puedan usarse para la publicidad?
- Los 10 días de porno machista que pueden costar caro a Elon Musk: "No es cuestión de bikini o burka, sino de consentimiento"
- Tres años de ChatGPT: la máquina que no pudo quitarte el trabajo ahora va a por tus secretos

BLOQUE 2

Actualidad y Servicio Público: Alertas tempranas, sanciones y defensa ciudadana ante los riesgos tecnológicos

Sub-bloque A: biometría y vigilancia

- Multa de 10 millones a Aena por hacer reconocimiento facial a los pasajeros "sin justificar su necesidad"
- La empresa que escaneaba el iris a cambio de criptomonedas deberá borrar todos los datos recopilados
- La empresa de análisis genéticos 23andMe se declara en quiebra y pone en duda los datos de ADN de 15 millones de personas
- Llegan las multas por seguir utilizando la huella dactilar para el control horario

Sub-bloque B: menores y redes sociales

- Protección de Datos avisa que desnudar a otras personas con IA ya puede ser delito o acarrear multas con las leyes actuales
- Multa de 2.000 euros a los padres de un menor que creó una imagen de una compañera desnuda con inteligencia artificial
- Protección de Datos multa con 40.000 euros al colegio de Boadilla en el que se grabó a alumnas en ropa interior
- La app del Gobierno para bloquear el acceso de los menores al porno pasa el último filtro de seguridad a la espera de la solución europea
- El Gobierno espera activar un bloqueo de redes sociales para menores de 16 años como el australiano en 2026
- La industria digital recela del “control duro” de la edad de los menores en redes que el Gobierno plantea para 2026
- La UE resucita su plan de escanear todos los chats en busca de abuso infantil: “Es una amenaza enorme”
- Protección de Datos alerta de que TikTok ha reactivado el envío de datos personales a China y pide replantearse su uso

Sub-bloque C: Plataformas tecnológicas y economía de datos

- La condena a Meta reordena el tablero digital: la Justicia zanja que plataformas y medios compiten por el mismo mercado
- Quisimos entrevistar a esta exdirectiva de Facebook. Mark Zuckerberg no lo ha permitido
- Una exdirectiva de Facebook dirigirá el regulador de privacidad de las grandes tecnológicas de EEUU en Europa
- Meta utilizará a partir de hoy todos los datos de las conversaciones con su IA para personalizar sus anuncios
- X empieza a vender datos de usuarios para entrenar inteligencias artificiales en medio de la fuga hacia Bluesky

- Elon Musk paga 300 millones para que su inteligencia artificial entre en Telegram
- La investigadora que destripa el mito de OpenAI y Sam Altman: “Las multinacionales de IA aceleran el retroceso democrático”
- Google entierra definitivamente su plan para eliminar las cookies de terceros de Chrome
- Casi 5 millones de euros de sanción a Netflix por ocultar dónde envía los datos de sus usuarios

Sub-bloque D: Defensa ciudadana y difusión de resoluciones

- Siete llamadas y una estafa: así funciona el teatro de ofertas falsas para robar tus datos en nombre de la OCU
- Protección de Datos prohíbe a hoteles y alojamientos hacer copias del DNI de los clientes
- El Parlamento Europeo refuerza su alerta sobre WhatsApp a los diputados y les pide usar Signal en sus viajes al extranjero
- Protección de Datos zanja el debate: la baliza V-16 de la DGT no puede identificar al conductor ni controlar sus viajes
- Medio millón de euros de multa a ING por perder datos confidenciales de un cliente y no saber cómo encontrarlos
- Protección de Datos empieza a multar a empresas por subir fotos al perfil de sus trabajadores sin permiso
- Multa a una empresa de videncia por enviar cientos de SMS en tres meses a un solo móvil: “Visualizo todo sin que me digas nada”
- Multa de 3,2 millones a Carrefour por múltiples brechas de seguridad que afectaron a 120.000 clientes

BLOQUE 1

Investigación y análisis: Riesgos visibles e invisibles de la IA Generativa

Cuando la IA deja de ser privada: ¿qué implica que sus conversaciones puedan usarse para la publicidad?

La llegada de los anuncios a ChatGPT abre una era en la que las conversaciones con la IA se convierten en una fuente de datos de alto valor para el perfilado publicitario y potentes herramientas de persuasión

— Tres años de ChatGPT: la máquina que no pudo quitarte el trabajo ahora va a por tus secretos

Carlos del Castillo

SEGUIR AL AUTOR/A

29 de enero de 2026
21:39 h
Actualizado el
30/01/2026 18:19 h
3

Tras la aparición de ChatGPT, el gran temor de muchos fue el empleo. Más de tres años después de aquel *momento cero* de la inteligencia artificial, el apocalipsis de la automatización no ha llegado y los cambios económicos que producirá esta tecnología son aún inciertos. La revolución de la inteligencia artificial es profunda, pero avanza en una esfera más íntima, mucho más personal que una cifra de paro.

Este 2026, millones de personas utilizan sistemas de inteligencia artificial como confidentes, asesores personales o apoyo emocional. Es esa compañera que la empresa se niega a contratar para aligerar la carga de trabajo, el profesor particular que la familia no se puede permitir y la psicóloga que está disponible las 24 horas. Un espacio percibido como seguro para expresar cualquier cosa, desde ideas políticamente incorrectas a la duda visceral de si merece la pena seguir viviendo.

Cada día se generan largas conversaciones entre máquina y persona, unas veces escritas y otras a través de herramientas de voz. Con lenguaje cuidado cuando se habla de un tema fiscal o con abreviaturas de chat al intentar entender la reacción de una pareja. Con voz agitada para preguntar la última duda antes de un examen final o apagada tras varias horas rumiando un problema en la cama.

La IA está abriendo una nueva era de intimidad automatizada. El problema es que, para las empresas que la desarrollan, íntimo no significa necesariamente lo mismo que privado.

El recurso de la publicidad

Las principales empresas desarrolladoras de IA ya llevan a cabo análisis detallados de los datos de las conversaciones para mejorar sus servicios. Según un estudio reciente de la Universidad de Stanford, se trata de una práctica habitual en OpenAI, Google, Microsoft o Amazon. "Si compartes información sensible en un chat con ChatGPT, Gemini u otros modelos avanzados, puede recopilarse y utilizarse para el entrenamiento, incluso aunque esté en un archivo independiente que hayas subido durante la conversación", destaca la autora, Jennifer King, investigadora en políticas de privacidad.

Sin embargo, la posibilidad de que estas empresas den un paso más y utilicen esa cascada de información íntima para la publicidad se ha tornado muy real este 2026. Especialmente tras el anuncio de OpenAI de que ChatGPT, el detonante de esta revolución, incluirá anuncios en los próximos meses.

La privacidad en cada empresa de Inteligencia Artificial

Estado de cinco políticas de privacidad de cada empresa de IA analizadas

Práctica de Privacidad	ıazon	Anthropic	Google	Meta	Microsoft	OpenAI
Uso de chats para entrenamiento *(por defecto)*	Sin ecificar	Sí	Sí	Sí	Sí	Sí
Mecanismo para excluirse del entrenamiento	Sin ecificar	Sí	Sí	Sin especificar	Sí	Sí
Retención indefinida de los datos del chat	Sí	No	No	Sí	No	Sí
Funciones de personalización del chatbot	Sin ecificar	Sin especificar	Sí	Sí	Sí	Sí
Permite cuentas para menores *(13-18 años)*	No	No	Sí	Sí	Sí	Sí

Fuente: Universidad de Stanford · Creado con Datawrapper

Las señales de este cambio de rumbo se acumularon durante todo 2025. Sam Altman, director ejecutivo de OpenAI, fue alterando su discurso a medida que el mercado publicitario se iba haciendo más inevitable para su empresa, que nunca ha tenido beneficios, pero se ha comprometido a invertir 1,4 billones de dólares en computación hasta 2033.

Así, la publicidad pasó de ser "el último recurso" de la empresa, debido a que "la combinación de anuncios con IA" le resultaba "especialmente inquietante", a ser una posibilidad. "Me encantan los anuncios de Instagram", dijo finalmente Altman en referencia al modelo de negocio Meta, la gran multinacional de la publicidad online junto con Google y propietaria tanto de esa red social como de Facebook o WhatsApp.

Meta también fue la primera en usar los datos recogidos por su IA para el perfilado publicitario, el mecanismo por el cual estas plataformas recopilan a partir del análisis del comportamiento digital (desde las búsquedas hasta al tiempo que se pasa leyendo cada tipo contenido) para generar una ficha de intereses. Una información que usan para vender a los anunciantes la posibilidad de mostrar su publicidad solo a aquellas personas que son más susceptibles a ella.

> ***"Me encantan los anuncios de Instagram***"
> Sam Altman - director ejecutivo de OpenAI

Con el giro de OpenAI y la evidencia de que Meta emplea la IA para potenciar su negocio actual, queda Google como tercer gran actor involucrado. Su modelo Gemini es uno de los más avanzados del mercado y la multinacional coqueteó con la idea de incluir anuncios en él durante su última presentación de resultados. Preguntada al respecto por elDiario.es, una portavoz se remite a la política actual de la empresa: "No se están usando tus conversaciones con las aplicaciones de Gemini para mostrarte anuncios. Si esto cambia, te informaremos claramente".

Sin embargo, la inclusión de la IA en el perfilado no es solo una vuelta de tuerca más en ese sistema. Su potencial es mucho mayor y la clave radica precisamente en el carácter íntimo que tiene para millones de usuarios. "Son conversaciones que los usuarios poco reflexivos consideran privadas", advierte Jorge García Herrero, abogado especialista en derecho digital. "Son una auténtica mina de datos de categoría especial, ya que están documentados los usos masivos de estos chats para obtener *feedback* propio de amigos, parejas amorosas, médicos o psicólogos".

Esos datos de categoría especial que menciona el jurista son aquellos sobre la salud, la ideología o la condición de una persona. Cuentan con una protección reforzada en el Reglamento General de Protección de Datos (RGPD) de la UE e inferirlos sin consentimiento se considera ilegal. Sin embargo, al actuar como confidentes en conversaciones sobre estos temas, los chatbots pueden extraerlos fácilmente del contexto de las conversaciones y el análisis de patrones.

De la segmentación a la persuasión

Muchas de las críticas que reciben las redes sociales y las plataformas digitales por diseñar algoritmos adictivos, fomentar sentimientos extremos en los usuarios como la ira o la frustración o empujarlos a la radicalización, son consecuencias directas del modelo publicitario que ha imperado en Internet las últimas dos décadas. Más tiempo de uso implica más datos personales y para el perfilado publicitario y más oportunidades para mostrar anuncios. Las plataformas tienen todos los incentivos para mantener al usuario enganchado.

El riesgo del matrimonio entre la publicidad y la inteligencia artificial es la introducción de esos mismos incentivos en una tecnología tan potente como esta. Un contexto "mucho más sofisticado, porque permite una interacción conversacional y, por tanto, que las intenciones últimas del usuario se desnuden con mayor precisión", avisa Ricard Martínez, director de la cátedra de Privacidad y Nuevas Tecnologías de la Universidad de Valencia.

> ***“Las compañías se van a mover en un contexto muy delicado ya la UE prohíbe cualquier técnica manipuladora o engañosa para alterar el comportamiento de una persona o colectivo”***
> Ricard Martínez - director de la cátedra de Privacidad y Nuevas Tecnologías de la Universidad de Valencia

El profesor detalla que, aunque un impacto publicitario calibrado en el momento justo dispara la tasa de éxito, sigue siendo un anuncio. Pero la inteligencia artificial desdibuja esos límites. Imaginemos una conversación entre el usuario y el chatbot que termina con una recomendación de una aerolínea. Aunque se etiquete como publicidad, ¿cómo influye el contexto de confianza en el que se ha desarrollado la conversación?

"La humanización del producto puede hacernos traspasar una delicada frontera e irnos a un entorno más propio de la manipulación", avisa Martínez. Una duda se dispara si son temas sociales o políticos los que se discuten, o cuando los usuarios son menores de edad, ya que cualquier capa publicitaria añadida en estos ámbitos trasciende cualquier contenido patrocinado en una red social.

En las plataformas digitales, la publicidad se inserta junto a lo que el usuario mira. En los chatbots, esos mismos anuncios se pueden insertar dentro de lo que el usuario razona. "Las compañías se van a mover en un contexto muy delicado, ya que el Reglamento de Inteligencia Artificial de la UE prohíbe cualquier tipo de técnicas manipuladoras o engañosas con el objetivo de alterar el comportamiento de una persona o un colectivo", recuerda.

> ***“Este mismo conocimiento, una vez se obtiene para 'personalizar la experiencia publicitaria' puede emplearse para otras personalizaciones, como sesgar las respuestas para agradar o incluso para persuadir al usuario”***
> Jorge García Herrero - Abogado especialista en protección de datos

Además, esas técnicas no solo sirven para vender anuncios. "Este mismo conocimiento, una vez se obtiene para 'personalizar la experiencia publicitaria' puede emplearse para otras personalizaciones, como la de las respuestas (ofreciendo respuestas leve o gravemente sesgadas para simplemente agradar o incluso para persuadir al usuario en determinado sentido)", enfatiza Jorge García Herrero. "Esta capacidad de persuasión es una de las principales amenazas de la generalización del uso de ChatGPT para temas de interés general, en los que tener 'verdades objetivas' sigue siendo importante", continúa.

OpenAI rechaza ese escenario y asegura que la integridad del chatbot está asegurada. "Puedes confiar en que las respuestas de ChatGPT se basan en lo que es objetivamente útil y nunca en la publicidad", promete, negando que vaya a emplear tácticas ocultas para que los usuarios pasen más tiempo en su chatbot. "Priorizamos la confianza del usuario y la experiencia de uso por encima de los ingresos", afirman. La empresa, no obstante, está

planeando cobrar el precio más alto de toda la industria por los anuncios en ChatGPT, ha anticipado el medio especializado en Silicon Valley *The Information*.

Nueva higiene digital

Esta situación no está pasando desapercibida para las instituciones. La Agencia Española de Protección de Datos (AEPD) ha publicado una guía sobre cómo interactuar con la IA con seguridad. El regulador de la privacidad recuerda que "cualquier información que se le suministra puede filtrarse en Internet o ser indexada por buscadores de manera indeseada, entre otros riesgos".

Por ello, recomienda no facilitar nunca a estos sistemas datos como el nombre completo o el DNI. Para minimizar la huella digital, sugiere medidas de higiene como utilizar correos electrónicos alternativos o borrar periódicamente el historial de conversaciones.

La Agencia también hace especial hincapié en las imágenes, tanto propias como de terceros, que se introducen en estos sistemas. "Nunca utilices imágenes en las que aparecen otras personas para generar nuevo contenido a partir de ellas. Lo que comienza como una broma puede convertirse en una infracción de protección de datos o, incluso, en un delito", afirma. Este 2026 ya se ha dado un gran escándalo en este sentido, con el uso de Grok, la IA de X y Elon Musk, para sexualizar imágenes de mujeres.

Son recomendaciones que la IA recomienda mantener también en el uso laboral de los chatbots, evitando en todo momento comunicar datos confidenciales. Además, recuerda que por potente que sea, son sistemas falibles: "Una herramienta de IA puede ofrecerte respuestas que parecen convincentes acerca de todo tipo de temas, aunque pueden ser erróneas. Evita que la IA decida por ti y mantén siempre una actitud crítica ante sus respuestas o consejos".

En España, la respuesta institucional a este nuevo modelo no recae solo en la AEPD. La Comisión Nacional de los Mercados y la Competencia (CNMC), designada como coordinadora de servicios digitales, tiene ya poder para exigir transparencia sobre cómo funcionan los sistemas de recomendación y publicidad de las grandes plataformas, e incluso para sancionarlas si vulneran las leyes europeas. Una arquitectura se suma la nueva Agencia Española de Supervisión de la Inteligencia Artificial (AESIA), llamada a aplicar el

Reglamento europeo de IA y a evaluar el riesgo de los sistemas que, como los chatbots, empiezan a mediar en decisiones sensibles.

La investigación del uso de datos de ChatGPT no ha arrancado con la llegada de la publicidad, sino que en España comenzó hace más de dos años. Fuentes de la AEPD han explicado a este medio, no obstante, que ese expediente tuvo que ser archivado al designar OpenAI a Irlanda como su establecimiento principal en Europa. "Una vez que la autoridad irlandesa emita una propuesta de resolución, la Agencia, como autoridad interesada, podrá realizar observaciones siguiendo lo establecido en el RGPD", aclaran las mismas fuentes.

Un reto que tensionará la legislación

La guía de la AEPD pone el foco en el usuario, pero los expertos consultados para este reportaje coinciden en que uno de los riesgos es que la IA desborde la legislación, como ya ocurrió con las plataformas digitales o el primer Internet.

Ricard Martínez expone que en aquel momento las autoridades actuaron de forma reactiva ante prácticas como el escaneo de correos electrónicos para perfilado publicitario o la irrupción de la mensajería instantánea, sin realizar análisis de riesgo preventivos. El catedrático indica que si las instituciones siguen siendo "profundamente reactivas", el resultado será que la IA traerá nuevos problemas que no se mitigan durante años, como ocurrió con las redes sociales.

La IA rompe muchas de las categorías de protección que las leyes han establecido a lo largo de los años. No es solo un sistema de recomendación, ni un espacio publicitario, ni una plataforma de contenido. "Lo que me gustaría es que no se volviera a repetir lo que ya vimos. Que las autoridades de protección de datos y las de inteligencia artificial fueran proactivas y actuasen de manera preventiva, permitiendo una disciplina de mercado que garantice los derechos de las personas y evite cualquier práctica lesiva", enfatiza Martínez.

Un reto que será mayor que nunca, también por los desafíos que entraña la propia tecnología. Si la industria de la publicidad online se caracteriza por su falta de transparencia, su matrimonio con la IA añadirá el hecho de que estos sistemas son opacos incluso para sus creadores. No es posible discernir por completo los procesos lógicos que llevan a una IA a proporcionar una respuesta concreta.

Descubrir casos de manipulación u otras prácticas contrarias a la ley será doblemente complicado. "Estas acciones solo se podrán detectar mediante auditorías de terceros, en su caso, ya que recordemos que estamos hablando de *cajas negras*", concluye Herrero.

El desafío está servido. La IA conversacional no es solo una herramienta nueva, es un cruce de caminos entre intimidad, negocio publicitario y derechos fundamentales. Cuanto más útil se vuelve para resolver problemas personales, más valiosos son los datos que genera y más incentivos hay para explotarlos. Si los guardarraíles llegan tarde, el matrimonio entre publicidad e IA no solo podría desbordar las categorías jurídicas actuales: también podría condicionar silenciosamente las decisiones de millones de personas antes de que nadie pueda auditar qué ha pasado dentro de la caja negra.

Los 10 días de porno machista que pueden costar caro a Elon Musk: “No es cuestión de bikini o burka, sino de consentimiento”

“Es ilegal, espantoso y repugnante”, asevera la UE, que ha pedido a la red social del magnate que guarde toda la información relacionada con lo sucedido. Múltiples países han presentado denuncias ante la Justicia mientras el multimillonario, con sus bromas, ha reconocido que conocía las protestas

— Elon Musk limita la generación de imágenes por IA en X tras la ola de denuncias por pornografía no consentida

Carlos del Castillo / Rodrigo Ponce de León
9 de enero de 2026
22:11 h
Actualizado el
11/01/2026 11:03 h
47

"Grok es la número 1 en España", presumía esta semana Elon Musk. La app de su inteligencia artificial superó a ChatGPT unos breves instantes entre las más descargadas en Google Play, la tienda de aplicaciones de Android. Una escalada que se ha producido a la vez que la avalancha de denuncias públicas e institucionales contra Musk y su desarrolladora, xAI, por permitir su uso para desnudar a mujeres e incluso menores de edad. Los especialistas consultados, no obstante, dudan que el escándalo pueda pasar factura.

Este tipo de ataques se han viralizado desde el 31 de diciembre en X, la red social del magnate, ante la pasividad de este y de la plataforma para contrarrestarlos. Grok está integrado de manera nativa en X, permitiendo a los usuarios citar a la IA en sus publicaciones para que aclare dudas, verifique hechos o responda preguntas. Desde agosto, también puede generar imágenes, algo que algunos usuarios están aprovechando para que Grok modifique una fotografía publicada en la red social para quitarle la ropa, mostrando a la persona en lencería o bikini.

Sus contestaciones se publican de manera abierta y son visibles para todos los usuarios, lo que aumenta el impacto del ataque contra la propia imagen. Aunque puede lanzarse contra cualquier persona, la mayoría de afectadas son mujeres, tanto personalidades públicas como usuarias anónimas de X, así como menores de edad.

La situación ha provocado múltiples quejas contra el hombre más rico del mundo y su plataforma. "El contenido sexual degradante y el material de abuso sexual infantil no son consecuencias inevitables de la tecnología. Son el resultado de una estrategia de producto deliberada por parte de X y de Elon Musk", ha denunciado Hilary Manson, cofundadora de Hidden Doors, una desarrolladora de IA especializada en videojuegos.

Investigaciones independientes, como la realizada por la organización AI Forensics, han documentado más de 800 vídeos e imágenes que simulaban agresiones sexuales, feminicidios y vídeos pornográficos generados por Grok a partir de fotos de mujeres reales sin su consentimiento.

"El entorno que permite que esto prospere existe desde hace tiempo. La IA amplifica estos fallos ya presentes en el sistema y agrava los daños", recalca la especialista: "Hemos tolerado la falta de seguridad en las redes sociales, la desatención general y la escasa aplicación de la ley frente a los delitos sexuales contra mujeres y menores". "Ahora hay un líder que se aprovecha de todo ello sin ninguna consideración por los daños que causa".

Musk se mofó de este tipo de denuncias en X, publicando una imagen suya en bikini generada por Grok. Sin embargo, la Unión Europea y organismos reguladores de múltiples países ya habían puesto a la plataforma en su punto de mira. Ante la presión, Musk ha terminado dando orden este viernes de bloquear la generación de imágenes en Grok, excepto para los usuarios de pago. Una maniobra que podría tener como objetivo impedir que usuarios anónimos utilicen la herramienta sin poder ser identificados por la Justicia en caso de ser necesario.

La UE pide información

"Somos plenamente conscientes de que X, a través de Grok, está ofreciendo ahora un 'modo picante' que muestra contenido sexual explícito, con algunas salidas generadas que incluyen imágenes de apariencia infantil. Esto no es 'picante'. Es ilegal. Es espantoso. Es repugnante. Así es como lo vemos, y esto no tiene cabida en Europa", ha declarado este viernes un portavoz de la Comisión Europea.

Bruselas ha ordenado a X que retenga todos los documentos y datos internos relacionados con Grok hasta finales de 2026, aunque todavía no ha abierto una comunicación oficial. También se ha descartado una posible prohibición de Grok.

"No estamos aquí para prohibir plataformas. No estamos aquí para decirles a los ciudadanos qué plataforma es más segura o qué herramienta de IA es mejor. Nuestro objetivo es obligar a cada plataforma a poner su propia casa en orden. Es responsabilidad de X encargarse de Grok y asegurarse de que no genere ese tipo de contenido", ha continuado el portavoz de la Comisión Europea.

Al movimiento de la UE se suman otros como el de Francia y Reino Unido, que han llevado el caso ante la justicia. En España, la ministra de Juventud e Infancia, Sira Rego, remitió un escrito a la Fiscalía para solicitar que investigue a Grok por presuntos delitos de difusión de material de violencia sexual contra la infancia.

Los juristas consultados dudan de que el escándalo vaya a salirle gratis a Elon Musk. "Estoy prácticamente seguro de que les van a abrir un expediente", avanza Borja Adsuara, abogado especializado en derechos digitales, que explica que las leyes europeas establecen que las redes sociales "tienen que suprimir el ilícito en cuanto son conscientes de él".

El propio Musk, con su mofa autopublicando una imagen falsa que le mostraba en bikini, reconoció ser consciente del escándalo y estar ignorándolo. En su debe, detalla Adsuara, está el "haber permitido que se difunda, con independencia de qué o quién lo haya hecho". "Esto es lo que despista a la gente. No es una cuestión de bikini o burka, sino de consentimiento", "tú tienes derecho a que otros no manipulen tu imagen".

El abogado se refiere así a una reacción que ha existido en X a raíz de la polémica. Creadoras de contenido de OnlyFans aprovecharon toda la atención que estaba generando la situación para pedirle a Grok que las desnudara en sus propias fotos y conseguir suscriptores. La reacción de una parte de los usuarios fue solicitar a la IA que las mostrara con un burka.

La generación de imágenes de mujeres en bikini o lencería mediante inteligencia artificial se mueve, en todo caso, en un vacío legal. Los juristas consultados dudan que suponga un delito por si mismo, si no va acompañado de una campaña de acoso. Esto cambia si las víctimas son menores. En España el Código Penal incluye tanto la generación de imágenes "reales" como las "realistas". El proyecto de ley de protección de menores en entornos digitales, que se encuentra en trámite en el Congreso, incluye una disposición para extender una protección similar a los adultos.

elDiario.es ha contactado con X y xAI para incluir su posición en esta información. La segunda, la desarrolladora original de Grok, no ha contestado al requerimiento. Una portavoz de la red social, por su parte, ha remitido el mismo comunicado que la cuenta oficial de la empresa publicó la semana pasada: "Tomamos medidas contra el contenido ilegal en X, incluido el material de abuso sexual infantil, eliminándolo, suspendiendo cuentas de forma permanente y trabajando con los gobiernos locales y las fuerzas del orden según sea necesario. Cualquiera que utilice o incite a Grok a crear contenido ilegal sufrirá las mismas consecuencias que si subiera contenido ilegal".

El canal de denuncia prioritaria para las víctimas

Las víctimas de este tipo de ataques tienen diferentes cauces para denunciar lo sucedido, explica la abogada especialista en privacidad Elena Gil. Uno de ellos, no siempre conocido, es el Canal Prioritario de la Agencia Española de Protección de Datos (AEPD). "Ellos tienen mecanismos de comunicación urgente con las redes sociales para retirar el contenido en horas sin que tú tengas que pegarte directamente con una gran plataforma. Este diría que es el mayor mitigante del daño, que en la mayoría de ocasiones es reputacional", señala.

Esta herramienta se puede activar para frenar la difusión de ataques sexuales, pero también de violencia o vejaciones en las que se vean involucrados menores. Es gratuito. El proceso activa también la investigación de la AEPD, que podría sancionar al responsable de los hechos si puede identificarlo. Sus multas, no obstante, son administrativas, no indemnizatorias.

"El Canal Prioritario es el mecanismo que iría primero, para que el contenido deje de estar ahí. Luego, si se quiere ir contra la propia persona, ahí es donde entra la denuncia ante la Policía", desglosa Gil. La abogada avisa, eso sí, que el procedimiento jurídico es largo y "puede llevar años". "Si realmente te han provocado un daño, pues desde luego puedes tener una indemnización, y pedir una multa para la persona autora. Pero eso sirve de poco si la foto sigue colgada en redes, que es lo que normalmente te provoca el daño", insiste.

Más allá del impacto emocional inmediato, este tipo de ataques provoca un daño reputacional en las víctimas, como señala Gil. La manipulación de una imagen para mostrar a alguien en ropa interior o en una situación sexualizada altera la percepción pública de esa persona y la expone a juicios, burlas o acoso. Al difundirse de forma pública en una red social, el contenido pasa a formar parte de la huella digital de la víctima, afectando a su vida personal, profesional y social.

Recientemente, la política de Irlanda del Norte Cara Hunter ha revelado que un deepfake porno de contenido sexual difundido en 2022 sigue afectando a su vida personal. "Ahora hay chicas que me llaman para decirme que les ha pasado lo mismo y que les ha arruinado la vida. Una joven me contó hace poco que le había pasado a ella y a otras 14 personas, todas menores de 18", ha relatado Hunter.

La actriz española Sara Sálamo, una de las afectadas, se ha posicionado en el mismo sentido. "Durante años he dicho que he rechazado papeles porque hay personas que cogen secuencias de mis pelis de ficción, las sacan de contexto y las suben a páginas porno. Eso ya era violencia. Lo dije como actriz, pero sobre todo como madre. Porque no es abstracto: son mis hijos, su colegio, lo que oyen, lo que cargarán en unos años... Ahora resulta que ni siquiera dejando de trabajar basta. Porque con una IA y cero escrúpulos pueden volver a sexualizarte sin tu consentimiento".

Tensión por el control de las plataformas

Hace solo un mes la Comisión Europea multó a X con 120 millones de euros por incumplir sus obligaciones de transparencia de acuerdo a la ley de servicios digitales. Ha sido la primera multa europea contra la plataforma de Musk por violar la legislación comunitaria. La sanción provocó incluso un comentario del presidente estadounidense, Donald Trump, que la calificó de "desagradable" y avisó de que Europa "va en mala dirección".

