

ISTOCK

CABLES SUBMARINOS, UNA RED TAN INVISIBLE COMO CRÍTICA

De los 1,5 millones de kilómetros que hay en el mundo depende el 99% del tráfico global de datos y la continuidad de innovaciones como la inteligencia artificial

Iberdrola INDRA GROUP MERCADONA Telefónica

Tecnología

La gran revolución tecnológica no está en la nube, sino bajo los océanos

De los cables submarinos depende el 99% del tráfico global de datos y la continuidad de innovaciones como la inteligencia artificial. Todo ello en un escenario de creciente tensión geopolítica y guerra híbrida

Isabel Gaspar

En un contexto en el que la IA se ha convertido en el principal foco de atención a nivel mundial, lo cierto es que esta tecnología no podría existir sin lo que ocurre bajo los océanos. En realidad, ninguna de las acciones que requieren conectividad (hacer un bizum, consultar las redes sociales, comprar *online*...) podría suceder. Y es ahí donde radica la enorme relevancia de los cables submarinos, una infraestructura tan invisible como crítica.

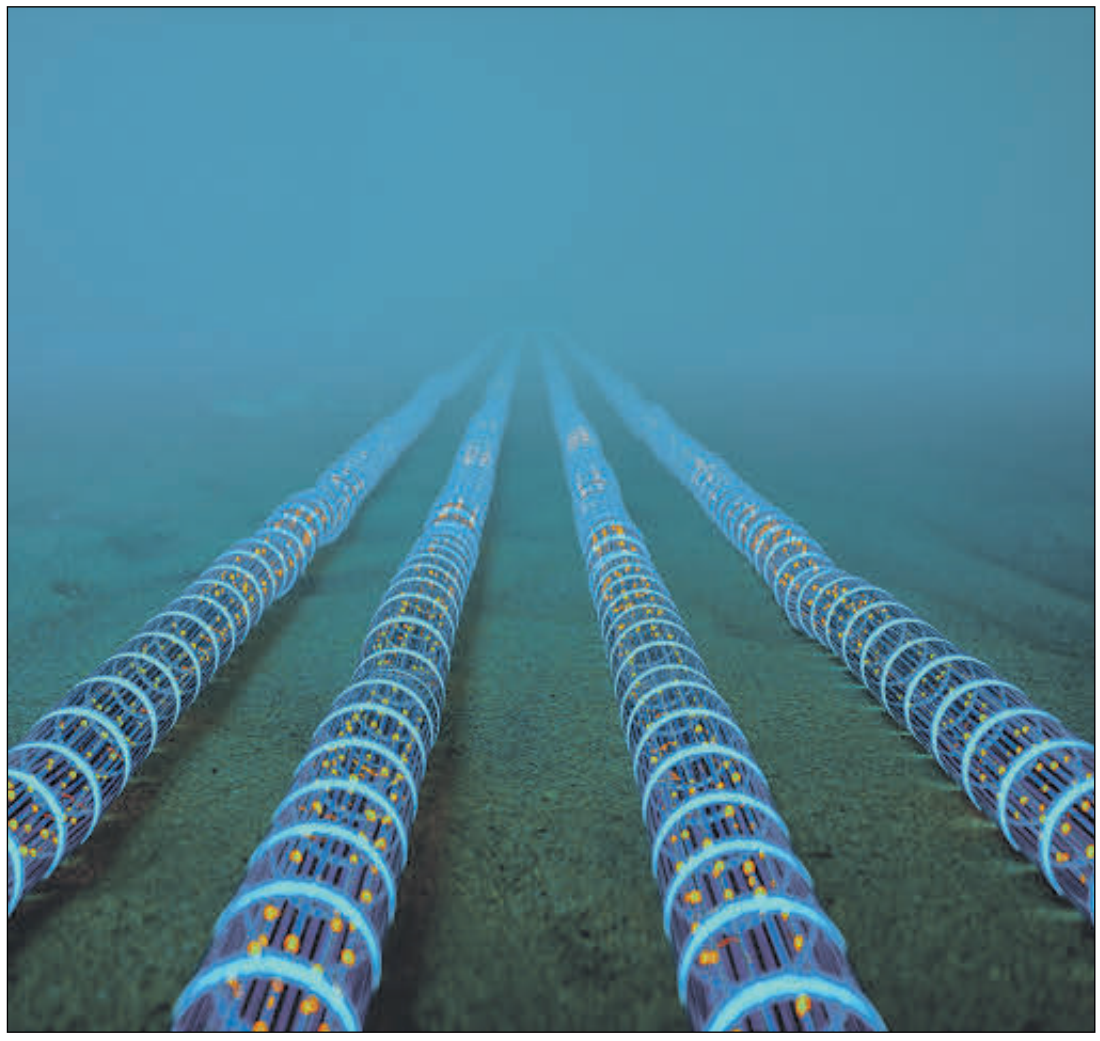
Actualmente, según los últimos datos disponibles de TeleGeography, hay 691 cables repartidos en 186 países y con 1.908 puntos de aterrizaje (instalaciones en tierra para que los cables puedan conectarse con las redes terrestres). De toda esta red depende el 99% del tráfico internacional de datos. La historia de esta infraestructura, que arrancó en el siglo XIX impulsada por la revolución del telégrafo eléctrico, se enfrenta a uno de sus capítulos más decisivos. Hoy, como entonces, el control de los cables submarinos es sinónimo de poder y control.

A este respecto, la vulnerabilidad de los cables en cuanto a poder protegerlos los sitúa como un elemento muy codiciado por algunos países a la hora de llevar a cabo tácticas agresivas, pero sin cruzar el umbral que justifique una respuesta militar convencional. Es lo que se conoce como *zona gris*. La eficacia reside en la ambigüedad: ni el autor ni sus intenciones pueden atribuirse con certeza.

"La importancia de los cables submarinos a nivel geopolítico es altísima, hasta el punto de haberse convertido en un objeto prioritario para acciones de guerra híbrida y estrategias de *zona gris*", señala Rafael García, profesor de Relaciones Internacionales en la Universidad Pablo de Olavide (Sevilla), quién añade que "en términos económicos, el valor de la información y de las actividades que se realizan a través de esta red multiplica con creces el valor de las mercancías físicas que transitan por medios de transporte convencionales. Pese a ser una infraestructura verdaderamente crítica, ha pasado históricamente desapercibida para la opinión pública por el simple hecho de ser submarina".

Como recoge la investigación *Infraestructura crítica en contexto de guerra híbrida*, del Instituto Español de Estudios Estratégicos (IEEE), la invasión rusa de Ucrania en 2022 y la adhesión de Finlandia y Suecia a la OTAN transformaron el mar Báltico en un frente de confrontación estratégica (se trata de uno de los espacios marítimos más densamente cableados). Desde 2023, los daños registrados en cables submarinos evidencian una fragilidad creciente. Aunque inicialmente se atribuyeron a accidentes, la repetición de patrones y su concentración espacial han incrementado las sospechas de intencionalidad encubierta.

Precisamente, el sabotaje físico es el reto más urgente en lo que a la seguridad de esta infraestructura se refiere, "especialmente para países con poca densidad de cables. Si se corta un cable que llega a la costa europea, no suele ser un problema: hay redundancia y tienes muchos otros cables por los que pueden ir los datos. Pero hay zonas de la costa africana donde apenas llegan cables y pueden quedarse países enteros sin Internet", destaca Javier Borràs, investigador de CIDOB. No en vano, en marzo de 2024 millones de personas en África Occidental se quedaron sin Internet debido a que los cables en el fondo del cañón Trou Sans Fond, situado frente a la costa de Costa de Marfil, comenzaron a fallar.



Existen casi 700 cables submarinos a nivel mundial. ISTOCK

"Otro problema fundamental es que apenas hay una decena de barcos especializados en reparación de cables submarinos. El desplazamiento más la reparación pueden tardar incluso meses. Si hubiera varias disrupciones críticas simultáneas a nivel mundial, sería problemático", añade Borràs. De hecho, "un ataque coordinado puede tener un valor disruptivo superior o equivalente al bombardeo de una infraestructura crítica en tierra, como podría ser un gran aeropuerto", apunta García.

> En la actualidad hay 1,5 millones de kilómetros de cables submarinos que implican a casi 200 países

Según el International Cable Protection Committee (ICPC), más del 70% de los daños en cables submarinos se atribuyen a actividades humanas accidentales, lo que contribuye a reforzar un entorno ambiguo en el que la frontera entre accidente y ataque es difusa. Hay que tener en cuenta que es prácticamente imposible proteger físicamente los 1,5 millones de kilómetros de cables submarinos en servicio. "Se pueden enterrar, proteger las instalaciones de amarre y dotar a los cables de sistemas de detección, pero no es posible garantizar la seguridad de todos a todas horas. El enfoque de resiliencia se basa en la admisión de que los cables pueden dejar de funcionar y que las medidas deben enfocarse a la recuperación del servicio", sostiene Félix Arteaga, investigador principal para Seguridad y Defensa del Real Instituto Elcano.

Ante este escenario, la redundancia, es decir, un sistema de rutas alternativas que desvía el tráfico si un cable falla, es una de las mejores defensas. Esta protección mediante redundancia, como explica Rafael García, es sólida en las regiones de gran tráfico y economías potentes, como el Atlántico o Extremo Oriente. Por el contrario, los territorios que dependen de una única conexión o que se encuentran más aislados son vulnerables.

En este mapa, España desempeña un papel fundamental. "La posición geográfica de España es estratégica porque conecta cables de todas las procedencias y en un número que no para de crecer debido a la demanda de cables submarinos para atender a los centros de datos que se instalan en España. La concentración de infraestructuras y el intenso tráfico marítimo incrementan su exposición a accidentes, sabotajes y posibles operaciones híbridas", expone Arteaga.

Titularidad privada

Si bien los cables submarinos son estratégicos y críticos a nivel estatal, su titularidad es privada. En los últimos años las grandes compañías tecnológicas han ido desplazando a los operadores tradicionales de telecomunicaciones como propietarios de estas infraestructuras. "Esta concentración otorga a un número muy reducido de corporaciones un poder absoluto sobre la tecnología, la IA y las redes globales", subraya García.

Eso sí, "esta situación se produce en todas las infraestructuras críticas: el coste y la responsabilidad de la protección y funcionamiento recae sobre los

Tecnología

Las autopistas de internet viajan por el fondo del mar

Más del 99% de los datos que viajan entre continentes lo hacen por cables de fibra óptica tendidos en el lecho marino.

EN EL MUNDO

607 cables activos y 102 en construcción

>1.800 estaciones de amarre

>1,5 mill. de km unas 37 vueltas a la Tierra

EN ESPAÑA

31 cables activos y 5 en construcción

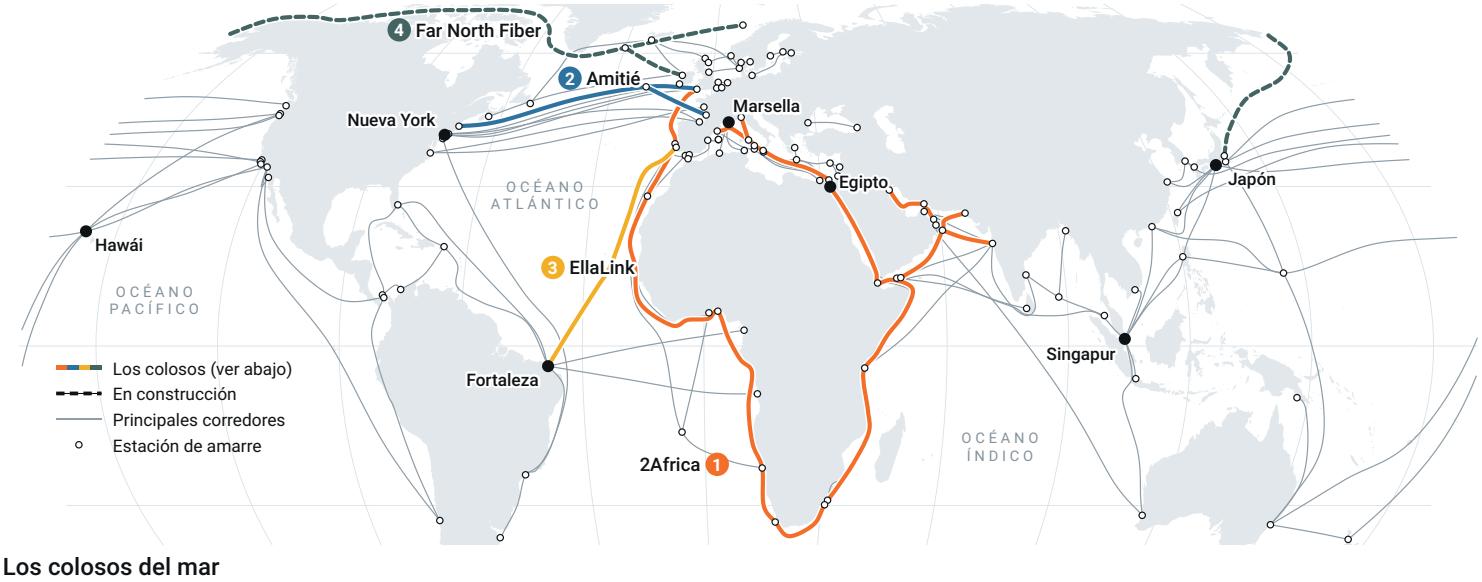
48 estaciones de amarre

>180.000 km* de cable con paso por España

BAJO EL MAR

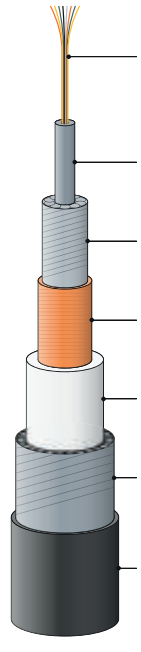
8.000 m de profundidad máxima, casi la altura del Everest

70-80% de las averías, por redes de pesca y anclas



Así es por dentro

Un cable de alta mar mide unos 2 cm, como una manguera. Cerca de la costa se refuerza con armadura de acero.



