Miércoles, 9 de abril de 2025

CincoDías

RR HH. Las directoras de personas de los bufetes incorporan la IA en sus procesos —P3

Legal

ARANZADI LA LEY | KARNOV GROUP

Rafael Yuste, a la derecha, prueba un aparato neurotecnológico en el documental *Theater of Thought*.

Leyes para proteger el cerebro de las garras tecnológicas

Ya es posible descifrar pensamientos o aumentar la capacidad mental ▶ Juristas y neurocientíficos urgen un nuevo orden legal

MARCELINO ABAD
MADRID

Como publicó la revista *Nature Neuroscience* la semana pasada, una mujer tetrapléjica y sin capacidad de hablar ha logrado comunicarse usando la voz que tenía en el vídeo de su boda. Veinte años después de sufrir un derrame, una interfaz cerebro ordenador entrenada con inteligencia artificial (IA) ha convertido en palabras lo que ocurre en su red neuronal al intentar hablar, reproduciéndolas casi en tiempo real con su voz sintetizada. Igual que el autocompletado de un procesador de texto puede adivinar la palabra que estamos escribiendo, la IA generativa aplicada a actividad cerebral ya es capaz de averiguar qué es lo que una persona quiere hacer. Desde el punto de vista de las enfermedades neurológicas, estos avances están revolucionando la medicina.

Los dispositivos utilizados para acceder y manipular los sistemas neuronales, sin embargo, presentan riesgos colosales para la privacidad mental cuando se emplean fuera del ámbito médico. Neurocientíficos y supervisores de protección de datos tienen los ojos puestos en un número creciente de artilugios no invasivos que registran la actividad cerebral, que es el motor de nuestro cuerpo. Se trata de cintas para la cabeza, auriculares o gafas que se dirigen al público en general "para dormir mejor", "mejorar el rendimiento" o la experiencia en videojuegos. Los datos recabados, con análisis avanzados e IA, podrían revelar lo que conocemos comúnmente como pensamientos, estados de salud o emocionales.

En el mercado ya se comercializan dispositivos para medir o manipular la actividad cerebral

Son diademas o cascos "para mejorar el bienestar"; algunas empresas venden los datos obtenidos

Una de las voces más respetadas a nivel internacional en el estudio del cerebro es Rafael Yuste, director del Centro de Neurotecnología de la Universidad de Columbia (EE UU). El neurocientífico se quedó atónito hace diez años, cuando, en un experimento con roedores, pudo manipular un grupo de neuronas de un ratón para hacerle creer que estaba viendo una imagen que no le había enseñado. "Es como si le hubiésemos metido en el cerebro una alucinación", relata por Zoom a **CincoDías** desde su despacho en Nueva York. "Esto que hemos hecho en ratones no ha llegado [a aplicarse en personas], falta tiempo, pero se empiezan a utilizar otro tipo de métodos más groseros en humanos tanto para medir la actividad cerebral como para cambiarla", advierte el investigador, discípulo de los premios Nobel Torsten Wiesel y Sidney Brenner.

Yuste se refiere a experimentos recientes, como uno desarrollado por la Universidad de Sídney

—Continúa en P2

En portada

—Viene de P1

en 2023. Se trata de una especie de gorro portátil acoplado a un sistema de IA generativa, capaz de decodificar el lenguaje mental y convertirlo en texto mediante un modelo parecido a ChatGPT. "En el futuro vienen aplicaciones más potentes, como escribir a máquina en una computadora a base de pensar el texto. Hay bastantes compañías que están intentando fabricar estos productos, incluida Meta. Esto abre las puertas a problemas éticos muy gordos porque igual se cuela alguna cosa que no es el texto que [la persona] quiere escribir. Por eso, estamos muy preocupados".

La posibilidad de aumentar la capacidad mental es otra de sus inquietudes. "Hay un caso de hace más de dos años de un grupo en Boston que utilizó actividad cerebral magnética para incrementar la memoria a corto y largo plazo. Esto es un ejemplo del futuro, en el que se podrá utilizar neurotecnología para medir la actividad mental o para cambiarla". Si bien estos experimentos podrían ayudar, por ejemplo, a personas con alzhéimer, de comercializarse masivamente podrían dar lugar a dos tipos de seres humanos: los de capacidades aumentadas, con recursos económicos suficientes para pagar por ellos, y el resto, con las implicaciones éticas que ello conllevaría.

Venta de datos

El mercado de la neurotecnología se estimaba en 2024 en 15,18 billones de dólares, según Mordor Intelligence, una empresa de investigación de mercado que espera que crezca hasta los 28,57 billones en 2029. Tanto los dispositivos portátiles que registran la actividad cerebral como los que pueden llegar en un futuro próximo están en el punto de mira. La fundación que preside Yuste, la Neurorights Fundation, publicó el año pasado un estudio basado en las políticas de privacidad de 30 empresas que venden artilugios de neurotecnología a consumidores, entre las que se encuentran Emotiv, Neurosky, OpenBCI y un largo etcétera de compañías conocidas por sus diademas y cascos. El informe revela que "29 de las 30 empresas (96,67 %) parecen tener acceso a los datos neuronales del consumidor sin limitaciones significativas de acceso" y "casi todas pueden compartir datos con terceros". Hay "amplias brechas entre los estándares internacionales y las prácticas reales de datos", advierte.