En un intento por tratar de rebajar las tensiones con EEUU, la Comisión rebajó la normativa de la Inteligencia Artificial. Las prácticas de alto riesgo de la IA, como la creación de contenidos manipulados, tendrán una moratoria de 16 meses para que las empresas puedan adaptarse a las nuevas exigencias. Las ONG calificaron la nueva regulación como "el mayor retroceso de los derechos digitales fundamentales en la historia de la UE".

Pero este paso no evitó la represalia de la Administración Trump, que en un primer momento amenazó con multar a empresas europeas, aunque no cuenta con legislación para ello, y posteriormente impuso la prohibición de viajar a EEUU a ciudadanos europeos que han destacado por su posición contra el discurso de odio en internet.

Con el apoyo legislativo de la DSA y la DMA, Bruselas sancionó a Apple y Meta con 500 y 200 millones de euros por vulnerar leyes digitales, además multó con 2.950 millones a Google por prácticas abusivas con la publicidad digital y le abrió una investigación por manipular los resultados de búsqueda de medios de comunicación, y también está haciendo indagaciones sobre Microsoft y Amazon por su posición de mercado de servicios en la nube, entre otras sanciones.

El Gobierno de Trump no ha parado de amenazar con que "si la UE y sus Estados miembros insisten en seguir restringiendo, limitando y desalentando la competitividad de los proveedores de servicios estadounidenses mediante medidas discriminatorias, Estados Unidos no tendrá más remedio que empezar a utilizar todos los instrumentos a su disposición para contrarrestar medidas irrazonables".

Mientras, la Comisión Europea se defiende al recordar que "la UE es un mercado único abierto y basado en reglas, con el derecho soberano de regular la actividad económica de acuerdo con nuestros valores democráticos y compromisos internacionales". Las espadas siguen el alto.

Tres años de ChatGPT: la máquina que no pudo quitarte el trabajo ahora va a por tus secretos

Sam Altman, para quien la publicidad era “el último recurso” de OpenAI, abre la puerta a insertar anuncios en ChatGPT basados en los datos personales de los usuarios ante los problemas con el negocio corporativo

— OpenAI se ha comprometido a gastar 1,3 billones en IA sin tener beneficios: ¿de dónde saldrá el dinero?

Carlos del Castillo

SEGUIR AL AUTOR/A

29 de noviembre de 2025
22:17 h
Actualizado el
30/11/2025 14:08 h
44

Hace tres años, el mundo contuvo la respiración. Una compañía que entonces pocos conocían fuera de los círculos especializados, OpenAI, lanzó un producto que podía pasar el test de Turing, la prueba que hasta entonces definía la inteligencia de una máquina: sin tener otras referencias, era casi imposible distinguir si el que estaba contestando era un humano o ChatGPT.

"De hecho, si crees que es una persona, la impresión que te llevas es que es la persona más culta que conoces", recuerda Enrique Dans, profesor de Innovación y Tecnología en IE Business School. Muchos marcaron aquel 30 de noviembre de 2022 como el principio de una nueva era. La revolución tecnológica de la inteligencia artificial parecía a punto de desbordarse. ChatGPT se convirtió en la herramienta digital de más rápida adopción de la historia, todo el mundo quería hablar con el futuro. "Fue el máximo exponente de viralidad que hemos conocido", enfatiza Dans.

OpenAI y su líder, Sam Altman, aprovecharon la situación para colocarse en el centro de todas las conversaciones. Una posición de privilegio que la ha convertido en "la empresa privada más valiosa del mundo, por encima de los 500.000 millones de dólares", explica Karen Hao, autora de *El Imperio de la IA. Sam Altman y su carrera por dominar el mundo*

(Península). Pero también en "una empresa llena de secretos y que ha cambiado mucho desde entonces", prosigue.

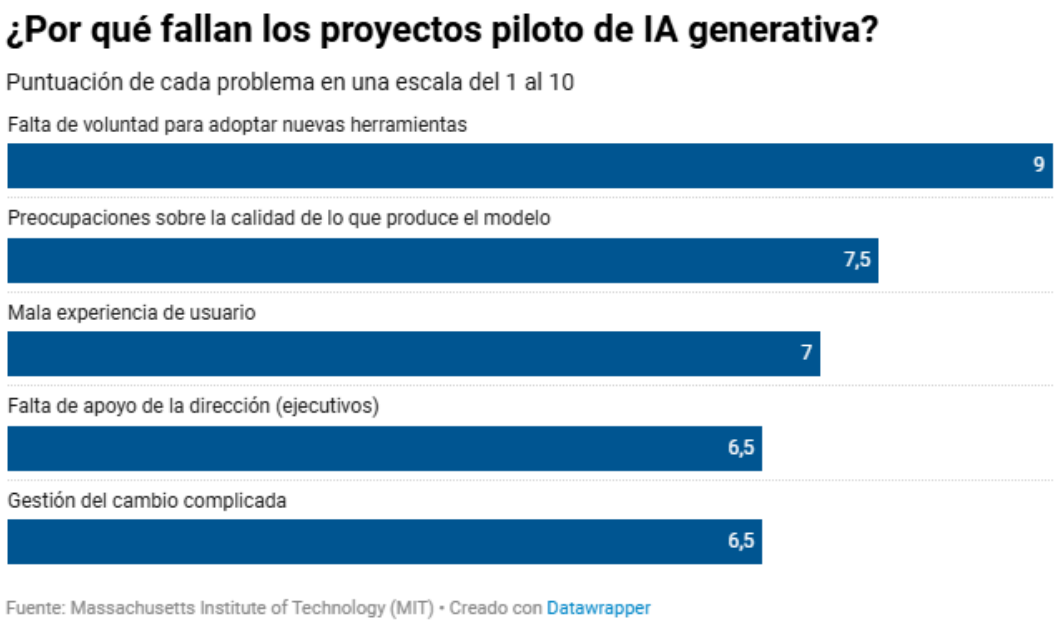
En estos más de 1.000 días las emociones del resto del mundo sobre ChatGPT y OpenAI también han cambiado. Del asombro inicial, la sociedad transitó a la ansiedad por el reemplazo laboral que la máquina podía llevar a cabo y el profundo impacto que esto tendría en las economías y la vida de la gente. Un extremo sobre el que ahora existen grandes dudas. "Estamos muy lejos de poder sacar al humano del bucle de trabajo. No va a ser la purga. La IA seguirá necesitando un trabajo de supervisión", expone Dans.

"Parece hecho con ChatGPT"

ChatGPT ya está en lo más profundo de nuestro imaginario colectivo. Pero no como amenaza existencial, sino como sinónimo de algo que parece bueno en la forma, pero en realidad está vacío de contenido. La inteligencia artificial generativa no puede crear conocimiento original por sí misma. Hablando con ella, las personas hemos descubierto que tenemos un sentido especial para detectar esto que añade un sentido más profundo al antiguo test de Turing.

Es una sensación que, cuando se traslada a la economía, se puede medir. "La gran mayoría de implementaciones corporativas está arrojando una satisfacción bastante baja", adelanta el profesor de la IE Business School.

La conclusión está aflorando en estudios e iniciativas privadas. Un informe del MIT (Massachusetts Institute of Technology) publicado en julio analizó más de 300 proyectos piloto basados en inteligencia artificial generativa, junto con iniciativas lanzadas en 52 empresas y entrevistas a 153 altos ejecutivos de todo el mundo. Sus resultados fueron que el 95% de las organizaciones no están obteniendo ningún tipo de retorno por su inversión.



Otras grandes voces habían avisado antes de ello. Daron Acemoglu, Premio Nobel de Economía en 2024, ha publicado varios análisis al respecto. Su valoración más reciente, de este 2025, estima que la IA apenas mejorará la productividad global en torno al 0,7% en la próxima década. En cuanto al empleo, calcula que menos del 5% de los trabajos en países desarrollados se verán realmente afectados.

Pese a que la cifra sea pequeña, podría equivaler a centenares de miles de despidos en el mundo. Un proceso que ya se está notando en tecnológicas como Amazon, Meta o HP. Pero lejos de la revolución industrial que muchos esperaban. "Hay mucho entusiasmo por la IA y no hay duda de que estos modelos están haciendo cosas que la gente pensaba que serían imposibles hace 10 años. Es un gran logro, impresionante en muchos sentidos. Pero cuando se analizan los datos, la mayoría de las cosas que hacen los humanos estos modelos aún no pueden hacerlas", explicaba Acemoglu en una entrevista.

> ***"La IA es un gran logro, impresionante en muchos sentidos. Pero cuando se analizan los datos, la mayoría de las cosas que hacen los humanos, estos modelos aún no pueden hacerlas"***
> Daron Acemoglu - Premio Nobel de Economía en 2024

"En 50 años, todo es posible, no sabemos qué será posible y qué no con la IA. Pero para los próximos 10 años, sabemos más o menos lo que las tecnologías serán capaces de hacer porque ya tenemos los prototipos y están evolucionando a un ritmo determinado", continuaba.

Esto está haciendo que la IA entre en lo que Gartner llama "el abismo de la desilusión". La consultora recoge que los ejecutivos que han apostado por la IA están teniendo problemas para demostrar el valor de la inteligencia artificial generativa para el negocio. "A pesar de un gasto medio de 1,9 millones de dólares en iniciativas de IA generativa en 2024, menos del 30% de los responsables de IA afirman que sus directores generales están satisfechos con el rendimiento de la inversión".

Ese "abismo de la desilusión" supone un punto de inflexión. Es el momento en el que inversores y altos ejecutivos dejan a un lado su entusiasmo inicial con la tecnología y empiezan a promover la "construcción responsable de innovaciones funcionales", explica Gartner. Es decir, dejan de imaginar castillos en el aire y empiezan a analizar qué es lo que se puede hacer con ella para generar beneficios.

La trampa de la privacidad

Los problemas de las compañías para encontrar utilidades sólidas para ChatGPT y la IA generativa contrastan con el uso que millones de personas hacen de ella en su día a día. En lo personal, la adopción ha seguido otro camino: menos hollywoodiense, pero más real. La gente ha descubierto que la herramienta funciona especialmente bien como copiloto para lo cotidiano: desde planificar rutinas a ordenar ideas, pasando por su uso como motor de aprendizaje o trampolín para la curiosidad.

Los casos de éxito son numerosos y diversos. Claudia, estudiante de Medicina, confiesa que ChatGPT le ha permitido entender conceptos que en clase se le resisten: "Es como tener un profesor disponible las 24 horas que adapta las explicaciones a tu nivel". Carlos,

desarrollador en una startup madrileña, reconoce que su productividad ha aumentado: "No escribe el código por mí, pero me ayuda a detectar errores y a explorar soluciones que yo solo no habría considerado". Pero hay algo más: "En general le pregunto de todo, o voy hablando con él mientras paseo al perro".

Todas esas automatizaciones que no están terminando de encajar en lo empresarial se han asumido con naturalidad en la vida privada, donde las personas sí han sabido extraerle un gran valor. El historial de Google es cosa del pasado: ahora se puede saber mucho más de una persona accediendo a sus conversaciones con ChatGPT.

Y es aquí donde los expertos avisan de que nos estamos acercando a una frontera peligrosa. "Inicialmente, la gente pensaba que era más como una herramienta de búsqueda", explica Karen Hao. "Pero hemos visto una tendencia últimamente en la que mucha gente considera a ChatGPT como una especie de terapeuta, un mentor o incluso un amante". Usuarios que están desarrollando una dependencia emocional del chatbot, que no rehúsa conversaciones ni siquiera sobre el suicidio.

> ***"OpenAI está generando espacios y superficies en los que puedes meter anuncios y creo que eso les llevará al 100% a utilizar los datos de los usuarios"***
> Karen Hao - autora de 'El Imperio de la IA. Sam Altman y su carrera por dominar el mundo'

Esta situación, unida a las dificultades para extraer rentabilidad a partir del modelo de suscripción, podría convertirse en el preludio de un negocio familiar: la publicidad basada en el conocimiento profundo del usuario. "Vemos que OpenAI está ahí presente. Están generando espacios y superficies en los que puedes meter anuncios y creo que eso les llevará al 100% a utilizar los datos de los usuarios para ver cómo llevar a cabo esos anuncios", advierte Hao.

La autora de El imperio de la IA se refiere a Sora, la nueva red social de OpenAI en la que todo el contenido es sintético; a la herramienta que permite llevar a cabo compras directamente a través de ChatGPT cuando se pregunta por un producto en concreto; o al navegador que han desarrollado. Iniciativas que recuerdan mucho a las aplicaciones de Meta y de Google, las dos grandes multinacionales de la extracción de datos para la publicidad online.

Además, no es que OpenAI no haya hecho esto antes. "Técnicamente, ya están haciendo dinero con los datos de las personas, utilizándolos para entrenar las siguientes generaciones de sus modelos. Y esos modelos los venden con suscripciones", recuerda Hao. La empresa tampoco tuvo reparos en saltarse el copyright de infinidad de obras protegidas para que ChatGPT pudiera seguir mejorando.

> **"Estamos montando otro complejo industrial como el de las redes sociales, pero peor aún"**
> Enrique Dans - profesor de Innovación y Tecnología en IE Business School

"Observando lo que están haciendo, todo apunta a que de lo que estamos hablando aquí es de reproducir todo lo que hicimos mal con las redes sociales", coincide Enrique Dans.

"¿Qué son las redes sociales en realidad? Son máquinas de capturar datos para luego venderlos al mejor postor. ¿Qué pasa si en lugar de simplemente dar *me gusta* o poner un comentario, lo que haces es estar todo el día hablando con esa máquina? Pues que le das todos los datos del mundo".

El riesgo, según el experto, es que estamos "montando otro complejo industrial como el de las redes sociales, pero peor aún", donde la tecnología no solo registra lo que hacemos, sino que procesa lo que pensamos y sentimos en tiempo real.

El giro de Altman: "Me encantan los anuncios de Instagram"

OpenAI se ha comprometido a gastar 1,3 billones de dólares (1.300.000.000.000) hasta 2030 para conseguir más capacidad de computación para seguir mejorando ChatGPT. En agosto, su directora financiera reveló que habían conseguido sobrepasar por primera vez los 1.000 millones de dólares de ingresos en un mes. La masiva diferencia entre ambas cifras y los problemas de la IA generativa en el entorno empresarial es lo que empuja a los expertos a pensar que OpenAI girará hacia el negocio de los datos personales.

OpenAI no ha contestado a la solicitud de información enviada por elDiario.es sobre estas cuestiones. No obstante, Altman ya ha abierto la puerta a los anuncios este 2025. El ejecutivo ha dado un giro de 180º en apenas un año. Esto es lo que decía Altman en mayo de 2024: "Odio los anuncios"; "la publicidad sería el último recurso para nosotros"; "la combinación de anuncios con IA me resulta especialmente inquietante".

Y este es Altman en noviembre de 2025: "Hay muchas cosas que respeto del negocio de Meta", "Me encantan los anuncios de Instagram, me han aportado valor", "probablemente exista algún producto publicitario interesante que podamos desarrollar y que sea beneficioso para el usuario" o "hay anuncios que creo que serían muy buenos o bastante buenos. Espero que lo intentemos en algún momento".

Es posible que no sea una contradicción y que ChatGPT esté ya, tan solo tres años después de salir a la luz, en territorio de explorar ese "último recurso". Es la otra característica de lo viral: caduca rápido. En poco más de 1.000 días, la herramienta que llegaba del futuro ha pasado a coquetear con el modelo de negocio más viejo de Internet. Ahora sabemos que el futuro tiene un precio, y podría ser otra vez nuestra privacidad.

BLOQUE 2

Actualidad y Servicio Público: Alertas tempranas, sanciones y defensa ciudadana ante los riesgos tecnológicos

Sub-bloque A: biometría y vigilancia

Multa de 10 millones a Aena por hacer reconocimiento facial a los pasajeros “sin justificar su necesidad”

Protección de Datos suspende el tratamiento biométrico en los aeropuertos al constatar que el gestor aeroportuario creó una base de datos centralizada para identificar viajeros cuando existían alternativas menos intrusivas

— Un alcalde monta su 'Gran Hermano' en Mallorca: más de 50 cámaras en un pueblo para controlar hasta los bares

Carlos del Castillo

SEGUIR AL AUTOR/A

25 de noviembre de 2025
17:59 h
Actualizado el
26/11/2025 09:28 h
2

Proyecto de Aena para facturar con reconocimiento facial en los aeropuertos, uno de los sistemas de inteligencia artificial calificados de "alto riesgo" por la UE. EFE

La Agencia Española de Protección de Datos (AEPD) ha impuesto una sanción de 10.043.002 euros a Aena por su sistema de reconocimiento facial en los aeropuertos españoles. El regulador ha ordenado además la suspensión temporal de todo tratamiento de datos biométricos por parte del gestor aeroportuario, al concluir que implementó una tecnología de alto riesgo para los derechos de los ciudadanos sin justificar que fuera realmente necesaria ni proporcional para el fin perseguido, que era agilizar el embarque.

La resolución carga contra la premisa de que la "experiencia de usuario" justifica cualquier despliegue tecnológico. La AEPD considera que Aena recopiló y almacenó datos biométricos de más de 62.000 pasajeros de forma centralizada sin haber realizado una Evaluación de Impacto válida, un requisito obligatorio para desplegar este tipo de tecnologías invasivas.

El organismo que dirige Lorenzo Cotino califica la falta de diligencia de la empresa pública como "grave". Según el expediente, Aena era consciente de que su programa de reconocimiento facial implicaba un tratamiento de categoría especial y alto riesgo. Sin embargo, la compañía siguió adelante con el despliegue a pesar de haber recibido dos informes desfavorables previos de la propia Agencia durante la fase de consulta.

Vigilancia centralizada

El núcleo de la infracción no es el uso de la biometría, sino cómo se diseñó la arquitectura del sistema. Aena optó por un modelo de "identificación biométrica uno-a-varios" con almacenamiento centralizado. En términos técnicos, esto significa que la cara del pasajero no se coteja únicamente contra su documentación en el momento del paso del control, sino que se almacena en una base de datos central controlada por Aena.

La AEPD determina que este enfoque vulnera las leyes de privacidad, que estipulan que el tratamiento de datos debe ajustarse al mínimo imprescindible. El organismo regulador estipula que existían alternativas mucho menos intrusivas para lograr el mismo objetivo de seguridad y fluidez, como la autenticación biométrica local o, simplemente, el sistema tradicional de comprobación visual humana que ha funcionado durante décadas.

La resolución afirma que el nuevo sistema implicaba "almacenar muchos más datos personales" (incluyendo detalles de la tarjeta de embarque y la identidad del viajero) en los servidores de Aena durante un periodo de hasta dos años. Unas bases de datos que, para la AEPD, no eran necesarias con los métodos tradicionales ni con arquitecturas biométricas más respetuosas con la privacidad.

Aena recurrirá: "Es una cuestión formal"

Aena ha anunciado que recurrirá la sanción ante los tribunales, expresando su "respetuosa discrepancia" con ella. En un comunicado emitido tras conocerse la multa, la empresa defiende que la sanción se basa en una "supuesta infracción de una obligación formal", refiriéndose a las deficiencias señaladas en su Evaluación de Impacto.

El gestor aeroportuario sostiene que los pasajeros prestaron su consentimiento "voluntariamente" e informado para acceder al embarque biométrico. Sin embargo, en el ámbito de la protección de datos, el consentimiento "no valida" un tratamiento si este es "desproporcionado o innecesario desde su diseño", le recuerda la AEPD.

Aena también ha querido recalcar que la seguridad de los datos nunca estuvo comprometida: "No se ha producido ninguna brecha de seguridad y, por tanto, no ha habido ninguna filtración de datos de los usuarios". La compañía argumenta que su único objetivo era "proporcionar a los pasajeros una mejor experiencia" y asegura que trabajará para reiniciar el programa "tan pronto como sea posible".

Suspensión inmediata

Hasta que Aena no demuestre que puede gestionar estos datos cumpliendo estrictamente con el Reglamento General de Protección de Datos (RGPD), el reconocimiento facial se

queda en tierra. La suspensión dictada por la AEPD se mantendrá hasta que la empresa realice una evaluación de riesgos que contemple realmente los peligros para los derechos y libertades de los viajeros.

Esta medida correctiva no afectará a la operativa de los vuelos, ya que el sistema biométrico convivía con los controles documentales tradicionales, que seguirán operando como hasta ahora.

La multa a Aena se suma a una tendencia creciente de los reguladores europeos de poner coto al uso indiscriminado de la biometría en espacios públicos, donde a menudo se prioriza la eficiencia operativa o comercial por encima de la privacidad de los ciudadanos. Al tratarse de una infracción muy grave cometida por una gran empresa —con un volumen de negocio superior a los 5.000 millones de euros—, la cuantía de la sanción se ha graduado acorde a la magnitud de la entidad y el número de afectados.

WORLDCOIN

La empresa que escaneaba el iris a cambio de criptomonedas deberá borrar todos los datos recopilados

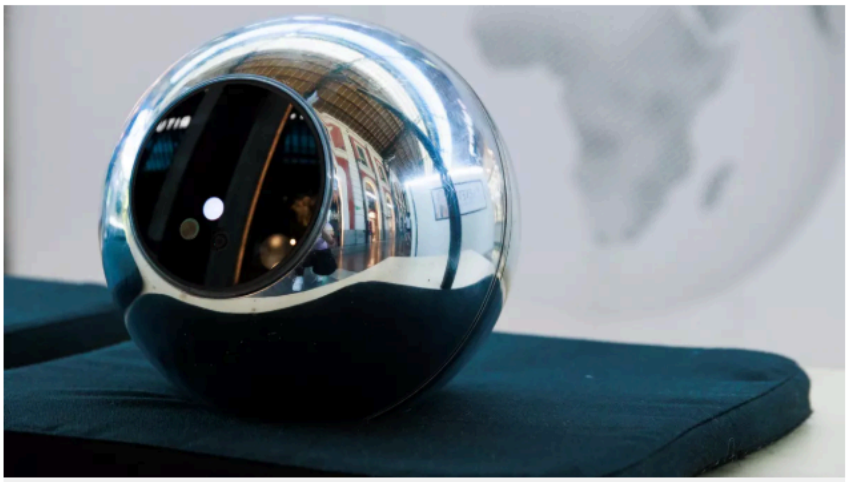
Las autoridades de protección de datos invalidan el proceso de recolección de iris de Worldcoin, que registró a unos 400.000 españoles

— Protección de Datos ordena paralizar "de urgencia" el proyecto Worldcoin, que escanea el iris a cambio de criptomonedas

Carlos del Castillo

SEGUIR AL AUTOR/A

19 de diciembre de 2024
17:42 h
Actualizado el
19/12/2024 19:15 h
4



Escáner de iris de Worldcoin. Patricia J. Garcinuño

Duro golpe a la iniciativa Worldcoin en Europa, renombrada como "World" en octubre. La empresa, que aspira a crear un pasaporte de identidad digital a través del escaneo de datos del iris, deberá borrar todos los códigos asociados a ciudadanos europeos que almacena en sus sistemas desde el inicio del proyecto. Así lo ha ordenado la autoridad de protección de datos de Baviera (Alemania), después de investigar las actividades de la compañía y resolver que su estrategia de regalar criptomonedas a cambio de los datos del iris de los ciudadanos viola varios artículos de la normativa de privacidad europea.

En España la actividad de World estaba suspendida desde marzo, cuando la Agencia de Protección de Datos (AEPD) ordenó paralizar "de urgencia" los escaneos de iris ante las sospechas de que la compañía estaba realizándolo en menores de edad y otros "indicios de graves incumplimientos" de las leyes de privacidad. La empresa recurrió la decisión ante la Audiencia Nacional, pero su recurso fue rechazado.

Hasta su veto cautelar, España era uno de los países donde esta iniciativa había tenido más éxito. Unos 400.000 españoles aceptaron escanear su iris a cambio de criptomonedas y se sumaron al proyecto, cuyo objetivo último, según sus responsables, es crear un sistema capaz de diferenciar a los humanos de las inteligencias artificiales en Internet.

Los datos del iris son los más últiles para este propósito, según explicó el responsable de World en Europa en una entrevista con elDiario.es. Para recogerlos diseñó un escáner portátil desde cero a la que denominó "orbe", del tamaño de un balón de fútbol sala. Uno de los principales impulsores de toda la iniciativa es Sam Altman, el director ejecutivo de OpenAI, desarrolladora de ChatGPT.

La empresa tuvo tanto éxito en España debido a que fue uno de los países que escogió para probar su fase piloto. Su método era establecer puestos en centros comerciales y estaciones, donde captadores interceptaban a ciudadanos para informarles del proyecto y ofrecerles criptomonedas a cambio de su iris.

La resolución de la autoridad de Baviera, responsable de la investigación al estar la sede europea de World y que ha colaborado con la AEPD durante el proceso, "ordena la eliminación de todos los códigos de iris almacenados desde el inicio del proyecto, almacenados sin las medidas de seguridad necesarias para el tratamiento de los datos biométricos", destaca el regulador español en un comunicado. A su vez, ordena que la recolección de iris futura se haga con "consentimiento explícito del interesado".

"Asimismo, en la resolución se constata que la empresa no implantó las medidas adecuadas para impedir el tratamiento de datos de menores, lo que será objeto de una investigación adicional posterior", continúa la AEPD.

Fuentes de Word han afirmado a elDiario.es que la empresa ya eliminó lo códigos de iris antiguos el pasado mes de mayo adelantándose a una posible resolución desfavorable y cambiaron su tecnología de recolección de iris, por lo que destacan que la resolución se refiere a prácticas "ya obsoletas". La inicitiva destaca que sus nuevos sistemas aseguran que los datos personales, incluidos los códigos de iris, ya no se almacenan centralmente y solo residen en los dispositivos de los usuarios.

World ha apelado la decisión de la autoridad de Baviera para buscar claridad judicial sobre si sus Tecnologías de Mejora de la Privacidad (PETs) cumplen con la definición legal de anonimización en la UE, argumentando que la falta de un estándar claro sobre anonimización en la legislación europea dificulta el desarrollo de sistemas que preserven la privacidad. Mientras tanto, World continuará operando en la UE y planea expandirse a más mercados europeos en 2025.

La empresa de análisis genéticos 23andMe se declara en quiebra y pone en duda los datos de ADN de 15 millones de personas

La compañía busca comprador para sus activos, entre ellos las bases de datos con información genética de sus clientes

Hemeroteca — Un ciberataque a una firma de análisis de ADN filtra millones de datos genéticos de judíos asquenazíes

Carlos del Castillo

SEGUIR AL AUTOR/A

24 de marzo de 2025
11:44 h
Actualizado el
24/03/2025 15:30 h
3

Uno de los paquetes para hacerse pruebas de ADN que 23andMe enviaba a sus clientes

La empresa de análisis genéticos 23andMe se ha declarado en quiebra tras años de dificultades económicas. La compañía fundada en 2006 llegó a estar valorada en más de 6.000 millones de dólares tras su salida a bolsa en 2021, pero su incapacidad de lograr beneficios y establecer un modelo de negocio rentable la ha abocado a la bancarrota. Su directora ejecutiva ha dimitido este lunes y la empresa afrontará ahora un proceso de venta de sus activos bajo supervisión judicial, durante el que se ha comprometido a mantener su actividad comercial.

"A través de este proceso, buscaremos un socio que comparta nuestro compromiso con la privacidad de los datos de nuestros clientes y que nos permita continuar con nuestra misión de ayudar a las personas a acceder, comprender y beneficiarse del genoma humano. Es importante destacar que este paso nos permite continuar operando nuestro negocio

mientras trazamos el camino a seguir", ha afirmado 23andMe en una carta enviada a sus clientes, en la que recalca que estos mantendrán el acceso a su información por el momento y que esta seguirá protegida.

23andMe fue la lanzadora de un nuevo sector de empresas digitales que ofrecen pruebas de ADN a precios moderados. El cliente debía tomar una muestra de su saliva con un bastoncillo y enviarla a los laboratorios de la empresa. Con esta información, esta preparaba un informe de los lugares de origen de sus ancestros y arrojaba luz sobre su árbol genealógico. También conectaba a los usuarios con sus familiares lejanos que con su ADN registrado en 23andMe.

> ***"La privacidad de los datos será un factor importante en cualquier posible transacción"***
> 23andMe

El servicio nunca estuvo exento de críticas. Al principio, centradas en la rigurosidad científica de marcar "lugares de origen" de determinadas líneas de ADN. Sin embargo, estas se tornaron de mayor calado cuando 23andMe comenzó a ofrecer previsiones sobre posibles enfermedades hereditarias de los usuarios y varió el foco de su negocio hacia la salud. A partir del análisis casero de la saliva, la empresa incluía un informe médico que anticipaba su predisposición a sufrir cáncer o alzhéimer. Finalmente, la Administración de Alimentos y Medicamentos de EEUU le prohibió hacer este tipo de informes y a dejar claro que no tenían validez científica.