Los colosos del mar

1 2Africa
EL MÁS LARGO
45.000 km Longitud
33 Países
3.000 mill. Población
180 Tbps Capacidad**

2 Amitié
EL MÁS RÁPIDO
6.792 km Longitud
3 Países
800 mill. Población
320-400 Tbps Capacidad**

3 EllaLink
EL ENLACE DIRECTO SUDAMÉRICA-EUROPA
6.200 km Longitud
4 Países
650 mill. Población
100 Tbps Capacidad**

4 Far North Fiber***
EL MÁS INNOVADOR: CRUZA EL ÁRTICO
~14.500 km Longitud
5 Países
~600 mill. Población
100 Tbps Capacidad**

Fuente: TeleGeography, consorcios, ICPC y UIT. (*) Incluye proyectos que pasan por España. (**) Terabits por segundo; 1 Tbps = 125 gigabytes por segundo. (***) En construcción. Trazados simplificados.

actores privados y los Estados solo se encargan de regular y exigir el cumplimiento de las obligaciones privadas", destaca Arteaga.

Google, Meta, Microsoft y Amazon lideran la inversión mundial en cables submarinos. De hecho, ante el crecimiento exponencial y continuo de la demanda de ancho de banda, la adquisición y el despliegue de nuevos cables submarinos es prioridad estratégica para estas compañías. Un analista del IEEE alerta a *elEconomista.es* de que estas grandes corporaciones, "tienen capacidad de imponer condiciones de acceso y explotación de la red por encima de la autoridad soberana de los Estados, lo que hace que países sin capacidad tecnológica para desarrollar sistemas propios están obligados a aceptar las condiciones que se le impongan o bien a renunciar a la conectividad".

A este respecto, como explican desde el organismo, la colaboración entre el Ministerio de Defensa y las grandes empresas tecnológicas (mayoritariamente americanas y chinas) no es fácil, pues los ámbitos de competencia son distintos: "Los Estados tienen soberanía sobre sus aguas territoriales y las estaciones de anclaje, el derecho internacional sobre los espacios que no son de soberanía nacional (ZEE y alta mar), pero sin una autoridad más allá de la voluntad de los estados por cumplir las normas, y las propias empresas, como entidades privadas, sobre sus activos".

Por ello, "ya no es una relación entre Estados como antes, sino entre Estados y empresas privadas (vinculadas a otros Estados, y que responden, si lo hacen, a los intereses de esos Estados) con capacidad de actuar por intereses propios y no nacionales. Actualmente España, como muchos países, carece de un marco jurídico específico para la gestión, protección, y seguridad de los cables submarinos".

Y es que la protección no es solo física, también digital. Como apunta Borràs, Estados Unidos ha vetado que se construyan cables con conexión directa de territorio estadounidense a China continental o Hong Kong, por miedo a que se pueda acceder a los datos *hackeando* las terminales de llegada en territorio chino". Cabe recordar que el régimen jurídico para la protección de los cables submarinos es pre-digital. La legislación actual es, esencialmente, la Convención de Naciones Unidas sobre el Derecho del Mar de 1982, la Convención para la protección de cables submarinos de 1884 y la Convención de Ginebra de 1958. "No contemplan de forma clara los dos grandes retos actuales; la seguridad digital de la red y la seguridad física contra ataques maliciosos intencionados", explican desde el IEEE.

En este sentido, Jose Luis Pérez, director del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), señala que "el modelo español de protección de infraestructuras críticas descansa precisamente sobre la colaboración público-privada. La protección de estas infraestructuras no se construye sobre la sustitución del operador por la Administración, sino sobre un reparto de responsabilidades.

La creciente amenaza de la guerra híbrida y la competición geoestratégica –evidenciadas por las nuevas estrategias marítimas de España, las directrices de la Unión Europea de 2024 y 2025 sobre resiliencia de cables submarinos, y la mayor vigilancia de la OTAN en el Atlántico– han impulsado un reforzamiento drástico de la vigilancia, la evaluación de riesgos y la protección de estas infraestructuras críticas.

La pregunta con todos elementos sobre la mesa parece obvia: si se detecta una maniobra sospechosa ¿cuál es el protocolo de respuesta? En el caso de España, como analiza Pérez, se activa "una respuesta coordinada e interdepartamental. Si la situación compromete una infraestructura crítica, entran en juego los mecanismos de comunicación y coordinación previstos entre el operador y las autoridades competentes. El sistema español dispone además de un Nivel de Alerta de Infraestructuras Críticas (NAIC)".

Del plano al fondo marino: así es la colosal obra de ingeniería para construir, fabricar e instalar los cables submarinos

El desarrollo de un cable submarino es una obra de ingeniería colosal que requiere varios años (en general entre 2 y 4). Además, su mantenimiento puede extenderse 25 años, que es, de media, su vida útil.

→Planificación: Un equipo define la ruta óptima considerando la topografía, la legislación marítima, los permisos de cada país cuyas aguas cruza el cable y los puntos de aterrizaje disponibles. Se evitan zonas con fosas profundas, fallas tectónicas, áreas de intensa pesca y zonas de anclaje comercial.

→Fabricación: Los cables se fabrican en centros especializados y se enrollan en grandes tanques o bobinas para su transporte. No es un simple hilo, sino una estructura de alta tecnología: cuenta con un núcleo de fibras ópticas y tubos de cobre para la energía, protegidos por capas de polímeros y aramida en las profundidades abisales, y reforzados con pesadas armaduras de acero en las zonas costeras y superficiales.

→Despliegue: Un buque cablero lo desenrolla y deposita de forma progresiva y controlada. En zonas costeras, el cable se entierra mediante arados submarinos a 1-3 metros bajo el sedimento; a gran profundidad se deposita directamente sobre la superficie.

→Conexión y pruebas: Una vez conectados los extremos a las estaciones de aterrizaje, se realizan pruebas exhaustivas de capacidad, latencia y atenuación.

Una tecnología imbatible

Si bien existen otras tecnologías que podrían cumplir la función de los cables submarinos, la realidad es que ninguna es tan eficiente. Un solo cable de fibra óptica en el mar transporta terabits por segundo con una latencia mínima y un coste imbatible. Ninguna red de satélites actual dispone de la capacidad de ancho de banda necesaria para absorber ese volumen masivo de información sin colapsar, lo que convierte a estas autopistas submarinas en una infraestructura insustituible.

Obviamente, la falta de alternativas no solo eleva a estas infraestructuras a una especie de agua en el desierto, sino que las dota de una vulnerabilidad en las que cualquier ataque o colapso podría dejar a la economía global completamente a oscuras y sin margen de maniobra.

Tecnología



Los 10 países que más invierten en IA soberanas representan, aproximadamente, el 90% de toda la inversión. ISTOCK

Soberanía digital: ningún país logrará la independencia total

El 90% de la capacidad de procesamiento necesaria para desarrollar e implementar IA de vanguardia se concentra en EEUU y China. Preocupados por esta concentración, no son pocos los países que se han lanzado a la carrera para desarrollar un modelo de IA soberana

Isabel Gaspar

Si la tecnología de IA fuera un suministro de agua, actualmente la mayoría de países dependería de embalses y de redes de distribución de terceros. Y esta realidad, como cualquiera en la que se no tenga control, entraña importantes riesgos. Por un lado, la falta de privacidad sobre datos que pueden ser muy sensibles (información médica, bancaria, direcciones...) y que se utilizan para entrenar modelos de otros países. Por otro, esos datos quedan sujetos a leyes de otros estados que pueden ser más laxas en cuanto a la utilización que se hace de dicha información. Asimismo, igual que ha ocurrido históricamente con otros activos estratégicos, como el petróleo, la tecnología de IA puede emplearse para hacer presión, por ejemplo, cortando su acceso o restringiendo funcionalidades.

En este contexto, la sartén por el mango la tienen Estados Unidos y China. Según los datos de la firma de investigación Epoch AI, el 90% de la capacidad de procesamiento necesaria para desarrollar e implementar IA de vanguardia se concentra en ambos territorios. Preocupados por esta concentración, no son pocos los países que se han lanzado a la carrera para desarrollar un modelo de IA soberana, es decir, sus propios sistemas de IA.

El *think tank* Centro para una Nueva Seguridad Americana (CNAS, por sus siglas en inglés) ha desarrollado el *Sovereign AI Index* (Índice de IA Soberana) que rastrea y clasifica iniciativas de inteligencia artificial respaldadas por gobiernos. En la actualidad, tienen registrados 184 proyectos. El 59% de todas esas iniciativas se concentra en infraestructura: centros de datos, supercomputadoras, clústeres de Unidad de Procesamiento Gráfico (GPU) y programas de acceso a la computación. Este tipo de proyectos ha crecido considerablemente desde 2024, de hecho, solo en el primer trimestre de 2026 se anunciaron más programas de infraestructura que en todo 2024.

Por su parte, los proyectos que incluyen iniciativas respaldadas por los gobiernos para desarrollar o adaptar modelos básicos representan el 32%, mientras que los proyectos de datos o iniciativas para crear conjuntos de datos de entrenamiento nacionales o plataformas para compartir datos, suponen solo el 9%.

> Oriente Medio y Asia Oriental representan más del 80% de la inversión en modelos soberanos de inteligencia artificial

Prioridad no es realidad

Pese a que el desarrollo de una IA soberana se haya convertido en una prioridad, los datos demuestran que está lejos de ser una realidad. "Existe una brecha sustancial entre la intención y la acción. La inversión sigue estando fuertemente concentrada en dos regiones –Oriente Medio y Asia Oriental– que, en conjunto, representan más del 80%", explican desde CNAS.

Acercando la fotografía, las apuestas por una IA soberana son más desproporcionadas. Los 10 países que más invierten representan, aproximadamente, el 90% de toda la inversión. Solo Emiratos Árabes Unidos, con 33.500 millones de dólares anunciados, y Japón, con 20.400 millones, suponen casi dos tercios. El único país de la Unión Europea que aparece en la lista, Alemania, lo hace en el puesto 10 con casi 840 millones.

"En la práctica, la mayoría de los proyectos de IA soberana dependen en gran medida de proveedores de tecnología extranjeros, principalmente estadounidenses", subrayan desde CNAS. Solo NVIDIA suministra GPU para el 45% de todos los proyectos de infraestructura monitoreados.

El pasado mes de junio la Comisión Europea anunció el *Paquete de medidas de soberanía tecnológica*, un conjunto de medidas para reforzar la capacidad de Europa en materia de semiconductores, IA, nube y código abierto. Así, articula iniciativas como el Reglamento de Chips 2.0, para impulsar la fabricación local de semiconductores avanzados; o la Ley de Desarrollo de la Computación en la Nube y la IA, diseñada para triplicar la capacidad de los centros de datos en suelo europeo y regular la nube soberana.

Modelos regionales

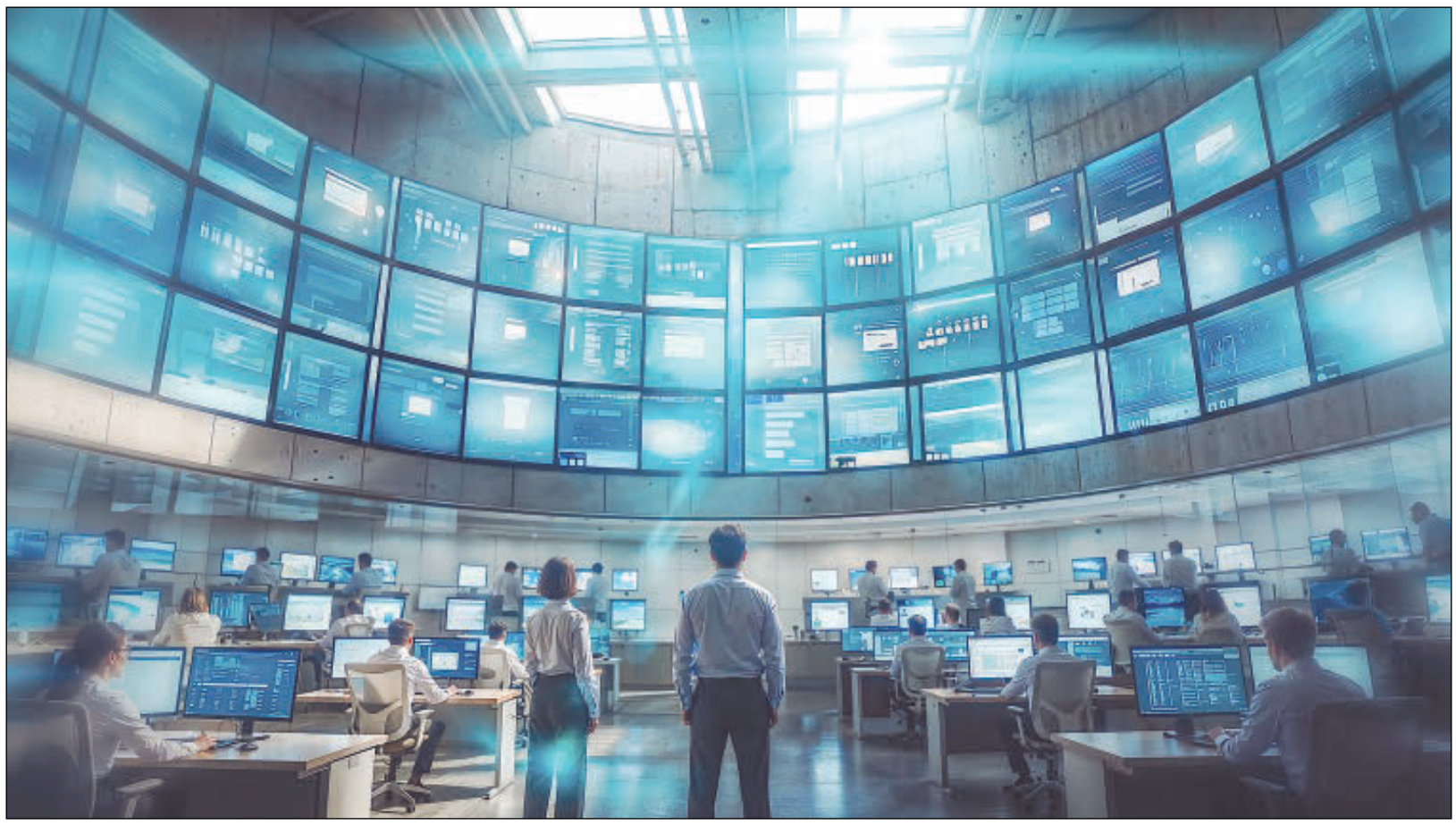
Si las previsiones de la consultora Gartner se cumplen, el año que viene el 35% de los países dependerá de plataformas de IA regionales, frente al 5% actual. Como explica Gaurav Gupta, vicepresidente y analista de la compañía, "los países están aumentando la inversión en plataformas de IA nacionales, buscando alternativas al modelo cerrado de Estados Unidos, incluyendo capacidad de procesamiento, centros de datos, infraestructura y modelos adaptados a las leyes y la cultura locales". Para lograrlo, los países que opten por una infraestructura de IA soberana deberán invertir al menos el 1% de su PIB para 2029.