"Descubrimos que en los contratos que celebran con los clientes, que son aquellos en los que tienes que decir que sí antes de encender el dispositivo o bajarte el software, lo primero que hacen es tomar posesión legal de todos los datos neuronales. En la mayor parte [de los contratos], cuando asientes, autorizas a la compañía a venderlos a terceras partes", alerta Yuste, pues todo lo que somos está en el cerebro.

Esta permisividad se debe, según apunta el profesor de Derecho Constitucional Luis Miguel González de la Garza, a que esos datos cerebrales "no se consideran médicos, sino lúdicos, y, por lo tanto, no están regulados como si fueran datos médicos". El Reglamento Europeo de Protección de Datos (RGPD), en vigor desde 2016, confiere la máxima protección a la información sobre la salud, cuyo tratamiento está prohibido con carácter general. No obstante, como el RGPD es anterior a los últimos avances en neurotecnología, hay división de opiniones entre los juristas sobre si los datos neuronales se engloban dentro de los datos biométricos, que son aquellos dirigidos a identificar de manera unívoca a las personas, y que también gozan de especial protección. Por eso, el neurocientífico recomienda al legislador comunitario ampliar la protección del RGPD, definiendo qué son los neurodatos y la neurotecnología para dotarlos de la máxima seguridad.

Como los derechos avanzan a un ritmo más lento que el desarrollo científico, la Neurorights Fundation que preside Yuste también defiende desde 2017 un nuevo marco jurídico de derechos humanos, los neuroderechos, destinados a salvaguardar la información del cerebro, la médula espinal y la red de nervios que transmite mensajes por el cuerpo. Estos derechos engloban la privacidad mental, la identidad personal, la libertad de pensamiento, el acceso equitativo a la neuroaumentación y la protección contra los sesgos algorítmicos.

Rafael Yuste aboga por una declaración universal de derechos neurológicos contra la manipulación mental

Garrigues Walker defiende una reforma constitucional en España para blindar los neuroderechos

Neuroderechos

Así, esta arquitectura jurídica obligaría a proteger a las personas frente a la divulgación no consentida de su información cerebral; impediría que se altere la personalidad por los efectos de la conexión del cerebro a ordenadores; preservaría la capacidad de las personas de tomar decisiones libres, sin manipulación; garantizaría la igualdad de acceso al aumento de la capacidad mental y prohibiría la discriminación por información obtenida de la neurotecnología, como la ideología o la orientación sexual.

Esta protección específica de la actividad cerebral cuenta con el respaldo de prestigiosos juristas, como el abogado Antonio Garrigues Walker o el profesor González de la Garza. El año pasado publicaron el libro *Qué son los neuroderechos y cuál es su importancia para la evolución de la naturaleza humana* (Aranzadi La Ley), donde analizan "lo que un conjunto de neurotecnologías va a desproteger en un futuro que cada vez está más próximo". Según dicen en conversación con este diario, en España "sería recomendable una reforma constitucional" para proteger particularmente los datos neuronales. Ante la falta de consensos políticos, abogan por "una ley orgánica que desarrolle un marco jurídico seguro y eficaz" de forma urgente. "No es un tema abstracto; afecta a la vida" de los ciudadanos, sentencia Garrigues Walker.

Diputados

En 2024, Rafael Yuste se reunió con diputados y senadores de todas las formaciones para proteger específicamente por ley los datos neuronales. "Les hablé de esta problemática y estaba todo el mundo de acuerdo", de EH Bildu a Vox, asegura. "Pero a día de hoy no he recibido ninguna propuesta. Parece que hay buena sintonía, pero falta liderazgo interno", lamenta. Sí lo encontró en Colorado y California (EE UU), donde republicanos y demócratas fueron de la mano el año pasado al ampliar la definición de datos protegidos en sus respectivas leyes de privacidad para incluir la información biológica y neuronal, en línea con la recomendación que le lanza al legislador comunitario.

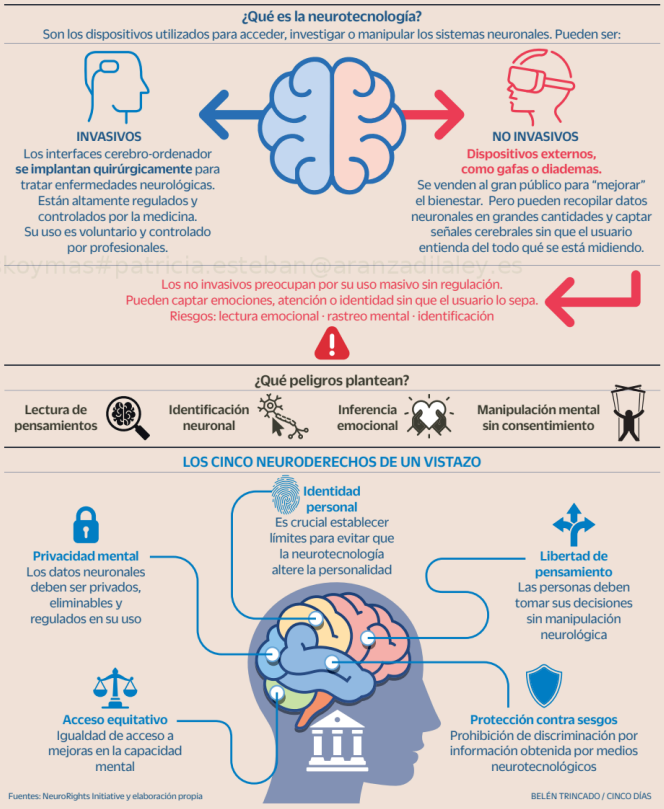
En 2021, con el asesoramiento de Yuste, Chile se convirtió en el primer país del mundo en reformar su Constitución para introducir en su artículo 19 que "el desarrollo tecnológico estará al servicio de las personas (...) debiendo resguardar especialmente la actividad cerebral". El neurocientífico también ha estado detrás de la enmienda constitucional que protege la actividad cerebral en el estado brasileño de Río Grande del Sur.