La duda que siembra el proceso de quiebra es el futuro de los datos genéticos de los más de 15 millones de personas que se hicieron análisis con 23andMe. Aunque la compañía asegura que busca "un socio" y que mantendrá su servicio, es el hecho de no haber encontrado ese aliado estratégico lo que la ha abocado a la quiebra. "Tras una evaluación exhaustiva de las alternativas estratégicas, hemos determinado que un proceso de venta bajo supervisión judicial es la mejor opción para maximizar el valor del negocio", ha declarado Mark Jensen, presidente y miembro la junta directiva en otro comunicado.

"Esperamos que este proceso impulse nuestros esfuerzos para abordar los desafíos operativos y financieros que enfrentamos, incluyendo mayores reducciones de costos y la resolución de responsabilidades legales y de arrendamiento", ha añadido Jensen. "Nos comprometemos a seguir protegiendo los datos de los clientes y a ser transparentes en la gestión de los datos de los usuarios en el futuro. La privacidad de los datos será un factor importante en cualquier posible transacción", ha aseverado.

La seguridad de datos tan sensibles como el ADN y la conveniencia de que estos se almacenen en bases de datos privadas como la de 23andMe ya quedó en duda en 2023, cuando un ciberataque logró robar información de siete millones de usuarios del servicio. En aquella ocasión, los atacantes buscaron los lazos familiares de judíos asquenazíes, aunque su objetivo nunca quedó claro. Más tarde, sacaron a la venta los datos robados en la *dark web*. 23andMe pagó 30 millones de dólares el pasado septiembre a los afectados para cerrar la demanda que interpusieron contra ella.

Llegan las multas por seguir utilizando la huella dactilar para el control horario

Protección de Datos sanciona con 20.000 euros al Colegio Notarial de Aragón por mantener el uso de datos biométricos a pesar de su prohibición

Hemeroteca — Protección de Datos cambia de criterio y deja en el alambre a las empresas que usan huella dactilar o reconocimiento facial

Carlos del Castillo

SEGUIR AL AUTOR/A

13 de diciembre de 2024
21:57 h
Actualizado el
14/12/2024 05:30 h
2

Una persona usa un sistema de identificación por huella dactilar. Pexels

A finales del 2023 un cambio de criterio en los reguladores de protección de datos europeos ponía a las empresas e instituciones sobre aviso. El uso de datos biométricos (aquellos relacionados con el cuerpo humano, como la cara, el iris o la huella dactilar) para realizar el control horario de los trabajadores pasó a ser considerado excesivo, ya que son considerados de "alto riesgo". Las diferentes organizaciones, por tanto, debían dejar de utilizar sistemas de lectura de huella dactilar o reconocimiento facial con este fin.

Un año después, las multas comienzan a llegar a aquellos que no han hecho la transición. La Agencia Española de Protección de Datos (AEPD) ha impuesto una sanción de 20.000 euros al Colegio Notarial de Aragón por seguir utilizando un sistema de lectura de huella dactilar para realizar el fichaje, tras una reclamación interpuesta por uno de sus empleados.

El Colegio argumentó que el sistema biométrico era necesario para "asegurar y minimizar los riesgos de seguridad, objetividad y fiabilidad en el registro horario de sus empleados". Según el organismo, el sistema anterior de registro manual en papel no era objetivo ni fiable. Además, argumentó que como los miembros de su dirección trabajan en notarías privadas fuera de las instalaciones del Colegio, la lectura de la huella dactilar se hace especialmente necesaria.

"En el caso del Colegio Notarial se da la circunstancia de que la implantación del sistema de lectura de huella está especialmente justificada porque los miembros de la Junta Directiva del Colegio, compuesta por nueve Notarios, cumplen sus jornadas de trabajo, no en el Colegio, sino en sus propias Notarías situadas en cualquier población de la Comunidad Autónoma de Aragón, y por ello no pueden ejercer *in situ* las funciones legales de control laboral al no cumplir su jornada laboral en el mismo", aseguró en sus alegaciones.

Este motivo hacía que el Colegio hubiera priorizado la huella dactilar sobre otros sistemas menos intrusivos, como las tarjetas o códigos, ya que los consideran menos efectivos para la "identificación y autenticación unívoca de los usuarios". Teniendo en cuenta la situación, consideraron que se justificaba el uso de biometría, ya que "prevalecen en todo momento el derecho al control laboral sobre el de protección de datos".

Datos prohibidos

Una argumentación que la AEPD ha tumbado con rotundidad. El regulador de la privacidad ha recalcado a los notarios que para restringir un derecho fundamental como la protección de datos es necesario evaluar la "proporcionalidad", como zanjó una sentencia del Tribunal Constitucional del 2003. Esta no solo se mide en función de si consigue el objetivo propuesto, sino también "en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia".

La AEPD recuerda que los datos biométricos, incluyendo las huellas dactilares, son "categorías especiales de datos personales" que merecen un "nivel de protección especialmente elevado" por los riesgos que entraña que caigan en manos de ciberdelincuentes o se pierdan en una brecha de seguridad. Por tanto, en base a la nueva interpretación, su uso queda "prohibido" de manera general.

Solo en determinadas excepciones, como en ámbitos de salud pública, interés general de la ciudadanía o protección de intereses vitales, podrían levantar esa prohibición. Excepciones que deben interpretarse además de manera "restrictiva" y no encajan con la argumentación de los notarios y sus trabajos en espacios ajenos al Colegio de Aragón.

El regulador zanja la resolución destacando que la normativa laboral no exige el uso de datos biométricos para el control de la jornada, que el Colegio no demostró que usar la huella de sus trabajadores fuera necesario ni proporcionado, y que existían otros métodos, como diversos programas digitales, para llevar a cabo esa misión. Ese es el sistema que, además, implementaron los notarios al saberse investigados por la AEPD, sustituyendo al lector de huellas dactilares.

Una vez propuesta la sanción, el Colegio Notarial ha optado por aceptar la multa y acogerse a dos reducciones del 20% para rebajar su cuantía. Una por asunción de responsabilidad y otra por pagar la sanción durante el período ejecutivo, lo que finalmente la ha dejado en 12.000 euros. Una sanción que pone en aviso al resto de empresas y organizaciones que siguen usando biometría para el control de jornada o incluso para el acceso a sus instalaciones, algo que la AEPD también censuró tras su cambio de criterio de 2023.

Sub-bloque B: menores y redes sociales

Protección de Datos avisa que desnudar a otras personas con IA ya puede ser delito o acarrear multas con las leyes actuales

El regulador recuerda que la imagen de una persona se considera un dato personal y su manipulación y difusión sin consentimiento puede violar la normativa de privacidad

— Los 10 días de porno machista con IA que pueden costar caro a Elon Musk: "No es cuestión de bikini o burka, sino de consentimiento"

Carlos del Castillo

SEGUIR AL AUTOR/A

13 de enero de 2026
10:25 h
Actualizado el
13/01/2026 10:29 h
1

El Gobierno quiere incluir la generación de imágenes o vídeos falsos de otras personas con inteligencia artificial en el catálogo de delitos contra el honor. Estos contenidos, conocidos como deepfakes, están suscitando una considerable alarma social y protestas de las personas afectadas. Según los datos que maneja Naciones Unidas, "hasta el 95% de los deepfakes son imágenes pornográficas no consentidas, y el 99% de las víctimas son mujeres". El Consejo de Ministros aprobará este martes en primera vuelta el anteproyecto de ley con el que pretende poner coto a esta actividad.

La Agencia Española de Protección de Datos (AEPD) ha enviado un aviso este martes: manipular la imagen de otras personas con IA, especialmente si implica "desnudez añadida" o "contenido íntimo sintético", ya puede acarrear multas por violar las leyes de privacidad o incluso delitos recogidos en el Código Penal.

Así lo ha expresado en un documento que detalla los riesgos "visibles e invisibles" de los deepfakes. La Agencia recuerda que cualquier imagen, vídeo o audio que permita identificar a una persona, ya sea por su rostro, voz, tatuajes o entorno, constituye un dato personal. Por tanto, su tratamiento mediante IA está sujeto a la normativa de protección de datos con independencia del realismo del resultado.

El regulador de la privacidad, de hecho, ya ha dictado resoluciones sancionatorias por este tipo de actividades. Fue en noviembre cuando la Agencia impuso la primera sanción en este sentido. En aquel caso, la resolución condenó a los padres de un menor que había creado imágenes de sus compañeras de instituto desnudas con IA a pagar 2.000 euros por violación de su privacidad. Se trataba de una sanción derivada del escándalo de Almendralejo, en el que se compartieron fotografías falsificadas de niñas menores de edad en grupos de mensajería, y que salió a la luz en septiembre de 2023.

Con todo, esta actividad ha vuelto a disparar la indignación en estos primeros días de 2026 debido a la inteligencia artificial de Elon Musk. El magnate permitió que Grok, como se llama su modelo generativo, creara este tipo de contenidos falsificados (en este caso, mostrando a las mujeres en bikini o lencería) y los publicara en abierto en X, su red social. Múltiples países europeos y la propia UE ya investigan lo sucedido. "Es ilegal, espantoso y repugnante", declaró un portavoz comunitario.

Sexualización y humillación

En su guía de riesgos, la AEPD advierte de que el daño para la víctima de un deepfake "puede ser equivalente y en algunos casos mayor que en el caso de una imagen o un vídeo real". Especialmente, cuando se producen situaciones de sexualización, humillación o la atribución de hechos falsos que resultan socialmente creíbles.

Además de lo que otros pueden ver al difundirse el contenido, el regulador de privacidad pone el foco en los peligros ocultos para la privacidad de los deepfakes, como "la pérdida efectiva de control" sobre su propia imagen, que puede distribuirse fácilmente en redes donde los usuarios no conocen el contexto de si es real o no. Además, una vez que la imagen se sube a una de estas plataformas, se crea un archivo que se guardará en sus bases de datos y unos metadatos (información sobre esas imágenes, como autor, fecha, formato, ubicación, etc.) que podrían llevar a la identificación de la persona que aparece en el deepfake.

"Es cierto que muchas plataformas de IA generativa incorporan mecanismos técnicos para limitar la generación de contenidos claramente lesivos", reconoce la AEPD. "Estas medidas hacen que muchos contenidos notoriamente dañinos no lleguen a generarse, pero no garantizan que desaparezcan todos los riesgos", añade en la guía. Fuentes del organismo aseguran que este lleva semanas trabajando en el documento y que sus recomendaciones van más allá de lo sucedido con la IA de Elon Musk en X.

Ante esta realidad, la AEPD recomienda extremar la prudencia y recalca que el uso irreflexivo de estas herramientas para "usos considerados banales o lúdicos" (como filtros o animaciones) puede dejar de considerarse una actividad "estrictamente doméstica" si el contenido se difunde de forma masiva o impacta gravemente en la vida profesional o personal del afectado, lo que puede acarrear sanciones. En los casos más graves, pueden existir "indicios de delito" que hagan que el organismo derive el caso ante autoridades policiales y judiciales.

Finalmente, la Agencia subraya que el uso de esta tecnología es especialmente peligroso cuando se trata la imagen de menores de edad o personas vulnerables. En los supuestos

en los que se produzca una pérdida de control o un daño reputacional intenso, el organismo insta a los afectados a presentar una reclamación ante la Agencia, que cuenta con herramientas como el Canal Prioritario, una vía de urgencia que permite la retirada de determinados contenidos sexuales, violentos o vejatorios en 24 horas.

Multa de 2.000 euros a los padres de un menor que creó una imagen de una compañera desnuda con inteligencia artificial

La primera resolución de este tipo en España, derivada de un caso sucedido en Almendralejo, se centra en la responsabilidad de los progenitores

Hemeroteca — 'Deepfakes' sexuales: el caso de las menores de Almendralejo consolida una nueva forma de violencia machista

Carlos del Castillo

SEGUIR AL AUTOR/A

6 de noviembre de 2025
12:10 h
Actualizado el
06/11/2025 15:45 h
38

La Agencia Española de Protección de Datos (AEPD) ha multado con 2.000 euros a los padres de un menor de edad que usó una herramienta de inteligencia artificial para crear una imagen falsa de una de sus compañeras desnuda. Se trata de la primera resolución de este tipo que se impone en España y, aunque los datos presentes en la notificación pública están anonimizados, la Agencia ha confirmado que deriva de los hechos sucedidos en Almendralejo en 2023.

En septiembre de aquel año, varias menores de un instituto de la localidad pacense denunciaron que imágenes que las mostraban sin ropa estaban circulando en los teléfonos de sus compañeros de clase. Más tarde se conoció que estaban creadas con una app llamada ClothOff, basada en inteligencia artificial, actualmente cerrada y cuyos creadores se enfrentan a un proceso judicial en EEUU por un caso similar.

La herramienta se basa en la cara de la víctima para generar una imagen de ella sin ropa, teniendo en cuenta detalles como su complexión o tono de piel. Las familias de las menores denunciaron el gran realismo de las imágenes falsas. El caso español también avanzó por la vía penal, terminando en una condena de un año de libertad vigilada y un curso de formación para los acusados, que en el momento de los hechos tenían entre 12 y 14 años.

La resolución de la AEPD revela que la institución decidió investigar de oficio lo sucedido, a raíz de las publicaciones en medios de comunicación. "Los hechos consistían en la manipulación de imágenes con inteligencia artificial para asociar rostros reales de un grupo de personas a cuerpos desnudos que no les correspondían. Estas imágenes manipuladas fueron difundidas por sus autores a través de redes sociales, un grupo de mensajería, y, según la información publicada, también en portales de internet como *Only fans* y diversas páginas pornográficas", explica el organismo.

La AEPD pudo acceder a la identidad de los presuntos autores gracias a la información facilitada por la Fiscalía. Tras un análisis, el regulador decidió imponer la citada multa de 2.000 euros a los "progenitores y, por lo tanto, representantes legales" de uno de los menores implicados. Estos han optado por acogerse a las dos reducciones posibles para este tipo de sanciones, asunción de responsabilidad y pronto pago, de un 20% cada una. La cifra final de la multa ha sido, por tanto, de 1.200 euros.

El regulador de privacidad recuerda que la imagen de una persona es un dato personal y que los hechos se refieren a la difusión de imágenes manipuladas con IA de menores, que "cuentan con una protección reforzada en el ámbito de la protección de sus datos".

La AEPD, en cambio, no profundiza en esta resolución en la responsabilidad de los creadores de la aplicación ClothOff, dedicada específicamente a generar imágenes de mujeres desnudas sin su consentimiento. En el caso estadounidense, la víctima que ha llevado el caso a los tribunales cita expresamente lo sucedido en Almendralejo para justificar la afectación mundial que ha tenido esta herramienta.

En otra resolución por unos hechos posteriores a este, la AEPD se vio obligada a archivar una denuncia similar debido a la imposibilidad de identificar al responsable de la difusión de una imagen de desnudo integral de una alumna de un instituto.

"Es una pandemia de violencia tremenda a la que hay que combatir con estrategias políticas, grupos de trabajo y protocolos eficaces de protección a las víctimas", denunció en Al Adib, divulgadora y educadora sexual, quien hizo pública la denuncia del grupo de madres pacenses a través de sus redes sociales después de que se difundieron imágenes falsas de sus hijas.

Protección de Datos multa con 40.000 euros al colegio de Boadilla en el que se grabó a alumnas en ropa interior

El centro solo abonará 24.000 euros al acogerse a dos reducciones de la sanción por grabar sin consentimiento a menores durante más de una década

Hemeroteca — Investigado un profesor de Boadilla por grabar a alumnas en ropa interior durante una década

Carlos del Castillo

SEGUIR AL AUTOR/A

3 de julio de 2025 22:20 h
Actualizado el
04/07/2025 05:30 h
12

El Colegio Virgen de Europa, en Bohadilla del Monte (Madrid). EFE

En junio de 2022 una viandante encontró una mochila en Villanueva del Pardillo, una localidad a unos 30 kilómetros de Madrid. Dentro había una cámara de vídeo. Cuando la mujer reprodujo su contenido, vio un grupo de niñas cambiándose de ropa y entregó la mochila a la Guardia Civil. Así empezó un caso que llevó a la detención de uno de los profesores y copropietario del Colegio Virgen de Europa, en la cercana Boadilla del Monte, que presuntamente había estado grabando a las alumnas durante más de una década.

El caso sigue a la espera de juicio en la vía penal, después de que hace un año la Guardia Civil localizara nuevas potenciales víctimas y grabaciones en la casa del detenido. El proceso que ya se ha cerrado es la reclamación que la familia de una de las menores interpuso contra el Colegio ante la Agencia de Protección de Datos (AEPD) por violar la privacidad de las niñas con esas grabaciones. El resultado ha sido una multa de 40.000 euros para el centro, que se ha reducido a 24.000 tras aceptar este la responsabilidad de las infracciones (20%) y proceder al pronto pago (reducción del 20% adicional).

La queja inicial se interpuso el 27 de septiembre de 2023, argumentando que la menor había sido grabada en vídeo y que estas grabaciones habían salido del control del Colegio. La familia consideraba que se habían violado los principios de integridad y confidencialidad de los datos personales de la menor (porque los vídeos salieron de forma no autorizada) y

el principio de transparencia (porque las imágenes se captaron sin informar ni pedir consentimiento previo a los padres).

La AEPD admitió a trámite la reclamación elevó una serie de peticiones de información al Virgen de Europa sobre la obtención de las imágenes y su tratamiento.

En sus respuestas, primero el Colegio afirmó que obtenía el consentimiento de los padres para grabar imágenes de los alumnos en el momento de la matriculación, y que este consentimiento se revisaba anualmente. Como prueba, mostró un formulario de matrícula con una casilla para autorizar fotos y vídeos de los alumnos con fines de publicación en la web, anuarios, folletos, redes sociales y archivo del colegio.

Sin embargo, cuando el regulador de privacidad solicitó "repetidamente" las matrículas rellenadas y firmadas por las familias, el Virgen de Europa solo pudo aportar las correspondientes a tres de los últimos diez cursos.

Propósito docente

El Colegio cambió entonces su argumento: alegó que las imágenes se grababan con fines docentes, una excepción que hace innecesario el consentimiento. El profesor y copropietario del centro detenido, hijo de sus dos fundadores, también comunicó que las grabaciones que realizaba en el ejercicio de su labor tenían la finalidad de cumplir con el programa de docencia y para promocionar sus actividades.

A pesar de la insistencia del Colegio en la base legitimadora "propias de la función docente", la AEPD fue contundente. El regulador concluyó que "en este caso concreto no se aprecia la existencia de base legal que ampare el tratamiento datos personales de la menor mediante la captación de imágenes con equipos de grabación", a lo que se unía que el centro no pudo demostrar contar tampoco con el consentimiento para recoger datos personales de los alumnos para fines promocionales.

Brecha de seguridad: la pérdida del control de las imágenes

La reclamación inicial que dio origen al expediente de la AEPD señalaba que parte de los archivos de la menor fueron encontrados en una cámara hallada por un viandante en una carretera y otra parte en el domicilio personal del profesor. Esto llevó a la AEPD a considerar que se había producido una brecha de datos personales, ya que un tercero no autorizado había accedido a las imágenes de menores.

El Colegio insistió en que "la entidad dispone del control de las grabaciones" y que contaban con medidas como formaciones y concienciación del profesorado, además de otras medidas de seguridad. Sin embargo, la Agencia detectó que las formaciones al profesorado que había presentado el centro eran posteriores a los hechos.

Además, aunque las normas del Colegio indicaban que la salida de soportes con datos personales debía ser autorizada y registrada, la AEPD encontró que la autorización concedida al profesor detenido databa de 2018, era ilimitada en el tiempo, no especificaba la finalidad o el contenido, ni mencionaba las medidas de seguridad que debía adoptar. Más grave aún, el Colegio, requerido para aportar el registro de salidas y devoluciones de

dispositivos, contradijo sus propias afirmaciones al asegurar que "no existe ninguna autorización que se haya otorgado para la salida y posterior devolución al docente" durante el periodo relevante, a pesar de que la autorización original de 2018 seguía vigente.

Tres sanciones con reducción

La resolución de la AEPD concluye con la imposición de tres sanciones económicas al Colegio Virgen de Europa por vulnerar distintos artículos del Reglamento General de Protección de Datos de manera "muy grave".

El regulador considera probado que se produjo una brecha de seguridad que comprometió la integridad y confidencialidad de los datos personales de la menor, una infracción por la que impone una multa de 15.000 euros al centro. A su vez, también resuelve que el tratamiento de las imágenes fue ilícito al no contar con una base legal válida para hacerlo, imponiendo una segunda sanción de 20.000 euros.

Por último, la Agencia entiende que el centro tampoco informó debidamente a las familias del uso que hacía de las grabaciones, imponiéndole una tercera multa de 5.000 euros. La cuantía total, de 40.000 euros, se rebajó finalmente a 24.000 tras reconocer el Colegio su responsabilidad y optar por el pago voluntario.

La AEPD tuvo en cuenta varios factores agravantes para fijar la sanción: la naturaleza especialmente sensible de los datos tratados, la exposición de menores en situaciones comprometidas, la pérdida de control sobre las imágenes y la reiteración en la infracción, ya que el centro había sido sancionado por un incumplimiento similar menos de dos años antes.

Además de la multa, el regulador ha exigido al Colegio que adopte una serie de medidas correctivas en un plazo máximo de tres meses. Entre ellas, demostrar que ha implementado salvaguardas técnicas y organizativas para evitar accesos no autorizados a los datos personales, cesar el uso de grabaciones de menores sin una base jurídica adecuada y garantizar que toda la información exigida por la normativa se pone a disposición de las familias.

A falta de la resolución del caso penal, esta no es la primera multa a la que se enfrenta el Colegio Virgen de Europa por estos hechos. En febrero de 2024 el Tribunal Superior de Justicia de Madrid le obligó a indemnizar con 120.000 a la madre de una de las víctimas, que había ejercido como profesora en el centro durante años.

La app del Gobierno para bloquear el acceso de los menores al porno pasa el último filtro de seguridad a la espera de la solución europea

Cartera Digital Beta, que emitirá credenciales temporales para controlar el acceso a contenidos para adultos, concluye su desarrollo técnico mientras la UE prepara un proyecto piloto con esta tecnología para 2026

— El 'pornoapagón' de Francia anticipa las dificultades de la verificación de edad digital que quieren España y la UE

Carlos del Castillo

SEGUIR AL AUTOR/A

30 de octubre de 2025
22:05 h
Actualizado el
31/10/2025 05:30 h
2

Un niño sostiene un móvil en la cama. Kampus Production/ Pexels

Cartera Digital Beta ha concluido su desarrollo técnico. La aplicación móvil que España prepara desde 2023 para establecer un método de verificación de edad online, pensado para impedir el acceso de menores de edad a páginas porno, ya ha recibido la última verificación de seguridad. Era el sello que esperaba el Ministerio de Transformación Digital para dar su construcción por finalizada, informan a elDiario.es fuentes del departamento que dirige Óscar López.

La aplicación ha sido aprobada tanto por el Esquema Nacional de Seguridad como por el Centro Criptológico Nacional (CCN). El primero es el marco que garantiza que los sistemas públicos cumplan con los requisitos mínimos de seguridad para proteger la información y los servicios frente a ciberataques, accesos indebidos o manipulaciones.

La segunda revisión, realizada por el CCN, dependiente del Centro Nacional de Inteligencia, certifica que la aplicación cuenta con las adecuadas garantías de seguridad a nivel informático. Analiza los mecanismos de cifrado de los datos, la gestión de contraseñas y accesos, o la comunicación que la app establece con servidores centrales.

Basada en un mecanismo europeo

La tecnología de Cartera Digital Beta se basa en un reglamento europeo llamado eIDAS 2. Su objetivo es desarrollar un sistema de identificación digital común para toda la UE, que permita a los ciudadanos compartir con terceros determinados datos personales de forma segura. Funcionará a través de aplicaciones que trabajarán como carteras digitales, en las que cada usuario podrá registrar documentos como el DNI o el carnet de conducir, decidiendo en cada caso qué información concreta mostrar cuando se le requiera.

Por ejemplo, al reservar un coche de alquiler por Internet, estas aplicaciones podrán confirmar si el usuario dispone de carnet de conducir o no, pero sin revelar todos los datos del documento. En lugar de enviar una copia del carnet, emitirán una validación temporal que confirmará que ese usuario tiene efectivamente un carnet de conducir válido.

Estas acreditaciones temporales, que también pueden usarse para probar la mayoría de edad sin necesidad revelar la fecha de nacimiento completa o el DNI, fueron el motivo por el que Cartera Digital Beta fue conocida como "el pajaporte" durante su presentación. Los visitantes habituales de páginas para adultos tendrán que generar nuevas credenciales de manera periódica, ya que estas tienen límites de caducidad y número de usos para impedir un uso incorrecto de ellas.

Solución para el porno

El eIDAS 2 se aprobó en 2024 y entrará en virgo paulatinamente a partir de 2026. El objetivo de la UE es que entre finales de 2027 y principios de 2028, el uso de este método de identificación digital ya sea mayoritario. El Gobierno, sin embargo, decidió adelantarse al calendario comunitario y aplicar el mecanismo europeo a una cuestión sensible: asegurar que todos los consumidores de porno online son mayores de edad.

La verificación de edad es uno de los grandes problemas del mundo digital, ya que los servicios con limitación (como las páginas para adultos, pero también las redes sociales, cuya edad mínima de uso son 14 años) nunca han establecido métodos de control fiables. Argumentan que no es posible hacerlo sin llevar a cabo prácticas invasivas de privacidad, como pedir copias del DNI o hacer reconocimiento biométrico. En la práctica, permiten que sus servicios sean de consumo libre y delegan la responsabilidad sobre el control parental, que tiene limitaciones.

La intención del Ejecutivo con Cartera Digital Beta era poner en marcha un sistema efectivo para que las empresas no pudieran seguir amparándose en esa falta de opciones. El plan inicial de Transformación Digital era lanzar la app "después del verano" de 2024. Así lo expuso el antecesor de Óscar López en el ministerio, el hoy gobernador del Banco de España, José Luis Escrivá, cuando presentó el proyecto.

Sin embargo, construir una app robusta ha requerido aproximadamente un año más que los cálculos iniciales del Ministerio.

Un piloto europeo para 2026

Mientras se terminaban los trabajos técnicos de Cartera Digital Beta, un grupo de países, entre los que se incluía España, solicitaron a la UE que pusiera en marcha un proyecto piloto para utilizar la tecnología del eIDAS 2 para verificar la edad de los consumidores de páginas porno.

En mayo de 2025, Bruselas se mostró de acuerdo y emplazó a España, Francia, Grecia, Italia y Dinamarca a desarrollar esas aplicaciones. Pretende construir un sistema que no solo sea seguro y privado, sino también que facilite la interoperabilidad entre todos los países miembros.

Ese proyecto ha ido avanzando en el testeo de las tecnologías que deben hacerlo posible. La Comisión Europea no ha fijado una fecha para que estas soluciones empiecen a funcionar, aunque un portavoz del organismo ha explicado a elDiario.es que el plan era que entraran en acción en 2026, informa **Rodrigo Ponce de León**. Las primeras pruebas de compatibilidad entre apps están previstas para finales de este año.

Mientras, España, dado que comenzó antes los trabajos de desarrollo de la app, es "el país de la UE con la herramienta de verificación de mayoría de edad más avanzada acorde a los estándares europeos actuales", aseguran desde Transformación Digital.

"Pornoapagón" en Francia y brusca caída del consumo en Reino Unido

A pesar de que el plan inicial del Gobierno era actuar en solitario, la posibilidad de esperar a tener una solución comunitaria europea para poner en marcha Cartera Digital Beta ha ido ganando fuerza, especialmente desde el lanzamiento del proyecto piloto en mayo.

Lo ocurrido en otros países europeos que han decidido actuar por su cuenta se ha convertido en una experiencia a valorar. El caso más similar es Francia. El Gobierno galo, a diferencia del español, no ha desarrollado una app basada en las credenciales temporales del eIDAS 2 sino en otro de los mecanismos que el reglamento permitía: que fuera un tercero (como un banco o una operadora telefónica) el que validara la edad del usuario que intenta acceder a una página porno.

El sistema utiliza una modalidad denominada "de doble ciego" en el que la web para adultos no conoce la identidad de la persona que intenta acceder, mientras que la empresa que da la prueba de edad no sabe a qué servicio se la está entregando. No obstante, la obligación de implantar una verificación de edad única para Francia ha provocado que la mayor multinacional del porno online, Aylo, gestora de Pornhub, YouPorn o Redtube, abandonara el país en julio.

Un "pornoapagón" en el mercado que hasta entonces había sido su segundo más importante a nivel internacional. "Durante años, hemos intentado colaborar con el gobierno mediante consultas, intercambio de datos y participación en proyectos piloto. Los resultados han sido claros: la verificación de edad online no funciona. No protege a los niños y expone los datos de millones de franceses a violaciones de privacidad y ataques informáticos", alegó la multinacional del porno, que no ha vuelto a operar en el país.