La preocupación sobre la soberanía de la IA queda patente en encuestas como la llevada a cabo por Capgemini Research Institute. Según el informe *Soberanía digital: de la ambición política al imperativo ejecutivo*, la soberanía es un tema central para los altos directivos, ya que el 44% de las organizaciones considera que la soberanía digital es la máxima prioridad de su consejo de administración.

"Las organizaciones actuales operan en ecosistemas tecnológicos altamente interconectados en los que rara vez es posible alcanzar una independencia total. La soberanía digital no consiste en alcanzar una autonomía total, sino más bien en garantizar que las organizaciones comprendan claramente sus dependencias tecnológicas, con el fin de recuperar el control y la flexibilidad necesarios para gestionar los riesgos", afirma Karine Brunet, directora de Operaciones y Ejecución de Capgemini.

Y es que la realidad, es que ningún país o empresa va a poder desarrollar un modelo de IA 100% soberana, ni siquiera Estados Unidos. En algún punto de la cadena, van a ser necesarios insumos de otros países. "La cuestión a la que se enfrentan los responsables políticos de todo el mundo no es si se puede lograr una IA totalmente soberana (no se puede), sino si pueden forjar alianzas, desplegar tecnologías e implementar marcos de gobernanza para otorgar a los países una capacidad de decisión sobre cómo se despliega la IA dentro de sus fronteras", alertan desde CNAS. Por tanto, hablar de IA soberana no es hacerlo de la eliminación de la dependencia de otros, sino más bien de gestión y colaboración.

Contenido ofrecido por Indra Group



IA.

La IA que no solo contesta: calcula, simula, organiza, actúa y protege

Indra Group conecta las capacidades tecnológicas más avanzadas para llevar la inteligencia artificial soberana de IndraMind a sistemas críticos y aplicaciones reales

EcoBrands

Durante los últimos años, la inteligencia artificial se ha explicado sobre todo a través de modelos capaces de conversar, resumir documentos o generar imágenes. Pero en los sistemas críticos el reto es otro. No basta con que una máquina responda bien: debe interpretar información incompleta, actuar con rapidez, mantener la trazabilidad y funcionar con garantías cuando están en juego una infraestructura clave, una operación de defensa o una emergencia.

Ese salto, de la IA que contesta a la IA que opera, está marcando una nueva etapa tecnológica. Es el terreno en el que Indra Group desarrolla IndraMind: no como una aplicación aislada, sino como un entorno que integra datos, inteligencia artificial, ciberseguridad, simulación y capacidad operativa. Una propuesta orientada a reforzar la soberanía tecnológica en defensa, seguridad, infraestructuras críticas o ciberespacio.

Europa ha situado esta cuestión en el centro de su agenda con el *Cloud Sovereignty Framework*. El marco plantea la soberanía no como un aislamiento tecnológico absoluto, difícilmente viable, sino como la capacidad de ejercer un control efectivo y proporcional sobre sistemas, datos e infraestructuras, reducir dependencias estratégicas y limitar la exposición a legislaciones extracomunitarias. Su modelo incremental de niveles de soberanía, denominado SEAL, permite graduar ese control según las características y criticidad de cada sistema.

El objetivo de fondo no es cerrar Europa tecnológicamente, sino aumentar su capacidad de elección: decidir qué tecnologías utiliza, cómo gobierna sus datos y activos digitales y qué capacidades esenciales mantiene bajo control propio. IndraMind se alinea ya con un nivel elevado de estas directrices y trabaja para ofrecer a España y Europa una alternativa que permita disponer de capacidades propias sin renunciar a interoperar y federarse con otras tecnologías, especialmente en el entorno de la OTAN. Una preocupación que alcanza también a regiones como Oriente Medio, interesadas en proteger activos estratégicos y reducir dependencias tecnológicas.

Pero la soberanía no se construye únicamente controlando dónde residen los datos. Requiere disponer de capacidades para gobernar infraestructuras y activos digitales, desarrollar y desplegar inteligencia artificial con garantías y proteger todo ese ecosistema frente a nuevas amenazas. IndraMind trabaja sobre esa combinación desde entornos de datos cercanos a la operación y centros propios hasta agentes de IA, simulación avanzada, gemelos digitales, ciberseguridad y nuevas capacidades de computación.

Entre ellas figura también la computación cuántica, llamada a complementar la computación convencional en problemas especialmente complejos. Su potencial para optimizar redes, simular escenarios con gran número de variables o acelerar determinados cálculos abre nuevas posibilidades en ámbitos críticos. Pero es una pieza más de un ecosistema tecnológico en el que el valor no procede de una tecnología aislada, sino de la capacidad para combinarlas y gobernarlas de manera segura.

IndraMind aspira así a gestionar infraestructuras y activos digitales desplegados en nube, instalaciones propias o entornos cercanos a los datos; controlar el ciclo de vida de los desarrollos potenciados con inteligencia artificial; y facilitar la experimentación e implantación de sistemas que combinen diferentes tipos de IA. El elemento diferencial no está únicamente en incorporar modelos cada vez más avanzados, sino en hacerlo con trazabilidad, control y capacidad para decidir dónde residen y cómo se utilizan tecnologías, datos y procesos.

Operación real

Esta lógica cobra especial relevancia cuando la IA deja de trabajar únicamente sobre información digital y empieza a intervenir en el mundo físico. Los gemelos digitales, la simulación avanzada o los agentes de IA permiten anticipar escenarios, ensayar alternativas y apoyar decisiones antes de trasladarlas a un sistema real. En defensa, seguridad o en la protección y funcionamiento de infraestructuras críticas, esa capacidad de experimentar sin comprometer la operación real adquiere un valor especial.

> La próxima ola de la IA se medirá por su capacidad para operar con fiabilidad

Ninguna de estas capacidades funciona por sí sola. La computación avanzada amplía las posibilidades de cálculo; los agentes de IA ayudan a analizar y responder; los gemelos digitales permiten ensayar escenarios; y la ciberseguridad protege el conjunto. La innovación aparece cuando todas estas piezas se conectan, se gobiernan y se llevan a operaciones reales bajo control humano. Ahí está el cambio de fondo. La próxima ola de la inteligencia artificial no se medirá solo por la fluidez de sus respuestas, sino por su capacidad para operar con fiabilidad, proteger activos críticos y contribuir a que países y organizaciones puedan decidir libremente sin dependencias.

Tecnología

Leyes que nacen desfasadas: el peligro de legislar más lento que el algoritmo

La ley europea que regula la inteligencia artificial está entrando en vigor por fases, lo que provoca retrasos y que nuevos peligros, como los agentes fuera de control, se queden fuera de su regulación

Judith Arrillaga Pérez

La inteligencia artificial ha supuesto un giro de 180 grados tanto en la vida de las personas como en el día a día de las organizaciones. Hay que tener en cuenta que, solo en España, cerca de la mitad de la población, un 45,1%, utiliza herramientas de IA generativa en su día a día, según se desprende del informe *Global AI Diffusion* elaborado por Microsoft. Esto posiciona a nuestro país en la sexta posición mundial solo superado por Emiratos Árabes, Singapur, Irlanda, Francia y Noruega. Otras potencias europeas como Alemania e Italia ocupan las posiciones 23 y 26, respectivamente

Sus ventajas son indiscutibles: automatiza tareas, facilita la vida a personas con discapacidad, optimiza recursos, mejora la eficiencia de los procesos, analiza grandes cantidades de datos... Sin embargo, es una moneda de dos caras y al otro lado de la balanza son muchos los riesgos, sobre todo, si se tiene en cuenta que la IA puede recopilar y analizar grandes cantidades de datos personales y tomar decisiones basadas en datos con sesgos. Además, puede ser utilizada en estafas, para suplantar identidades o realizar ataques informáticos.

Es por eso por lo que su regulación es ahora más importante que nunca. Ya el 1 de agosto de 2024 entró en vigor la Ley de Inteligencia Artificial de la Unión Europea, sin embargo, su aplicación es gradual, con fechas clave que se extienden desde 2025 hasta 2028 según el nivel de riesgo de cada sistema. El próximo paso se espera para el 2 de diciembre de 2027 cuando haya pleno cumplimiento para sistemas de alto riesgo en áreas como biometría, salud, empleo o justicia. Sin embargo, es llamativo que se redacten leyes que tardan varios años en estar en pleno funcionamiento cuando se trata de una innovación que avanza a un ritmo vertiginoso.

> Con una regulación tardía de la IA, las autoridades no pueden prevenir, sino dedicarse a curar los daños ya sufridos

"La Ley de IA protege ante ciertos usos de riesgo, pero se ha quedado corta ante importantes problemas que tenemos actualmente. La regulación debería ser más iterativa y poder responder rápidamente a los problemas que van apareciendo en el sector", explica a *elEconomista.es* Javier Borràs, investigador del centro de investigación en relaciones internacionales CIDOB.

Desde que en 2024 se aprobó la Ley IA han surgido nuevos problemas como los casos de agentes fuera de control que han hackeado webs o bases de datos de empresas o gobiernos durante entrenamientos que estaban realizando empresas como OpenAI o Anthropic. "La Ley de IA, sin embargo, no menciona los agentes o prácticas como el autoentrenamiento entre agentes, que han causado alarma entre los expertos. Además, la Ley de IA regula lo que pueden hacer las IA a disposición del usuario, pero ¿y las IA que están usando internamente las grandes tecnológicas, pero todavía no están a disposición del público, y que suelen ser los modelos más potentes? De allí también pueden surgir accidentes y problemas graves", alega el experto a este respecto.

> Hay que regular la IA como antes pensábamos en regular el uso de la energía o las armas nucleares

Además, a esto hay que sumarle que son muchas las compañías que no cumplen con los plazos que establece la regulación. "La obligación de la alfabetización está en vigor desde enero del año 2025. Es de lo más básico, una serie de normas que tienen que conocer todas las personas que en el ámbito de su trabajo usan herramientas de inteligencia artificial. Y, aun así, hay muchas empresas que no lo hacen", detalla a este respecto Pedro Toledo, abogado experto en IA.

Entonces, ¿cómo se puede acompasar la regulación al avance de la tecnología? Para Borràs la clave podría estar en China. "Aunque tienen objetivos políticos muy distintos, creo que para la Unión Europea son un ejemplo de regulación de IA interesante, no en el contenido sino en los procedimientos. En China, no tienen una sola ley paraguas para regular toda la IA como tenemos en la UE, sino que han creado leyes específicas aplicadas a sectores concretos donde hay presencia de IA, desde una ley sobre algoritmos de recomendación hasta una sobre el uso de IA generativa. Eso hace que cada ley pueda adaptarse a las necesidades del caso concreto", matiza Borràs.

También hay que tener en cuenta que China es más ágil imponiendo regulaciones cuando surge un problema vinculado a la IA. "Mientras se prepara la ley, las autoridades lanzas medidas provisionales o borradores de regulación, que pueden ser adaptados sobre la marcha según el desarrollo de la tecnología. Hay más capacidad de iteración, rapidez y flexibilidad ante

Calendario para la aplicación de la Ley de IA de la UE

1 de agosto de 2024 — **Entrada en vigor**

2 de febrero de 2025 — **Se aplican disposiciones generales** (definiciones y amplificación; alfabetización en IA) y prohibiciones

2 de agosto de 2025 — **Se aplican normas para la IA de uso general y debe existir gobernanza**

- Las obligaciones de la Ley de IA para los proveedores de modelos de IA de uso general entran en vigor
- Los Estados miembros deben designar a las autoridades nacionales competentes y adoptar leyes nacionales sobre sanciones.
- Debe crearse una gobernanza a escala de la UE (Consejo de IA, Comisión Técnica Científica, Foro Consultivo)

2 de agosto de 2026 — **La mayoría de las normas de la Ley de IA entran en vigor y comienza su aplicación**

- Entran en vigor las normas relativas a los sistemas de IA de alto riesgo que figuran en el anexo III
- Comienzan a aplicarse las normas de transparencia (artículo 50)
- Se aplican medidas de apoyo a la innovación
- Los Estados miembros deben disponer de al menos un espacio controlado de pruebas para la IA por país establecido
- La aplicación de la Ley de IA comienza a escala nacional y de la UE

2 de diciembre de 2026 — **Nuevas prohibiciones**. Se aplica la transición prevista en el artículo 50, apartado 2

- Entran en vigor las prohibiciones relativas a los sistemas de IA que generan deepfakes sexuales no consentidos y material de abuso sexual infantil.
- Plazo transitorio para que determinados proveedores de sistemas de IA, incluidos los sistemas de IA general (GPAI), que generen contenido sintético y que ya se hubieran comercializado antes del 2 de agosto de 2026, cumplan lo dispuesto en el artículo 50, apartado 2

2 de agosto de 2027 — **Se aplican normas para la IA de alto riesgo** integrada en productos regulados

2 de diciembre de 2027 — Se aplican las normas relativas a los sistemas de IA de alto riesgo recogidas en el anexo III

2 de agosto de 2028 — Se aplican las normas relativas a la IA de alto riesgo integrada en productos regulados incluidos en el anexo I

Fuente: elaboración propia. eE

los retos que suceden", apunta el investigador del CIDOB.

Para Toledo, una posible solución sería actuar por vía de urgencia: "Hay que ver las necesidades de cada momento. Si hay algún avance que, por ejemplo, invade la privacidad de las personas pues igual hay que coger y legislar por vía de urgencia. Pero puede ser que políticamente no interese. Lo estamos viendo con el Verifactu, que no para de aplazarse su entrada en vigor".

Unos retrasos que acarrean riesgos: "El problema de una regulación tardía es, por un lado, que mientras no la tengamos hay posibilidad de que se produzcan todos los problemas y accidentes anteriormente mencionados, y las autoridades no pueden prevenir sino simplemente dedicarse a curar los daños ya sufridos", denuncia Borràs.

¿Por qué es importante regular?