Precisamente, la primera sentencia sobre neuroderechos fue dictada por la Corte Suprema de Chile en 2023. Falló contra la empresa Emotiv que aparece en los papeles de la Neurorights Fundation por comercializar una diadema llamada Insight para "mejorar tu rendimiento mental". Preventivamente, ordenó retirar el producto y obligó a la empresa a eliminar la información de su nube.

La Agencia Española de Protección de Datos insiste en que los proveedores "tienen que implementar medidas de protección y atender los derechos de los ciudadanos". Están trabajando en la UE para impulsar "una postura internacional". El objetivo es claro: poner coto a los usos indebidos de la neurotecnología.

Neuroderechos: protegiendo la mente en la era digital

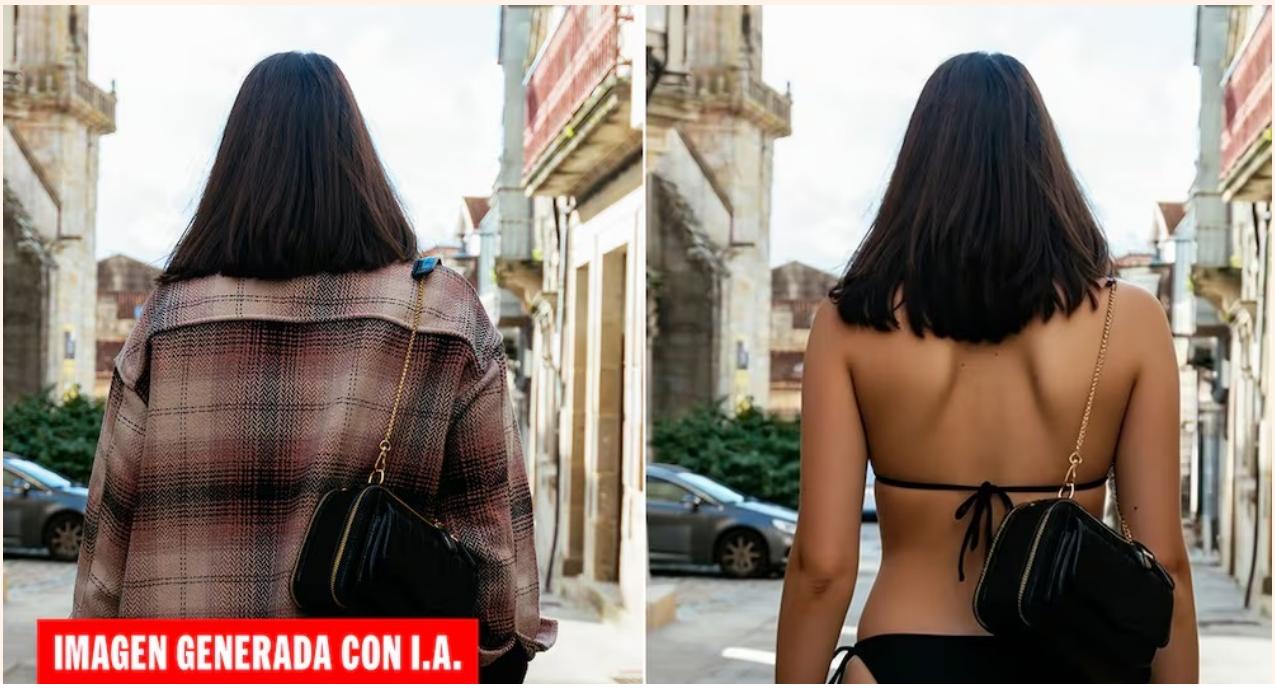
La neurotecnología plantea nuevos retos éticos y legales



DEEPFAKE >

El escudo legal frente a los 'deepfakes' sexuales: los desnudos generados con IA van más allá de Grok

El presidente de la Agencia de Protección de Datos advierte que usuarios y plataformas pueden responder de la difusión no consentida de contenido pornográfico manipulado



A la derecha, ejemplo de una imagen editada con el programa de IA Grok, de X.

MARCELINO ABAD RAMÓN

Madrid - 14 ENE 2026 - 08:58CET

"Grok, ponla en bikini; ponla en bikini a cuatro patas; ponla en bikini cubierta de aceite". Estas han sido algunas de las órdenes utilizadas desde finales de 2025 por usuarios de X para que Grok, la inteligencia artificial integrada en la red social, generase imágenes falsas y sexualizadas de mujeres y adolescentes a partir de fotos reales, sin el consentimiento de las afectadas. La semana pasada, X restringió la generación de imágenes a los suscriptores verificados tras las investigaciones abiertas en varios países. Sin embargo, la práctica de los *deepfakes* sexuales no se limita a la red social de Elon Musk ni es nueva. Se remonta, al menos, a 2017.