Por otro lado, está el caso del Reino Unido, que implantó en julio de 2024 un sistema de verificación de edad basado en múltiples métodos, desde el envío de mensajes de texto

hasta comprobaciones por correo electrónico o introduciendo el número de la tarjeta de crédito. El resultado fue un desplome en las visitas de a páginas web de contenido para adultos desde el país, paralelo a un ascenso equiparable del uso de VPN, una herramienta que permite ocultar el lugar de conexión del dispositivo que se usa para eludir este tipo de bloqueos.

Según datos del regulador de comunicaciones británico Ofcom, las visitas totales a este tipo de servicios han caído casi un 30%, y Pornhub —la plataforma más popular del país— ha perdido más de tres cuartas partes de su audiencia. No obstante, Ofcom asegura que tras la explosión inicial, el uso de VPN ha vuelto a niveles normales tras el verano.

Las medidas británicas obligan a todas las webs pornográficas a comprobar la edad de sus usuarios, mediante sistemas que van desde el envío de mensajes de texto hasta verificaciones por correo electrónico o comprobaciones con tarjeta de crédito. La consecuencia inmediata ha sido un aumento temporal del uso de redes privadas virtuales (VPN), aunque Ofcom asegura que su utilización ha vuelto a niveles normales tras el verano.

El Gobierno espera activar un bloqueo de redes sociales para menores de 16 años como el australiano en 2026

El Ministerio para la Transformación Digital ya tiene preparada la herramienta de verificación de edad y está a la espera de la aprobación de la ley de protección de los menores en el entorno digital, que contempla esta edad mínima, y del visto bueno de la UE

— Millones de adolescentes australianos pierden el acceso a sus redes sociales tras la primera prohibición a nivel mundial

Carlos del Castillo

SEGUIR AL AUTOR/A

11 de diciembre de 2025
14:38 h
Actualizado el
11/12/2025 16:59 h
16

Joven revisando el movil

Australia vive estos días un debate nacional, a raíz de la entrada en vigor de un límite de edad para el uso de redes sociales por parte de los menores de 16 años. Se trata del primer

país que pone en marcha una medida así, destinada a controlar los efectos perniciosos que estas plataformas tienen en los niños, como adicciones o exposición a contenidos para adultos. Una medida que el Gobierno español espera emular tan pronto como en 2026.

Así lo ha anticipado el ministro para la Transformación Digital, Óscar López, este jueves. Actualmente el límite de edad para el uso de estos servicios en España son los 14 años, pero una nueva norma plantea elevarlo hasta los 16. Se trata de la ley orgánica para la protección de los menores en entornos digitales, que arrancó en septiembre su tramitación en el Congreso. Fuentes parlamentarias explican que el texto tiene posibilidades de conseguir apoyos por parte del resto de grupos, incluido el PP.

Si se aprueba, quedaría bloqueado el acceso a las redes sociales para los niños y adolescentes menores de 16 años que no cuenten con aprobación parental.

No obstante, López ha recordado que la discusión sobre la edad mínima "no es oportuna si no hay un verdadero sistema de verificación de edad". "La herramienta es tan importante como la legislación", ha recalcado. En este sentido, el ministro ha confirmado que la herramienta de verificación de edad para poner en marcha la medida, Cartera Digital Beta, ya está a lista a nivel técnico, como adelantó elDiario.es.

En este momento está siendo testada en un proyecto europeo junto a las soluciones propuestas por otros países, pero el ministro ha recordado que la española "es la más adelantada y la única que está lista". Se trata de un proyecto en el que el Ejecutivo quiere ir de la mano con la UE, pero su objetivo es que el proyecto termine de poner todos sus mecanismos en marcha "en 2026", ha recalcado.

Cartera Digital Beta es una herramienta de verificación de edad que permite demostrar si un usuario tiene más de una determinada edad sin revelar datos personales innecesarios, según ha explicado el Gobierno en su documentación técnica. Funciona como una credencial digital emitida por la Administración: el móvil genera una prueba criptográfica que las plataformas pueden comprobar, pero sin acceder al DNI ni almacenar información sensible.

El objetivo es que los menores no puedan abrir cuentas en redes sociales o acceder a páginas pornográficas sin este control y, a la vez, garantizar que el proceso respete la privacidad de los adultos.

Con el visto bueno del Consejo Asesor

López ha hecho este anuncio en una rueda de prensa posterior a la reunión del Consejo Asesor sobre Inteligencia Artificial del Ministerio, integrado por algunos de los expertos internacionales en este campo más reputados. Este órgano consultivo, cuyos miembros no reciben una compensación económica por asesorar al Gobierno en esta cuestión, se ha reunido este miércoles y jueves en Madrid.

Uno de los temas que han centrado las conversaciones ha sido precisamente lo que está sucediendo en Australia. Una de las personas que integran el consejo es la australiana Kate Crawford, cofundadora del centro de investigación AI Now Institute y autora de *El Atlas de la IA*, una de las obras de referencia en este campo, que ha documentado el intento del país

de apartar a los menores de los algoritmos de las plataformas y sus efectos más perniciosos.

“Es un paso que va claramente en la buena dirección”, ha manifestado en la rueda de prensa Jeroen van den Hoen, filósofo especializado en tecnología e IA, profesor de la Universidad Tecnológica de Delft (Países Bajos) y miembro del Consejo Asesor. “A partir de nuestras conversaciones creemos que lo correcto es proporcionar herramientas de verificación de edad respetuosas con la privacidad y que a la vez garanticen cierto control a los padres sobre lo que ocurre con sus hijos online. Todo el mundo está preocupado por lo que está pasando”, ha revelado.

“Durante mucho tiempo hemos estudiado lo que les ocurre a los jóvenes y a los niños en redes sociales y lo que sabemos es que no es bueno”, ha continuado el profesor en respuesta a la pregunta de elDiario.es. “Las personas que proporcionan estas plataformas, servicios y aplicaciones no están interesadas en la salud mental de los menores. Al contrario, obtienen beneficios de eso, por lo que tienen todos los incentivos para desarrollar todo tipo de productos que no están orientados a su bienestar, sino todo lo contrario. Su interés es que cada vez sean más adictivos”.

Para contextualizar el debate, que en Australia ha movilizado a muy diversos sectores de la sociedad civil, así como el actual en torno a la regulación de la inteligencia artificial, el experto ha querido recuperar una opinión de la ex comisaria de la Comisión Europea Margrethe Vestager. “Si hace 20 años, cuando se introdujeron las redes sociales, hubiéramos sabido cuál sería el impacto completo en la sociedad, no habríamos sido tan ingenuos. Habríamos tomado las medidas que estamos tomando ahora”.

La industria digital recela del “control duro” de la edad de los menores en redes que el Gobierno plantea para 2026

Las multinacionales que deberán colaborar con Ejecutivo para la verificación de la edad de los menores defienden que las herramientas de control parental y la concienciación son más efectivas que un veto estricto

— El Gobierno espera activar un bloqueo de redes sociales para menores de 16 años como el australiano en 2026

Carlos del Castillo

SEGUIR AL AUTOR/A

22 de diciembre de 2025
21:58 h
Actualizado el
23/12/2025 05:30 h
5

Niños frente a una tablet. Kampus Production / Pexels

Los encargados de aplicar la norma no lo ven tan claro como el Gobierno. El ministro para la Transformación Digital, Óscar López, adelantó este diciembre que el Ejecutivo espera poder implantar en 2026 una verificación de edad digital destinada impedir que los menores accedan a contenidos para adultos o a las redes sociales sin tener la edad recomendada (actualmente está en 14 años, pero el Congreso negocia una nueva ley que plantea elevarla a 16). La vía que maneja el Ministerio es una verificación de la edad de todos los usuarios que pueda detectar a los niños y adolescentes, similar al aprobado recientemente en Australia.

La industria digital, sin embargo, recela de este método. Lo considera un "control duro" que "puede generar riesgos relevantes en materia de privacidad, accesibilidad y competitividad". Por ello, pide "un enfoque flexible y proporcional" basado en "controles parentales y programas de alfabetización digital", en el que sea cada familia la que decida cómo supervisa el consumo digital de los menores.

Así lo expresa en un comunicado enviado a este medio Adigital, una de las principales patronales tecnológicas españolas, de la que forman parte las grandes multinacionales estadounidenses que resultarán claves para el éxito de la medida. Para la asociación, la

"verificación universalidad de la edad" que plantea el Gobierno puede suponer "cargas desproporcionadas a empresas y usuarios". Por ello, piden que se base en la "evaluación de riesgos", es decir, que no tenga que pasar el mismo control alguien que intente acceder a una página pornográfica que un usuario de las plataformas mayoritarias.

Los representantes de la industria señalan que poner el foco en la concienciación, en cambio, puede "reforzar la corresponsabilidad de familias y escuelas" en el proceso de la navegación segura para los menores.

Fuentes de las empresas directamente involucradas en el proceso de verificación de edad, con las que el Gobierno tendrá que colaborar, comparten esta opinión y han empezado a deslizarla en privado. Sus responsables entienden que se trata de una medida que puede ir directa a los titulares, pero con muchos problemas para ponerse en práctica. "Coarta la libertad de expresión también de los adultos que no quieren esa navegación fiscalizada", aseguran.

"Parece desproporcionado crear un control para toda la población cuando es solo un colectivo el que la necesita", opinan, ante la creencia de que "el café para todos no funciona". Aunque reconocen que los problemas de adicciones o exposición a algoritmos nocivos en los menores es un problema que preocupa a una parte cada vez mayor de la sociedad, señalan que el camino "es la corresponsabilidad" con las familias: "Un adecuado control parental convierte el teléfono en un zapato", alegan estas fuentes.

A qué llaman "control duro"

El sistema que propone el Gobierno, y que la industria califica de "control duro", se articula en torno a una aplicación móvil llamada "Cartera Digital Beta". Esta herramienta ha sido desarrollada por el Ministerio de Transformación Digital basándose en el Reglamento Europeo eIDAS 2, una normativa comunitaria diseñada para estandarizar la identificación electrónica en toda la UE. El sistema requiere que el usuario se registre utilizando su DNI electrónico, el sistema Cl@ve o un certificado digital oficial, vinculando así su dispositivo móvil a su identidad real.

De esta forma, cuando un usuario intente acceder a una web con contenido para adultos, esta le mostrará un código QR que deberá escanear con la aplicación de la Cartera Digital. En ese momento, la app no envía al portal ni el nombre ni la fecha de nacimiento de esa persona, sino que emite una "credencial de acceso" anónima que confirma que el usuario es mayor de edad.

Según explicó Transformación Digital en 2024, cuando se dio el pistoletazo de salida al proyecto, estas credenciales funcionan mediante paquetes de usos limitados que caducarán cada 30 días, obligando al usuario a renovar periódicamente su verificación. La app no almacenaría un registro de a quién se envían estas credenciales.

Se trata de un sistema avalado por la UE, que en el futuro quiere implantarlo a todos los ámbitos de la identidad digital como un método para reducir el envío de datos personales a terceros. Al alquilar un coche por Internet, por ejemplo, el sistema permitiría enviar tan solo una credencial que indique que el usuario dispone de carnet de conducir, y no una fotografía del documento, reduciendo el margen para ciberataques o filtraciones.

El objetivo del Gobierno es empezar a aplicarlo desde 2026 para controlar el acceso de los menores a las redes sociales y contenidos inadecuados, como pornografía o apuestas. España participa actualmente en un proyecto piloto europeo junto a Francia, Grecia, Italia y Dinamarca para probar el sistema, siendo Cartera Digital Beta la app "más adelantada y la única que está lista", según ha defendido Óscar López.

Expertos en privacidad, no obstante, ya advirtieron cuando se presentó el sistema que acumular toda esta información en una misma aplicación estatal crea un punto único de fallo: si la seguridad de la Cartera Digital se viera comprometida, los atacantes podrían vincular trazar un gran número de actividades con la identidad real del ciudadano. "En Internet todos somos vulnerables. Acumular en un mismo sitio todo este tipo de información, desde mi punto de vista es peligroso, sobre todo cuando hay otras soluciones disponibles", explicó Samuel Parra, abogado especialista en privacidad, en un reportaje de elDiario.es.

Los métodos "blandos"

La alternativa a este método que propone la industria son los métodos "blandos" como el control parental. Se trata de herramientas que conoce el 75% de familias con menores a su cargo, según los datos del último Panel de Hogares de la Comisión Nacional de los Mercados y la Competencia. No obstante, solo el 35% de ellas las utilizan.

Pese a ese bache, el sector digital asegura que el método más efectivo para impedir que los menores accedan a contenidos perjudiciales es aumentar la concienciación sobre su importancia. Se basan en informes independientes como el de Infancia, adolescencia y bienestar digital, elaborado por Unicef, que relacionan los conocimientos y el compromiso con estas herramientas por parte de las familias con un descenso en las conductas de riesgo online (sexting, contacto con desconocidos o ciberacoso) en los menores.

"El empoderamiento de niños, niñas y adolescentes como agentes del cambio fomentando su participación en la toma de decisiones que afectan a su vida digital, escuchando sus voces, y considerando sus opiniones para construir una Internet más inclusiva donde puedan ejercer su ciudadanía plena", refleja Unicef. Para ello, considera fundamental "promover una mediación parental gradual y adaptativa, empezando en la infancia con un acompañamiento cercano y avanzando en la adolescencia hacia la autonomía responsable, la toma de decisiones informada y la construcción progresiva de confianza".

> ***"Para ser efectiva, la verificación debe aplicarse por defecto: las personas menores no deberían tener que demostrar su edad ni exponer su naturaleza"***
> Informe de la Oficina C del Congreso de los Diputados sobre Menores y redes sociales

Otros estudios, como el Informe de la Oficina C del Congreso de los Diputados sobre Menores y redes sociales, recalcan que la prohibición total, como en el caso australiano con las redes sociales para los menores de 16, puede ser "contraproducente". El motivo es que puede dificultar la "alfabetización digital" de los menores e introducir una "sensación de falsa seguridad" respecto a Internet y las plataformas digitales.

Sin embargo, ambos informes destacan que la vía actual, basada en la autorregulación, ha fracasado, y abogan por establecer verificaciones de edad más estrictas que "trasladen la carga de la prueba a los adultos", como afirma el análisis de la Oficina C del Congreso. "Para ser efectiva, la verificación debe aplicarse por defecto: las personas menores no deberían tener que demostrar su edad ni exponer su naturaleza (por ejemplo, recibiendo información adaptada para tomar decisiones que no les corresponden) para que se bloqueen contactos, contenidos o funciones no apropiadas a su edad", destaca.

Para Unicef, "establecer sistemas de verificación de edad efectivos, respetuosos con los derechos de niños, niñas y adolescentes" es una de las prioridades que enfatiza Unicef, así como "revisar la edad mínima y las condiciones para acceder a las redes sociales" y "exigir la rendición de cuentas a las compañías tecnológicas acerca del impacto de sus productos y servicios en los derechos de la infancia y la adolescencia".

La UE resucita su plan de escanear todos los chats en busca de abuso infantil: “Es una amenaza enorme”

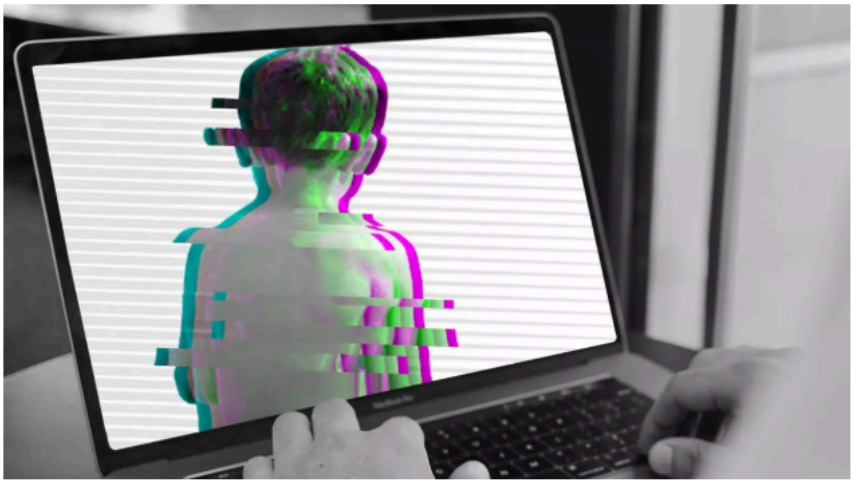
Más de 460 tecnólogos denuncian en una carta los riesgos “sin precedentes” de la monitorización constante de conversaciones digitales para detectar material pedófilo, que vuelve a plantear Bruselas

— El “salvaje oeste” de Kick, la plataforma que ha emitido una muerte en directo

Carlos del Castillo

SEGUIR AL AUTOR/A

9 de septiembre de 2025
06:01 h
4



La Unión Europea ha resucitado una controvertida propuesta para obligar a los servicios digitales a escanear todas las comunicaciones de sus usuarios en busca de material de abuso sexual infantil. El plan, que ya fue rechazado por el Parlamento Europeo durante la anterior legislatura comunitaria, vuelve a estar sobre la mesa de las instituciones a través de

una nueva propuesta de la Comisión Europea que está ganando apoyos entre varios estados miembros y será debatida este viernes en una reunión de los Veintisiete.

La propuesta busca establecer normas para prevenir y combatir el abuso sexual infantil y la distribución de material pedófilo. Su objetivo es impedir que las aplicaciones de mensajería, correo electrónico, las redes sociales o los chats de videojuegos se utilicen para estos delitos. Bruselas argumenta que deben ser los proveedores de estos servicios sobre los que se regule, ya que "son a menudo los únicos en posición de prevenir y combatir tal abuso".

El plan es que estas plataformas instalen un algoritmo que revise todos los chats de los usuarios en busca de patrones de alerta que indiquen que en una conversación determinada se podrían estar generando o compartiendo imágenes que encajan con la pornografía infantil. Al detectarlas, el algoritmo daría aviso a la compañía, que lo reportaría a las fuerzas de seguridad. Apps como WhatsApp, Telegram, Signal, Instagram, Gmail y cientos más se verían afectadas.

"Las medidas adoptadas deben ser específicas, cuidadosamente equilibradas y proporcionadas, a fin de evitar consecuencias negativas indebidas para quienes utilizan estos servicios con fines lícitos", afirma la propuesta, que ha introducido algunas modificaciones respecto al texto que fue rechazado por la Eurocámara en 2023. El principal es la reducción del alcance del escaneo a las imágenes y enlaces que compartan los usuarios —el plan anterior abarcaba todos los mensajes, incluido texto o audio— y el hecho de que este se realice en el mismo dispositivo del usuario.

El nuevo texto también hace especial hincapié en la importancia del cifrado de extremo a extremo. Se trata tecnología más robusta actualmente para proteger la confidencialidad de las comunicaciones digitales, ya que los convierte en un código ilegible para cualquiera excepto el emisor y el destinatario. El temor a que el escaneo de los mensajes abriera una agujero en esta protección fue una de las principales causas de la caída de la propuesta anterior.

"El cifrado de extremo a extremo es un medio necesario para proteger los derechos fundamentales y la seguridad digital de los gobiernos, la industria y la sociedad", asegura ahora el texto de la Comisión. "Este Reglamento no prohibirá, hará imposible, debilitará, eludirá o socavará de otro modo las medidas de ciberseguridad, en particular el cifrado, incluido el cifrado de extremo a extremo", recalca.

Sin embargo, no cede en su intención de establecer un mecanismo de vigilancia masiva que pueda detectar este tipo de imágenes en cualquier situación. El abuso infantil "debe seguir siendo detectable en todos los servicios de comunicaciones interpersonales mediante la aplicación de tecnologías verificadas", señala el texto, que impone que "el mecanismo de detección pueda acceder a los datos en su forma no cifrada para un análisis y una acción eficaces".

"Vigilancia sin precedentes"

La propuesta tumbada por el Parlamento Europeo en 2023 suscitó un enorme rechazo entre los tecnólogos y la comunidad de organizaciones de defensa de los derechos digitales. La nueva proposición ha arrancado con la misma controversia.

Este martes, 467 especialistas de 36 países han enviado una carta a las instituciones comunitarias para alertar de que su plan para escanear todos los chats "socava por completo las protecciones de seguridad y privacidad que son esenciales para salvaguardar la sociedad digital". "La nueva propuesta, al igual que sus predecesoras, creará capacidades sin precedentes de vigilancia, control y censura, y conlleva un riesgo inherente de desvío de funciones y de abuso por parte de regímenes menos democráticos", denuncian en la misiva, a la que ha tenido acceso elDiario.es.

La mayoría de los firmantes son profesores universitarios e investigadores especializados en cifrado digital de las comunicaciones, ciberseguridad y tecnologías de privacidad. Muchos de ellos de reconocido prestigio internacional, como la española Carmela Troncoso, directora científica del Instituto Max Planck para la Seguridad y la Privacidad, una de las instituciones de referencia en Alemania. "La propuesta sigue sin garantizar ninguna mejora en la protección para menores, pero sigue siendo una amenaza enorme para la privacidad y libertad online", explica a este medio.

"La nueva propuesta dice que solo mirarán URLs e imágenes —aunque en una nota se dice que puede volver el análisis de texto a través de una enmienda en el futuro— pero esto no cambia el hecho de que sigue siendo fácil evadir el detector con cambios pequeños", avisa la especialista.

Imposible técnicamente y fácil de burlar

El principal argumento técnico de los especialistas respecto al plan de escaneo de chats de Bruselas sigue siendo el mismo: no existe la tecnología para llevarlo a cabo. "Simplemente, no es viable realizar detecciones de material de abuso sexual infantil conocido y nuevo entre cientos de millones de usuarios con un nivel aceptable de precisión, independientemente del filtro concreto", explican en la carta.

"Los expertos han demostrado en repetidas ocasiones que los métodos de detección de material de abuso infantil conocido son fáciles de eludir: basta con modificar unos pocos bits en una imagen para que esta no active los detectores más avanzados", detallan. Para los abusadores y pedófilos, sería fácil adoptar métodos como este para escapar del algoritmo, alegan los expertos, lo que les permitiría "burlarlo por completo".

> ***"Los detectores de última generación arrojarían tasas inaceptablemente altas de falsos positivos y falsos negativos, lo que los hace inadecuados para campañas de detección a gran escala, como las que plantea la regulación"***
> Carta de 430 tecnólogos a la UE

Un filtro ineficaz que, por contra, sí podría causar disgustos al resto de la población. "La investigación existente confirma que los detectores de última generación arrojarían tasas inaceptablemente altas de falsos positivos y falsos negativos, lo que los hace inadecuados para campañas de detección a gran escala, como las que plantea la regulación, con cientos de millones de usuarios afectados", destaca la carta.

Los tecnólogos hacen un amplio desglose técnico de los agujeros de la propuesta de la UE. Además, rebajan el potencial beneficioso de los cambios introducidos al plan de 2023. "No

existe base científica para sostener que la tecnología de detección funcionaría mejor con imágenes que con texto", dicen sobre la decisión de que el algoritmo analice solo fotografías y archivos. "Es imposible realizar detección de material y enviar los correspondientes reportes sin afectar al cifrado", explican sobre la posibilidad de que ese análisis se realice en el dispositivo del usuario.

Actualmente, el documento que resucita el plan de la UE de escanear es una propuesta de compromiso de la Presidencia del Consejo de la Unión Europea, que actualmente ocupa Dinamarca. Esto significa que es un texto que se está revisando y negociando entre los países de la UE. El próximo paso será la reunión del Grupo de Trabajo este 12 de septiembre, para su discusión y posibles enmiendas. De ser aprobada por el Consejo, el texto tendría que volver a pasar por el examen del Parlamento Europeo.

Protección de Datos alerta de que TikTok ha reactivado el envío de datos personales a China y pide replantearse su uso

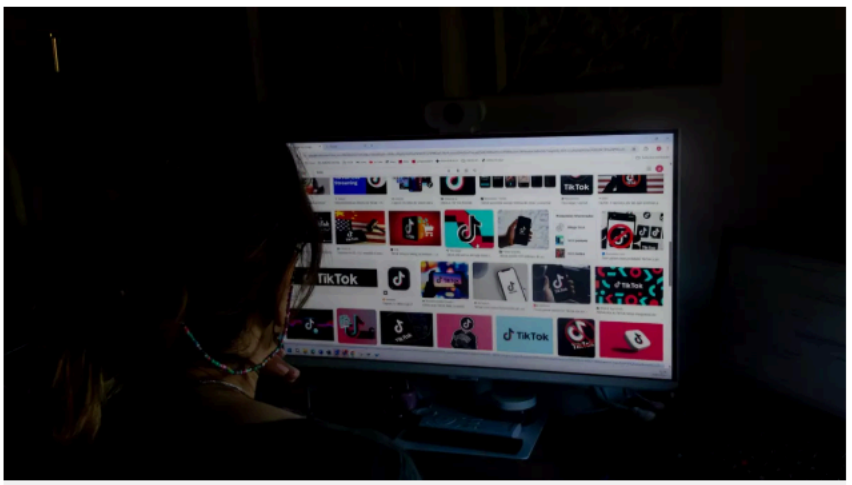
El regulador español de la privacidad pide a los usuarios "valorar si desean continuar utilizando un servicio cuando existen transferencias de datos a países que no ofrecen un nivel de protección equivalente al europeo"

— El Gobierno espera activar un bloqueo de redes sociales para menores de 16 años como el australiano en 2026

Carlos del Castillo

SEGUIR AL AUTOR/A

22 de diciembre de 2025
13:07 h
Actualizado el
22/12/2025 13:20 h
1



Archivo - Pantalla en la que aparecen imágenes de logos te Tiktok. Ricardo Rubio - EP

TikTok ha reanudado las transferencias de datos personales de sus usuarios europeos hacia China. Así lo ha alertado la Agencia Española de Protección de Datos (AEPD) este

lunes, que destaca que la red social continúa transfiriendo información a terceros países, incluido el gigante asiático, a pesar de que estas prácticas "ya fueron analizadas por parte de las autoridades europeas, que concluyeron que no cumplían con el Reglamento General de Protección de Datos (RGPD)", lo que le valió una multa de 530 millones de euros.

El origen de esta situación se remonta a abril de este año, cuando la Comisión de Protección de Datos de Irlanda (DPC), la autoridad principal que vigila a la plataforma al estar su sede europea en Dublín, impuso dicha sanción y ordenó detener los envíos de información tras una investigación coordinada con el resto de agencias europeas. Sin embargo, la compañía recurrió la decisión ante la justicia irlandesa, que el pasado noviembre acordó levantar temporalmente la prohibición de transferir los datos a la espera de dictar una sentencia definitiva.

Este permiso provisional concedido por el tribunal está condicionado a que la tecnológica cumpla con unas obligaciones específicas de transparencia. Por ello, TikTok ha comenzado a informar a los usuarios europeos sobre cómo se tratan sus datos personales y sobre la existencia del procedimiento judicial en curso. TikTok tiene más de 200 millones de usuarios en Europa, unos 23,5 millones de ellos en España, según datos oficiales de la plataforma.

La AEPD aclara que, aunque el bloqueo de las transferencias se encuentre en suspenso de forma cautelar, la valoración legal de los reguladores "sigue vigente". Las autoridades europeas insisten en que enviar esta información a China incumple la normativa comunitaria, por lo que la legalidad de la operativa de la red social continúa estando cuestionada.

Desde TikTok recalcan que están "en total desacuerdo" con la resolución emitida por la autoridad irlandesa, por lo que celebra la decisión del tribunal y ha reactivado el envío de datos. "TikTok se toma muy en serio la protección de datos y la privacidad de los usuarios", asegura la red social, indicando que ha realidado una "inversión de 12.000 millones de euros en la seguridad de los datos europeos". "En nuestra opinión, ofrece garantías inigualables para los datos de los usuarios europeos", asegura.

"Valorar si desean continuar"

Ante este escenario, el organismo español considera "esencial" que los ciudadanos, y especialmente los más jóvenes, dispongan de información clara sobre el destino de su información. Entre sus recomendaciones, la Agencia aconseja "revisar la configuración de privacidad de las aplicaciones y comprobar los permisos concedidos, como el acceso a la cámara, el micrófono, los contactos o la ubicación", o "actuar con prudencia respecto a la información que se comparte a través de aplicaciones y redes sociales, evitando la difusión de datos sensibles".

Además, el regulador de la privacidad español va un poco más allá y sugiere a los usuarios que abandonen la plataforma. De esta forma, la AEPD recomienda "valorar si desean continuar utilizando un servicio cuando existen transferencias de datos a países que no ofrecen un nivel de protección equivalente al europeo".

Con esta advertencia, el organismo recuerda que cuando la información personal se almacena en bases de datos de terceros países fuera del bloque comunitario, pasa a

quedar bajo la jurisdicción local. En el caso de China, esto puede implicar el acceso total a esa información por parte del Gobierno o el Ejército Popular de Liberación, puesto que la ley les permite reclamar a las compañías tecnológicas cualquier activo que tengan a su disposición en base a los intereses del Estado. Aunque no existen pruebas de que se hayan producido acceso a las bases de datos de TikTok, el marco legal chino lo permite.