A día de hoy es indiscutible la importancia de regular el uso de la inteligencia artificial. El experto del CIDOB habla de multitud de riesgos e impactos inmediatos "desde los agentes fuera de control, pasando por los *deepfakes*, hasta la posible pérdida de empleos o su uso por parte de organizaciones criminales o terroristas". Entonces, ¿qué solución plantean los expertos?

"Una regulación inteligente y adaptativa debe buscar el equilibrio adecuado entre las promesas de innovación y crecimiento económico de esta tecnología, a la vez que limita o reduce sus efectos negativos. A la vez, debe asegurar que los derechos fundamentales de los ciudadanos son respetados y la tecnología no produce accidentes graves de ciberseguridad o disrupción económica o social.



FIRMA

Teniendo en cuenta las diferencias, hay que pensar en la importancia de regular la IA como antes pensábamos en regular el uso de la energía o las armas nucleares", detalla Borràs.

A los riesgos que acarrea una regulación tardía de la inteligencia artificial hay que sumarle un importante desconocimiento por parte de los usuarios de la letra pequeña. "A falta de regulación, la clave es la educación y el sentido común. Cuando algo es gratis es porque el producto eres tú. ¿Por qué es gratis? Porque estás pagando con tus datos. ChatGPT es gratis porque todos los datos que se vuelcan ahí se van a vender a unos o a otros. Tanto a nivel usuario como a nivel empresa", añade Toledo.

Pese a que la regulación es necesaria, Borràs añade también que no va a suponer la solución de todos los problemas y riesgos. "Una regulación rápida a nivel europeo no solucionará todos los problemas. Los grandes laboratorios de IA están en Estados Unidos y China. Si estas ponencias no ponen límites, o no hay un acuerdo global, el resto del mundo quedará en parte desprotegido ante los efectos adversos de esta tecnología", asegura. Hay que tener en cuenta que Estados Unidos sufre un importante vacío legal en materia de seguridad en inteligencia artificial que se traduce en múltiples normativas en cada estado, pero sin una regulación de alcance federal. China, por el contrario, lleva a cabo un férreo control gubernamental sobre sus laboratorios.

Tecnología



Más de 92.000 trabajadores tecnológicos a nivel han perdido su trabajo. EE

Una ‘tasa robot’ para paliar la caída de cotizantes por los despidos tecnológicos

Funcas calcula que la inteligencia artificial supondrá la destrucción de entre 1,7 y 2,3 millones de puestos de trabajo en España entre 2025 y 2035. Esta destrucción se concentra en los grupos de empleados administrativos y técnicos de nivel medio y superior

Judith Arrillaga Pérez

La inteligencia artificial se ha convertido ya en un compañero de trabajo más en muchas empresas. Puede automatizar tareas, complementar el trabajo humano y crear nuevas ocupaciones. Pero se trata también de una moneda de dos caras ya que puede reducir la demanda de determinados perfiles de empleo. Un recorte a la que desde Funcas ponen cifras y calculan que su adopción podría suponer una destrucción bruta de entre 1,7 y 2,3 millones de puestos de trabajo en España entre 2025 y 2035, que se concentrará entre los administrativos y técnicos de nivel medio y superior. Aunque, aclaran, que no desaparecerían de forma automática, sino que será un escenario condicionado por el ritmo de adopción, por la creación de nuevas ocupaciones y por el rediseño del trabajo.

Esto está llevando a que cada vez sean más las voces que piden implantar una tasa robot, es decir, una propuesta fiscal que consiste en gravar a las empresas por el uso de IA, sistemas automatizados o robots que sustituyen a los trabajadores humanos. De hecho, el debate ni siquiera es nuevo. En el año 2017, cuando la inteligencia artificial estaba a años luz de lo que es hoy y todavía no se podía ni imaginar los usos y aplicaciones que iba a tener, ya la Unión Europea abrió un intenso debate sobre la fiscalidad de los robots y el impacto de la automatización en el empleo y los sistemas de bienestar.

“Considerando que el desarrollo de la robótica y la inteligencia artificial puede dar lugar a que los robots asuman gran parte del trabajo que ahora realizan los seres humanos sin que puedan reemplazarse por completo los empleos perdidos, deberá estudiarse la posibilidad de someter a impuesto el trabajo ejecutado por robots o exigir un gravamen por el uso y mantenimiento de cada robot, a fin de mantener la cohesión social y la prosperidad”, recogía un informe del Parlamento Europeo de 2017.

La Unión Europa alertaba de que, debido a la proliferación de este tipo de tecnologías, sumado a la viabilidad de los sistemas de seguridad y bienestar sociales y a la insuficiencia continuada de las cotizaciones para los regímenes de jubilación, se podría acarrear una mayor desigualdad en la distribución de la riqueza y el poder.

Pero ¿es posible implantar algo así en España? Teresa Pérez Cruz, abogada experta en derecho laboral, cree que sí. “Desde el punto de vista jurídico, es perfectamente posible establecer una contribución económica vinculada a la automatización, aunque conviene distinguir entre una cotización social propiamente dicha y un tributo destinado a financiar la Seguridad Social”, explica la experta. “Con nuestra legislación actual, un robot no puede sustituir jurídicamente a un trabajador a efectos de cotización. No existe una relación laboral, una remuneración salarial ni un sujeto protegido que genere los derechos propios de la Seguridad Social. Ahora bien, el legislador podría crear una contribución específica sobre determinadas actividades automatizadas y destinar su recaudación a financiar pensiones, prestaciones por desempleo o programas de formación”, detalla al respecto.

> Meta y Micrososft han anunciado 8.000 despidos cada una con motivo de la implementación de la IA

Hay que tener en cuenta que en lo que va de 2026, más de 92.000 trabajadores tecnológicos a nivel han perdido su trabajo, según datos del portal Layoffs.fyi. Las empresas se han escudado en la inteligencia artificial a la hora de hacer estos recortes. Solo los gigantes Meta y Microsoft anunciaron a principios de año despidos que afectan a más de 16.000 empleados. En el caso de la propietaria de Facebook se trata del 10% de su plantilla.

Pese a los despidos, se trata de compañías que están presentando unas cuentas muy sólidas. La empresa que dirige Satya Nadella cerró 2025 con un beneficio neto de 101.832 millones de dólares (en euros, aproximadamente, 88.965 millones), lo que supone un crecimiento del 15% en comparación con el año anterior. Mientras que Meta vio reducidas sus ganancias un 3,1% el año pasado, pero en lo que va de 2026 ha obtenido unas ganancias cifradas en 52.481 millones de dólares (unos 46.676 millones de euros), lo que representa un incremento del 39%.

Las tecnológicas están poniendo como excusa el alto coste que pone la implementación de la IA. Sin embargo, cada vez son más las voces que avisan de que la automatización supone un beneficio económico para las compañías. “La automatización también genera riqueza, mejora la productividad y puede crear nuevas oportunidades laborales. Estamos entrando en un escenario en el que las empresas pueden mantener, e incluso incrementar, su productividad reduciendo considerablemente sus plantillas gracias a la automatización y a la inteligencia artificial”, destaca Pérez Cruz.

Francia decidió en 2025 seguir los pasos de la Unión Europea y poner sobre la mesa una proposición de ley que plantea establecer una contribución económica a las empresas que sustituyan trabajadores por sistemas automatizados, incluidos los programas de inteligencia artificial. La propuesta pretende compensar la pérdida de cotizaciones sociales derivada de la destrucción de empleo, destinando el 60% de la recaudación a financiar las pensiones y el seguro de desempleo, y el 40% restante a reducir las cotizaciones empresariales sobre el trabajo humano. Además de esta proposición legislativa, el Senado francés debatió el 29 de noviembre de ese mismo año una enmienda al proyecto de presupuestos para 2026 que proponía gravar con un 1% el valor producido por cada robot, con un límite vinculado al salario mínimo francés.

Este debate va más allá. Italia llegó a plantear un incremento del impuesto sobre sociedades para aquellas empresas cuya actividad productiva dependiera principalmente de robots o sistemas de inteligencia artificial, aunque la propuesta no prosperó. Mientras que Corea del Sur fue pionera en 2017 al reducir los incentivos fiscales a las inversiones en automatización.

Tecnología

El cuello de botella eléctrico amenaza con acumular millones de chips sin usar

La anticuada red eléctrica de Estados Unidos no soporta la demanda de la IA y amenaza con frenar la revolución tecnológica, que exige una red eléctrica moderna que la infraestructura actual no puede ofrecer

Victor Blanco Moro

La inversión en la inteligencia artificial se ha convertido en uno de los motores del crecimiento más importantes para Estados Unidos y ha sostenido las subidas de las bolsas en los últimos trimestres gracias a las perspectivas de un fuerte crecimiento de los beneficios empresariales gracias a esta nueva tecnología. En un escenario de optimismo generalizado, los mercados han decidido enfocarse en las hipótesis más positivas sobre el impacto de la IA, pero, la revolución tecnológica que supone no está exenta de riesgos, y hay algunos que pueden materializarse en los próximos meses.

La posibilidad de un entorno regulatorio más duro para los centros de datos está pesando ya entre los inversores, pero no es el único evento negativo que puede afectar al sector. La electricidad, y especialmente, un cuello de botella en la red eléctrica estadounidense asoma ahora como un riesgo real en los próximos meses.

La red eléctrica es una infraestructura que se ha puesto a prueba en distintas partes del mundo en los últimos años. La capacidad de la red es limitada, y en muchos casos, diseñada hace tiempo para usos diferentes a los que han aparecido en los últimos años. La irrupción de las energías renovables y, más recientemente, la construcción de los centros de datos, el cerebro de los sistemas de IA, están creando un cuello de botella en distintas regiones, como Estados Unidos o Europa.

"La electrificación en desarrollo de la economía ha hecho que las redes eléctricas se conviertan en un freno para la transición energética y, en algunos casos, está frenando el desarrollo de la economía digital. Una red eléctrica que envejece, y que no está diseñada para la demanda moderna se está viendo presionada por las cargas eléctricas que genera la demanda de la IA", explican desde Macquarie.

"La red eléctrica global está entrando en el ciclo de inversión con mayores consecuencias de toda una generación. En distintas geografías y estructuras de mercado, está surgiendo el mismo reto: las redes deben ser más robustas, más flexibles y significativamente más grandes", indica Macquaire. "Los motivos son varios, desde la integración de las energías renovables en Europa, hasta el aumento de la demanda por la IA en Estados Unidos, pero todos apuntan al mismo imperativo: la red, que desde hace mucho se ha tratado como una infraestructura estable, se ha convertido en un cuello de botella para la transición energética, la economía digital y el crecimiento industrial", advierten desde la gestora.

> Según Elon Musk, a final de año habrá un excedente de chips por la falta de electricidad para activarlos

Esta presión en la red eléctrica, en el contexto de una inversión masiva en la creación de centros de datos, ahora presenta el riesgo de que se haya producido un exceso de producción de semiconductores por parte de la industria, hasta el punto de que, en los próximos meses, existe la posibilidad de que los chips se acumulen por la imposibilidad de ponerlos en funcionamiento.

Elon Musk lo señaló hace unas semanas, e incluso pone fecha a un momento clave que generará este problema, al declarar que cree que "hacia final de este año, la producción de chips va a adelantar a la capacidad de encenderlos". "Hasta que lleguemos al espacio y evitemos le problema de la electricidad, el freno para la computación va a ser ese, la electricidad. Mi estimación es que, para finales de este año, los chips se van a empezar a acumular", ha advertido Musk.

Una más moderna

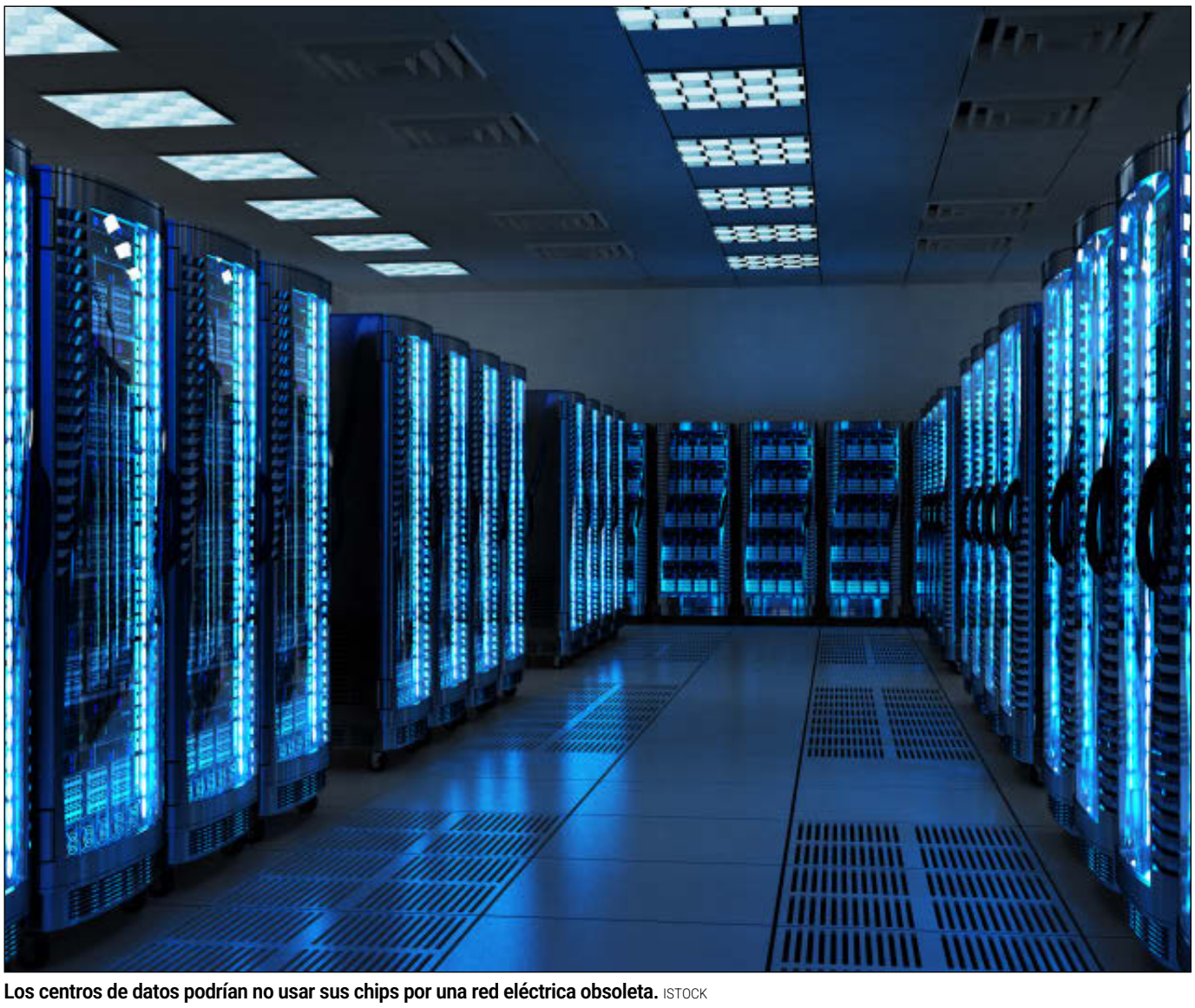
El reto para la industria es de capacidad de generación, con la excepción de China, pero no es el único: el tipo de red es clave, ya que el impulso a las fuentes de energía renovable también exige una reforma de las redes, algo de lo que advierte Macquaire: "La capacidad de generación renovable está escalando rápidamente, pero la infraestructura de redes para entregar esa energía de forma segura no mantiene el ritmo. En 2025 se añadieron 814 gigavatios de nueva capacidad solar y eólica de forma global, un 17% más que el año previo", señala.