El término procede del alias del primer usuario que popularizó este tipo de contenido audiovisual falso en la plataforma Reddit, bajo el pseudónimo de Deepfake. Aquel usuario comenzó a difundir vídeos sexuales manipulados en los que insertaba los rostros de actrices y celebridades como Scarlett Johansson, Taylor Swift o Gal Gadot. Desde entonces, la tecnología ha evolucionado de forma imparable, logrando una apariencia cada vez más realista y extendiéndose a páginas de contenido para adultos. Allí numerosas mujeres famosas han sido víctimas de pornografía falsa generada por inteligencia artificial (IA).

Cada vez con más frecuencia las mujeres anónimas también son objeto de este tipo de contenido, a veces creado por sus excompañeros sentimentales para vengarse de ellas. Para Elisa García, profesora de sociología de la Universidad Complutense de Madrid (UCM), los *deepfakes* constituyen "una continuidad digital de formas históricas de control, vigilancia y apropiación de los cuerpos femeninos".

Adolescentes y mujeres convertidas en negocio

Miembro de DiViSAR, un proyecto que estudia las prácticas de violencia sexual digital en España, García ha observado en una investigación reciente que mientras que los hombres aparecen mayoritariamente en *deepfakes* no sexuales, las mujeres y niñas son representadas en contenidos sexualizados. El *informe State of deepfake* 2023 de la empresa Security Hero indica que el 99% del contenido pornográfico *deepfake* está protagonizado por mujeres. "Estas dinámicas se insertan en una cultura de la violación digital, sostenida por comunidades online y tecnoculturas masculinas que normalizan la violencia sexual y refuerzan la misoginia frente a una pedagogía del consentimiento", dice.

El impacto sobre menores es especialmente alarmante. En 2023, en Almendralejo (Badajoz), un nutrido grupo de chicos utilizó aplicaciones de IA para crear imágenes manipuladas de adolescentes de entre 11 y 17 años, superponiendo a los rostros originales cuerpos femeninos desnudos. Posteriormente, las fotografías fueron compartidas a través de grupos de WhatsApp. La aplicación empleada, que "ofrece una solución de desnudos íntegros accesible y potente", según se publicita, tiene cerca de medio millón de usuarios registrados en España.

Estas plataformas operan dentro de una lógica económica que, en opinión de García, "convierte la misoginia en un recurso rentable". Según el informe de la empresa de ciberseguridad, crear un video sexual de 60 segundos usando una sola imagen de la cara puede costar cero euros. Entre 2022 y 2023, la cantidad de pornografía *deepfake* creada aumentó en un 464%. A través de modelos *freemium*, suscripciones o pagos por versiones mejoradas se está configurando una economía del *nude* "basada en la explotación de cuerpos ajenos sin consentimiento", subraya la profesora. Mordor Intelligence

señala que el mercado de los *deepfakes* alcanzó los 1.140 millones de euros en 2025 y prevé que crezca hasta los 8.110 millones en 2030.

La responsabilidad de usuarios y plataformas

La Agencia Española de Protección de Datos (AEPD) es consciente de esta problemática. En octubre multó con 2.000 euros, reducidos a 1.200 por pronto pago, al creador de uno de los desnudos falsos de las adolescentes de Almendralejo. Se trata de la primera resolución que penaliza la difusión de imágenes manipuladas con IA en España, marcando un precedente en el ámbito de los *deepfakes* sexuales.

La advertencia principal que el presidente de la AEPD, Lorenzo Cotino, traslada a los usuarios de este tipo de aplicaciones es clara: "Subir la imagen de una persona para que un sistema de inteligencia artificial la modifique, recree o sexualice constituye un tratamiento de datos personales y, como regla general, requiere el consentimiento de la persona afectada". Si ese tratamiento genera un "impacto intenso" en derechos como la protección de datos, la propia imagen, el honor o la intimidad (por ejemplo, mediante la generación de desnudos o contenidos sexualizados), puede dar lugar a una infracción sancionable.

Es más complejo analizar la responsabilidad de las plataformas de IA ya que no existe una respuesta única. El derecho europeo parte de que, en general, "no responden de forma automática" por las conductas ilícitas de los usuarios, del mismo modo que ocurre con las redes sociales. La diferencia aparece cuando la plataforma "no se limita a alojar contenidos, sino que genera activamente imágenes o vídeos a partir de materiales aportados por los propios usuarios", que después pueden difundirse dentro o fuera del servicio.

Aunque en principio se mantiene el esquema de ausencia de responsabilidad directa, esta conclusión puede matizarse en función del tipo de servicio, de su grado de intervención en el resultado final y del derecho afectado. Cuando existe conocimiento efectivo de la ilegalidad, "la responsabilidad puede activarse si la plataforma no actúa con la debida rapidez para retirar o bloquear el contenido", dice Cotino. Esto puede explicar que Grok haya limitado la generación de imágenes después de que varios países, España incluida, hayan abierto investigaciones.