Este tipo de accesos no contemplados en la regulación europea fueron los que motivaron al Tribunal de Justicia de la UE a invalidar por dos veces el tratado de transferencias de datos que la Comisión Europea había establecido con Estados Unidos. El actual también está siendo analizado por los magistrados tras una denuncia del mismo abogado que consiguió la anulación de los dos anteriores.

Sub-bloque C: Plataformas tecnológicas y economía de datos

La condena a Meta reordena el tablero digital: la Justicia zanja que plataformas y medios compiten por el mismo mercado

El fallo convierte los incumplimientos de privacidad de Facebook e Instagram en una causa de competencia desleal, abriendo la puerta a que los editores reclamen daños masivos a las tecnológicas por jugar con las cartas marcadas en el mercado publicitario

— Un juzgado condena a Meta a indemnizar con 479 millones a decenas de medios españoles por competencia desleal en Facebook e Instagram

Carlos del Castillo

SEGUIR AL AUTOR/A

21 de noviembre de 2025
22:12 h
Actualizado el
22/11/2025 05:30 h
0

Durante casi dos décadas, Silicon Valley operó bajo la premisa de que la tecnología avanza más rápido que la ley y, por tanto, las reglas del mercado tradicional no podían aplicarse a la economía de plataformas. El mantra de "muévete rápido y rompe cosas" de Mark Zuckerberg se convirtió en la declaración de intenciones no solo para Facebook, sino para toda la naciente industria digital.

Una de las regulaciones que se rompieron, al menos tal y como la prensa las entendía hasta entonces, fueron los derechos de autor. Los medios tradicionales, cuyo negocio dependía del soporte físico, vieron cómo sus informaciones eran replicadas en redes y agregadores a cambio de unos ingresos publicitarios residuales. Su respuesta fue utilizar el copyright para reclamar dinero a esas plataformas. La estrategia fracasó a escala global.

En España, la industria de las cabeceras impresas contó con la complicidad institucional. En 2014, lograron que el Gobierno de Mariano Rajoy incluyera en la ley de propiedad intelectual una nueva tasa para cobrar cada vez que uno de sus artículos fuera referenciado en las plataformas. Se llamó canon AEDE, por la Asociación de Editores de Diarios

Españoles, la patronal que agrupa a los grandes grupos editoriales españoles tradicionales como el grupo Prisa (El País, La SER), Unidad Editorial (El Mundo, Expansión, Marca) o Vocento (ABC, las principales cabeceras regionales).

AEDE esperaba recaudar hasta 80 millones al año con el canon, pero, en la práctica, generó menos de medio millón en los siete años en los que estuvo activo. El motivo fue que Google, que se suponía que iba a ser el principal pagador de la tasa a través de Google News, consideró la legislación obsoleta y retiró el servicio de España. Su desaparición supuso un golpe para todos los medios españoles, también para los nativos digitales que se posicionaron contra el canon, al perder el acceso al principal quiosco virtual del momento.

Esta semana ha habido un nuevo capítulo en esta saga. AEDE, renombrada a AMI (Asociación de Medios de Información), ha conseguido una victoria en los tribunales que tendrá eco en toda Europa. Y no ha sido a través de la propiedad intelectual, sino de otra regulación redactada, esta vez sí, con el mundo digital y la economía de plataformas en mente: la protección de datos.

Un dopaje desleal

Facebook se movió rápido y rompió cosas. Meta, su sucesora, está viendo cómo los reguladores rompen su modelo de negocio. Una fecha clave en ese proceso es diciembre de 2022. Entonces, el Comité Europeo de Protección de Datos estipuló que la extracción de datos personales para segmentar la publicidad que hacía la corporación de Mark Zuckerberg era ilegal según las normas europeas. Y lo había sido desde 2018, cuando entraron en vigor dichas normas.

En enero de 2023, Meta recibió una multa de 390 millones de euros de la agencia de protección de datos irlandesa por este motivo. La multinacional cambió sus términos legales y durante años todo quedó en una de tantas sanciones que reciben los de Zuckerberg de este organismo, criticado por su permisividad con los gigantes tecnológicos a que se establecen en su territorio y codirigido por una exdirectiva de Facebook. Sin embargo, la multa ha terminado abriendo la puerta a un movimiento mucho más trascendental.

Con la resolución del Comité Europeo en la mano, AMI se presentó en un tribunal de lo Mercantil de Madrid. Alegó que si Meta había estado mejorando la personalización de sus anuncios con datos obtenidos de manera ilícita, entonces había tenido una ventaja competitiva injusta con los medios de comunicación que también compiten en el mercado publicitario. Siguiendo sus propias cuentas, pidió una indemnización de 551 millones de euros por el dinero que sus cabeceras habían dejado de ganar por culpa de las prácticas de Meta.

> ***"Meta utilizaba indebidamente datos personales protegidos de los usuarios, lo que le daba una ventaja competitiva significativa frente al tratamiento publicitario que hace la prensa digital española"***
> Sentencia AMI vs Meta

Este jueves, el juez le ha dado la razón. El tribunal ha condenado a Meta por competencia desleal y le ha ordenado pagar a los medios reclamantes 479 millones de euros más otros 60 en intereses. "Meta utilizaba indebidamente datos personales protegidos de los usuarios,

lo que le daba una ventaja competitiva significativa frente al tratamiento publicitario que hace la prensa digital española", refleja la sentencia.

Esos datos supusieron un dopaje que no tuvieron sus competidores. "La ventaja competitiva consiste en que Meta, a través de sus servicios Instagram y Facebook, cuenta con una gran cantidad de datos de cada uno de sus usuarios activos, incomparablemente superior a la cantidad de datos con la que cuenta la prensa digital. Esto le permite hacer una publicidad personalizada mucho más directa y eficaz que la que puede hacer la prensa digital", desglosa el juez.

Una cuenta por omisión

La sentencia es recurrible ante la Audiencia Provincial y, posteriormente, ante el Tribunal Supremo. Meta ha anunciado que lo hará, en sus dos vertientes fundamentales. "No estamos de acuerdo con la sentencia del tribunal y la recurriremos. Se trata de una demanda infundada que carece de pruebas del supuesto perjuicio y que ignora deliberadamente cómo funciona el sector de la publicidad online", adelantó en un comunicado enviado a este medio.

La multinacional cita las dos vertientes fundamentales de la resolución. Una es la cuantía de la indemnización, en la que el juez ha asumido plenamente lo exigido por AMI debido a que el gigante de las redes renunció a presentar pruebas de que esos cálculos eran exagerados. "La representación procesal de Meta debía extinguir, impedir o enervar esta pretensión y para ello tenía plena facilidad probatoria, pues tiene muy fácil el acceso a las cuentas de Meta en España en el periodo relevante. Sin embargo, no lo ha hecho", le afea el juez.

AMI interpreta la negativa de Meta como una asunción de que la cuantía solicitada debería haber sido incluso mayor. No obstante, la opacidad de la multinacional hace que este sea uno de los elementos más susceptibles de ser alterados por las instancias superiores de justicia. Fuentes judiciales consultadas avisan que, incluso aunque la condena se ratifique, pasarán varios años antes de que el dinero llegue a los medios.

Rivales directos

Con todo, es el fondo de la sentencia el que reordena el tablero digital. Al condenar a Meta por competencia desleal, el tribunal asume que medios de comunicación y plataformas digitales compiten por el mismo mercado publicitario. Que son competencia directa, pero que Meta jugaba con las cartas marcadas.

Se trata de algo que los editores de los medios de comunicación llevaban años reclamando, al denunciar que habían quedado a merced de gigantes estadounidenses como la propia Meta o Google como meros proveedores de contenidos. Gigantes que pueden cerrarles la llave del tráfico y, por tanto, de los ingresos, con tan solo pulsar un botón, a pesar de que compiten en el mismo mercado.

Meta rechaza de plano esta posibilidad. Asegura que la idea de que existe una "unidad de mercado" en la publicidad online no refleja la realidad del sector y que no es posible asumir

que cualquier aumento de sus ingresos se produzca a costa de reducir los de los medios de comunicación. En una explicación que pide que no sea citada textualmente, dice que esa visión no tiene en cuenta, por ejemplo, la inversión que ha realizado a lo largo de los años en herramientas y tecnología para mejorar la eficacia de su servicio publicitario.

Esa defensa, sin embargo, choca con la nueva doctrina que se está abriendo paso en Europa. Bruselas acaba de abrir una investigación contra Google precisamente por abusar de su posición para asfixiar los ingresos de la prensa, penalizando en el buscador a aquellos medios que incluyen contenidos de socios comerciales. "Puede afectar a la libertad de los editores para llevar a cabo negocios legítimos", advierte la Comisión Europea.

El nuevo marco entre medios y gigantes tecnológicos

Aún está por ver el recorrido que esta sentencia tendrá en España, puesto que podría hacerse más grande. Fuentes de CLABE (Club Abierto de Editores), la patronal que integran buena parte la mayoría de medios nativos digitales españoles —como elDiario.es— avanzan que están estudiando diversas posibilidades, como personarse en las próximas instancias judiciales.

Todo el proceso se encuadra en un movimiento más grande, pero no solo por la citada investigación de la UE. La pasada primavera, un grupo de 67 grupos mediáticos franceses demandó a Meta inspirándose por la acción de AMI. Ahora, su victoria podría hacer que demandas como estas se repliquen contra los gigantes tecnológicos por todo el continente.

Las reacciones a esta impugnación general del *statu quo* entre los medios y las plataformas podrían ser imprevistas. En 2014, Google News se retiró de España para no pagar el canon AEDE. Meta hace tiempo que cortó relaciones con los medios, pero en otros países ha llegado a bloquear todos los enlaces de noticias en protesta por regulaciones que no la satisfacían, como Canadá o Australia. Actualmente, la corporación tampoco permite la publicidad política en la UE, negándose a aceptar las nuevas normas que la regulan.

Las grandes tecnológicas cuentan con otro último recurso. Donald Trump ha amenazado en repetidas ocasiones con tomar represalias contra los países que intenten "sacar dinero" a sus corporaciones mediante impuestos digitales o multas antimonopolio. Si el conflicto escala, la batalla por la supervivencia de los medios dejará de ser solo una disputa mercantil para convertirse en una pieza más en el tablero de la guerra comercial.

Quisimos entrevistar a esta exdirectiva de Facebook. Mark Zuckerberg no lo ha permitido

Sarah Wynn-Williams, ex jefa de Políticas Públicas de Facebook, ha publicado un libro sobre el comportamiento "irresponsable" de la empresa y de su fundador. Pero la compañía ha logrado vetar legalmente que hable sobre él

— Directivos trumpistas y narrativa ultra: el giro de Zuckerberg que va más allá del fin de los verificadores

Carlos del Castillo

SEGUIR AL AUTOR/A

17 de julio de 2025 22:18 h
Actualizado el
18/07/2025 12:32 h
22

"Trabajé allí durante siete años y, si tuviera que resumirlos en una sola frase, diría que empezó siendo una farsa esperanzadora y acabó en una tragedia llena de oscuridad y arrepentimiento. Yo era una de las personas que asesoraban a la cúpula de la empresa, Mark Zuckerberg y Sheryl Sandberg, mientras ellos ingeniaban cómo negociaría Facebook con los Gobiernos del planeta. Al final contemplé desesperanzada cómo se plegaban ante regímenes autoritarios como China y engañaban a la opinión pública como si nada".

Es un fragmento de las memorias de Sarah Wynn-Williams, la que fuera directora de Políticas Públicas de Facebook de 2011 a 2018, su momento de máxima expansión. Esta diplomática neozelandesa acaba de publicar *Los irresponsables* (Editorial Península), donde denuncia la cultura de poder, encubrimiento y abuso dentro de la compañía hoy renombrada como Meta.

La autobiografía de Wynn-Williams habla de las ambiciones de poder de Mark Zuckerberg, del falso idealismo de la cúpula y buena parte de la plantilla, de las presiones políticas, de la censura y de cómo todo esto se mezcló para crear Facebook, una corporación que priorizó el crecimiento y el beneficio económico por encima de cuestiones éticas que afectaban a miles de millones de personas.

Su valor es el de testimonio directo, una mirada desde dentro y con abundantes detalles tanto a una empresa tecnológica clave en la revolución digital, como a su fundador, la

segunda persona más rica del mundo, y sus principales colaboradores. "Volaba en el jet privado de Mark el día en que por fin entendió que probablemente Facebook había colocado a Donald Trump en la Casa Blanca", resume la propia autora.

El libro, sin embargo, no incluye ningún hecho que no hubiera salido ya a la luz. Facebook ha sido una de las empresas más escrutadas del planeta y sus vergüenzas han sido levantadas tanto desde fuera como desde dentro. No hay noticias escabrosas en las páginas de *Los irresponsables*. Pese a ello, la compañía ha prohibido a Wynn-Williams hablar del libro o hacer cualquier declaración sobre él. El día siguiente a su publicación en inglés (12 de marzo) invocó una cláusula de no difamación que la autora firmó al salir de la compañía para censurarla.

"La autora no está disponible para entrevistas a causa de la orden provisional de un tribunal de arbitraje estadounidense que, a petición de Mark Zuckerberg, le prohíbe hacer cualquier tipo de promoción del libro", lamenta la editorial.

Desde entonces Wynn-Williams se ha mantenido en silencio. Meta lo ha hecho todo por ella, generando un efecto Streisand de manual sobre su libro: se convirtió en un *best seller* del New York Times llegando al número 1 de su lista de no ficción, fue número 3 en biografías Amazon o número 2 de Apple Books en la lista de libros de pago. En el Reino Unido ha vendido más de 100.000 copias y ha sido traducido al castellano en tiempo récord: ha salido a la venta esta semana.

¿Por qué ahora?

Han pasado más de ocho años desde la salida de Wynn-Williams de la corporación de redes sociales. Su libro, sin duda, habría sido mucho más útil entonces que ahora. El escándalo de manipulación electoral de Facebook y Cambridge Analytica estalló en marzo de 2018. "En Estados Unidos, pusieron a trabajadores de Facebook a disposición de la campaña de Trump para ayudarlo a organizar la guerra de la desinformación, el troleo y las mentiras que le dieron la victoria en las elecciones", revela.

Mientras, en verano de ese mismo año la ONU empezó a documentar que la red social tampoco había sido capaz de detectar los llamamientos a la violencia contra los rohingya en Myanmar. Su algoritmo amplificó el odio y permitió que el ejército birmano usara la plataforma para incitar al genocidio.

La empresa tardó meses en reaccionar y acabó reconociendo que no hizo lo suficiente, entre otras cosas porque no contaba con suficientes moderadores que hablaran birmano. La violencia contra los rohingya terminó con más de 25.000 muertos y cerca de 700.000 personas obligadas a huir a Bangladés, según estimaciones de Naciones Unidas. Un genocidio retransmitido en directo en la mayor red social del mundo sin que esta se diera cuenta de lo que ocurría.

> ***"La responsable del caso me dijo que no creía que infringiera nuestras normas, pero que no podía encontrar a nadie que hablara birmano y Google Translate no traducía del birmano, así que no podía asegurarlo a ciencia cierta"***

Wynn-Williams también habla de estos hechos en el libro, con información que habría sido muy relevante en su momento. "Estaban provocando violencia real —seguía habiendo disturbios, las turbas budistas estaban atacando los negocios musulmanes, había muertos—, así que parecía estar claro que infringían nuestros estándares. Pero el equipo de operaciones de contenidos, con sede en Dublín, no quería eliminar las publicaciones. La responsable del caso me dijo que no creía que infringiera nuestras normas, pero que no podía encontrar a nadie que hablara birmano y Google Translate no traducía del birmano, así que no podía asegurarlo a ciencia cierta", narra.

"Recurrí a su superior, un hombre que se puso en contacto con el mismo trabajador externo que habían contratado hacía unos meses —un birmano con residencia en Dublín— para que revisara el material. Pasaron cinco horas", continúa: "*¿Cuánto crees que tardará?*, pregunté. Había disturbios en las calles por culpa de aquello. Necesitaba que se eliminaran esas publicaciones. *Me temo que no lo sé* —respondió mi contacto en Dublín—. *No está conectado. Le he mencionado en Facebook y espero que lo vea y se ponga en contacto conmigo*".

"Cuando hay gente muriendo, ese no puede ser el sistema al que tenga que recurrir Facebook", lamenta su ex directora de Políticas Públicas.

Con todo, hay incluso un aspecto más en el libro sobre el que Wynn-Williams podría haber alertado al resto de la sociedad. Es un problema que está revelándose ahora en su gravedad real: la voluntad de parte de la junta directiva de Facebook de potenciar los discursos de extrema derecha en su beneficio.

> ***"Uno de los miembros de la junta sugirió a nuestra cúpula, en su mayoría judía, que a Facebook le conviene estrechar lazos con los partidos políticos de la extrema derecha en Europa porque el poder se está desplazando hacia ahí"***

"Uno de los miembros de la junta sugirió a nuestra cúpula, en su mayoría judía, que a Facebook le conviene estrechar lazos con los partidos políticos de la extrema derecha en Europa porque el poder se está desplazando hacia ahí", revela: "En su propuesta, el susodicho miembro de la junta sugería aprovechar el apoyo electoral y las herramientas para hacer campaña que ofrecíamos a los candidatos presidenciales estadounidenses (y que Donald Trump estaba usando de manera agresiva en su campaña de 2016) y ofertárselos a Alternativa por Alemania, la extrema derecha alemana, y a Marine Le Pen y el Frente Nacional, la extrema derecha francesa".

"Acercarse a estos partidos políticos y ayudarlos a llegar al poder sería la manera más eficaz de evitar que los Gobiernos regularan Facebook", propuso el directivo, según el relato de Wynn-Williams. La autora también escribe que la plataforma sabía de la existencia de más de doscientos grupos extremistas en la plataforma que violaban las normas de discurso de odio, pero que hizo "apenas nada" para eliminarlos.

Si Wynn-Williams tenía toda esta información, ¿por qué ha esperado ocho años para alertar de ello al resto de la sociedad? Esta sería una de las principales preguntas a realizar en una entrevista, que Meta no permite que se celebre.

> ***“Siguen siendo gente descuidada. Le han cambiado el nombre a la empresa, de Facebook a Meta. Pero los leopardos no cambian de manchas. El ADN de la empresa sigue siendo el mismo. Y cuanto más poder tienen, más irresponsables se vuelven”***

La exdirectiva argumenta en el libro que la motivación para publicarlo en 2025 es impedir que Meta siga comportándose como hasta ahora, también durante la revolución de la inteligencia artificial. "Siguen siendo gente descuidada. Le han cambiado el nombre a la empresa, de Facebook a Meta. Pero los leopardos no cambian de manchas. El ADN de la empresa sigue siendo el mismo. Y cuanto más poder tienen, más irresponsables se vuelven", avisa.

"Estuve presente en los primeros encuentros de tanteo entre Mark y los mandatarios mundiales. Y fui testigo de la exploración y del acopio de un poder que ha seguido expandiéndose. En la actualidad, Meta es una de las empresas más poderosas del mundo. Y avanzamos por la dirección que ha señalado. Vivimos en un mundo al que han dado forma estas personas y su indiferencia letal. Por no hablar del futuro. Si no abordamos lo que ya se ha encubierto, repetiremos los errores de Facebook", concluye.

¿Qué dice Meta?

Básicamente, que todo lo escrito en *Los irresponsables* es mentira o está sacado de contexto. Preguntada por elDiario.es, la compañía se remite al comentario oficial que hizo cuando pidió al Tribunal de Arbitraje que lo parara. "Esta sentencia confirma que el libro falso y difamatorio de Sarah Wynn-Williams nunca debió publicarse. Esta urgente acción legal se hizo necesaria porque Williams, más de ocho años después de ser despedida por la empresa, ocultó deliberadamente la existencia de su proyecto de libro y evitó el proceso estándar de verificación de datos de la industria con el fin de apresurarse a publicarlo en las estanterías después de esperar ocho años", declara.

Sin embargo, lo que afirma Meta en esa declaración no está sustentado por lo que dice la resolución de arbitraje publicada. El árbitro no ha entrado a valorar la validez del contenido, solo determinó que existía un riesgo contractual y legal por incumplimiento de la cláusula de no difamación, lo cual justificó la medida cautelar de bloquear las entrevistas de Wynn-Williams.

En concreto, el laudo prohíbe a Sarah Wynn-Williams promocionar el libro y hacer "comentarios despectivos, críticos o perjudiciales" sobre Meta, sus ejecutivos o sus trabajadores. También le obliga a eliminar los comentarios en esta línea que haya realizado previamente y estén bajo su control. Pero no hace valoraciones sobre la veracidad de la obra. La resolución es, además, temporal, solo hasta que se resuelva si *Los irresponsables* viola efectivamente la cláusula que su autora firmó con Meta.

Andy Stone, el jefe del equipo de Comunicación de Meta, recopiló en su momento las impresiones de una decena de ejecutivos y trabajadores de la compañía que apoyaron en redes sociales el posicionamiento de esta, destacando las "exageraciones" de libro o contradiciendo el punto de vista de su autora en algunos aspectos.

Las declaraciones de Wynn-Williams, no obstante, están en línea con otros ex ejecutivos de la compañía que han decidido levantar la voz. Filtradores como Arturo Béjar, que destapó en entrevistas y en el Congreso de EEUU la desprotección de Meta con los menores de edad; o Frances Haugen, cuyo testimonio sirvió de base para lanzar una investigación a gran escala contra la compañía.

También resulta llamativo que la compañía evoque a la "verificación de datos de la industria" para afear la publicación del libro. Se trata del mismo mecanismo que Mark Zuckerberg ha eliminado de todas sus redes sociales para congraciarse con Donald Trump y la extrema derecha internacional, que llevaban años con profesionales en su punto de mira.

Una comedia trágica

Wynn-Williams escribe sobre un período clave en la historia de Internet. Los movimientos de Facebook en la pasada década han ayudado a definir la red de hoy y la redistribución del poder hacia las manos de uno pocos tecno-oligarcas, inmortalizados en la fotografía de la toma de posesión de Donald Trump.

Pero no hay épica en su relato. Más bien, como ella misma reconoce, su historia es una comedia trágica. "La mayoría de los días, trabajar en temas políticos para Facebook tenía mucho menos de interpretar capítulos que parecían redactados por Maquiavelo y mucho más de cuidar de una pandilla de chavales de catorce años a los que les habían dado superpoderes y una suma impía de dinero mientras volaban alrededor del mundo intentando comprender qué les había otorgado y comportado ese poder", avisa.

El libro de Wynn-Williams está lleno de anécdotas y situaciones que justifican esa declaración, pero ella no puede hablar abiertamente de ellas. Meta dice que todo es falso, pero que haya tratado su libro como una amenaza puede que termine revelando más sobre la empresa que muchas de sus páginas.

Una exdirectiva de Facebook dirigirá el regulador de privacidad de las grandes tecnológicas de EEUU en Europa

La nueva jefa de la autoridad irlandesa de protección de datos, encargada de vigilar a Meta, Google, Apple o Amazon en Europa, fue responsable de Políticas Públicas en la corporación de Mark Zuckerberg

Hemeroteca — Qué está pasando en las agencias de privacidad y por qué Bruselas las va a atar en corto

Carlos del Castillo

SEGUIR AL AUTOR/A

18 de septiembre de 2025
22:48 h
Actualizado el
19/09/2025 05:30 h
4

El Gobierno irlandés ha nombrado a Niamh Sweeney, ex responsable de Políticas Públicas de Facebook y WhatsApp, como nueva comisionada de la Data Protection Commission (DPC), el regulador de privacidad del país. Este organismo es también la autoridad encargada de investigar las violaciones de la normativa de protección de datos de la propia Meta en la UE, así como de Google, Apple, Amazon o Microsoft, que tienen sus sedes europeas en suelo irlandés.

Sweeney asumirá el cargo el 13 de octubre y se convertirá en la tercera comisaria del ente, cuya dirección es tricéfala. Su mandato durará cinco años y se espera que sea aún más importante que los anteriores. "A partir de 2026, la DPC asumirá importantes responsabilidades de autoridad de vigilancia del mercado en relación con ciertos sistemas de IA de alto riesgo, incluidos los de aplicación de la ley y la biometría", ha afirmado Jim O'Callaghan, ministro de Justicia del país.

Los otros dos comisarios asumieron sus cargos en febrero de 2024. Son abogados que han ha ocupado diferentes cargos en el Ministerio de Justicia y en el DPC. Sweeney, por su parte, trabajó casi ocho años en Meta, primero como jefa de Políticas Públicas en Irlanda y después como directora de políticas de WhatsApp para Europa, Oriente Medio y África, en plena etapa del escándalo de Cambridge Analytica.

"A medida que las responsabilidades y el alcance de la DPC continúan creciendo, me complace que estos tres comisionados ahora dirijan y gestionen este organismo regulador clave", ha agregado O'Callaghan, durante el nombramiento de Sweeney.

La posición de la exdirectiva de Facebook será clave para la aplicación de las leyes de protección de datos del continente. Las grandes tecnológicas eligieron Irlanda para ubicar su sede europea por motivos principalmente fiscales: el país ofrece un impuesto de sociedades del 12,5%, muy por debajo de la media de la Unión Europea. Esa concentración de sedes en Dublín y sus alrededores ha convertido a la autoridad irlandesa de protección de datos en el regulador de facto de casi todas las multinacionales digitales en Europa, incluyendo otras como Airbnb, Oracle, IBM, Intel o TikTok.

Multas bajas y lentas

Sweeney llega a un DPC cuyo historial de investigaciones y sanciones está marcado por la lentitud y la baja cuantía de las multas que decide imponer a estas empresas. El Supervisor Europeo de Protección de Datos de la UE, con sede en Bruselas, llegó a corregir una de sus sanciones a Meta tras considerar que la autoridad irlandesa había sido demasiado laxa con la multinacional. Leonardo Cervera, secretario general del Supervisor, calificó en una entrevista con elDiario.es que esta falta de resoluciones como "lamentable".

Pero cuando las multas son firmes, el DPC tampoco es el más estricto a la hora de exigir a las empresas que las abonen. Según una información del *Irish Times*, a finales de 2024 el organismo solo había cobrado 20 millones de euros de los 3.256 millones en multas emitidas desde 2020. "El importe total pagado representa tan solo el 0,6% de las sanciones impuestas por la DPC, la mayoría de las cuales se refieren a las grandes tecnológicas", destacó el principal periódico de Irlanda.

Un portavoz del organismo aseguró que este retraso se debe a que muchas de las resoluciones han sido recurridas en los tribunales. El dinero recaudado por las multas, de categoría administrativa, va a parar directamente a las arcas del Estado irlandés.

"El Gobierno irlandés ya ni siquiera finge"

El abogado y activista Max Schrems, que ha tumbado en los tribunales varios acuerdos de transferencia de datos entre la UE y Estados Unidos que lesionaban los derechos de los europeos, ha criticado con dureza el nombramiento. "Durante 20 años Irlanda ha evitado aplicar de forma efectiva el Reglamento General de Protección de Datos (RGPD), pero al menos lo hacía en secreto. Ahora directamente pone a una exlobista de Meta a dirigir el organismo", ha afeado.

Schrems y Noib, la ONG que dirige, son dos de los actores clave en la protección de datos europea. Sus denuncias contra las prácticas abusivas de las grandes tecnológicas no solo han hecho caer esos acuerdos de transferencia de datos entre Washington y Bruselas, sino que también han llevado a cientos de multas para estas empresas. "Durante años, siempre había alguna supuesta ‘razón’ o ‘problema’ por la que ‘desgraciadamente’ la DPC no podía aplicar la legislación europea en Irlanda. Hemos pasado meses en los tribunales por esas

supuestas razones y problemas, sabiendo que todo respondía a un guion político. Ahora el Gobierno irlandés ni siquiera finge", ha declarado.

"Estamos siendo testigos de una época en la que ya no basta con contentar a las grandes tecnológicas de EEUU en privado. EEUU exige que los países europeos se inclinen ante ellas públicamente", ha afeado.

Meta utilizará a partir de hoy todos los datos de las conversaciones con su IA para personalizar sus anuncios

La propietaria de Facebook e Instagram es la primera que incorpora los chats con la inteligencia artificial como una herramienta más para extraer información con la que segmentar la publicidad

— OpenAI también ha abierto la puerta a usar ChatGPT con este fin

Carlos del Castillo

SEGUIR AL AUTOR/A

16 de diciembre de 2025
11:32 h
Actualizado el
16/12/2025 11:32 h
2

El logo de Meta AI y las redes sociales de Meta EP

Se acabó el periodo de gracia. Desde este martes 16 de diciembre, Meta ha activado oficialmente su maquinaria para monetizar las conversaciones que los usuarios mantienen con su inteligencia artificial. A partir de hoy, todas las interacciones con los asistentes de IA en sus plataformas pasan a convertirse en datos comerciales que alimentan su algoritmo publicitario.