Además, la gestora destaca que "lo que se necesita no es solo más red, sino un tipo diferente de red", ya que "el modelo viejo entregaba energía en una dirección, desde las grandes plantas centralizadas, a los consumidores pasivos. El modelo emergente debe gestionar la distribución, la entrega variable de generación en todas direcciones, desde las plantas eólicas hasta las de paneles solares, al mismo tiempo que mantiene la estabilidad y seguridad de la que dependen los consumidores y la industria".

El problema de una red obsoleta para las necesidades actuales se convierte en una amenaza global para todo el sistema eléctrico, del que ahora depende de forma vital la industria tecnológica, centrada en la IA, y que plantea inversiones billonarias para desarrollar esta nueva tecnología, hasta el punto en el que esta inversión se ha convertido en uno de los principales motores de crecimiento económico en Estados Unidos.

Parte del problema, además, se debe a la lentitud a la hora de aprobar los permisos necesarios para el desarrollo de las redes eléctricas, a juicio de Citi. "La demanda de más infraestructura energética y equipamiento de generación sigue creciendo, sobre todo impulsada por los centros de datos de la IA en Estados Unidos, y por un aumento en la preocupación de la seguridad energética". Sin embargo, las redes eléctricas en muchas regiones están teniendo problemas para mantener el ritmo, castigadas por los cuellos de botellas en la cadena de suministros y por procesos muy lentos para conseguir los permisos, argumenta Citi.

"Incluso si se modera el crecimiento del consumo por parte de la inteligencia artificial, las tendencias generalizadas de seguridad energética, electrificación, desarrollo de renovables y adopción de coches eléctricos por sí solos van a requerir una inversión sustancial en infraestructuras energéticas y de equipos de generación", avisa el banco.



Los centros de datos podrían no usar sus chips por una red eléctrica obsoleta. ISTOCK

Tecnología



Las empresas desconocen el uso de la IA que hace su plantilla. ISTOCK

El 80% de las plantillas usa sistemas autónomos a espaldas de la empresa

Esta práctica, conocida como "Shadow AI", pone en riesgo los datos confidenciales y la seguridad de las compañías y obliga a reforzar la supervisión y la formación de los empleados

María Juárez

La inteligencia artificial (IA) se ha colado en nuestras vidas casi sin hacer ruido, y no solo en lo cotidiano, sino también en el entorno laboral. Se ha convertido en una herramienta capaz de ahorrar tiempo, agilizar procesos y elevar la productividad, pero es un arma de doble filo, pues esta herramienta no sabe guardar secretos, y esto es un riesgo que muchas empresas todavía no ven. Datos internos, documentos, información de clientes o contenidos sensibles pueden acabar en servicios externos sin que la organización sea consciente de ello. Esto es lo que se conoce como *Shadow AI*, la inteligencia artificial que los empleados utilizan por su cuenta y al margen de los sistemas y controles de la compañía.

España se sitúa a la cabeza en la adopción de IA en el entorno laboral. Ocho de cada diez trabajadores españoles utilizan estas herramientas en sus tareas diarias sin informar de ello a su empresa, según el estudio *El momento de la verdad de la IA en la empresa*, elaborado por OpinionWay a partir de 2.006 profesionales de Francia, España, Portugal y Alemania. Ahora bien, más allá del número de empleados que recurren a estas herramientas, el dato que marca la diferencia está en la frecuencia. El 40% de los trabajadores españoles utiliza la IA de forma habitual, la proporción más elevada entre los mercados analizados. Además, esta cifra se ha disparado 16 puntos en apenas un año, reflejando hasta qué punto estas tecnologías han pasado de ser una novedad a integrarse en la rutina de las empresas.

Siguiendo esta línea, Javier Torres, *general manager* de Cegid en Iberia, Latinoamérica y África, considera que "la velocidad con la que los empleados están incorporando la IA en su trabajo diario demuestra que ya no estamos ante una tecnología de futuro, sino ante una realidad presente en las organizaciones. La IA en la sombra evidencia que los profesionales ya están transformando su forma de trabajar".

Sin embargo, esta rápida incorporación también plantea interrogantes sobre el control de la información que los trabajadores comparten con estas herramientas. "Cada vez que un empleado le pega a ChatGPT la hoja de un cliente con nombre, NIF, situación familiar, datos de salud o el desglose de la nómina, está mandando esos datos a un servidor que no tiene contrato de encargado del tratamiento con tu despacho. En cristiano: estás cediendo datos personales de un tercero sin amparo jurídico. Y eso, según la Agencia Española de Protección de Datos (AEPD) se llama infracción", explica a este periódico Pedro de Toledo, director de Asesoría Toledo. Abogado Fiscalista y Laboralista

¿Cuáles son los riesgos?

Cada vez más empleados usan la IA en sus tareas diarias sin comunicárselo a la empresa, y esto tiene muchos riesgos. Un claro ejemplo, es lo que ocurrió hace tres años en la sede de Samsung. Varios ingenieros recurrieron a ChatGPT para resumir una reunión interna en la que se trataban temas confidenciales sobre la fabricación de semiconductores. Días después, otros empleados hicieron lo mismo con el código fuente de un programa informático que compartieron con la herramienta para corregir errores y mejorar su funcionamiento. Cuando la empresa surcoreana detectó lo que estaba ocurriendo, tomó medidas para frenar estas prácticas. Sin embargo, la información ya se había introducido en la plataforma.

No cabe duda de que el uso de estas herramientas sin una supervisión adecuada puede acarrear riesgos como la fuga de datos confidenciales, incumplimientos legales y pérdida de la propiedad intelectual al compartir información sensible con plataformas externas. Del mismo modo, estas herramientas pueden generar respuestas erróneas o sesgadas que afecten a las decisiones empresariales. Todo ello se agrava cuando la empresa desconoce qué aplicaciones utilizan sus empleados y pierde capacidad para controlar los riesgos de seguridad.

> Uno de los mayores retos de las compañías es integrar de forma segura estas herramientas en su día a día

Pero ¿qué pueden hacer las empresas ante esta situación? En palabras de Pedro de Toledo, "lo única que funciona es gobernarla. No prohibir. No mirar a otro lado. Gobernar". El asesor continúa explicando que se deben tener herramientas. "Pocas herramientas. Las que sean, pero contratadas en versión profesional", subraya. Además, pone el foco en la necesidad de dar formación a la plantilla. "Media tarde de formación al equipo. Esa media tarde es exactamente la "alfabetización en IA" que te exige Bruselas. No te están pidiendo un máster. Te están pidiendo que tu gente sepa qué datos le está soltando a la herramienta y qué no".

Más allá de controlar el uso de estas herramientas, el verdadero reto es intégralas de forma segura en la actividad de las empresas. En este sentido, Javier Torres considera que las compañías deben avanzar hacia un modelo en el que la IA deje de utilizarse de forma individual y pase a integrarse en los procesos de negocio bajo la supervisión de la organización. "El reto pasa por conectar la IA con los procesos críticos del negocio y con información fiable y contextualizada, para convertirla en una herramienta capaz de aportar valor tangible a la organización", concluye.

Contenido ofrecido por Mercadona

Mercadona apuesta por Atenea, su propia IA para desarrollar software

Se trata de un agente que integra el conocimiento, los procesos y los estándares de la compañía para acelerar y optimizar el ciclo de vida del desarrollo de software

EcoBrands

Mercadona ha creado y puesto en marcha ATENEA, una plataforma propia de inteligencia artificial con el objetivo de ayudar a sus equipos tecnológicos a generar software con mayor rapidez y más calidad. Más de 500 ingenieros ya utilizan esta plataforma de IA agéntica creada para transformar y acelerar el desarrollo de software a gran escala. Con esta herramienta, que no solo responde o genera contenidos junto al usuario, sino que también puede ejecutar tareas de forma autónoma, la compañía busca ganar agilidad y eficiencia en la creación de aplicaciones y, con ello, impulsar la digitalización de sus procesos físicos.

ATENEA es una solución propia de Mercadona IT, el departamento responsable de la digitalización de la compañía. La plataforma integra el conocimiento, los procesos, las herramientas y los estándares de calidad de Mercadona, y coordina agentes especializados capaces de ejecutar distintas misiones dentro del ciclo de desarrollo. Con esta solución, la compañía busca optimizar el desarrollo del software que da soporte al negocio.

"Esta plataforma propia de inteligencia artificial ayuda a los equipos tecnológicos a crear software de forma más rápida, con mayor calidad y, lo más importante, integrando el conocimiento y el contexto propio de nuestra empresa", explica Sergio Pajares, CTO de Mercadona.

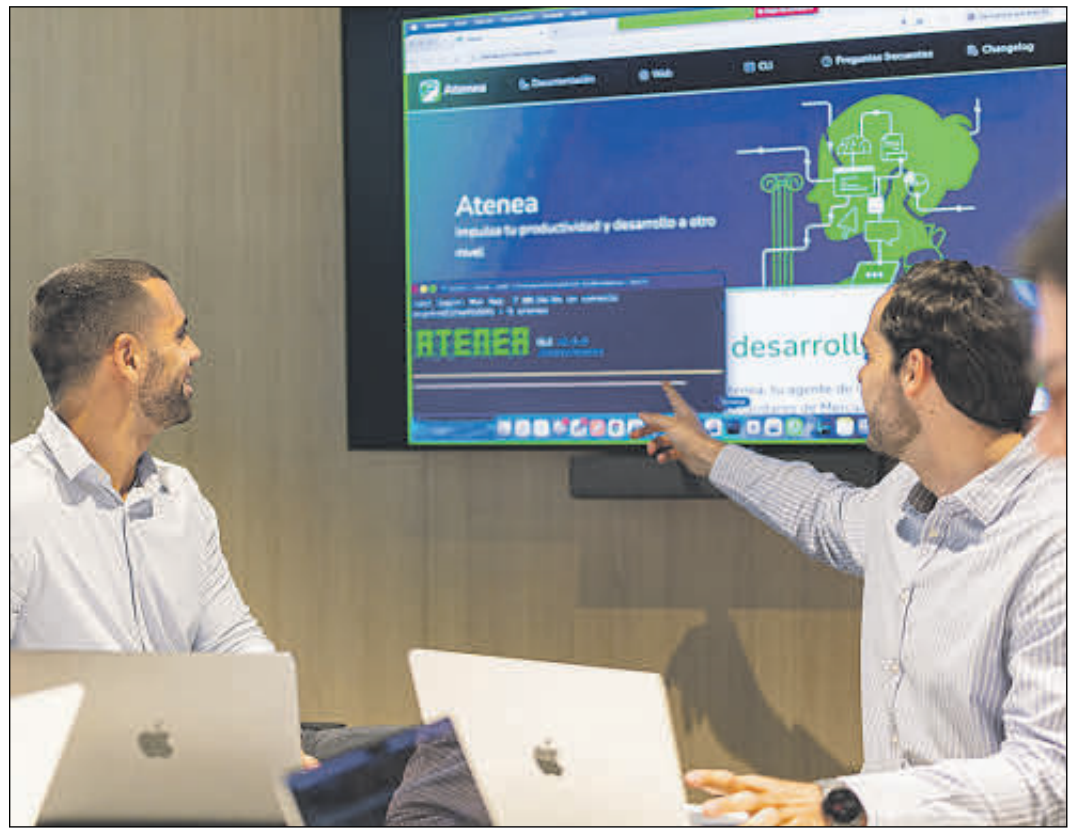
En el desarrollo y la implantación de ATENEA participan equipos de diferentes ámbitos de Mercadona IT, entre ellos los de procesos, tecnología, operaciones, infraestructura, diseño o seguridad entre otros.

Además, la compañía ha formado un equipo de ingenieros *early adopters*, encargado de impulsar su implantación en los diferentes verticales de desarrollo para el negocio, así como de formar y acompañar a los equipos en la adopción de esta nueva forma de trabajar.

> La compañía ha formado un equipo de ingenieros 'early adopters', para su implantación

Según Sergio Pajares, "con el desarrollo y puesta en marcha de ATENEA la compañía persigue crear una nueva forma de desarrollar software, más rápida, más consistente y más alineada con las necesidades del negocio. En este sentido, el reto principal ha sido que la IA entienda cómo trabaja Mercadona y que ATENEA funcione como un equipo formado por distintos agentes especializados, cada uno preparado para realizar una tarea concreta o trabajar con una tecnología específica".

La siguiente fase pasa por extender el uso de agentes a todo el ciclo de vida del desarrollo, hacer la plataforma más eficiente y evolucionarla para que pueda trabajar con modelos de IA de diferentes fabricantes.



Equipos de Mercadona IT trabajando con Atenea. MERCADONA



Sergio Pajares, CTO de Mercadona. MERCADONA

Una IA que entiende a Mercadona

El factor diferencial no está únicamente en disponer de modelos de IA cada vez más capaces, sino en conseguir que estos entiendan cómo trabaja la compañía y actúen dentro de sus criterios técnicos. "La inteligencia artificial es cada vez más capaz y eficiente. Pero, si no se le marcan límites y objetivos claros, puede cometer errores o trabajar en una dirección equivocada. Lo importante no es solo contar con una IA muy potente, sino asegurarse de que está alineada con las necesidades de la empresa", señala Pajares.