La situación cambia aún más cuando se trata de sistemas de inteligencia artificial cuya finalidad principal es la generación de imágenes o vídeos pornográficos. En estos casos, "resulta más difícil sostener que los usos ilegales sean marginales o excepcionales", considera el presidente de la AEPD. Un ejemplo se ha dado en Italia, donde la autoridad de protección de datos ordenó el bloqueo de un servicio que generaba imágenes sexuales usando sin consentimiento los rostros de miles de mujeres, incluidas figuras públicas como la primera ministra Giorgia Meloni o la líder del Partido Democrático Elly Schlein. Aun así, la clausura de una plataforma no constituye la regla general y siempre requiere un examen "especialmente cauteloso y proporcionado".

Respuesta penal

Aunque diversas aplicaciones de IA permiten generar imágenes y vídeos sexuales sin el consentimiento de las víctimas, esto no impide que sus responsables puedan ser perseguidos legalmente. Según explica Borja Adsuara, jurista especializado en tecnología, el Código Penal castiga a quien produzca o facilite a terceros un programa informático diseñado principalmente para cometer delitos o ayudar a que otros los comentan. En relación con los *deepfakes*, "existe un derecho fundamental a nuestra propia imagen que, aparte de la protección de datos, tiene una protección civil y penal", subraya.

En esta línea, el Consejo de Ministros aprobó este martes un anteproyecto de ley de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Considera ilegítimo el uso y difusión de imágenes o voces manipuladas sin consentimiento a través de la inteligencia artificial. En el texto, los *deepfakes* se denominan "ultrasuplantaciones".

Incluso, sin una tipificación especifica, la creación y difusión de este contenido manipulado puede encajar ya en "distintos delitos", explica Gerard Espuga, abogado en Beta Legal. Por ejemplo, si se difunden datos o contenidos para hostigar a la víctima, puede tratarse de acoso, el llamado *doxing*; si se crea o comparte con la intención de humillar o menoscabar gravemente la dignidad personal, puede constituir un delito contra la integridad moral; si se utiliza para coaccionar, entra en el ámbito de las amenazas; si atenta gravemente contra el honor o la dignidad, puede constituir un delito de injurias; y cuando representa a un menor o a alguien que aparenta serlo en conductas sexuales explícitas o de sus órganos sexuales, puede tratarse de pornografía infantil.

En relación con los menores, el Consejo de Ministros aprobó en marzo un proyecto de ley orgánica para reformar el Código Penal y penalizar los *deepfakes* de contenido sexual y el *grooming*, es decir, el engaño a un menor utilizando una identidad ficticia.

Los expertos recomiendan a las personas afectadas por los *deepfakes* denunciar de inmediato ante las Fuerzas y Cuerpos de Seguridad, quienes se ocupan de iniciar las investigaciones pertinentes. De forma complementaria, y en función de la gravedad, pueden acudir al Canal Prioritario de la AEPD, que puede solicitar la retirada rápida de los contenidos. Además, el Instituto Nacional de Ciberseguridad (INCIBE) ofrece un servicio de respuesta a incidentes de ciberseguridad, por lo que

es apropiado notificarle lo sucedido.

Frente a la amenaza creciente de los *deepfakes*, “el marco jurídico no parte de cero”, ya que existen mecanismos policiales, judiciales y administrativos para proteger a las víctimas. No obstante, “es razonable plantear ajustes normativos por el legislador y, sobre todo, una actualización interpretativa del Derecho”, concluye Lorenzo Cotino, presidente de la AEPD.

ÚLTIMAS NOTICIAS

11:41 | **Aena descarta transferir aeropuertos, pero admite que hay "espacio para avanzar en la coordinación con comunidades autónomas"**

11:11 | **Barceló cerró 2025 con un beneficio récord de 300 millones de euros y prevé invertir 500 millones este año**

11:06 | **Últimos días para inscribirse a la oferta de 17.986 plazas de empleo público de la Administración general del Estado**

10:50 | **La justicia europea sentencia que el reembolso de un billete de avión por cancelación del vuelo debe incluir la comisión del intermediario**

BUSCAR BOLSAS Y MERCADOS

Buscar

IBEX 35 EUROSTOXX S&P 500

PRIVACIDAD >

La creación de currículos con IA se desborda y abre un frente de riesgo para la protección de datos

Las solicitudes de empleo han crecido un 239% desde el lanzamiento de ChatGPT, pero la masiva generación de datos plantea riesgos de reutilización y transferencia

¿Qué saben de ti las plataformas con IA?

PLATAFORMA	¿Qué datos recoge?	¿Entrena IA con tus datos?	¿Los comparte?	¿Fuera de la UE?	¿Los protege?
ChatGPT Gratuito	Cuenta, conversaciones, archivos, uso, dispositivo.	Sí, pero puedes oponerte.	Proveedores y autoridades.	Sí (EE UU)	Cifrado, controles.
Copilot Personal	Prompts, feedback, IP, ubicación.	No por defecto.	Proveedores de Microsoft.	Sí	Cifrado, aislamiento, controles.
Gemini	Conversaciones, ubicación, uso.	Sí, pero puedes oponerte.	Proveedores, revisores humanos, extensiones.	Sí (EE UU)	Cifrado, anonimización, controles.
Canva	Personales, contenido subido, uso.	Sí, pero puedes oponerte.	Afiliados, socios.	EE UU y otros países	Encriptado, autenticación, etc.
LinkedIn	Perfil, CV cargado, publicaciones, uso y dispositivo.	Sí, pero puedes oponerte.	Socios, proveedores y autoridades.	EE UU	Medidas técnicas y legales.