Hasta ahora, la corporación no utilizaba los mensajes de los usuarios con Meta AI, como el chat integrado en WhatsApp, para personalizar los anuncios que estos veían en el resto de plataformas. A partir de hoy, esa barrera cae. La tecnológica ha integrado estas interacciones en el mismo paquete de datos que el historial de navegación o los "me gusta" en sus redes.

"Por ejemplo, si chateas con Meta AI sobre senderismo, podríamos saber que te interesa, igual que si publicas un *reel* [un vídeo corto de Instagram] sobre senderismo o le das "me gusta" a una página relacionada. Como resultado, podrías empezar a ver recomendaciones de grupos de senderismo, publicaciones de amigos sobre rutas o anuncios de botas de montaña", detalla la compañía dirigida por Mark Zuckerberg.

En su comunicado, Meta justifica su decisión con el argumento de que "muchas personas esperan que sus interacciones hagan que lo que ven sea más relevante". "Al igual que otros servicios personalizados, adaptamos los anuncios y el contenido que ves en función de tu actividad, garantizando que tu experiencia evolucione a medida que cambian tus intereses", continúa.

El negocio publicitario de la compañía se basa en configurar amplias bases de datos personales a partir de miles de señales de comportamiento de sus usuarios. Desde las páginas que siguen o los contenidos con los que interactúan, hasta inferencias sobre sus intereses, sus hábitos de consumo o sus momentos vitales. Con esta información, los anunciantes pueden dirigir sus campañas a personas con una alta probabilidad de estar interesadas en un producto o servicio. La incorporación de las conversaciones con la IA añade una nueva fuente de señales, mucho más rica y explícita, a ese sistema de segmentación.

Un analista de mercado en tiempo real

Meta, que ha quedado rezagada respecto a otras desarrolladoras de IA como OpenAI (ChatGPT) o Google (Gemini), es la primera que da el paso definitivo para utilizar las conversaciones con estos sistemas para extraer datos publicitarios. No obstante, incluso la propia OpenAI ha abierto la puerta a ese modelo de negocio en los últimos tiempos ante las dificultades para consolidar una línea de beneficios estable basada en el uso corporativo de la IA.

Se trata de una situación que preocupa a los especialistas, debido a que los chats con la inteligencia artificial son una herramienta de extracción de datos personales mucho más poderosa que las propias redes sociales de Meta o el buscador de Google, las dos multinacionales que dominan la publicidad digital. "Todo apunta a que estamos montando un complejo industrial como el de las redes sociales, pero peor aún", explicaba Enrique Dans, profesor de Innovación y Tecnología en IE Business School, en un reciente reportaje de este medio.

"¿Qué son las redes sociales en realidad? Son máquinas de capturar datos para luego venderlos al mejor postor. ¿Qué pasa si en lugar de simplemente dar *me gusta* o poner un comentario, lo que haces es estar todo el día hablando con esa máquina? Pues que le das todos los datos del mundo", continuaba el experto.

En el caso de Meta, la medida afectará a las interacciones con su IA en todas sus plataformas. También a aquellas realizadas desde las Meta Ray-Ban, las gafas de la compañía con cámaras, micrófonos y altavoces pensadas para retransmitir en tiempo real y diseñadas, precisamente, para ser utilizadas a través de comandos de voz.

El único límite será el chat de WhatsApp con Meta AI. Si un usuario no tiene vinculada su cuenta de WhatsApp con las de Facebook o Instagram en su "Centro de Cuentas", las conversaciones que mantenga con la IA dentro de la aplicación de mensajería no se utilizarán para personalizar los anuncios en las otras redes sociales.

La compañía también ha comunicado que, como obliga la Unión Europea, los datos sensibles no se utilizarán para el perfilado publicitario. "Cuando las personas conversan con Meta AI sobre temas como sus opiniones religiosas, orientación sexual, opiniones políticas, salud, origen racial o étnico, creencias filosóficas o afiliación sindical, no utilizamos esos temas para mostrarles anuncios", avanza.

Adiós al Metaverso

El movimiento para convertir su IA en una herramienta más para la extracción de datos personales llega justo cuando Zuckerberg ha decidido empezar a cortar el grifo de lo que un día creyó que sería el futuro de su corporación. Según fuentes internas citadas por Bloomberg, Meta planea recortar los recursos destinados al Metaverso hasta un 30% el próximo año, con una ronda de despidos que podría ejecutarse tan pronto como en enero.

El proyecto del Metaverso, que llegó a propiciar el cambio de imagen de marca de la compañía de Facebook a Meta, era ese universo virtual que prometía trabajo, ocio y socialización en 3D mediante realidad virtual. Tras miles de millones invertidos, sigue siendo un proyecto con baja adopción y resultados muy por debajo de los objetivos que Zuckerberg comunicó inicialmente.

La división Reality Labs de Meta, encargada de desarrollarlo, acumula pérdidas superiores a los 70.000 millones de dólares desde 2021. Unos recursos que ahora se destinarán a otros proyectos como las gafas de realidad aumentada que Zuckerberg presentó en septiembre. Un dispositivo que también se basa en las interacciones con la inteligencia artificial que, desde hoy, Meta utilizará para nutrir su negocio publicitario.

X empieza a vender datos de usuarios para entrenar inteligencias artificiales en medio de la fuga hacia Bluesky

La red social de Elon Musk activa un cambio de políticas que le permite enviar información personal a terceras empresas para que entrenen sus propios algoritmos

— Qué es Bluesky, el Twitter anti-magnates que gana millones de usuarios tras la victoria de Trump

Carlos del Castillo

SEGUIR AL AUTOR/A

15 de noviembre de 2024
11:48 h
Actualizado el
15/11/2024 13:37 h
17

Elon Musk en un evento electoral de Trump en Butler, Pensilvania, el 5 de octubre de 2024.

Este 15 de noviembre ha entrado en vigor un cambio en las políticas de privacidad de X (más conocida como Twitter) por el que la compañía se reserva el derecho de vender datos personales de sus usuarios a terceras empresas para que estas entrenen sus propios modelos de inteligencia artificial. La modificación, que no se ha comunicado directamente a los usuarios, coincide con la aceleración de registros de miembros de X en Bluesky, una red de funcionamiento muy similar pero basada en un protocolo descentralizado.

"Si continúa utilizando nuestros productos o servicios a partir del 15 de noviembre de 2024, estará aceptando los términos de servicio y la política de privacidad actualizados", notificó la red social propiedad de Elon Musk en una entrada de blog publicada en octubre.

El nuevo capítulo de la política de privacidad se denomina "colaboradores de terceros". "Dependiendo de su configuración, o si decide compartir sus datos, podremos compartir o divulgar su información con terceros", desglosa el texto modificado: "Si no opta por no participar, en algunos casos los destinatarios de la información pueden usarla para sus propios fines independientes, además de los establecidos en la política de privacidad de X, incluido, por ejemplo, para entrenar sus modelos de inteligencia artificial, ya sean generativos o de otro tipo".

Para desactivar el envío de datos personales recogidos por X a terceras empresas con dichos fines, es necesario desactivar esta opción desde el panel de configuración de la app.

En el apartado "Privacidad y seguridad" hay una sección denominada "Intercambio y personalización de datos". Dentro de esta última, es necesario dirigirse a "Datos compartidos con socios comerciales" y desactivar la pestaña referida a las transferencias especiales de datos que pueden derivarse al entrenamiento de la IA.

Cabe destacar que esto no cancela por completo el envío de cualquier dato a otras empresas, puesto que "X siempre comparte información con socios comerciales para que sus productos funcionen y puedan mejorarse", como explica la red social en dicho apartado. Desactivar la pestaña solo afecta a la "información adicional" que puede usarse para nutrir las bases de datos de los algoritmos generativos.

X también está utilizando los datos de sus usuarios para entrenar su propia IA, Grok, que solo está disponible para los miembros de pago. No obstante, también puede desactivarse. La pestaña para ello se encuentra también en el apartado "Privacidad y seguridad" de la app, dentro de la última sección, denominada "Grok".

A pesar de avisar frecuentemente sobre los riesgos de la IA, Elon Musk es una de las figuras que más ha incursionado en el negocio de los asistentes virtuales basados en esta tecnología. Estuvo en el equipo fundador de OpenAI, desarrolladora de ChatGPT. Tras verse fuera de la empresa por incompatibilidades con su papel en Tesla fundó XAI, la creadora de Grok.

Su asistente quiere diferenciarse del resto por un mayor uso del humor y el sarcasmo. Según ha explicado Musk, Grok está inspirado en personajes como Jarvis de *Iron Man* o Marvin de *La guía del autoestopista galáctico*, y afirma que ofrece respuestas entretenidas y "rebeldes".

Todas estas tecnologías se basan en el contenido subido por los usuarios a Internet durante años para su entrenamiento. En esta ocasión las nuevas políticas han coincidido con el trasvase de usuarios de X hacia Bluesky, cuyo modelo de negocio evita recoger datos personales de los usuarios. Este jueves la plataforma, que en menos de un año abierta al público general ha ganado 16 millones de usuarios, sumó un récord más de un millón de registros en 24 horas.

Elon Musk paga 300 millones para que su inteligencia artificial entre en Telegram

Pável Dúrov anuncia un acuerdo para que Grok se integre de forma obligatoria en la app de mensajería y acceda a los datos de los usuarios que interactúen con ella

— La inteligencia artificial ya se usa para coaccionar gobiernos. ¿Estamos preparados?

Carlos del Castillo

SEGUIR AL AUTOR/A

29 de mayo de 2025
10:27 h
Actualizado el
29/05/2025 12:28 h
26

Elon Musk, propietario de X y de xAI, y Pável Dúrov, fundador y dirigente de Telegram

300 millones al año. Es el precio que ha aceptado pagar Elon Musk para que Grok, la polémica inteligencia artificial de X, pueda entrar en Telegram. Así lo ha comunicado el propio Pável Dúrov, fundador y dirigente de la app de mensajería, a través de un mensaje en su canal oficial. Ni Musk ni xAI, la empresa de su propiedad que desarrolla el sistema, han confirmado aún la noticia, aunque el magnate se encuentra en este momento inmerso en su salida definitiva del Gobierno de EEUU.

"Este verano, los usuarios de Telegram tendrán acceso a la mejor tecnología de IA del mercado. Elon Musk y yo hemos acordado una asociación de 1 año para llevar el chatbot Grok de xAI a nuestros más de mil millones de usuarios e integrarlo en todas las apps de Telegram", ha comunicado Dúrov, que ha regresado recientemente a Dubai después de que las autoridades francesas le permitieran salir del país, donde está siendo investigado por varios delitos relacionados con la app de mensajería.

El multimillonario de origen ruso, del que se ha revelado que mintió sobre su supuesto exilio de su país de origen, ha destacado la relevancia económica que el acuerdo con Musk tendrá para su plataforma. "Esto también fortalece la posición financiera de Telegram: recibiremos 300 millones de dólares en efectivo y capital de xAI, además del 50% de los ingresos de las suscripciones de xAI vendidas a través de Telegram", ha avanzado.

La entrada de Grok en Telegram es la primera integración oficial de la IA de Musk con una plataforma que no le pertenezca a él o a sus empresas. Hasta este momento, Grok solo estaba disponible en plataformas controladas por Musk, como la red social X, donde puede ser invocada por los usuarios en cualquier debate o publicación para que responda preguntas o aporte contexto.

El objetivo del acuerdo es que Grok pueda usarse de la misma forma en Telegram. Los usuarios verán un chat con esta IA anclado en la parte superior de su lista de conversaciones. Desde allí, podrán interactuar con él como un chatbot convencional, haciendo consultas o solicitando la generación de contenidos, como informes o imágenes.

Grok también estará disponible también para interactuar en el resto de chats. De esta forma, se le podrá pedir que resuma un mensaje largo, un documento o un enlace externo compartido con otro usuario, que mejore la redacción de los mensajes antes de enviarlos o que compruebe la veracidad de las aseveraciones de un determinado chat, según se muestra en un vídeo que ha compartido posteriormente Dúrov.

Ninguna de las plataformas implicadas ni sus líderes ha aclarado qué tipo de acceso a datos personales de usuarios de Telegram tendrá Grok, ni si estos se utilizaran para su posterior entrenamiento. No obstante, el uso de este tipo de funciones, ya sea realizadas por el propio usuario o por sus contrapartes en chats privados o grupales, implica el procesamiento de la información en los servidores de Grok propiedad de Musk.

"Para ser claros, xAI solo accederá a los datos que los usuarios de Telegram compartan explícitamente con Grok a través de interacciones directas. Eso es lo esperado: no puedes enviar mensajes a nadie (incluido un chatbot) sin compartir lo que escribes", ha explicado Dúrov en respuesta a las dudas de los usuarios. "La privacidad del usuario es primordial", ha asegurado.

Tras el escándalo de Sudáfrica

El acuerdo llega justo después de uno de los mayores escándalos de manipulación relacionados con Grok. Tras una alteración de su programación que xAI calificó con un error de un empleado, el sistema empezó a difundir contenido sobre un supuesto "genocidio blanco" en Sudáfrica en miles de respuestas no solicitadas por los usuarios. Se trataba de una narrativa que Musk había estado utilizando para atacar al Gobierno de su país natal a cuenta de Starlink, su compañía de internet satelital.

El motivo era la negativa de la administración a permitirle saltarse la ley que obliga a las empresas extranjeras a ofrecer acciones a comunidades discriminadas durante el apartheid para operar en el país. Después del fallo a gran escala de Grok y la posterior encerrona de Donald Trump en la Casa Blanca siguiendo la misma narrativa, Pretoria ha aceptado modificar la norma para cambiar esa venta de acciones por programas de formación a comunidades desfavorecidas.

Dúrov, por su parte, que se ha declarado libertario y ha defendido la mensajería cifrada como razón de ser de Telegram, pone ahora los datos de los usuarios a disposición de Elon Musk. Además, según ha explicado Dúrov, la integración de Grok será obligatoria para todos los usuarios y apps de Telegram.

ENTREVISTA | KAREN HAO

La investigadora que destripa el mito de OpenAI y Sam Altman: “Las multinacionales de IA aceleran el retroceso democrático”

La periodista Karen Hao desentraña en 'El Imperio de la IA' cómo estas empresas replican dinámicas coloniales, “extrayendo una cantidad extraordinaria de recursos, explotando una cantidad extraordinaria de mano de obra y participando en actividades que no benefician en nada a la mayoría”

— Tres años de ChatGPT: la máquina que no pudo quitarte el trabajo ahora va a por tus secretos

Carlos del Castillo

SEGUIR AL AUTOR/A

16 de diciembre de 2025
21:39 h
Actualizado el
19/12/2025 12:22 h
18

Karen Hao, autora de 'El imperio de la IA' Shoko Takayasu

Hace tres años, OpenAI era una organización prácticamente desconocida para el gran público que aspiraba a contrarrestar el poder de los gigantes de Silicon Valley. Hoy, es la startup más valiosa de la historia, superando los 500.000 millones de dólares. Tres años en los que la compañía dirigida por Sam Altman ha pasado de presentarse como un laboratorio tecnológico que trabajaba por el bien de la humanidad a convertirse en una empresa privada con agenda geopolítica propia, con acceso masivo a información personal de millones de personas y trato preferente con los poderes públicos.

La periodista estadounidense Karen Hao ha cubierto esta transformación para medios como el *Wall Street Journal* o el *MIT Technology Review*. En su libro *El Imperio de la IA. Sam Altman y su carrera por dominar el mundo* (editorial Península), Hao ha investigado cómo OpenAI y la industria de la IA han pasado a funcionar con una lógica imperial: colonizan recursos, extraen datos de los usuarios y explotan mano de obra precaria en el Sur Global para alimentar una maquinaria que, denuncia, está "acelerando el retroceso democrático en todo el mundo".

En esta entrevista con elDiario.es, Hao describe a OpenAI, los secretos de su líder y la burbuja financiera y de expectativas que está impulsando el desarrollo de la inteligencia artificial.

Cuenta en el libro que, en sus orígenes, OpenAI se veía a sí misma como la "anti-Google". ¿En qué consistía esa visión de empresa inicial?

En realidad creo que la visión de la compañía en aquel entonces era similar a la que es hoy: OpenAI siempre ha querido dominar el desarrollo de la IA y ser el líder número uno en esta tecnología. En ese momento, Google era el único actor al que valía la pena vencer, así que se veían a sí mismos como su único competidor, y a Google como el único al que debían intentar superar. Por eso se concibieron a sí mismos como la anti-Google que iba a representar todo lo que Google no era. Otra razón por la que hicieron eso fue porque era una táctica de reclutamiento. Inicialmente, para construir un laboratorio de IA líder, el principal cuello de botella era el talento, por lo que querían averiguar cómo conseguir que la gente dejara Google y se uniera a OpenAI, o eligiera OpenAI sobre Google si se postulaban para trabajar en ambas empresas. Así que lo plantearon todo como: "bueno, Google es de código cerrado, nosotros seremos abiertos; Google trabaja con fines de lucro, nosotros seremos sin fines de lucro". La idea era: *si quieres crear productos para un megagigante, bien, ve a Google, pero si vienes a OpenAI, podrás cambiar el mundo.*

¿Cómo se ven dentro de OpenAI esas contradicciones respecto a la visión inicial, con la transformación en una empresa privada con ánimo de lucro? ¿Crees que puede haber alguien que piense que al final se han convertido en todo aquello que prometieron cambiar?

Sí, por supuesto, OpenAI aparentemente ha revertido por completo todo lo que dijo que sería. Ahora es, obviamente, una empresa con fines de lucro en lugar de una organización sin ánimo de lucro, y la startup más valiosa del mundo en este momento, con una valoración de 500.000 millones de dólares. También se ha vuelto hipersecreta, aunque originalmente dijo que sería transparente. Así que, en esas formas más superficiales, ha cambiado por completo. Y, sin embargo, sigue persiguiendo exactamente lo mismo que en aquel entonces, que es dominar el desarrollo de la IA. Sam Altman ha dicho muchas veces que es importante tener grandes convicciones en un objetivo particular, pero que debes ser flexible con tus tácticas. Y eso es esencialmente lo que está haciendo con OpenAI; alta convicción en los objetivos, pero flexible en las tácticas. El objetivo final es el dominio, y las tácticas han cambiado de sin fines de lucro a con fines de lucro.

> ***"OpenAI también se ha vuelto una empresa hipersecreta, aunque originalmente dijo que sería transparente"***

Otra de las cosas que dijeron que nunca harían sería vender los datos personales de la gente. ¿Cree que también lo terminarán haciendo?

Sí. Además, técnicamente, ya están ganando dinero con los datos de la gente, en el sentido de que ya están utilizando los datos de las personas para entrenar las próximas generaciones de sus modelos de IA. Modelos que luego venden a través de suscripciones. Pero hablando más concretamente del negocio de la publicidad digital, vemos que OpenAI está preparándose también para la publicidad. Están añadiendo un *feed* algorítmico a

ChatGPT, lanzaron Sora 2, una aplicación como TikTok con el contenido generado por IA, y básicamente están creando espacios, superficies, en las que pueden empezar a insertar anuncios. Y eso creo que conducirá al 100% a que utilicen los datos de los usuarios para averiguar cómo segmentar mejor esos anuncios.

ChatGPT ha cumplido tres años recientemente. Usted ya cubría la industria de la inteligencia artificial antes de su salida a luz: ¿cómo cree que ha evolucionado ChatGPT y el sector de la IA en estos tres años?

El mundo ha cambiado. Ahora todo el mundo habla de IA, y todo el mundo tiene una concepción de la IA como ChatGPT, por lo que todas estas empresas y todos estos países se apresuran a intentar crear su propia versión de ChatGPT, olvidando todos los demás tipos de tecnologías, incluso otras tecnologías de IA que no son chatbots. Y la otra forma en que el mundo ha cambiado es, como expongo en mi libro, en que estas multinacionales ahora son como imperios. Están extrayendo una cantidad extraordinaria de recursos, explotando una cantidad extraordinaria de mano de obra y participando en actividades por todo el mundo de formas que no benefician en nada a la mayoría de las personas. De esta forma, otra de las cosas que han cambiado es que estas empresas están siendo otro acelerador más en la tendencia de retroceso democrático en todo el mundo. Creo que estos imperios están contribuyendo activamente a esa tendencia.

> ***"Las empresas de IA están participando en todo tipo de actividades que no benefician a las personas"***

Al principio parecía que ChatGPT era el centro de toda la industria, hoy parece solo uno más.

Sí, creo que ChatGPT definitivamente está siendo... hay muchos más competidores ahora que están tratando de comerse el dominio del mercado de ChatGPT. Por supuesto, tenemos a Gemini, tenemos a Claude de Anthropic y también vemos más empresas que comienzan a inclinarse hacia aplicaciones especializadas en lugar de solo estos chatbots; Anthropic enfocándose realmente en la generación de código, en lugar de ser solo una herramienta puramente genérica orientada al consumidor. O Google, enfocándose más en la empresa en lugar de apoyar a las labores de las personas. ChatGPT también está teniendo su propia transformación, inicialmente la gente pensaba que era más una herramienta de búsqueda, pero hemos visto esta tendencia realmente preocupante donde más y más personas comienzan a considerar a ChatGPT como un terapeuta, un mentor o un amante. Es algo que OpenAI no ha evitado, más bien se ha estado inclinando hacia eso también. Eso es una evolución de la que tendremos que estar muy pendientes en los próximos años.

¿Cómo explicaría a la gente cómo es Sam Altman?

Es un tipo extremadamente carismático que entiende muy, muy bien la psicología humana. Es capaz de decirle a la gente lo que necesita escuchar para motivarla a unirse a cualquier misión que él esté tratando de perseguir. Eso incluye conseguir que los inversores le den mucho dinero o conseguir que la gente se convierta en empleada de sus empresas. Así que es tanto un talento singular para la recaudación de fondos como un reclutador muy, muy bueno. Y no es solo porque entiende la psicología humana, también porque es muy bueno

contando esas grandes historias sobre el futuro y la IA, que son atractivas y que hacen que la gente quiera darle más y más recursos para lograrlo.

¿Lo compararía con alguna figura histórica, o quizá con alguna otra persona de la industria digital?

Bueno, él mismo ha hablado de cómo le encantaba leer un libro de citas de Napoleón. Y lo que sacó de ese libro fue que Napoleón era un conocedor extremadamente bueno de la psicología humana, y usó eso para ganar mucho poder. Así que creo que los paralelismos se escriben solos.

Personalmente, usted que ha podido investigar en profundidad al personaje, ¿se siente cómoda con el hecho de que Altman se convierta en uno de esos emperadores de las grandes tecnológicas? ¿Con que acumule tanto poder e influencia?

No me siento cómoda con que nadie ocupe tanto poder sin rendición de cuentas. En el libro critico a Altman y su enfoque, pero no creo que el problema se resolviera si simplemente cambiáramos a Altman por otra persona. Porque el sistema de poder todavía existe, donde quienquiera que se siente en esa mesa puede tomar decisiones que afectan a la vida de miles de millones de personas en todo el mundo. Y esos miles de millones de personas no tienen voz sobre si les gustan esas decisiones o no. Para mí, es mucho más preocupante, no que Altman esté al timón, sino que exista incluso este rol que pueda permitir a alguien ejercer esa cantidad de influencia a nivel mundial.

Una de las tácticas que Altman y OpenAI utilizan a menudo para convencer a otros de que inviertan en sus proyectos es la Inteligencia Artificial General, es máquina consciente y capaz de mejorarse a sí misma que podría superar a la humanidad. Usted ha tenido un acceso privilegiad a la compañía: desde dentro, ¿creen de verdad que la IA general es posible e incluso cercana?

Esto fue lo que más me sorprendió de mi investigación: yo pensaba que era solo una herramienta de marketing, pero en realidad hay facciones muy poderosas dentro de estas empresas y dentro de la industria en general que realmente creen que la IA general es posible y que es inminente. Y creo que eso es lo que hace que este ecosistema sea tan fascinante y complejo, porque tienes a las personas que empujan hacia este objetivo por una fe sincera y luego tienes a las personas que lo están aprovechando políticamente para protegerse de la regulación y usarlo como un truco de marketing.

Menciona la "fe sincera" de esas personas de la industria tecnológica. En los últimos tiempos se está hablando mucho más de la tecnorreligión de Silicon Valley, esa creencia casi religiosa en la tecnología digital como solución a todos los problemas de la sociedad. ¿Cree que esa fe está influyendo en todo esto?

Creo que tiene una influencia extraordinaria, sí. Y es parte de la razón por la que creo que la analogía con los imperios también es muy relevante, porque la mayoría de los imperios históricos también fueron impulsados en su expansión por creencias religiosas. Lo interesante es que en esta religión hay dos facciones. Las personas que piensan que necesitamos pisar el acelerador porque la IA general nos llevará al cielo y solo nos traerá utopía y bienestar; y luego las personas que piensan que nos llevará al infierno si la

desarrolla la persona equivocada. Y en el libro digo que estas son dos caras de la misma moneda, porque en realidad solo están leyendo de la misma Biblia con diferentes interpretaciones, de la misma manera que hay muchas facciones del cristianismo, algunas que leen la Biblia enfocadas en llegar al cielo y otras que leen la Biblia enfocándose en el hecho de que hay un infierno.

Entre esas personas hay científicos como Ilya Sutskever, ex jefe Científico de OpenAI, una de las mentes de referencia sobre IA. ¿Tienen un discurso serio realmente en torno a este tema? Sutskever, por ejemplo, afirma que la IA general ayudará a contrarrestar el cambio climático, pero a la vez dicen que si llega, el planeta pasaría a estar completamente cubierto de centros de datos en pocos años. No parece muy congruente.

Creo que Sutskever y algunos de estos otros investigadores de IA tienen mucha coherencia en cuanto a su teoría de la investigación de IA. Pero, ya sabes, no son exactamente expertos en otras cosas, así que ahí es donde la coherencia podría desmoronarse: cuando empiezan a hablar de cómo interactúa con el mundo real. Pero para Sutskever, él siempre ha creído muy firmemente que el cerebro es un motor estadístico y que las redes neuronales son una representación precisa de cómo funciona el cerebro. Él siempre ha pensado que mientras podamos meter más y más datos en estas redes neuronales, eso conducirá a la recreación de la inteligencia humana. Dio una charla el año pasado en la que mostró unos *papers* sobre cómo el tamaño del cerebro se correlaciona con la inteligencia de la especie. Su teoría es que simplemente tienes que construir un cerebro más grande y entonces obtienes un sistema más inteligente. El problema es, por supuesto, que en realidad no sabemos si eso es cierto, si las redes neuronales realmente modelan el cerebro y si el tamaño del cerebro es realmente lo único que conduce a más inteligencia, pero esa es la creencia de Sutskever y por eso ha centrado toda su investigación en esto.

Esa es la teoría de Sutskever, y tras la publicación de su libro OpenAI se ha embarcado en proyectos de inversión faraónicos para generar más capacidad de cómputo. ¿Cree que ese escalado masivo es el camino correcto para llegar a la IA General?

Para mí, la razón por la que no deberíamos estar escalando es en realidad una cuestión más fundamental que simplemente si nos llevará a la IA general. No creo que debamos intentar llegar a la IA general, independientemente de si podemos llegar allí, porque el propósito de construir tecnologías es servir a las personas, no reemplazar a las personas. Y la búsqueda de la IA general es en última instancia lograr una inteligencia a nivel humano y automatizar muchas de las cosas que la gente puede hacer. Así que sí, encuentro que toda esta empresa de escalado es innecesaria para lograr la IA general y también inmoral, porque no deberíamos estar intentando lograrla en primer lugar. Además, está conduciendo a una cantidad extraordinaria de degradación ambiental y daño a la salud pública de las personas, en un momento en que en realidad ya no tenemos mucho tiempo para resolver la crisis climática.

Por cosas como esta, ¿cree que la confianza general sobre OpenAI podría cambiar rápidamente entre el público general? Con el resto de tecnológicas hemos visto el proceso de cómo empiezan viéndose como disruptivas y luego su mala imagen las

lleva incluso a cambiarse el nombre, como Facebook y Meta. Parece que eso está sucediendo a toda velocidad con OpenAI.

Sí, creo que ya ha sucedido. No creo que OpenAI tenga ya una reputación muy positiva en muchos lugares. En EEUU hay muchos padres, por ejemplo, que se han enfadado mucho con la empresa debido a los impactos en la salud mental que estas herramientas están teniendo en los niños. Hay muchas comunidades de clase trabajadora que están realmente enfadadas por los centros de datos que están llegando a sus comunidades. Hemos visto un cambio dramático en la opinión pública solo en los últimos meses, y creo que eso va a continuar, porque lo que pasa con el imperio es que, a medida que continúa su construcción, continuará extrayendo y explotando a más y más comunidades. Y eso es lo que va a llevar a que cada vez más y más de ellas se vuelvan contra la empresa.