Antes de abordar una tarea, ATENEA proporciona a los agentes información sobre cómo desarrolla software Mercadona: sus procesos, herramientas, normas, diseños y criterios de calidad. De esta forma, la IA puede generar soluciones que encajan con la forma real de trabajar de la compañía.

"La IA no sustituye la responsabilidad técnica; la amplifica. Los profesionales mantienen el control y el criterio sobre las decisiones, mientras la plataforma multiplica su capacidad de ejecución", añade Pajares.

La IA en Mercadona

La compañía lleva años desarrollando una estructura tecnológica que aproveche la IA cuando verdaderamente aporte valor. De ahí la importancia y, especialmente en una empresa de su volumen, con cientos de aplicaciones y procesos, de identificar correctamente donde la inteligencia artificial aporta un impacto real.

Además de ATENEA, Mercadona cuenta con otras soluciones que incorporan IA en diferentes procesos. Algunos de ellos incluyen la planificación y gestión de vacaciones y horarios, el reconocimiento automático de facturas de proveedores o un proyecto propio para gestionar con IA todos los datos maestros de producto.

Tecnología

Los ciberdelincuentes ya no ‘hackean’, ahora fichan a los trabajadores

Las redes criminales ofrecen primas de hasta 22.300 euros a trabajadores con acceso a sistemas y datos confidenciales para facilitar operaciones fraudulentas desde dentro

María Juárez

Ya no te puedes fiar ni de tu propia sombra”, es una expresión popular que significa que existe una desconfianza extrema hacia todo. Y es que nada más lejos de la realidad, porque los ciberdelincuentes han encontrado una nueva vía para infiltrarse en las empresas mediante la reclutación de los empleados, que ya cuentan con un acceso privilegiado a los sistemas, procesos y datos confidenciales. En este contexto, según recoge la última investigación de TrendAI, estas redes ofrecen primas de hasta 25.000 dólares –unos 22.300 euros– a trabajadores capaces de facilitar operaciones fraudulentas desde dentro de las organizaciones, sin necesidad de vulnerar sus defensas tecnológicas.

Pero ¿por qué recurren a los trabajadores? La respuesta es sencilla: si ya están dentro, no levantan sospechas y pueden aprobar pagos, recuperar cuentas, cambiar procedimientos internos, consultar información confidencial o acceder a los sistemas de la empresa sin tener que superar sus barreras de seguridad. En definitiva, el objetivo ya no es solo entrar en los sistemas de una empresa, sino controlar desde dentro procesos clave para su funcionamiento. Siguiendo esta línea, el informe identifica ofertas dirigidas a empleados de bancos, compañías telefónicas, plataformas digitales, empresas de transporte, organismos públicos, centros sanitarios y grandes cadenas comerciales. Según el sector, los delincuentes buscan manipular tarjetas SIM, alterar el seguimiento de paquetes, aprobar devoluciones de dinero, consultar historiales médicos o vender accesos a los sistemas internos de las empresas.

En palabras de David Sancho, investigador de amenazas de TrendAI, “durante años hemos centrado la atención en proteger el perímetro de las organizaciones, pero los propios ciberdelincuentes están demostrando que el acceso más eficiente no siempre pasa por romper las defensas, sino por convencer a quien ya trabaja dentro”. Y agrega que “estamos asistiendo a la profesionalización de un mercado que convierte la confianza en un activo comercializable”.

No cabe duda de que esta tendencia obliga a las empresas a ampliar su forma de entender la ciberseguridad. Ya no basta con proteger los sistemas informáticos o gestionar los riesgos relacionados con el personal: también es necesario vigilar los procesos clave del negocio y los accesos que permiten llevarlos a cabo. La captación de empleados se convierte así en una amenaza que puede afectar directamente al funcionamiento de las organizaciones, al aprovechar la confianza depositada en quienes están autorizados a operar desde dentro.



Los ciberdelincuentes recurren a los trabajadores. ISTOCK

Aumento de los ataques

Con los datos sobre la mesa, tal y como apunta el Instituto Nacional de Ciberseguridad (INCIBE), los incidentes relacionados con el robo de información ascendieron a 3.849 casos de acceso o sustracción no autorizada de datos digitales o confidenciales. Una amenaza que adquiere especial relevancia en un contexto en el que los ciberdelincuentes no solo buscan vulnerar las defensas tecnológicas de las organizaciones, sino también aprovechar los accesos legítimos de sus propios empleados para infiltrarse en los sistemas y manipular procesos internos. Sin embargo, esto va más allá, y en general la situación de los ciberataques es alarmante, pues estos actos han ido ganando poco a poco peso en España durante la última década. Así, los datos del Ministerio del Interior recogen que en 2016 se registraron 92.716 hechos conocidos, una cifra que ascendió hasta los 488.426 en 2025, lo que supone un incremento del 427%. La tendencia al alza se mantuvo en el último año, con un aumento del 5,1% respecto a 2024, cuando hubo 464.801 casos.

A este respecto, tendiendo en cuenta el seguimiento del INCIBE, los sectores más expuesto son la banca, que concentró el 34%, seguida del transporte, con un 14%, y la energía, con un 8%. También se vieron afectadas las infraestructuras de los mercados financieros, que representaron el 7%, y las aseguradoras y los fondos de pensiones, con un 6%.

> Según los datos del Ministerio de Interior, España registró 488.426 ciberdelitos en 2025, un 427% más que en 2016

Entre los incidentes de ciberseguridad más frecuentes está el *malware*, con 55.411 casos registrados. De ellos, 392 correspondieron a ataques de *ransomware*, una modalidad en la que los ciberdelincuentes bloquean sistemas o archivos para exigir un rescate económico. Asimismo también preocupa la proliferación de redes de dispositivos infectados que pueden controlarse por *botnets* (una red de robots) desde la distancia. Según los sistemas identificados por INCIBE-CERT, el 85% de los dispositivos afectados estaban relacionados con el internet de las cosas (IoT), como televisores, decodificadores y reproductores multimedia.

En relación con esto, el fraude online constituyó otra de las principales amenazas, con 45.445 incidentes, un 19% más que el último dato registrado. Esta modalidad representó el 40% de los incidentes de seguridad, siendo el *phishing* una de sus principales manifestaciones. De hecho, se registraron 25.133 casos de mensajes o páginas fraudulentas. Ahora bien, ante esta situación el INCIBE no ha cedido y, en colaboración con Red.es, ha cerrado 4.600 dominios web bajo la extensión “.es” potencialmente fraudulentos.

En definitiva, ante este nuevo escenario, las empresas deben reforzar sus medidas de seguridad desde una doble perspectiva. Ya no basta con proteger los sistemas informáticos frente a posibles ataques externos, sino que también es necesario controlar los accesos internos. Porque, cuando se puede comprar la colaboración de un empleado, el mayor riesgo para una empresa puede venir de alguien que ya está dentro y conoce cómo funciona la organización.

Tecnología

Ciberseguridad a velocidad de máquina: los parches tradicionales ya no son suficientes



Sam Curry

CISO de Zscaler

Los recientes ciberataques sufridos en las últimas semanas son un claro ejemplo de la velocidad a la que se explotan actualmente las vulnerabilidades, un ritmo para el que los equipos de seguridad de la mayoría de las empresas no están preparados. En el caso de PHP, una vulnerabilidad que permitía a atacantes no autentificados ejecutar comandos en servidores expuestos se convirtió rápidamente en un problema de seguridad global. Los equipos de seguridad no solo tuvieron que hacer frente a un fallo grave, sino también al hecho de que los atacantes ya habían comenzado a explotarlo antes de que muchas organizaciones hubieran terminado siquiera de identificar dónde se estaba utilizando PHP en sus entornos.

Esta urgencia obligó a algunas empresas a desconectar sistemas, acelerar las medidas de corrección de emergencia y recurrir a controles temporales para ganar tiempo. La principal lección es que la velocidad se ha convertido en un factor determinante del impacto de los incidentes de ciberseguridad. El tiempo que transcurre entre la divulgación de una vulnerabilidad y su explotación es tan reducido que muchas empresas quedan expuestas antes incluso de que puedan poner en marcha sus procedimientos habituales de respuesta. Sin embargo, este patrón de ataque era previsible.

El principio que guía a los ciberdelincuentes a la hora de seleccionar sus objetivos es mucho más amplio. Actualmente, los atacantes no eligen sus objetivos al azar, sino que buscan vulnerabilidades en todo tipo de sistemas y programas. Priorizan las tecnologías más extendidas, profundamente integradas, fáciles de localizar y con un elevado potencial de impacto una vez comprometidas, con el objetivo de maximizar el alcance de sus ataques. Entre ellas se encuentran los dispositivos de seguridad perimetral y acceso remoto, las cadenas de suministro de software, los planos de control de la nube y los sistemas de gestión de aplicaciones SaaS, por citar algunos ejemplos. Si una tecnología está ampliamente implantada, proporciona acceso a numerosos recursos, permite ejecutar código o se encuentra próxima a infraestructuras críticas, tiene muchas posibilidades de convertirse en un objetivo prioritario.

PHP encaja perfectamente en este modelo. No solo está presente en webs públicas y sistemas de gestión de contenidos, sino también en herramientas administrativas internas, dispositivos que lo incorporan, aplicaciones heredadas y sistemas no documentados que se han ido acumulando con el tiempo. Esto lo convierte en un objetivo atractivo para los atacantes, ya que una única vulnerabilidad en una tecnología ampliamente implantada y de gran importancia puede provocar consecuencias a gran escala. En este sentido, el ataque no resultó sorprendente. Siguió un patrón que previsiblemente veremos con mayor frecuencia en el futuro. Si una tecnología es habitual, está expuesta y permite comprometer otros sistemas, será analizada, puesta a prueba y, finalmente, utilizada como herramienta de ataque.

Diferencia de velocidad

Este reciente ataque también pone de manifiesto las limitaciones de las operaciones de seguridad de las empresas. La mayoría de los procesos de aplicación de parches y corrección de vulnerabilidades se diseñaron pensando en plazos de actuación humanos, siguiendo un procedimiento que consiste en identificar el problema, localizar los activos afectados, probar las actualizaciones, programar las tareas de mantenimiento y, finalmente, implementar las correcciones de forma controlada.

Sin embargo, los atacantes operan cada vez más a velocidades propias de las máquinas, mientras que los grupos maliciosos que planifican sus inversiones en investigación y desarrollo priorizan los objetivos más fáciles de comprometer. La automatización y la inteligencia artificial les permiten analizar la información publicada sobre vulnerabilidades, adaptar las cadenas de explotación y pasar del reconocimiento inicial a la ejecución del ataque en cuestión de minutos.

Esta diferencia de velocidad cambia por completo las reglas del juego. Si toda la estrategia defensiva de una organización depende de aplicar parches en cada sistema vulnerable antes de que un atacante encuentre uno expuesto, las probabilidades de éxito ya no juegan a su favor. Un enfoque más realista consiste en asumir que algunos sistemas vulnerables permanecerán sin actualizar durante un determinado periodo, ya sea por su complejidad, las dependencias de aplicaciones heredadas, la falta de soporte del software o los riesgos operativos asociados.

> Los atacantes no eligen sus objetivos al azar, sino que buscan vulnerabilidades en todo tipo de sistemas y programas

La cuestión ya no es únicamente con qué rapidez se pueden aplicar los parches, sino hasta qué punto es posible limitar la exposición mientras se completan las actualizaciones.

Reducir la visibilidad

Las empresas deben prepararse para este tipo de ataques identificando, en primer lugar, qué tecnologías de su entorno pueden resultar más atractivas para los ciberdelincuentes. Una forma práctica de hacerlo consiste en evaluar tres factores: su grado de implantación, su capacidad para proporcionar acceso y su capacidad para otorgar control sobre otros sistemas.

En otras palabras, ¿qué tecnologías están presentes en todas partes, ¿cuáles abren puertas y cuáles permiten tomar el control una vez que se accede a ellas? Estas tecnologías deberían situarse entre las principales prioridades de seguridad para 2027. A partir de ahí, la estrategia debe ser clara: los equipos de TI han de reducir su uso siempre que sea posible, limitar su visibilidad cuando resulte viable y garantizar su capacidad de recuperación en caso de ataque.

Esto implica evitar que las aplicaciones internas queden expuestas innecesariamente al exterior, restringir las posibilidades de acceso e implementar medidas de protección online cuando no sea posible aplicar los parches de inmediato.

Aquí es donde el modelo Zero Trust adquiere una importancia operativa real, más allá de su utilidad conceptual, para garantizar la continuidad del negocio. Las lecciones que dejan los ciberataques contra PHP, y el resto de las brechas de seguridad que se han sucedido, no es simplemente que las empresas deban aplicar los parches con mayor rapidez. Es que necesitan una arquitectura de seguridad que reduzca la superficie de ataque, asuma que los intentos de explotación pueden producirse rápidamente y evite que una única tecnología vulnerable desencadene una crisis que afecte a toda la empresa.



ISTOCK

Tecnología



Los expertos alegan que hay que sospechar de cualquier llamada fuera de lo común. ISTOCK

Voces clonadas y vídeos falsos: así evoluciona el fraude digital

Los ciberdelincuentes recurren a la inteligencia artificial para suplantar identidades, aprovechar datos personales y construir fraudes cada vez más difíciles de detectar

María Juárez

Las estafas son cada vez más elaboradas y difíciles de detectar. La inteligencia artificial se ha convertido en una aliada para los delincuentes, que usan vídeos, imágenes y audios manipulados para crear mensajes más realistas y convincentes que engañan tanto a particulares como a empresas. A este fenómeno se le denomina *deepfakes*. Pero ¿cómo consiguen esta información? "Los ciberdelincuentes necesitan conocer los vínculos afectivos de la persona, sus hábitos diarios, nombres de allegados o mascotas y muestras de voz. Para conseguirlo analizan en redes sociales vídeos, historias publicadas con sonido o notas de voz públicas para entrenar el modelo de clonación", explica a este periódico Doris Seedorf, CEO de Softtek para España. Y agrega que "aprovechan los datos de ubicación en tiempo real, viajes en curso y fotos etiquetadas para crear una historia contextual altamente creíble, como simular un accidente, una detención o un robo en un lugar determinado".