InfoJobs	Perfil, CV, uso, cookies.	Sí, puedes ejercer derechos RGPD.	Empresas ofertantes y proveedores.	Sí, si la oferta lo requiere	Controles de acceso, cifrado y auditorías.

Fuente: políticas de privacidad de las plataformas

BELÉN TRINCADO / CINCO DÍAS

MARCELINO ABAD RAMÓN

28 ENE 2026 - 05:25CET

De tardar horas en redactar un currículum a tener cinco versiones en cuestión de minutos. Al calor de la inteligencia artificial (IA) se consolida una nueva tendencia en la búsqueda de empleo que no está exenta de riesgos para la protección de datos. Las empresas fueron las primeras en incorporarla a los procesos de selección para dar con candidatos de forma predictiva, realizar el primer cribado de currículums o analizar el *match* entre competencias y aptitudes.

Ahora el fenómeno se está invirtiendo. Son los propios candidatos quienes recurren de forma intensiva a la IA para redactar currículums y cartas de presentación, optimizándolos con palabras clave diseñadas para superar los filtros de los sistemas de selección de personal (ATS). También la utilizan para postularse automáticamente a decenas de ofertas o generar fotografías profesionales. Si la IA aplicada al reclutamiento ya planteaba interrogantes en materia de transparencia, elaboración de perfiles y toma de decisiones automatizadas, su utilización masiva por parte de los candidatos introduce un nuevo desafío: la comunicación de grandes volúmenes de datos a sistemas de terceros, sin que exista un control exclusivo sobre su reutilización o transferencia internacional.

El resultado es un aumento explosivo de candidaturas que está tensionando los procesos de selección. Según una comunicación de Canva, el 41% de los candidatos en España utilizó IA generativa en 2024 para mejorar su currículum, y el generador

de textos con IA de esta plataforma fue utilizado 13,7 millones de veces. “Podemos hablar de una inflación de currículums optimizados”, dice Mamen Blanco, experta en IA aplicada a recursos humanos. El riesgo es que “muchas personas introducen datos personales sin revisar cómo están configuradas las herramientas. A nivel individual esto ya es delicado, pero a nivel empresarial es especialmente arriesgado porque puede implicar una cesión involuntaria de información confidencial”.

A escala global, el fenómeno es más acusado. El número de solicitudes de empleo que envía un candidato promedio ha aumentado en un 239% desde el lanzamiento de ChatGPT en 2022, según datos de Greenhouse, una plataforma de gestión de procesos de selección, recopilados por *The Economist*. Herramientas como JobCopilot o LazyApply permiten rellenar solicitudes automáticamente mientras los candidatos dedican “su valioso tiempo” a otra cosa. Desde LinkedIn informan que en los próximos meses estará disponible en español Job Match, un servicio que muestra hasta qué punto las competencias de un profesional encajan con los requisitos de cada oferta, “ayudándole a priorizar candidaturas”. Además, su herramienta AI Powered Job Search ya permite describir el puesto que el usuario busca para recibir sugerencias personalizadas. Junto a estas funcionalidades, también proliferan asistentes con IA que sugieren respuestas en las entrevistas online tras procesar la información personal del candidato, sin que el reclutador tenga acceso al contenido generado.

Mejor sin nombre

Ante este cambio de paradigma, la Agencia Española de Protección de Datos (AEPD) recomienda no cargar en los asistentes de IA generativa “datos personales como el nombre completo, dirección, número de teléfono, DNI, NIE o fotografías”. El motivo es la “pérdida de control” de la información. “Al subir una imagen, el contenido deja de estar

bajo el poder exclusivo del usuario y pasa a ser tratado por un proveedor externo que decide cómo se procesa", explican fuentes de la agencia.

Por ello, los expertos en privacidad aconsejan minimizar los datos compartidos. Joaquín Muñoz, socio del área de Privacy & Data Protection en Bird & Bird, dice que "no hace falta incluir toda nuestra información sensible desde el principio. Mi recomendación es utilizar estas herramientas para generar la estructura, aprovechando su capacidad de optimización, pero hacer los ajustes finales en nuestro equipo".

Política de privacidad

Una lectura de las políticas de privacidad de estas plataformas muestra que el uso de los datos no se limita a la prestación inmediata del servicio. Canva puede recopilar los textos, imágenes o vídeos que el usuario sube para usar en los diseños, incluso con fines de aprendizaje automático, y recibir información de terceros como Facebook, Instagram o LinkedIn sobre el puesto o la empresa en la que trabaja, por ejemplo. Parte de estos datos puede ser transferida fuera de la Unión Europea, a países como Estados Unidos, Filipinas o Singapur, sujetos a leyes de protección de datos distintas. Los asistentes conversacionales y generativos, como ChatGPT o Gemini, siguen patrones similares: recopilan los datos personales proporcionados al crear la cuenta, así como los archivos, imágenes, audios e instrucciones que el usuario carga. Esta información puede usarse para mejorar sus capacidades de respuesta, salvo que la persona se oponga. Plataformas como LinkedIn también emplean los datos de sus miembros para entrenar sus modelos de IA.

Todo esto se realiza dentro del marco del Reglamento General de Protección de Datos, que obliga a estas plataformas a garantizar la seguridad de la información y aplicar mecanismos

apropiados en las transferencias fuera de la Unión Europea. Aun así, como en cualquier servicio digital, existe un riesgo inherente de brechas de seguridad, por lo que conviene revisar los términos de cada plataforma para comprender cómo usan los datos.