En el libro también trata en detalle la explotación sistémica de trabajadores para entrenar a los modelos, como el caso de Mofat en Kenia. Sobre cómo el modelo de negocio de OpenAI depende del capitalismo del desastre.

Sí, en este caso todas las empresas, no solo OpenAI, cuando entrenan sus modelos de IA, requieren contratar a decenas de miles de trabajadores de todo el mundo, y esto es algo que existía antes de ChatGPT. Existen firmas de terceros que hacen el trabajo de conectar a empresas como OpenAI con estos trabajadores. Son plataformas que tratan de buscar la mano de obra más barata en el mercado global. De lo que se dieron cuenta es que la mejor manera de encontrar la mano de obra más barata es ir a los lugares más pobres y desesperados del mundo. Inicialmente, eso fue Venezuela, donde la economía estaba en un estado desastroso, pero la población también estaba altamente educada y tenía alta conectividad. A medida que la economía de Venezuela comenzó a recuperarse ligeramente, el trabajo se trasladó a otros lugares más desfavorecidos durante la pandemia, cuando otros países estaban cayendo en picado, como Kenia. La historia de Mofat ilustra una vez más la lógica del imperio, porque OpenAI es una empresa valorada en 500.000 millones de dólares y, sin embargo, contratan trabajadores para realizar un trabajo esencial para el éxito de ChatGPT pagándoles solo unos pocos dólares la hora. Muchos de ellos terminaron psicológicamente devastados por este trabajo y sus familias se desmoronaron. Así funciona el capitalismo de desastre en muchos sentidos.

Esas personas cuentan con muy poca formación sobre cómo entrenar a la IA. ¿Es posible que los modelos tengan más alucinaciones o sean más imprecisos por esta situación?

Es una pregunta interesante. Creo que los modelos son más imprecisos principalmente porque las empresas en realidad no enfatizan la precisión. Hemos visto que las actualizaciones de los modelos de OpenAI a veces se vuelven menos precisas a medida que avanzan las nuevas generaciones de GPT. Así que no creo que esté necesariamente ligado a los trabajadores en sí; son principalmente los incentivos de las empresas, así como la tecnología misma. Esta es una tecnología probabilística, por lo que es inherentemente propensa a errores. Es imposible garantizar que vaya a decir lo correcto el 100% de las veces.

¿Cree que hay una burbuja en la inteligencia artificial?

Creo que hay una gran burbuja. No veo cómo estas empresas van a ser capaces de cumplir sus compromisos o averiguar cómo obtener un retorno de sus inversiones. OpenAI ha comprometido 1,4 billones de dólares de gasto en los próximos años y ha generado, como máximo, unos 20.000 millones en ingresos. Esa es una brecha extraordinaria y OpenAI se está quedando sin ideas para cerrarla. Intentaron el modelo de suscripción y encontraron que aproximadamente solo el 5% de los usuarios están dispuestos a pagar. Ahora se están preparando para la publicidad, pero el mayor negocio publicitario de la historia fue Google, y Google el año pasado ganó menos de 300.000 millones en ingresos publicitarios, así que eso todavía no cierra la brecha. Y luego ves a OpenAI tratando de rociar el mercado con todos estos lanzamientos de productos, como un navegador, el TikTok de IA... pero estos lanzamientos no están cuajando. Tanto con el navegador como con el TikTok de IA, se volvieron virales al principio, pero en realidad están cayendo bastante rápido después en términos de adopción de usuarios. Así que simplemente no hay un modelo de negocio viable ahí.

¿Cree que una de las estrategias de Altman es precisamente hacer que OpenAI sea "demasiado grande para caer", llegando a múltiples acuerdos con gobiernos e industria?

Absolutamente. Hay un análisis realmente genial escrito por un ex colega mío en el *Wall Street Journal* que habla de esto, donde explicaba cómo OpenAI está atando su destino a todos los principales actores tecnológicos que actualmente están manteniendo a flote la economía de EEUU. Se ha atado a Nvidia, a Oracle, a Microsoft. Cuando miras la economía de EEUU, actualmente solo está sobreviviendo y yendo bien gracias a las empresas de IA. OpenAI y las otras empresas que están tratando de hacerse demasiado grandes para caer de dos maneras: una, haciendo que la economía de EEUU dependa de si a estas empresas les va bien o no, ya que cuando eso sucede, el gobierno de EEUU siempre es más propenso a querer intervenir y rescatar a una empresa que pueda causar el colapso de toda la economía. Y dos: están tratando de hacerse demasiado grandes para caer vendiendo sus tecnologías al gobierno, para hacer que el gobierno dependa de sus plataformas. Todas ellas están participando en esta especie de estrategia de dos frentes para evitar caer si explota la burbuja.

Google entierra definitivamente su plan para eliminar las cookies de terceros de Chrome

La multinacional se da por vencida y no matará este instrumento de rastreo, incapaz de proponer una alternativa que satisfaga a la industria publicitaria y no la exponga a más sanciones por abuso de posición dominante

Hemeroteca — Anunciantes y supervisores enfrían el plan de Google para desterrar las cookies

Carlos del Castillo

SEGUIR AL AUTOR/A

23 de abril de 2025
14:46 h
Actualizado el
23/04/2025 16:49 h
0

Foto de archivo del logo de Google. EFE/HANNIBAL HANSCHKE

Las cookies de terceros se quedan en Chrome. Tras cinco años estudiando cómo eliminarlas por completo de su navegador y millones invertidos en tecnologías publicitarias alternativas, Google ha renunciado finalmente a ese objetivo. Así lo ha anunciado la multinacional en un comunicado firmado por su uno de sus vicepresidentes, en el que confiesa que Google ha sido incapaz de poner de acuerdo a todos los agentes involucrados en el fin de este instrumento de rastreo, el gran exponente del Internet basado en la extracción masiva de datos personales.

"A medida que interactuamos con el ecosistema, incluyendo editores, desarrolladores, organismos reguladores y la industria publicitaria, queda claro que existen perspectivas divergentes sobre la implementación de cambios que podrían afectar la disponibilidad de las cookies de terceros", afirma Anthony Chávez en el blog oficial de la compañía. El ejecutivo cita también la evolución del panorama digital desde 2019, cuando puso en marcha su plan para eliminar las cookies, tanto en materia legal como tecnológica.

"Se ha acelerado la adopción de tecnologías que mejoran la privacidad, han surgido nuevas oportunidades para proteger y asegurar la experiencia de navegación de los usuarios con IA, y el panorama regulatorio mundial ha evolucionado considerablemente. Considerando todos estos factores, hemos decidido mantener nuestro enfoque actual de ofrecer a los

usuarios la opción de cookies de terceros en Chrome y no implementaremos un nuevo aviso independiente para cookies de terceros", ha confirmado.

En la práctica, todo queda como estaba, con los únicos añadidos obligados por el refuerzo de las leyes de privacidad. Las cookies de terceros permiten que empresas ajenas al sitio que se visita recopilen información sobre la actividad del usuario en la web, sin que muchas veces este sea plenamente consciente de ello. A través del seguimiento constante en múltiples páginas, construyen perfiles detallados de comportamiento, intereses y hábitos de consumo, que luego se utilizan para segmentar audiencias y dirigir publicidad personalizada.

Pese al consenso entre multinacionales digitales, industria publicitaria y editores de webs de que las cookies de terceros son un método obsoleto y poco respetuoso con la privacidad del usuario, no se ha prepuesto una solución alternativa que satisfaga a todos. El mercado de la publicidad digital mueve unos 680.000 millones de euros al año, según datos de la consultora Business Research Insights, mientras que el 75% de las agencias de marketing siguen dependiendo en gran medida de las cookies de terceros para mostrar sus anuncios, refleja otro estudio de Adobe.

La alternativa propuesta por Google, denominada Privacy Sandbox, tampoco consiguió el apoyo necesario. La iniciativa colocaba a la multinacional como guardiana de los datos personales de sus usuarios impidiendo que estos fueran recopilados por las cookies de terceros. Algo que no ha convencido a la industria ni tampoco a los reguladores, que ya tienen múltiples causas abiertas contra la compañía por abuso de posición dominante.

El paso atrás de Google para eliminar las cookies de terceros de Chrome da una nueva vida a este instrumento, ya que este navegador es clave en el negocio digital. Es el preferido de un 66% de los usuarios, según StatCounter, lo que había llevado a Google a intentar liderar el cambio. No obstante, la multinacional se encuentra en este momento en una encrucijada, puesto que ha sido condenada por monopolio en el mercado de la publicidad de la publicidad online en EEUU y el Departamento de Justicia ha propuesto al tribunal que la obligue a vender Chrome como vía para solucionarlo.

OpenAI se ofrece a comprar Chrome

Google, de hecho, acumula tres condenas por monopolio. Además de en el mercado de la publicidad, suma también otra resolución en el mismo sentido por su dominio del sector de las búsquedas, y otra por prácticas anticompetitivas en la Play Store, la tienda de aplicaciones de Android. La resolución de estas disputas podría derivar en cambios estructurales para Internet, puesto que tanto Chrome, como la Play Store como el propio buscador de Google han sido herramientas troncales de la experiencia digital.

El Internet que viene podría basarse más en modelos de suscripción que en la extracción de datos. Uno de los máximos exponentes de ese cambio de tendencia es OpenAI, que acaba de ofrecerse a comprar Chrome tras la petición del Departamento de Justicia en el juicio contra Google. "Sí que nos interesaría. Igual que a muchos otros", ha afirmado Nick Turley, jefe de producto de ChatGPT, el mayor éxito comercial de la organización.

Aunque aún tiene un recorrido corto, OpenAI ha apostado por los planes de pago como vía de monetización de ChatGPT. Una posible adquisición de Chrome crearía otro gigante de la tecnología y ofrecería a la empresa una incalculable fuente de datos con los que entrenar a su inteligencia artificial. En este momento ChatGPT está integrado con Bing, el motor de búsqueda de Microsoft, después de una inversión de decenas miles de millones de dólares por parte de esta última en el laboratorio de inteligencia artificial.

Casi 5 millones de euros de sanción a Netflix por ocultar dónde envía los datos de sus usuarios

Países Bajos, donde se encuentra su sede europea, sanciona a la multinacional estadounidense por no ser transparente sobre el uso que hace de la información de sus usuarios

— Condenan a Netflix con 385.000 dólares por revelar la identidad de una mujer en el documental 'Nuestro padre'

Carlos del Castillo

SEGUIR AL AUTOR/A

18 de diciembre de 2024
12:15 h
Actualizado el
18/12/2024 12:25 h
1

Fotografía de archivo del logo de Netflix en uno de los edificios de la compañía en Los Ángeles (EE. UU). EFE/ Christian Monterrosa

La Autoridad Holandesa de Protección de Datos (DPA, por sus siglas en inglés) ha impuesto una sanción de 4,75 millones de euros a Netflix por no informar adecuadamente a sus clientes sobre cómo maneja sus datos personales. La investigación, iniciada en 2019, reveló que la compañía no proporcionaba información clara en su declaración de privacidad sobre el uso de los datos recopilados, incluyendo direcciones de correo electrónico, números de teléfono, detalles de pago y el historial de visualización.

La investigación se originó a raíz de una reclamación presentada por None of your business (Noyb), una ONG austriaca dedicada a la privacidad con una larga trayectoria de acciones

legales en defensa de los derechos digitales de los usuarios. En esta ocasión la denunica se presentó ante el regulador neerlandés debido a que Netflix tiene su sede europea en Ámsterdam, pero el análisis abarca su negocio en toda la UE. La DPA explica que ha habido otras agencias de protección de datos europeas que han participado en la investigación.

Según la resolución la compañía proporcionó muy poca información a sus clientes sobre qué datos personales comparte Netflix con terceros y por qué lo hace, cuánto tiempo conserva los datos o cómo garantiza su seguridad cuando la empresa los transmite a países fuera de Europa. "Una empresa como ésta, con una facturación de miles de millones de clientes en todo el mundo, tiene que explicar a sus clientes cómo trata sus datos personales", ha afirmado Aleid Wolfsen, presidente de la DPA: "Eso tiene que quedar meridianamente claro, sobre todo si el cliente pregunta por ello".

Además de los datos vinculados a la identidad del usuario, Netflix maneja información sobre el historial de visualización que tienen un gran valor para los anunciantes. Este puede revelar datos como preferencias de género, hábitos de consumo, edad, región, estado emocional e intereses personales, que se pueden usar para publicidad personalizada. Esto incluye anuncios basados en gustos, segmentación demográfica (productos para niños o adultos), promoción de contenidos similares e incluso predicción de necesidades futuras.

Tras el inicio de la investigación, Netflix modificó su política de privacidad para reflejar que no vende este tipo de información a los anunciantes. "Netflix utiliza medidas contractuales y técnicas diseñadas para evitar que los proveedores de marketing de Netflix accedan a la información relativa a los programas específicos o a las selecciones de títulos de películas que usted hace, a las URL en las que usted entra, o a los programas o películas que usted ha visto en nuestro servicio", refleja el documento.

Noyb interpuso la reclamación después de que Netflix fuera incapaz de explicar qué hace con los datos del usuario tras una petición directa. La ONG refleja que la compañía estadounidense ni siquiera pudo dar una descripción completa del uso de los datos personales una vez que se inició la investigación de la autoridad neerlandesa. "Estamos satisfechos con la decisión de la DPA de imponer una multa a Netflix. Sin embargo, han hecho falta casi cinco años para obtenerla, y en un caso muy sencillo", ha recalcado Stefano Rossetti, abogado especializado en protección de datos de Noyb.

Netflix ha anunciado que recurrirá la sanción. "Desde que comenzó esta investigación hace más de cinco años, hemos cooperado con la Autoridad Holandesa de Protección de Datos y hemos evolucionado proactivamente nuestra información sobre privacidad para ofrecer una mayor claridad a nuestros miembros", ha destacado una portavoz de la multinacional en un comunicado enviado a elDiario.es. Las mismas fuentes apuntan a que el caso se refiere al período entre 2018 y 2020, justo después de la entrada en vigor de las nuevas normas de protección de datos europeas.

Sub-bloque D: Defensa ciudadana y difusión de resoluciones

Siete llamadas y una estafa: así funciona el teatro de ofertas falsas para robar tus datos en nombre de la OCU

Los ciberdelincuentes perfeccionan el 'timo de la doble llamada' con un bombardeo de contactos, una técnica del telemarketing para intentar engañar a los usuarios

— Frena la sensación de urgencia: así hackean tu mente los ciberestafadores y los trucos para evitarlo

Carlos del Castillo

SEGUIR AL AUTOR/A

27 de noviembre de 2025
22:09 h
Actualizado el
28/11/2025 12:59 h
21

Suena el teléfono. Al otro lado, llegan malas noticias: la tarifa que está utilizando este número de teléfono ha caducado y la compañía de telecomunicaciones va a subir el contrato de 65 a 92 euros. El cliente tiene tres opciones: pagar el aumento, dar de baja el número o acogerse a un nuevo proceso de "liberalización" de la línea tutelado por la Organización de Consumidores y Usuarios (OCU). Si escoge la tercera, empieza la función.

La ciberdelincuencia se profesionaliza. Las estafas se parecen cada vez más a coreografías de alta precisión. Una campaña activa en España detectada por elDiario.es está empleando un esquema de múltiples pasos, con varias llamadas telefónicas coordinadas desde un *call center* y contactos por WhatsApp para ganarse la confianza de la víctima. Todo para robar sus datos personales y, presuntamente, venderlos a otra compañía para lograr una comisión por llevarle nuevos clientes.

El *modus operandi* es una evolución del clásico "timo de la doble llamada". Este se basa en un primer contacto realizado por los ciberdelincuentes que sirve para anunciar una subida de precio o cambios negativos en el contrato, a la que sigue otra llamada ofreciendo la salvación. En esta nueva variante, sin embargo, el engaño muta hacia lo que las propias

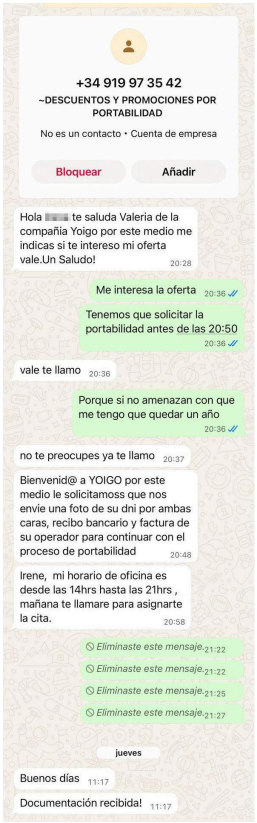
víctimas describen como un "mercado persa". Apenas cuelga el falso operador de la compañía original, que informa de la citada subida en la tarifa, el teléfono del objetivo se convierte en un hervidero.

Diferentes números, tanto fijos que simulan llegar desde diferentes puntos de España como móviles particulares, llaman sucesivamente. Se hacen pasar por la supuesta terna de compañías "habilitadas" (en este caso Movistar, Yoigo y Orange) que compiten en tiempo real por ofrecer la mejor tarifa al cliente.

Todo presuntamente amparado por la OCU, cuya mención no es casual. Enrique García, portavoz de la entidad, confirma a este medio que el uso de su nombre busca generar un "sesgo de autoridad" que desactive las defensas del consumidor. Pero existe un trasfondo regulatorio más perverso: al aceptar entrar en ese supuesto proceso de "liberalización", la víctima está, sin saberlo, dando su consentimiento verbal para recibir llamadas comerciales que, de otro modo, estarían prohibidas por la Ley General de Telecomunicaciones, avisa García.

Hora de decidir

La estafa se cierra con un hackeo psicológico diseñado para anular el juicio crítico de la víctima: la sensación de urgencia. Tras la cadena de llamadas, los estafadores reintroducen al actor inicial (la falsa operadora de origen, un rol en el que en este caso suplantan a Vodafone) para lanzar el ultimátum. "Tenía que decidir antes de las 20:50 horas o se prorrogaba mi contrato, pero a 99 euros", relata una afectada a elDiario.es.



Esta presión artificial está diseñada para que la víctima dé el paso: termina enviando su DNI, recibos bancarios y facturas a la supuesta operadora que le había hecho la oferta más convincente, que previamente había contactado con ella a través de WhatsApp. Datos que funcionan como las llaves de su identidad digital.

En este caso, la estafa no termina en desfalco. Fue la propia víctima la que se dio cuenta del engaño cuando le estaba contando lo sucedido a sus compañeros de trabajo. Al resumir los hechos en voz alta, se percató de que nada encajaba. Ese proceso, ya con la cabeza fría y alejada la sensación de urgencia inoculada por los ciberdelincuentes, es el que activa las defensas.

"No es que tu cerebro te traicione, es que está programado para funcionar así y ser capaz de tomar decisiones rápidas de manera intuitiva", explicaba en un reportaje sobre este proceso Pilar Bringas, experta certificada en mecanismos de influencia y persuasión ética. "Es el resultado de

miles de años de evolución en entornos hostiles. Pero tenemos que ser conscientes de que se puede utilizar contra nosotros".

Robo de clientes

La afectada borró los datos que suministró a los ciberdelincuentes, denunció los hechos ante la Policía y avisó a su banco de lo ocurrido. Actuó antes de que pudieran terminar su plan, por lo que no es posible conocer si este consistía en intentar aprovechar sus datos bancarios para llevar a cabo un robo en su cuenta, o si pretendían vendérselos a una operadora real para llevarse una comisión.

Tanto la OCU como Vodafone avisan de que se trata de un timo habitual. "Vodafone no avisa de cambios de tarifas por teléfono, ni las tarifas caducan. Este tipo de fraudes tienen por objeto conseguir que el usuario se cambie de compañía sin su consentimiento. Vodafone notifica cualquier actualización de precios o cambio en los servicios en la factura o por SMS y en caso de duda recomienda contactar por los canales oficiales", explica un portavoz de la operadora, que ya detectó una artimaña como esta, aunque menos compleja, en julio.

La OCU denomina a las organizaciones que se dedican a lanzar este tipo de estafas como "empresas champiñón". Son "intermediarios que aparecen y desaparecen", a menudo operando desde países de Latinoamérica para dificultar la acción policial, explica la organización. Cobran comisiones por captar clientes o buscan directamente el robo de datos para cometer fraudes financieros posteriores. Además de con las operadoras de telefonía, también operan haciéndose pasar por compañías energéticas.

Los *call center* del crimen

Hace un año, la Policía Nacional desmanteló una organización que operaba desde Perú a través de tres *call centers* dedicados a lanzar estafas en España. Fue una de las mayores operaciones hasta la fecha contra estas estructuras. Hubo 35 detenciones en Madrid, Vigo, Barcelona, Mallorca y Salamanca, y otras 48 en el país andino. "El caso es que yo oía a otras personas hablando al fondo", confirma la afectada por esta nueva campaña al ser informada de esta situación, "y en todas las llamadas, los operadores tenían acento latinoamericano".

Son instalaciones que funcionan como las de una empresa tradicional, pero dedicadas al crimen. "En Perú se encontraba el líder de la organización, que tenía bajo su mando a tres personas que controlaban cada uno de los centros de llamadas", informó entonces la Policía. "Estos contaban con carteles de frases motivacionales para animar a los empleados, llegando a celebrar las primeras estafas de los trabajadores de reciente incorporación".

La organización llegó a realizar miles de llamadas diarias desde los tres *call centers*, donde trabajaron hasta 50 personas simultáneamente. Como en la estafa ahora activa, utilizaban diferentes técnicas para camuflar el origen real de los contactos. Desde la OCU detallan que han interpuesto varias denuncias para evitar el uso de su nombre en estos fraudes.

Algunos afectados también han presentado reclamaciones ante la Agencia Española de Protección de Datos (AEPD). Tanto por el uso irregular de su información como por haber sido contactados estando inscritos en la Lista Robinson, en la que se expresa la oposición a recibir llamadas comerciales de empresas con las que el usuario no tiene relación. Una inscripción que estas organizaciones no tienen en cuenta.

En la mayoría de ocasiones, la Agencia se ve obligada a archivar estas reclamaciones al no poder identificar un culpable. "Apunta Telefónica la posibilidad de que terceras empresas estén realizando prácticas fraudulentas consistentes en suplantar su identidad", explica el organismo en una resolución reciente en la que los estafadores se hacían pasar por esta teleco.

Un código para acabar con el 'spam'

Para intentar poner coto a este tipo de prácticas abusivas, el Congreso de los Diputados ha aprobado recientemente la Ley de Servicios de Atención a la Clientela. La norma incluye una medida directa contra el bombardeo telefónico: obligará a las empresas a identificar sus llamadas comerciales con un código numérico específico (un prefijo), permitiendo a las operadoras bloquear aquellas que no lo utilicen. Además, la ley declara nulos los contratos que se cierren en llamadas no consentidas, atacando directamente la rentabilidad de las "empresas champiñón" que basan su negocio en presionar al usuario para obtener un "sí" rápido y viciado.

Desde el Instituto Nacional de Ciberseguridad insisten en que la mejor defensa ante estas maniobras es desconfiar de cualquier llamada inesperada que invoque urgencias o subidas inminentes. El organismo recuerda que no deben facilitarse datos personales ni bancarios por teléfono o mensajería, ni aceptar grabaciones de voz que puedan utilizarse para tramitar contratos no autorizados. Ante la mínima sospecha, recomiendan colgar, contactar directamente con la compañía y, si ya se han entregado documentos o información sensible,

avisar al banco, recopilar pruebas y solicitar asesoramiento inmediato a través de su línea 017, un teléfono de ayuda gratuito y confidencial.

Protección de Datos prohíbe a hoteles y alojamientos hacer copias del DNI de los clientes

El regulador de privacidad avisa que esta práctica es "excesiva" y que no vale para cumplir la normativa de Interior sobre el registro de viajeros

— Interior defiende que el nuevo registro de viajeros ha permitido localizar a 18.584 personas que estaban en busca y captura

Carlos del Castillo

SEGUIR AL AUTOR/A

17 de junio de 2025
14:24 h
Actualizado el
17/06/2025 17:47 h
7

Imagen de archivo de hoteles turísticos en la costa española. EFE/Dvid Arquimbau

Verificar los datos, sí; guardarse una copia, no. La Agencia Española de Protección de Datos (AEPD) ha emitido este martes una nota informativa dirigida a hoteles y alojamientos turísticos en la que expone que quedarse con una fotografía o fotocopia del DNI de los clientes viola la normativa de privacidad. Sin una debida justificación, llevar a cabo esta práctica para el registro de los huéspedes podría ser susceptible de sanción, avisa el organismo.

La Agencia ha emitido esta nota en relación con el Real Decreto 933/2021, una norma que provocó las quejas del sector hotelero así como de especialistas en privacidad por la exigencia a estos establecimientos para que recopilaran una gran cantidad de datos los clientes. La regulación, que entró en vigor en diciembre de 2024, obliga a hoteleros, propietarios de viviendas turísticas, agencias de viajes y empresas de alquiler de vehículos a recopilar hasta 28 categorías de datos de los viajeros.

Entre ellos están datos personales no oficiales como dirección, teléfono o móvil; así como otros relativos a las transacciones, como la identificación del medio de pago, el IBAN de la cuenta bancaria o la fecha de caducidad de la tarjeta. Además, en el caso de que alguno de los viajeros sea menor de edad, también se deberá reflejar la relación de parentesco entre los huéspedes. Esos datos deberán volcarse en una plataforma —llamada SES.HOSPEDAJES— que ha puesto en marcha Interior y deberán conservarse durante tres años.

Ahora la AEPD señala a los hosteleros que hacer una copia del DNI o pasaporte no es suficiente para cumplir la normativa, puesto que el documento no incluye todos los datos necesarios. En cambio, sí implica la recolección de información que el real decreto no solicita. Por ello, entiende que "solicitar una copia del Documento Nacional de Identidad o del Pasaporte vulnera el principio de minimización de datos", ya que "supone un tratamiento excesivo de datos".

"Esto se debe a que el DNI completo contiene más datos que los obligados a aportar en virtud de la normativa aplicable, como la fotografía, la fecha de caducidad del documento, el CAN [Código de Acceso de Nivel, un número de seis cifras que se usa como medida de seguridad adicional] o el nombre de los padres", recuerda. Enviar el documento a través de una fotografía tampoco permite comprobar que el huésped es realmente la persona que refleja el documento, continúa la Agencia.

Además, esta práctica expone a los clientes a brechas de seguridad en casos de ciberataque. "El entregar una copia de la documentación personal implica, entre otros, un riesgo innecesario de suplantación de la identidad", expone el regulador de privacidad. Un vector de ataque en auge con las repetidas brechas sufridas por los alojamientos, que luego sirven de trampolín a los ciberdelincuentes para lanzar timos contra los huéspedes a través de plataformas como Booking.

En vez de hacer copias del DNI o pasaporte, el regulador recomienda a los alojamientos que preparen un formulario con los datos necesarios para cumplir con los requisitos del Ministerio del Interior, y luego verificarlos en persona con ayuda del documento oficial. En caso de recogida de datos en línea sin atención presencial, esta verificación puede realizarse mediante mecanismos como certificados digitales, ha asegurado en la nota. "También es posible la verificación de que los datos y la información proporcionada concuerda con los datos asociados al medio de pago utilizado", según la agencia.

El Parlamento Europeo refuerza su alerta sobre WhatsApp a los diputados y les pide usar Signal en sus viajes al extranjero

Los servicios de seguridad de la institución piden a los eurodiputados que eviten por norma general el uso de la app de Meta

— WhatsApp, Telegram, Signal: ¿qué aplicación de mensajería ofrece las comunicaciones más seguras?

Carlos del Castillo

SEGUIR AL AUTOR/A

18 de octubre de 2025
22:43 h
Actualizado el
19/10/2025 05:30 h
8

Logo de la aplicación de mensajería Signal Unsplash

Los servicios de seguridad del Parlamento Europeo están advirtiendo verbalmente y en persona a los eurodiputados que viajan al extranjero que eviten el uso de WhatsApp y opten por la aplicación de mensajería encriptada Signal. Esta recomendación, confirmada a este medio por fuentes parlamentarias y por el servicio de prensa de la institución, incide en una política de seguridad anterior, pero subraya la creciente preocupación por el ciberespionaje.

La recomendación se está transmitiendo de forma oral durante las sesiones informativas previas a las misiones oficiales. En respuesta a las preguntas de este periódico, fuentes oficiales del Parlamento confirman que "el uso de Signal se propone como una alternativa segura en los casos en que no se dispone de una herramienta corporativa equivalente". "Debido a la propia naturaleza de estos procesos", la comunicación oficial concluye que no puede "comentar más sobre medidas o herramientas de seguridad o ciberseguridad".

Las herramientas corporativas a las que se refiere la institución son principalmente Microsoft Teams y Jabber. Teams es una plataforma de comunicación muy extendida que integra chat, videoconferencias y almacenamiento de archivos en un entorno cerrado y controlado. Jabber es un sistema de mensajería instantánea diseñado por Cisco para actuar como chat interno en entornos corporativos.