La principal diferencia con otras estafas está en el realismo y en la rapidez con la que se cometen estos fraudes. Mientras que las estafas tradicionales recurrían a mensajes engañosos o suplantaciones más fáciles de detectar, la inteligencia artificial, actualmente, permite clonar una voz con apenas 30 segundos de audio obtenidos, por ejemplo, de las redes sociales, con una precisión casi imperceptible para nuestro odio, siendo capaz de recrear incluso estados emocionales, como susurros, llanto o desesperación. Esta tecnología dificulta la identificación del fraude, ya que elimina muchas de las señales que antes despertaban sospechas, como los errores de redacción o los tonos poco naturales, y hace que los engaños resulten mucho más creíbles.

Otro factor clave es que la urgencia anula la capacidad crítica y la lógica, pues "los estafadores usan amenazas con plazos muy cortos, como cancelaciones de reservas en 24 horas o falsas emergencias de un familiar, para forzar una respuesta apresurada e impulsiva", comenta Rafa López, *Workspace Security Engineer* de Check Point Software en España.

> Taylor Swift, Scarlett Johansson o Messi, son algunos de los famosos a los que han suplantado la identidad

La necesidad de verificar

El perfil más vulnerable suelen ser las personas mayores, pues no están tan familiarizados con los avances tecnológicos. Sin embargo, la realidad es que estas estafas parecen tan reales que cualquiera podría caer. "Si se recibe una llamada de este tipo, se debe mantener la calma, colgar la llamada actual sin tomar decisiones precipitadas y ponerse en contacto directamente con el familiar o con su entorno cercano", comenta Doris Seedorf. Del mismo modo, expertos en la materia como Rafa López, recomiendan "acordar una palabra clave o pregunta de control privada e imprevista dentro del ámbito familiar ya que es una de las medidas más eficaces contra las voces clonadas. También es fundamental verificar la identidad llamando por un canal secundario de confianza, escribir directamente las URL oficiales en el navegador en lugar de pulsar enlaces recibidos, y revisar los ajustes de privacidad para restringir quién nos añade a grupos. Estas medidas prácticas refuerzan la seguridad del día a día".

Asimismo, es importante destacar, que no siempre se hacen pasar por familiares o conocidos, sino que también imitan a celebridades y altos ejecutivos. Sin ir más lejos, en marzo de 2024, la imagen de Lionel Messi fue suplantada mediante *deepfake* para promocionar una falsa aplicación de inversiones llamada *Wildcat Dive*. Los estafadores utilizaron un audio modificado a partir de una entrevista real que el jugador concedió al canal de *streaming Olga*. A partir de eso, crearon un vídeo manipulado en el que aparecía recomendando una aplicación como una supuesta fuente de ingresos con la que miles de personas podían ganar dinero. Pero detrás de esto, en realidad había una estafa piramidal, donde las víctimas invertían su dinero en la plataforma, pero después no podían retirar los fondos. Este fraude fue detectado y denunciado por la compañía de ciberseguridad ESET, que alertó sobre el uso malicioso de la IA para suplantar la identidad de personajes públicos y así dar credibilidad a este tipo de engaños.

Este caso no es el único. McAfee ha realizado una lista que recoge los famosos que suelen ser más suplantados por los ciberdelincuentes. Esta lista, a nivel mundial, la encabeza Taylor Swift, seguida de Scarlett Johansson, Jenna Ortega y Sydney Sweeney. El motivo de recurrir a estar personalidades es que "cuando ves una cara conocida, tu cerebro baja automáticamente la guardia. Y ellos cuentan con esto", explica la compañía.

El papel de las compañías

Ahora bien, ante este panorama las firmas tecnológicas, las plataformas digitales, los bancos y las compañías telefónicas deben ayudar a los usuarios a detectar y frenar estos fraudes. Para Rafa López, "las empresas deben asumir una responsabilidad activa creando un ecosistema colaborativo que interconecte la detección de anomalías y la inteligencia contra amenazas"–y continúa afirmando– "las operadoras y plataformas deben bloquear la falsificación de identidad *(spoofing)* y limitar el envío de *spam* o grupos no autorizados". En relación con esto, según Doris Seedorf, "los bancos deben reforzar los sistemas de monitorización antifraude para detectar patrones inusuales en transferencias urgentes hacia cuentas desconocidas e incorporar pausas de seguridad.

De cara al futuro, la situación no parece que vaya a mejorar, sino más bien todo lo contrario. "Estas estafas evolucionarán hacia suplantaciones en tiempo real que combinarán voz y vídeo *(deepfakes* en videollamada) mediante agentes de IA interactivos capaces de mantener conversaciones fluidas por múltiples vías de comunicación al mismo tiempo", alega Doris Seedorf. Por ello, ante estos ataques tan rápidos y personalizados se debe responder "protegiendo de forma unificada la red, la nube, los dispositivos y los propios entornos de IA para ir siempre un paso por delante de la amenaza", asevera Rafa López.

En definitiva, ante estas llamadas o mensajes con exigencias de dinero o de información confidencial, se debe desconfiar y cortar la comunicación para poder verificar que no es una estafa.

Contenido ofrecido por Telefónica

Velocidad y calidad: Movistar ofrece la mejor experiencia móvil de España

La marca comercial en España de Telefónica encabeza las seis categorías analizadas por MedUX, con una posición destacada en Accessibility, referida a la capacidad de respuesta de la red

EcoBrands

Movistar, marca comercial de Telefónica en España, ofrece la mejor experiencia móvil nacional entre los operadores evaluados, según el último estudio de MedUX, compañía especializada en el *benchmarking* independiente de la calidad de la experiencia en las redes de telecomunicaciones.

El objetivo del estudio de MedUX sobre redes móviles en España, realizado con datos recopilados entre julio y septiembre de este año, tanto con medición en campo con *drive test* como con muestras de *crowdsourcing* desde dispositivos reales, es evaluar de forma independiente la calidad del servicio desde la perspectiva de los usuarios.

Según plasma MedUX, "Movistar obtiene el mayor MedUX Experience Score combinado con 3,97 sobre 5. De acuerdo con la metodología MedUX y el criterio estadístico establecido para el *benchmark*, el resultado sustenta su reconocimiento como líder único del *benchmark* nacional 3T 2026". El informe, que distingue seis categorías principales para evaluar el rendimiento y la calidad de la experiencia, concluye: "En todas ellas se identifica a Movistar como ganador, sumando seis liderazgos".

Con 3,97 puntos sobre 5, Movistar ofrece la mejor experiencia móvil, liderando las dos clasificaciones generales del informe, la de experiencia móvil global (*Best Mobile Experience*) y la de fiabilidad del servicio (*Most Reliable Mobile Experience*), con 3,97 y 4,20 puntos sobre 5, respectivamente.

En este sentido, la experiencia móvil global resume el comportamiento de la red en el conjunto de los servicios evaluados tales como velocidad, calidad de transmisión y continuidad de la conexión, mientras que la fiabilidad mide con qué consistencia se completan correctamente los servicios que el cliente utiliza. El informe sitúa además a Movistar en el primer puesto de las cuatro categorías adicionales analizadas en el informe:

- **Accessibility**, que hace referencia a la capacidad y rapidez de respuesta de la red (3,47 puntos), categoría en la que destaca especialmente Movistar.

- **Value for Speed**, que mide la velocidad de bajada y de subida en 4G y 5G y cómo dichas velocidades responden a las necesidades de trasmisión para ofrecer los mejores servicios (4,04 puntos). Cabe destacar que el 83,2% de las pruebas de campo de Movistar analizadas en esta categoría se realizó por 5G.

- **Data y OTT**, que agrupa los servicios de datos y la conexión a plataformas *over-the-top* (3,89 puntos).

- **Streaming**, como la experiencia de reproducción de vídeo (3,68 puntos).

Este reconocimiento refuerza el liderazgo de la red móvil de Telefónica para acceder a la tecnología más innovadora, aspecto que corroboran otros estudios y entidades independientes. La Asociación Española de Consumidores ha concluido que Movistar cuenta con la red móvil con mejor cobertura y experiencia global de España. También, la CNMC destaca a Telefónica como la operadora con mejor velocidad de descarga en móvil en sus últimos datos trimestrales sobre calidad de servicio publicados.



Los clientes Movistar disfrutan de la mejor experiencia en el uso de los servicios analizados. ISTOCK

Además, los clientes de Movistar son también los que disfrutan del mejor resultado del mercado en cuanto a la experiencia de los servicios analizados, en concreto navegación web; interacción en redes sociales; *streaming* de vídeo y juegos online.

El estudio incorpora como novedad la medición de la experiencia con asistentes de inteligencia artificial generativa, un servicio que depende de la latencia extremo a extremo y de la velocidad del transporte más que del ancho de banda. Movistar registra el mejor tiempo de respuesta en los tres percentiles medidos.

> Movistar obtiene el mayor MedUX Experience Score combinado con 3,97 sobre 5

En cuanto a la voz, medida por la calidad del audio recibido en llamadas reales, Movistar también sobresale entre el resto de los operadores con 4,59 puntos sobre 5.

Juan José Marfil, director de Red, TI e Infraestructuras de Telefónica en España, señala: "Este reconocimiento tiene para Telefónica un valor especial porque avala nuestro propósito como operadora de ser la mejor vía de acceso de los ciudadanos a las tecnologías digitales y nuestro esfuerzo para ofrecer más y mejores servicios, apoyados en la mejor red para acceder a la tecnología más innovadora, una red fiable y de máxima calidad que convierte toda la complejidad tecnológica en una experiencia diferencial".

Por su parte, Luis Molina, CEO de MedUX, afirma: "Nuestro objetivo no es solo dar un ranking sino ofrecer conclusiones que se puedan sostener con rigor. Por eso medimos la experiencia tal como la vive el usuario final, con los servicios que usa cada día, y la validamos con dos fuentes complementarias: medición en campo y millones de mediciones desde móviles reales. Con esa exigencia, aplicada por igual a todos los operadores, Movistar es hoy el líder único de la experiencia móvil en España".

Metodología empleada

Para realizar el informe, MedUX recorrió 4.480 kilómetros en 85 municipios españoles entre el 20 de julio y el 26 de septiembre de 2026, a lo largo de 45 días de medición, con sondas idénticas midiendo tres operadores en paralelo, en las mismas rutas y al mismo tiempo. De ese recorrido salieron cerca de 180.000 tests de servicio.

A esa campaña, se suma una muestra nacional de *crowdsourcing* recogida entre el 1 de julio y el 30 de septiembre desde dispositivos de usuarios finales reales, con cerca de 9 millones de mediciones en el trimestre, que amplía la observación a una diversidad de terminales, ubicaciones, horarios y condiciones de uso. El resultado final pondera un 80% la medición en campo y un 20% el *crowdsourcing*.

Tecnología

Las normativas buscan defender a los menores del 'scroll' infinito

La hiperconexión de los menores ha puesto a las redes sociales en el foco de los gobiernos europeos. Alrededor del 97% de los jóvenes de la Unión Europea utilizan internet a diario y las RRSS son la principal fuente de información para el 65% de ellos

Mónica G. Moreno

Ver el mundo por una pantalla. Relacionarse, estudiar, comprar, divertirse, informarse... La vida los niños y jóvenes transcurre a través de dispositivos móviles, aplicaciones y redes sociales. Así, la tecnología ocupa un lugar central en su día a día y dependen de ella para todo tipo de cuestiones cotidianas. El mundo digital tiene una gran influencia en el desarrollo de las generaciones actuales. Tanto es así que, alrededor del 97% de los jóvenes de la UE utilizan Internet a diario y las redes sociales son la principal fuente de información para el 65% de ellos.

Si bien es cierto que el acceso a Internet abre un mundo de aprendizaje, enseñanza y relaciones, los nativos digitales a menudo pierden el control frente a las pantallas. En lugar de aprovechar su potencial, muchos jóvenes pasan horas consumidos por el *scroll* infinito, enganchados a un consumo digital sin propósito. En este contexto, el reflejo de las pantallas muestra una hiperconexión que ha puesto a los menores en el punto de mira de los gobiernos europeos.

La Unión Europea ha dado un paso al frente con la *EU KIDS ACT,* un marco normativo para mejorar la seguridad en línea de los menores. La propuesta prohíbe que las plataformas de redes sociales permitan el acceso a los menores de 13 años y un sistema escalonado que se extiende hasta la mayoría de edad. Los menores solo podrán abrir una cuenta propia en redes sociales a partir de los 15 años. Así, entre los 13 y 15 años, solo podrán utilizar *minicuentas* estrictamente supervisadas, ya que los menores solo podrán acceder a ellas mediante la cuenta de sus padres o tutores. Esto les permitiría acceder a redes sociales y plataformas de intercambio de vídeos adecuadas a su edad. Estos servicios deben diseñarse con medidas de protección como un número restringido de contactos sociales y limitando además el tiempo de exposición frente a las pantallas a un máximo de una hora diaria.

"Actualmente, nuestros menores interactúan con las tecnologías más sofisticadas jamás creadas. Unas tecnologías que nunca se crearon pensando en su bienestar. Nuestra *EU KIDS ACT* invierte la carga de la prueba: corresponde a las plataformas demostrar que son seguras desde su diseño. Y devolvemos el control a los progenitores, proporcionándoles las herramientas necesarias para ayudar a sus hijos e hijas a navegar por un mundo en línea más seguro", declaro a este respecto la presidenta de la Comisión Europea, Ursula von der Leyen.

Las normativas serán "eficaces e indispensables", considera Marc Masip, fundador y presidente de Desconect@, resaltando que los menores están muy olvidados en este sentido, y es muy importante "protegerlos de las redes y de los contenidos a los que pueden acceder. La única forma realista de protección es que se delimite a las propias tecnológicas y que tengan que cumplir de verdad unas normas. Los padres no podemos hacerlo, no por falta de voluntad, sino porque es un entorno demasiado potente".



La Unión Europeoa busca mejorar la seguridad en línea de los menores. ALAMY

Seguridad desde el diseño

La normativa introduce un marco de seguridad desde el diseño que obliga a plataformas digitales, redes sociales y sistemas de IA dirigidos a menores de 18 años a desactivar de forma predeterminada funciones adictivas como el desplazamiento infinito, las notificaciones nocturnas y los *chatbots* interactivos, previniendo así la dependencia emocional y los perfiles de riesgo. Los perfiles de los menores deben ser privados por defecto, con acceso a geolocalización, cámaras y micrófonos desactivado. Para garantizar su cumplimiento sin vulnerar el derecho a la intimidad, la regulación exige implementar sistemas de verificación de edad basados en soluciones de privacidad garantizada –como la futura aplicación europea que no almacena identificadores ni datos biométricos–, exigiendo la comprobación estricta en nuevos registros y la estimación razonada de la edad en las cuentas vigentes. Con la *EU KIDS ACT* serán los proveedores los que tengan que demostrar que sus servicios están adaptados a la edad de los menores y son seguros.