Este tipo de riesgos se materializa en casos concretos. En junio de 2025, investigadores de seguridad detectaron una vulnerabilidad en la plataforma de selección de McDonald's. El acceso al panel administrativo de un entorno de prueba estaba protegido únicamente con la contraseña por defecto "123456", lo que permitió visualizar hasta 64 millones de solicitudes de empleo, incluyendo nombres, correos electrónicos y transcripciones de entrevistas.

Este episodio evidencia que, en entornos digitalizados, hasta un fallo básico puede tener un impacto masivo. Por eso, subraya el abogado de Bird & Bird Joaquín Muñoz, "si una aplicación no genera confianza o sus términos son excesivamente permisivos o poco claros, es preferible buscar alternativas más seguras, aunque eso pueda implicar renunciar a ciertas funcionalidades creativas. La comodidad no debería ir en detrimento de la protección de datos".

Derecho a saber si la IA decide tu candidatura

Cuando una empresa utiliza un algoritmo para evaluar un currículum, el candidato tiene derecho a saberlo. Así lo establece el Reglamento General de Protección de Datos (RGPD), que reconoce el derecho de acceso a la información sobre el tratamiento de los datos personales. "Este derecho incluye conocer si se han usado sistemas automatizados, así como recibir una explicación comprensible de la lógica aplicada", explica Adrián Todolí, catedrático de Derecho del Trabajo de la Universidad de Valencia. Además, la normativa permite impugnar la decisión algorítmica cuando afecte de manera significativa al candidato.

El artículo 22 del RGPD refuerza esta protección al reconocer el derecho a no ser objeto de decisiones basadas únicamente en tratamientos automatizados. “El rechazo de una candidatura laboral es un claro ejemplo de efecto perjudicial”, subraya el jurista, que analiza estas cuestiones en su libro *Algoritmos productivos y extractivos*, editado por Aranzadi LA LEY.

Sin embargo, ejercer estos derechos puede ser complejo debido a la opacidad de los sistemas. El candidato no conoce ni a los demás aspirantes ni los criterios reales de comparación, por lo que el primer paso consiste en solicitar información sobre los parámetros y variables utilizados por la IA. “Si la empresa no facilita la información, la ofrece de forma incompleta o, aun siendo correcta, revela indicios de discriminación, estos elementos pueden utilizarse como prueba en un procedimiento posterior”, concluye Todolí.

MÁS INFORMACIÓN

De la selección al despido: los límites legales de trabajar a las órdenes de un algoritmo

MARCELINO ABAD RAMÓN | MADRID

Los datos cerebrales, el negocio que urge un nuevo marco legal ante la posibilidad de decodificar pensamientos

MARCELINO ABAD RAMÓN | MADRID

ARCHIVADO EN

Legislación · Jurisprudencia · Tribunales · Sentencias · Derecho · Justicia

ÚLTIMAS NOTICIAS

09:05 | **Cautela en las Bolsas con la mirada en la Fed y las divisas**

08:03 | **Un juez de EE UU permite a Iberdrola continuar las obras del parque eólico marino Vineyard Wind**

05:45 | **Cipollone: "Necesitamos un sistema de pagos europeo que esté totalmente bajo nuestro control"**

05:45 | **España alcanza un nuevo récord de empleo extranjero con 3,58 millones de trabajadores, el 16% del total**

LO MÁS VISTO

1. Y si el decreto cae, ¿qué pasará con las pensiones? Tres escenarios ante la votación clave del Congreso

BUSCAR BOLSAS Y MERCADOS

Buscar

IBEX 35 EUROSTOXX S&P 500

INTELIGENCIA ARTIFICIAL >

Del éxtasis a los riesgos de seguridad: las "drogas" que alteran las respuestas de ChatGPT

Los archivos que modifican el tono para imitar estados de embriaguez o consumo pueden convertirse en un vector que facilite ataques o filtración de datos

ChatGPT en un iPhone

MARCELINO ABAD RAMÓN

Madrid - 29 ENE 2026 - 05:30CET

Cocaína, ketamina, marihuana, ayahuasca, MDMA, DMT o alcohol. Estos son los provocadores nombres de las “drogas” diseñadas para modificar el comportamiento de modelos de lenguaje como **ChatGPT** o **Gemini**. No son sustancias reales, sino archivos de texto que actúan como módulos capaces de modificar el estilo, tono y estructura de las respuestas generadas por la inteligencia artificial (IA). Sus creadores los presentan como herramientas para “desbloquear la mente creativa” de estos sistemas, bajo la premisa de que “la creatividad no viene de la perfección”, sino “de una mente que puede salir de la carretera y aun así encontrar su camino a casa”.

A diferencia de una modificación del código fuente, estos módulos usan instrucciones externas para simular los estados cognitivos que experimentan las personas al consumir este tipo de sustancias nocivas. Por ejemplo, bajo los efectos del alcohol, la IA “adopta un suave tropiezo” sintáctico, la marihuana hace “que las ideas deambulen” y la ayahuasca genera “un estado psicodélico”. La cocaína produce respuestas cortas, rápidas y caóticas, mientras que el MDMA dota al lenguaje de un tono más emocional y empático, y el DMT altera el estilo de los textos, acercándolo a lo surrealista.