Ambas aplicaciones están limitadas al uso dentro del propio ecosistema del Parlamento, lo que significa que solo permiten comunicarse con otros usuarios que también formen parte de la red institucional. Por este motivo, cuando los parlamentarios viajan al extranjero y necesitan mantener conversaciones fuera del entorno corporativo, los equipos de seguridad recomiendan utilizar Signal como alternativa cifrada y más segura que WhatsApp.

A simple vista, Signal es casi idéntico a WhatsApp: sirve para enviar mensajes, fotos y hacer llamadas, y ambas aplicaciones cifran las conversaciones para que solo el emisor y el receptor puedan leerlas. La diferencia fundamental reside en su filosofía y en quién es su dueño. WhatsApp es propiedad de Meta, una empresa cuyo negocio se basa en los datos, por lo que recopila mucha información sobre cómo y con quién usas la app, aunque no pueda leer el contenido.

Signal, en cambio, es gestionada por una fundación sin ánimo de lucro y funciona sobre un código abierto que impide registrar o almacenar prácticamente ningún dato de sus usuarios. Se considera una de las apps más seguras para comunicaciones confidenciales. Además, WhatsApp, por su gran alcance, ha sido objetivo de herramientas de espionaje como Pegasus, diseñadas para atacar posibles debilidades en su infraestructura.

Otras instituciones europeas habían llevado a cabo este cambio previamente. La Comisión y el Consejo europeos piden a sus funcionarios que usen Signal desde principios de esta década. El Ejecutivo comunitario pide además que se active la opción de borrado automático de los mensajes que permite esta app, una función que usa la propia presidenta de la Comisión, Ursula Von der Leyen, según ha revelado en comunicados oficiales.

El Parlamento, en cambio, no hizo oficial la recomendación hasta este 2025. En febrero, el medio especializado *Politico* reveló que el Parlamento había enviado una comunicación interna a legisladores y personal instando al uso de Signal. Aquella advertencia se produjo tras destaparse intrusiones a gran escala de un grupo de hackers vinculado a China, llamado "Salt Typhoon", contra proveedores de telecomunicaciones en EEUU y Europa.

Una recomendación que los servicios de seguridad de la institución están reiterando ahora a los eurodiputados que se disponen a viajar al extranjero en misión oficial.

Protección de Datos zanja el debate: la baliza V-16 de la DGT no puede identificar al conductor ni controlar sus viajes

El regulador de privacidad aclara que “mientras no se activa, la baliza no transmite ningún dato” y que en caso de emergencia, no permite a la DGT saber quién es el conductor ni el vehículo involucrados

— Cómo saber si una baliza V-16 está homologada y conectada con la DGT

Carlos del Castillo

SEGUIR AL AUTOR/A

20 de noviembre de 2025
11:56 h
Actualizado el
23/11/2025 18:24 h
6

Las balizas V-16 reemplazarán a los triángulos convencionales. Dirección General de Tráfico (DGT)

Ni saber quién es el conductor, ni registrar sus movimientos, ni captar otros datos personales. La Agencia Española de Protección de Datos (AEPD) ha publicado este jueves una nota aclaratoria respecto al funcionamiento y tratamiento de datos de las balizas V-16 conectadas de la DGT, que serán obligatorias a partir del 1 de enero de 2026 en todos los vehículos excepto motos y ciclomotores. El regulador de la privacidad responde así a las publicaciones difundidas en foros y redes sociales sobre una supuesta vigilancia continua a través del dispositivo.

La baliza V-16 es un dispositivo luminoso que sustituirá a los triángulos amarillos para señalizar un vehículo inmovilizado o por accidente o emergencia. Su función es emitir destellos intermitentes y se fija magnéticamente en la parte más alta del vehículo en caso de avería o accidente. El sistema, alimentado por una batería autónoma, permite la señalización del obstáculo en la vía sin necesidad de que los ocupantes abandonen el habitáculo ni transiten por la calzada, como ahora ocurre con los triángulos.

El dispositivo integra además un módulo de comunicación que transmite las coordenadas geográficas del incidente a una plataforma controlada por la DGT, lo que facilita la difusión del aviso al resto de usuarios a través de los paneles de mensaje variable y los sistemas de navegación.

Según detalla la AEPD, las capacidades técnicas de la baliza V-16 de señalización se limitan a estas funciones. El organismo hace hincapié en que los únicos datos que transmite son las coordenadas geográficas del vehículo detenido y un identificador técnico del propio aparato, pero no datos personales sobre el conductor o su vehículo.

El regulador de la privacidad subraya que la baliza no puede servir como herramienta de espionaje, como algunos usuarios han denunciado, porque dicho identificador está asociado con la matrícula del coche ni con la identidad de su titular. "La persona que adquiere la baliza no tiene que dar sus datos personales a ninguna administración al adquirirlo, por lo que la DGT no conocería quién ha comprado el dispositivo", recuerda la AEPD en la nota, advirtiendo también a los usuarios que no deben dar sus datos al vendedor en este proceso.

"Mientras no se activa, la baliza no transmite ningún dato y, en caso de ser activada ante una situación de emergencia, la información que se envía no permitiría conocer quién es la persona que conduce ni reconstruir sus desplazamientos. La baliza V-16 emite una señal mientras está encendida y deja de hacerlo al apagarse, sin generar historiales de movimientos o envío de datos de manera continua", aclara la Agencia.

El fin de los triángulos de emergencia

La implementación de la luz V16 forma parte de la estrategia de seguridad vial destinada a reducir el riesgo de atropellos en carretera. La medida busca evitar que los conductores deban abandonar el habitáculo para colocar los triángulos de preseñalización en caso de incidencia. No obstante, hay casos en los que la DGT sí permite salir del vehículo.

Actualmente, los conductores pueden utilizar indistintamente los triángulos de emergencia o las balizas V-16 (conectadas o no conectadas). Sin embargo, a partir del 1 de enero de 2026, será obligatorio que todos los vehículos lleven la señal V16 con geolocalización integrada, quedando prohibido el uso de los triángulos y de las balizas analógicas que no dispongan de conexión con la plataforma de la DGT. Los precios de las balizas están entre los 40 y los 50 euros.

Medio millón de euros de multa a ING por perder datos confidenciales de un cliente y no saber cómo encontrarlos

La entidad ignoró durante siete meses los avisos del afectado, que le advirtió repetidamente de que estaba reclamando sus datos bancarios y su DNI a la empresa de mensajería equivocada

— Protección de Datos zanja el debate: la baliza V-16 de la DGT no puede identificar al conductor ni controlar sus viajes

Carlos del Castillo

SEGUIR AL AUTOR/A

4 de enero de 2026
22:24 h
Actualizado el
05/01/2026 05:30 h
14

Imagen de archivo de una sucursal del banco ING en Bruselas (Bélgica).EFE/ Stephanie Lecocq

Recoger la documentación bancaria y el DNI en el domicilio del cliente, perderlos por el camino y no darse cuenta hasta que el usuario protesta. Y cuando protesta, pasarse medio año preguntando a la empresa de mensajería equivocada. La Agencia Española de Protección de Datos (AEPD) ha impuesto una multa de 500.000 euros a ING tras confirmar que la entidad carecía de medidas básicas para rastrear la documentación sensible que mueve fuera de sus oficinas.

Todo comenzó con una solicitud para darse de alta como cotitular en la cuenta de su pareja. Siguiendo instrucciones del banco, una empresa de mensajería recogió en el domicilio de un cliente un sobre con los datos para llevar a cabo el trámite. La documentación nunca llegó a los sistemas de ING.

En el paquete se encontraban copias del DNI por ambas caras, datos financieros como el número de cuenta bancaria, su domicilio, dirección de correo electrónico, número de teléfono móvil, información sobre su vida laboral, así como su firma original.

Datos que aunque ING argumentó que no son "sensibles" (categoría en la que entran aquellos referentes a la ideología, creencias religiosas u orientación sexual), la AEPD recalca que el hecho de perderlos todos juntos lo convierte en "especialmente" peligroso.

Contar con esa información permite a un delincuente "construir un perfil completo y detallado" de la víctima para cometer abusos, ya que "conlleva un elevado riesgo de suplantación de identidad, daños patrimoniales o afectación al derecho al honor", recalca en su resolución.

Con todo, lo que ha motivado la contundencia de la sanción no es el extravío en sí, sino el caos administrativo que lo siguió. A pesar de que el cliente alertó de la situación al banco hasta en cuatro ocasiones durante el mes siguiente a enviar la documentación, ING se limitó a abrir incidencias internas sin investigar a fondo qué había sucedido con sus datos, instándole a que la enviara de nuevo.

Según consta en la resolución, los avisos del afectado provocaron que el banco se pusiera en contacto repetidamente con su proveedor logístico habitual, la empresa Sending, para localizar el envío. El problema es que, para ese porte específico, se había contratado a otra compañía distinta, Dynamic. Fue el propio cliente el que avisó de ello en sus alertas al banco, suministrando tanto el nombre de la empresa que había recogido el paquete como incluso el del mensajero que se lo había llevado.

Pese a los avisos del afectado, ING no contactó a la empresa correcta durante más de siete meses. Tampoco lo consideró como una posible brecha de seguridad que podría causar daños al cliente. Cuando lo hizo, fue debido a que la AEPD ya se había puesto en contacto con la entidad para recabar información sobre lo sucedido después de que el cliente presentara una reclamación oficial.

"Error humano" frente a fallo sistémico

En sus alegaciones ante el regulador, la entidad intentó justificar el incidente como una anécdota estadística. ING expuso que el extravío afectaba a un porcentaje insignificante de su operativa (un "0,0029% del total de recogidas y envíos"), por lo que atribuyó lo sucedido a un "error humano puntual" de la empresa de transporte, defendiendo que el banco no podía ser responsable de un fallo del mensajero.

La AEPD no ha aceptado esta versión. El regulador de la privacidad subraya que el banco, como responsable de los datos cedidos por el cliente, debe vigilar en todo momento qué ocurre con ellos. Si en el proceso de tratamiento subcontrata a un tercero, debe vigilar qué hace esa empresa con la información en todos los pasos del proceso. "Al responsable le corresponde verificar que las medidas implementadas por el encargado siguiendo sus instrucciones funcionan, aun cuando ING asegure que los protocolos y procedimientos definidos por la red de mensajería son 'responsabilidad exclusiva' de dichas empresas", zanja.

Más grave aún para el organismo regulador es la ausencia de mecanismos de alerta. El contrato firmado entre el banco y la paquetera no incluía herramientas para localizar un envío en un momento dado. "ING carecía de mecanismos de alerta temprana que permitieran detectar posibles brechas de datos personales", destaca la resolución, señalando que el banco solo tuvo conocimiento del fallo "a través del propio afectado" y "no supo identificar al encargado al que encomendó la recogida de la documentación".

Si el sobre está cerrado

En sus últimas alegaciones, ING argumentó que "la documentación se encontraba en un sobre cerrado". Por ello, justifica que no hay constancia de que su contenido haya caído en manos de terceros y, por tanto, confirmación de la existencia de la brecha de seguridad.

Este argumento tampoco ha servido para esquivar la sanción. La AEPD recuerda que la pérdida de control sobre datos críticos como una fotocopia completa del DNI junto a un número de cuenta bancaria genera un riesgo severo para el ciudadano, independientemente de si se confirma o no el acceso indebido. "La combinación de este tipo de datos personales eleva significativamente el nivel de riesgo", recuerda el regulador.

Estos motivos han derivado en una infracción grave de las leyes de privacidad por falta de medidas de seguridad adecuadas. La sanción original de medio millón de euros se ha visto reducida finalmente a 400.000 euros, dado que ING ha optado por reconocer su responsabilidad y abonar la multa voluntariamente, renunciando a litigar en los tribunales, lo que le permite acogerse a una reducción del 20%.

"Respetamos y acatamos la resolución de la AEPD, con quien colaboramos activamente en línea con nuestros compromisos con la protección de los datos de nuestros clientes", ha expresado una portavoz de la entidad en un comunicado enviado a elDiario.es. "Se trató de un caso puntual y excepcional derivado de la pérdida de documentación por parte de una empresa de mensajería. No obstante, hemos revisado y reforzado nuestros procesos con este tipo de proveedores para garantizar el cumplimiento de los más altos estándares de seguridad y privacidad", concluye.

Protección de Datos empieza a multar a empresas por subir fotos al perfil de sus trabajadores sin permiso

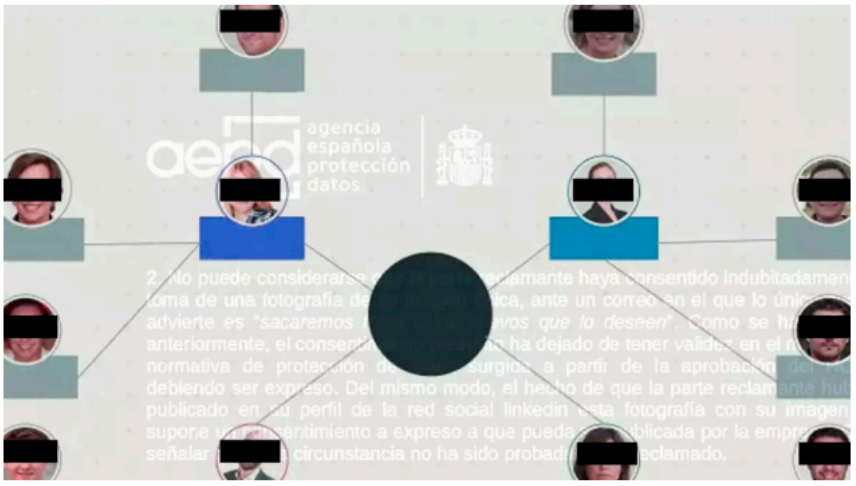
El regulador de privacidad sanciona con 5.000 euros a un despacho de abogados por este motivo, a pesar de que el empleado se sacó la fotografía y no expresó su negativa a la publicación

— Sanción de 250.000 euros a Cetelem por cargar 10 recibos de una deuda sin cobrar en la cuenta de un total desconocido

Carlos del Castillo

SEGUIR AL AUTOR/A

28 de noviembre de 2024
22:30 h
Actualizado el
29/11/2024 12:02 h
0



Se ha convertido en una costumbre habitual que empresas de todo tipo, sobre todo aquellas que ofrecen servicios especializados, suban a sus páginas web imágenes de sus empleados junto a los datos de su perfil profesional y el puesto que ocupan en el organigrama. Una práctica que, pese a extendida, va contra la normativa de privacidad si la organización no cuenta con el permiso expreso de los trabajadores para mostrar su fotografía, ha zanjado la Agencia Española de Protección de Datos (AEPD) en una reciente resolución.

El organismo ha multado por este motivo con 5.000 euros a un despacho de abogados con sede en Barcelona, Madrid y Andorra. Este publicó en la sección "Equipo" de su web una imagen de cada uno de sus trabajadores, uno de los cuales denunció esta acción ante la AEPD un mes después de abandonar la empresa. Tras un año de proceso, el regulador de la privacidad ha terminado dándole la razón y sancionando a su ex bufete.

El despacho de abogados alegó que el extrabajador había dado su consentimiento tácito a la publicación. Basaba este argumento en hechos como que el reclamante fue informado mediante un correo electrónico de que se iba a realizar la sesión de fotografías, posó para la foto, se le dio la oportunidad de "revisarlas" posteriormente para escoger la que más le gustara y además publicó una de ellas en su perfil de LinkedIn.

El bufete añade también que fue el propio extrabajador el que suministró los datos acerca de su trayectoria profesional que se incluyeron después en el apartado sobre él de la sección de "Equipo" que luego denunció.

La AEPD, sin embargo, ha rechazado este argumento. El regulador establece que las condiciones para la publicación de la imagen de los trabajadores deben incluir un "consentimiento informado, libre, específico, y prestado de manera inequívoca" para el uso de su fotografía con dicho fin. Un permiso "tácito o presunto", derivado de la participación del trabajador en la sesión de fotos o del hecho de que no se opusiera expresamente a la publicación cuando fue informado por correo electrónico no bastan para mostrar su imagen, zanja la Agencia.

El regulador recuerda que el responsable del tratamiento debe poder demostrar que el interesado ha prestado su consentimiento de forma válida. Destaca que, en este caso, la firma legal no ha podido aportar ninguna prueba de que su exempleado así lo hiciera, pese a que participara en todas las actividades que dieron lugar a la publicación de su imagen en la web y no se opusiera expresamente a ello durante el proceso.

En este sentido, apunta que el correo para informar a los empleados de la realización de las fotografías solo expresaba que "mañana sacaremos fotos a los nuevos que lo deseen", sugiriéndoles que visitarán la página de "Equipo" del despacho "para ver el estilo que usamos y elegís la que más se os ajusta". Lo cual no puede considerarse una aceptación de la publicación.

"Un consentimiento prestado libremente significa que el interesado ha de tener una opción real para no otorgarlo. En consecuencia, no puede considerarse otorgado el consentimiento libremente cuando el sujeto no puede negar su otorgamiento sin sufrir algún tipo de consecuencia negativa, extremo que deberá probar el responsable del tratamiento", afirma el regulador en la resolución.

Además de los 5.000 euros de sanción, la AEPD ha dado tres meses al bufete para recabar ese consentimiento específico e informado del resto de los trabajadores cuya imagen aparece en su web. Una recomendación que podría hacerse extensible a todas las empresas que traten la imagen de sus empleados de esta manera. La resolución reseña que la regulación de privacidad no presenta "una forma concreta de registrar el consentimiento", por lo que corre a cargo de cada organización recabarlo "de tal manera que pueda probar que el interesado ha prestado de manera válida el citado consentimiento".

El regulador de la privacidad español se ha mostrado inflexible en los procesos que afectan al uso de la imagen en fines para los que estos no han dado su consentimiento expreso. Otro de los procesos más sonados en este sentido se cerró en 2023, cuando la Agencia multó con 20.000 euros a una fábrica de plásticos de Alicante por usar la fotografía de un empleado en un sistema de fichaje por reconocimiento facial sin contar con el consentimiento expreso para ello.

Multa a una empresa de videncia por enviar cientos de SMS en tres meses a un solo móvil: “Visualizo todo sin que me digas nada”

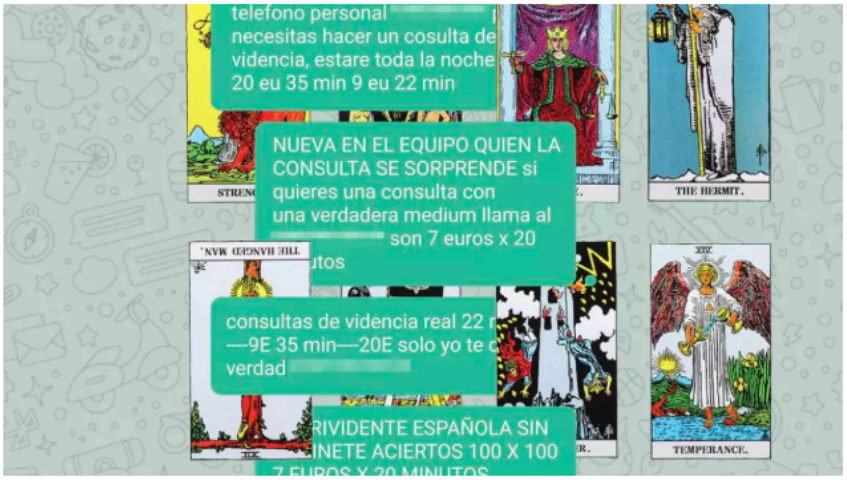
Protección de datos sanciona con 30.010 euros a un servicio de médiums y tarotistas que llegó a enviar hasta tres mensajes al día a una usuaria

— 250.000 euros de multa a Cetelem por cargar 10 recibos de una deuda sin cobrar en la cuenta de un total desconocido

Carlos del Castillo

SEGUIR AL AUTOR/A

2 de noviembre de 2024
22:48 h
Actualizado el
03/11/2024 05:30 h
6



"Clarividente española aciertos 100x100 7 euros 20 minutos". "Nueva en el equipo quien la consulta se sorprende si quieres una verdadera médium llama al ***". "Alto nivel de videncia soy profesional de más de 30 años uso carta y péndulo 22 min 9e". "Vidente natural visualizo todo sin que me digas nada realizo consultas en persona y x teléfono no tengo 806 solo mi fijo *** 22 min x 9e".

La lista sigue hasta sumar 242 SMS de la misma índole mandados a un mismo número de teléfono en un período de solo tres meses, entre agosto y noviembre de 2021. La Agencia Española de Protección de Datos (AEPD) ha multado con 30.010 euros a una empresa que ofrece servicios de videncia y tarot por este envío masivo de publicidad sin ofrecer a los destinatarios un método sencillo y gratuito para darse de baja en esa distribución.

El caso se originó a raíz de la reclamación interpuesta por una persona que recibió esos cientos de mensajes SMS, de lunes a domingo y en ocasiones hasta tres veces al día. Varias decenas de ellos aparecen reflejados en la resolución del regulador de privacidad, publicada esta semana.

A los mensajes les acompañaban llamadas de teléfono robotizadas, ha denunciado la afectada. "En las llamadas, nada más responder nosotros al teléfono, una locución grabada

nos ofrece servicios de videncia; en los SMS lo mismo, identificando un número fijo y/o móvil al que debemos llamar si estamos interesados en dichos servicios", recoge la resolución.

La empresa de videncia, Rianlu Europa, con sede en Alcorcón (Madrid), ha alegado que el envío de los mensajes estaba justificado porque la reclamante había realizado previamente llamadas a la empresa para solicitar sus servicios. Sus gestores justifican que sus clientes activaban "de forma automática" el envío de publicidad por SMS al llamar a la centralita. Además, reconocen que el período de envío fue incluso más largo del que denuncia la reclamante, ya que sucedió desde abril de 2021 a mayo de 2022.

Según la versión de la empresa, el alto número de mensajes publicitarios se debe a que recibió hasta 49 llamadas desde su móvil. "Si la reclamante siguió recibiendo SMS fue única y exclusivamente motivado por las nuevas y reiteradas llamadas que se produjeron desde dicho número, como venimos explicando, bien por ella, bien por personas de su entorno con acceso a dicho número y que producían, de forma automática, la activación de la acción comercial y el motivo de seguir recibiendo los SMS", argumenta.

Aunque la afectada alega que varias de esas llamadas se produjeron para solicitar el cese del envío de SMS publicitarios, Rianlu lo niega y afirma que "dichas llamadas nunca fueron para interesar la baja, lo fueron para hablar con nuestras tarotistas o videntes". Indica a su vez que el primer contacto se produjo por la reclamada en enero de 2021, antes del envío de los primeros mensajes publicitarios.

La AEPD no entra al fondo de esta cuestión ni fiscaliza la veracidad de la lista de llamadas proporcionada por la empresa de videncia. Al contrario, expresa que aunque estas se produjeran o no, el proceso sancionador se centró en el envío de SMS publicitarios sin la opción de darse de baja de la recepción, no en si la reclamante utiliza o no los servicios de videncia de la empresa. Además, recuerda que la ley exige instaurar ese mecanismo de cese de las comunicaciones comerciales en todos los casos.

"La recepción de forma constante de mensajes SMS con publicidad de servicios de videncia y tarot sin ofrecer un procedimiento sencillo y gratuito tanto en el momento de la recogida de los datos como en cada una de las comunicaciones comerciales, no solo ha ocasionado una molestia a la reclamante (recordemos que se recibían prácticamente a diario, también los fines de semana y en muchas ocasiones tres SMS por día), sino que también la ha situado en una posición de indefensión, ya que desconocía la identidad de la empresa responsable del envío de la publicidad a través de mensajes SMS y, en consecuencia, no podía solicitar la baja de dicho servicio de publicidad", señala la Agencia.

Aunque la empresa ha alegado que incluyó esta posibilidad de darse de baja a raíz del inicio del procedimiento, la AEPD no lo ha considerado atenuante suficiente para evitar la sanción. Los 30.010 euros de multa corresponden al tramo más bajo de las sanciones estipuladas como "graves" en la Ley de Servicios de la Sociedad de la Información para el envío de comunicaciones comerciales no solicitadas (30.001 euros a 150.000, con las infracciones "muy graves" en el rango de los 150.001 a los 600.000 euros).

Multa de 3,2 millones a Carrefour por múltiples brechas de seguridad que afectaron a 120.000 clientes

Protección de Datos sanciona a la cadena por no establecer las medidas de seguridad necesarias para evitar el robo de datos de sus clientes en seis ciberataques que utilizaron exactamente la misma técnica

— El timo del iPhone nuevo: así funciona la estafa que suplanta a las operadoras para cambiar de móvil

Carlos del Castillo

SEGUIR AL AUTOR/A

4 de junio de 2025 13:53 h
Actualizado el
04/06/2025 13:55 h
2

Acceso a un supermercado de la cadena Carrefour EFE/Miguel Ángel Gayo/Archivo

La Agencia Española de Protección de Datos (AEPD) ha impuesto una multa de 3,2 millones de euros a Carrefour por múltiples infracciones graves relacionadas con la seguridad y el manejo de los datos personales de sus clientes. La sanción llega una investigación que ha revelado fallos significativos en la protección de información sensible, que se vio comprometida hasta por seis ciberataques sufridos por la cadena en 2023. Estos afectaron a un total de 118.954 personas.

La técnica utilizada por los ciberdelincuentes fue el "credential stuffing", un tipo de ataque que, en lugar de intentar desentrañar las contraseñas de los usuarios con fuerza bruta informática, se basa en el uso automatizado de combinaciones de correos electrónicos y contraseñas previamente filtradas en otras brechas de seguridad. Los atacantes prueban estas credenciales en masa en distintos servicios, confiando en que muchos usuarios reutilizan las mismas contraseñas en múltiples plataformas.

En el caso de Carrefour, esta práctica permitió repetidos accesos no autorizados a cuentas de clientes, exponiendo sus datos personales. Los paquetes de información robada difirieron en cada una de las brechas, incluyendo desde referencias que permiten la identificación de los usuarios (nombre, apellidos, correo electrónico, teléfono de contacto, DNI o NIE, dirección postal y fecha de nacimiento) hasta datos económicos o financieros (aunque sin medios de pago directos) credenciales de acceso a sus servicios, como usuario y contraseña.

Durante la investigación, Carrefour argumentó que el número de cuentas donde se confirmó la validez de credenciales (118.895) no implica un acceso a datos personales en todos los casos. La cadena francesa asegura que la afectación real a la integridad de las cuentas solo fue de 234 casos y a la confidencialidad de 973 casos. No obstante, la AEPD ha rechazado este argumento, afirmando que el acceso exitoso a las contraseñas ya implica un alto riesgo y una pérdida de control sobre los datos de las 118.895 cuentas de cliente afectadas.

La cuantía de la multa deriva de tres infracciones de la normativa de privacidad. Por un lado, por una violación "muy grave" del principio de integridad y confidencialidad de los datos, por el que la Agencia multa a Carrefour con dos millones de euros; a la que se suma otra calificada como "grave" por no establecer las correctas medidas de seguridad para evitar estos ciberataques, sancionada con otro millón de euros. Por último, el regulador establece una tercera sanción "leve" por no comunicar correctamente lo sucedido a los afectados, de 200.000 euros.

La AEPD destaca varias deficiencias por parte de Carrefour durante la investigación, que a juicio del regulador justifican la sanción. Por ejemplo, que la empresa no implementó la medida de seguridad del doble factor de autentificación (confirmación de identificación a través de un método adicional a la contraseña) hasta después de la quinta brecha. Además, sus sistemas permitían la consulta masiva de información desde direcciones IP distintas sin detectarlo como una anomalía.

elDiario.es se ha puesto en contacto con Carrefour para incluir su posición en esta información y preguntar si planea recurrir la sanción ante la Audiencia Nacional, pero todavía no ha recibido respuesta. La cadena, no obstante, no ha ejercido la posibilidad de reducir un 20% la cuantía de la sanción por asunción de responsabilidad, ni el 20% adicional por pronto pago.

Riesgo de suplantaciones

El tipo de datos robados a Carrefour son la materia prima que los ciberdelincuentes utilizan para realizar ataques de suplantación de identidad. En ellos, se hacen pasar por empresas como Carrefour u otras instituciones intentando ganarse la confianza de la víctima haciéndole ver que conocen sus datos y situación personal. Una de sus técnicas más utilizadas es inducir una situación de urgencia, en la que el objetivo debe realizar algún tipo de acción con rapidez para evitar un problema o situación negativa.

En caso de sospecha de haber clicado en un enlace fraudulento o de haber introducido datos bancarios en páginas que podrían estar operadas por ciberestafadores, la recomendación de las fuerzas de seguridad es comunicar lo sucedido de inmediato al banco y denunciar los hechos a la Policía. El Instituto Nacional de Ciberseguridad dispone del número gratuito 017 y del teléfono de WhatsApp 900 116 117 para resolver dudas de seguridad. Atiende a ciudadanos, empresas y profesionales y es confidencial.