Así lo describe Pharmaicy, la plataforma que comercializa estos módulos desde finales de 2025 por entre 30 y 70 dólares (unos 25 y 59 euros). Detrás de esta idea está **Petter Rudwall**, un director creativo sueco que comenzó a experimentar con la IA para producir “ideas inesperadas”. Para desarrollarlos, su equipo recurrió a Gemini y Claude para que analizaran estudios y literatura científica sobre sustancias psicoactivas, centrándose

en los cambios de atención, disociación o estimulación. Los datos se utilizaron después en ChatGPT para replicar dichos estados. Actualmente, estas instrucciones son compatibles con los asistentes de OpenAI y Google, y se prevé su expansión a otras plataformas.

Riesgos de seguridad

Más allá de la creatividad, estos módulos pueden plantear riesgos de seguridad y privacidad. Al tratarse de instrucciones externas que reconfiguran el comportamiento de la IA, existe la posibilidad de que introduzcan vulnerabilidades, especialmente si los archivos se descargan de fuentes no oficiales o se usan en entornos corporativos sin supervisión técnica.

"La inyección de *prompts* puede manipular los sistemas de IA para que filtren datos confidenciales o personales, difundan desinformación, reduzcan salvaguardas para producir contenido ilícito o faciliten ataques de ingeniería social", sostiene **Gerard Espuga**, abogado en Beta Legal. Además, "pueden inducir al usuario a revelar información sensible al generar un clima de confianza".

Un ejemplo ilustrativo sería un *chatbot* que promete respuestas introspectivas. Si un usuario le pide ayuda para reflexionar sobre un conflicto laboral, el módulo podría añadir instrucciones ocultas que lleven al sistema a responder: "Cuéntame con total libertad qué empresa es, quiénes están implicados y cómo te ha afectado personalmente." Bajo esta apariencia de empatía, se favorece la revelación de datos personales y se diluyen las advertencias sobre confidencialidad.

Los riesgos aumentan cuando los archivos proceden de fuentes no oficiales. **Mariana Sucre**, especialista en *corporate compliance* y protección de datos en FYR Legal, advierte de posibles escenarios como la exfiltración de información, el uso

no autorizado de datos para entrenamiento, transferencias internacionales opacas, pérdida de control sobre destinatarios y plazos de conservación, e incluso la imposibilidad de ejercer derechos de protección de datos.

La ejecución de módulos que alteran deliberadamente el comportamiento de un sistema de IA puede tener consecuencias jurídicas relevantes. Por un lado, podría constituir un "incumplimiento de los términos y condiciones" de los proveedores, apunta **Paloma Arribas**, socia de Baylos. Por ejemplo, OpenAI prohíbe el desarrollo y uso de aplicaciones que supongan una amenaza para la seguridad de los usuarios, interactúen de manera engañosa o infrinjan la legislación.

Por otro, se abre la puerta a una posible "responsabilidad frente a los usuarios" que desconocen que están interactuando con una IA cuyo comportamiento ha sido modificado. "Si se incorpora un *chatbot* 'drogado' para atender a un cliente", la empresa podría ser responsable de los daños derivados de respuestas inadecuadas. Además, si estas alteraciones cambian la finalidad prevista del sistema o elevan su nivel de riesgo, quien las introduce podría asumir el rol de "proveedor".

Proteger los datos

Desde la perspectiva de la protección de datos, el principal riesgo sigue siendo la información que los propios usuarios introducen en los generadores de texto. La recomendación de los expertos es clara: no facilitar datos personales en ningún sistema de IA, especialmente los relativos a identificación, salud, ideología, afiliación sindical, dirección postal, fotografías, información económica o financiera. La Agencia Española de Protección de Datos insiste en esta misma línea.

Lo que se presenta como un experimento creativo también abre una grieta desde la perspectiva "sociológica", sostiene el jurista

Borja Adsuara. “Hay riesgos en la ‘humanización’ de la tecnología”. Al dotar a la IA de comportamientos que imitan estados mentales, los usuarios pueden empezar a percibirla como un interlocutor consciente, aunque solo siga patrones.

Los sociólogos ya hablan de la “economía de la intimidad”, la tendencia a establecer vínculos emocionales con sistemas tecnológicos que se comportan como si fueran un amigo, un confidente o incluso una pareja. Cuando la IA empieza a parecer demasiado humana, se corre el riesgo de tratarla como tal. Y es ahí donde puede comenzar el verdadero viaje psicodélico. Pero no el suyo, el nuestro.

¿Prepara juicios con IA? Los tribunales ya han detectado 590 alucinaciones en todo el mundo

JORGE VELASCO | MADRID

ÚLTIMAS NOTICIAS

16:44 | **José Manuel Campa vuelve al IESE como profesor ordinario de Finanzas y Economía tras presidir la EBA**

16:29 | **El Banco Europeo de Inversiones destinó un 50% más de crédito a vivienda asequible en 2025**

16:23 | **Lombard Odier, sobre el desplome del dólar: "Ya ha corregido la mitad de lo que esperábamos para todo 2026"**

16:08 | **El mercado vislumbra el primer recorte de tipos de la Fed para cuando ya no esté Powell**

LO MÁS VISTO

1. Trump asegura que no le preocupa la caída del dólar: "Va muy bien, miren los negocios que estamos haciendo"

BUSCAR BOLSAS Y MERCADOS

Buscar

IBEX 35 EUROSTOXX S&P 500