"Regular es imprescindible, pero hay que regular lo que importa: el diseño", explica Liliana Arroyo, profesora y directora de la Chair for Socially Responsible Digital Innovation (SoReDI) de Esade, quien añade que "lo más valioso de la ley que se tramita es que obliga a las plataformas a demostrar ante la CNMC que no utilizan diseños adictivos. Si todo se reduce a poner una edad



El 51,6% del alumnado de Primaria dispone ya de móvil propio. ALAMY

mínima, desplazamos la responsabilidad a las familias y a los propios chavales". Arroyo menciona el caso de Australia, que en diciembre de 2025 se convirtió en el primer país del mundo en prohibir el acceso a las redes sociales a menores de 16 años: "Ya lo está viendo. La mayoría de quienes tenían cuenta antes de la prohibición pudo mantenerla o crear una nueva".

La profesora llama al cuidado porque "proteger no puede convertirse en vigilar. Una verificación de edad mal planteada nos pone a todos bajo control biométrico. Hace falta un efecto dominó, con plataformas, administraciones, escuelas, universidades y sociedad civil empujando en la misma dirección".

Francia se convirtió en el primer país europeo en vetar el acceso a estas plataformas a los menores de 15 años. Sin embargo, el pulso político no está exento de obstáculos jurídicos. El Consejo Constitucional francés bloqueó la medida del gobierno galo al considerarla una "vulneración desproporcionada" de la libertad de expresión y comunicación de los menores.

A los 10 años, el primer móvil

Con el objetivo de proteger a los menores, España también está trabajando para prohibir el acceso de los menores de 16 años a las redes sociales, obligando a las plataformas digitales a implementar sistemas efectivos de verificación de edad.

La presencia de los dispositivos digitales en el día a día de niños, niñas y adolescentes es abrumadora. Según el informe *Infancia, adolescencia y bienestar digital. Una aproximación desde la salud, la convivencia y la responsabilidad social*, resultado del trabajo conjunto entre Red.es, Unicef España, la Universidad de Santiago de Compostela y el Consejo General de Colegios de Ingeniería Informática, el 82,4% dispone de su propio teléfono móvil, al que acceden de media a los 10,8 años. El 51,6% del alumnado de Primaria dispone ya de móvil propio, porcentaje que asciende al 92,8% en la ESO. "El acceso a pantallas con conexión empieza a una edad muy temprana, y el uso de redes sociales y plataformas de vídeo se consolida antes incluso de la adolescencia. El teléfono móvil, antaño considerado un dispositivo para adultos, es hoy una herramienta habitual en los entornos escolares, familiares y de ocio infantil", recoge el estudio.

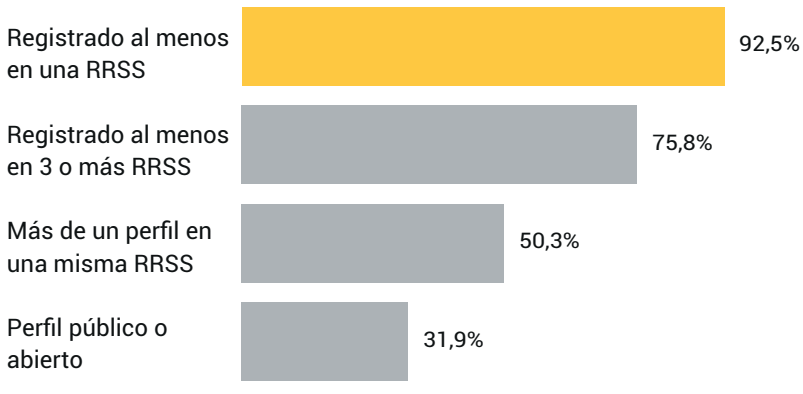
Las redes sociales también forman parte de su rutina. Prueba de ello es que el 92,5% está registrado al menos en una red social y el 75,8% en tres o más. En 5º y 6º de Primaria, el 78,3% del alumnado está ya registrado en alguna red social y el 43,6%, en tres o más. El 50,3% cuenta con más de un perfil en una misma red social y casi uno de cada tres tiene un perfil público.

El control parental es clave en la relación de los menores con la tecnología, así lo considera Lucía Redondo, madre de una preadolescente de 12 años: "Tiene restringido totalmente el acceso a redes sociales, juegos y aplicaciones y para poder instalarlo me tiene que pedir permiso. En cuanto al tiempo que puede utilizar los dispositivos tecnológicos está limitado a una hora de acceso, tanto en el móvil como en la tablet, de lunes a viernes y los fines de semana puede utilizarlo dos horas".

A este respecto, la profesora de ESADE resalta que "no se trata tanto de controlar como de acompañar. Las normas que funcionan son las que se pactan con los hijos, no las que se imponen, y sirven de poco si los adultos no damos ejemplo. Retrasar el primer móvil propio, dejar la noche libre de pantallas y usar el control parental como un andamio temporal ayuda", sin embargo, añade que "lo más eficaz es ofrecer alternativas reales: tiempo, espacios y vínculos fuera de la pantalla. Muchas veces el móvil llena un vacío que no ha creado él".

Según el *Informe sobre Adicciones Comportamentales ESTUDES 2025,* elaborado por el Ministerio de Sanidad, un 19,4% de los estudiantes de 14 a 18 años presenta riesgo elevado de uso problemático de Internet y el 15,3% un posible uso problemático de redes sociales. "Es una cifra preocupante, pero también significa que más de ocho de cada diez no tienen ese problema", valora Arroyo, enfatizando que "la pregunta que me interesa no es cuánto miran el móvil los jóvenes, sino qué les pasa a los entornos que habitan. Hemos pasado de una economía de los datos a una economía de la atención, y ahora entramos en la del apego, con tecnologías diseñadas para generar vínculo emocional, como los compañeros de IA. Si lo leemos como un fallo individual del menor, lo culpabilizamos. Si lo leemos como un problema de diseño, podemos exigir tecnologías afectivamente responsables. Los jóvenes no son el problema. Son la parte más expuesta de un modelo que tenemos que cambiar entre todos, y con ellos", señala la profesora de Esade.

Los adolescentes se registran en RRSS de forma masiva



Fuente: Red.es, Unicef España, Universidad de Santiago de Compostela y Consejo General de Colegios de Ingeniería.

El 92,5% de los niños y adolescentes está registrado, al menos, en una red social y el 75,8% en tres o más

Tecnología

La pantalla protectora: utilizar el móvil como freno de la hiperconectividad

Existen aplicaciones, bloqueadores, limitadores de tiempo y dispositivos básicos diseñados para ofrecer descanso digital con el objetivo de ayudar a la concentración y la productividad, evitar distracciones y controlar el tiempo de uso del móvil

Mónica G. Moreno

Abrir los ojos y buscar la pantalla a tientas en la mesilla, incluso antes de que el cuerpo reaccione. Repetir el mismo gesto en la oscuridad, justo antes de dormir. El día empieza y termina de la misma manera: mirando el móvil. Así lo reconoce el 60% de los españoles, más de 17 millones, tal y como recoge la *VI Edición del Estudio sobre Adicción al Móvil,* elaborado por Rastreator. Hace unos años esto sería una dependencia extrema, sin embargo, se ha convertido en un hábito normalizado, prácticamente, en un acto reflejo.

Un aluvión de notificaciones, distracciones y sobreexposición a las redes sociales, *scroll* infinito sin prestar apenas atención... Más de 7 millones de ciudadanos se consideran adictos al móvil, es decir, cerca del 25% de la población de entre 18 y 65 años, según el comparador. El uso del *smartphone* puede suponer un problema cuando es excesivo en tiempo y, de media, las personas usan el móvil entre tres y cuatro horas al día.

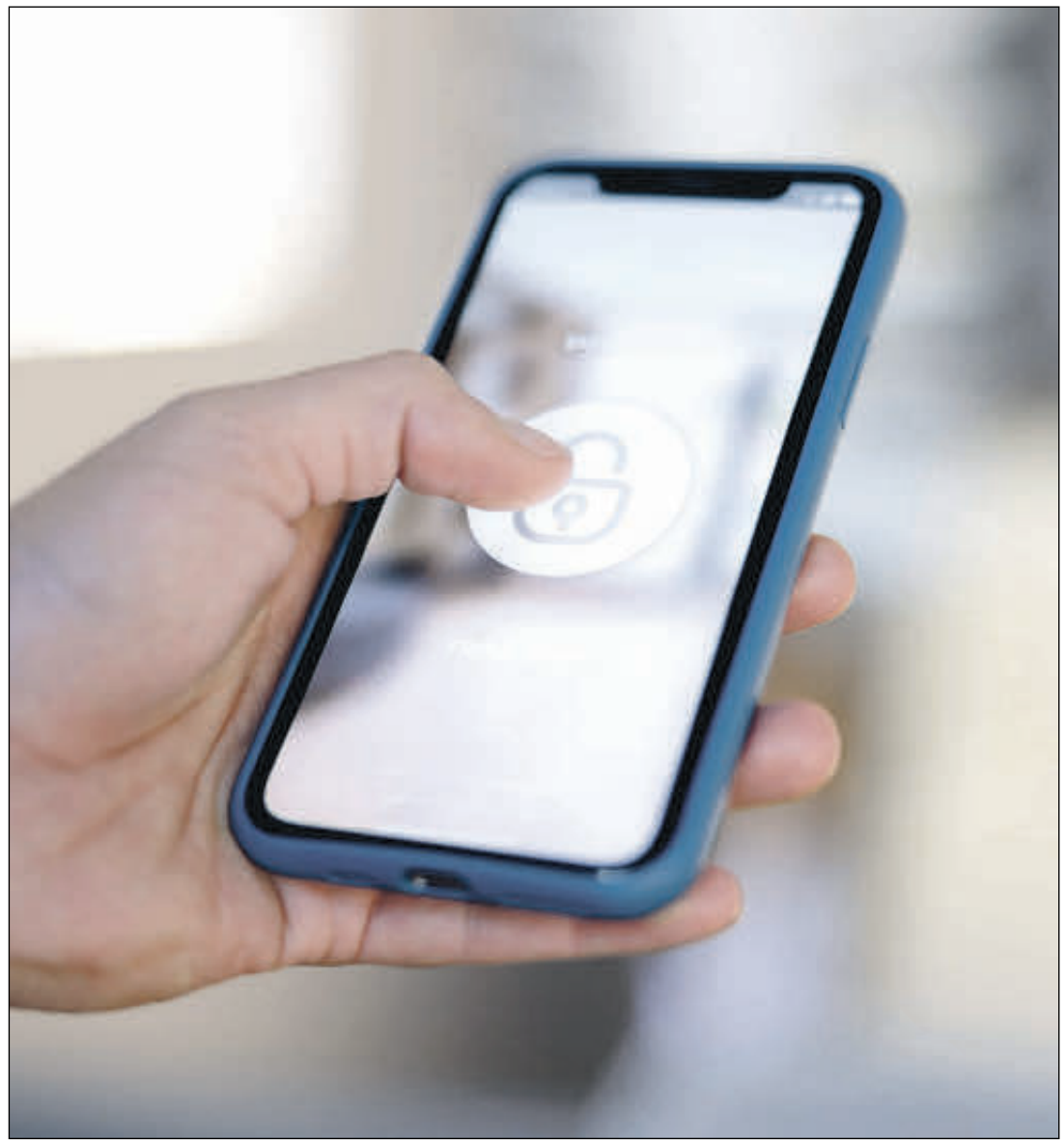
¿Y si en plena era de la hiperconectividad la protección está en las propias pantallas? Limitar el tiempo destinado a utilizar el móvil siendo el mismo dispositivo un aliado está en auge. Y es que existen aplicaciones, bloqueadores o limitadores de tiempo diseñados para ofrecer un descanso digital, por lo que las personas recurren al teléfono para frenar su uso.

Los propios *smartphones* disponen de la opción de *Bienestar digital* o *Tiempo de uso*, donde es posible establecer temporizadores en las aplicaciones más utilizadas y en las que se consumen más minutos, activar periodos de descanso o recordatorios de tiempos de uso para controlar los hábitos digitales, entre otras funciones. También existen aplicaciones que permiten bloquear el acceso a apps, redes sociales o páginas webs durante periodos determinados. El objetivo de estas herramientas es ayudar a la concentración y la productividad, evitar distracciones y controlar el tiempo de uso del móvil.

Guillermo López, usuario de aplicaciones de bloqueo del móvil y limitadores de tiempo, recurrió a estas herramientas al comprobar por curiosidad la cantidad de consumo que hacía de cada app: "Me di cuenta de que podía pasar hasta cinco horas diarias navegando en una red social concreta. Eso me hizo reflexionar sobre la sensación de estar perdiendo el tiempo, la sobreestimulación o cómo influye en nuestra manera de pensar y estado de ánimo dependiendo del contenido que consumimos".

"Es curioso utilizar la tecnología para bloquearnos de la tecnología, si bien es cierto que, en muchas ocasiones, no hay otra forma de hacerlo porque nuestro cerebro está tan metido en el contenido de las redes sociales o de las aplicaciones que no nos damos cuenta del uso que estamos haciendo", expone Alba Gutiérrez, psicóloga especializada en adicciones y subdirectora del área de gestión de psicología del centro multidisciplinar Más que palabras.

Y es que el uso del móvil sin control puede interferir en las actividades cotidianas y laborales, además de afectar a las relaciones sociales y familiares, e incluso, perjudicar la salud física. Así lo explica Gutiérrez, quien considera que los desencadenantes más peligrosos a nivel psicológico o emocional son "la ansiedad o el nerviosismo al no tener el móvil cerca; la baja autoestima al compararse constantemente en redes sociales; la tristeza por no recibir mensajes, comentarios o *likes*; o la falta de concentración, ya que en ocasiones dificulta la atención activa". En cuanto a los problemas a nivel social, la psicóloga destaca "el aislamiento por tener menos contacto directo entre las personas y dificultades a la hora de mantener relaciones cara a cara".



De media, las personas usan el móvil entre tres y cuatro horas al día. EE

'Dumbphones'

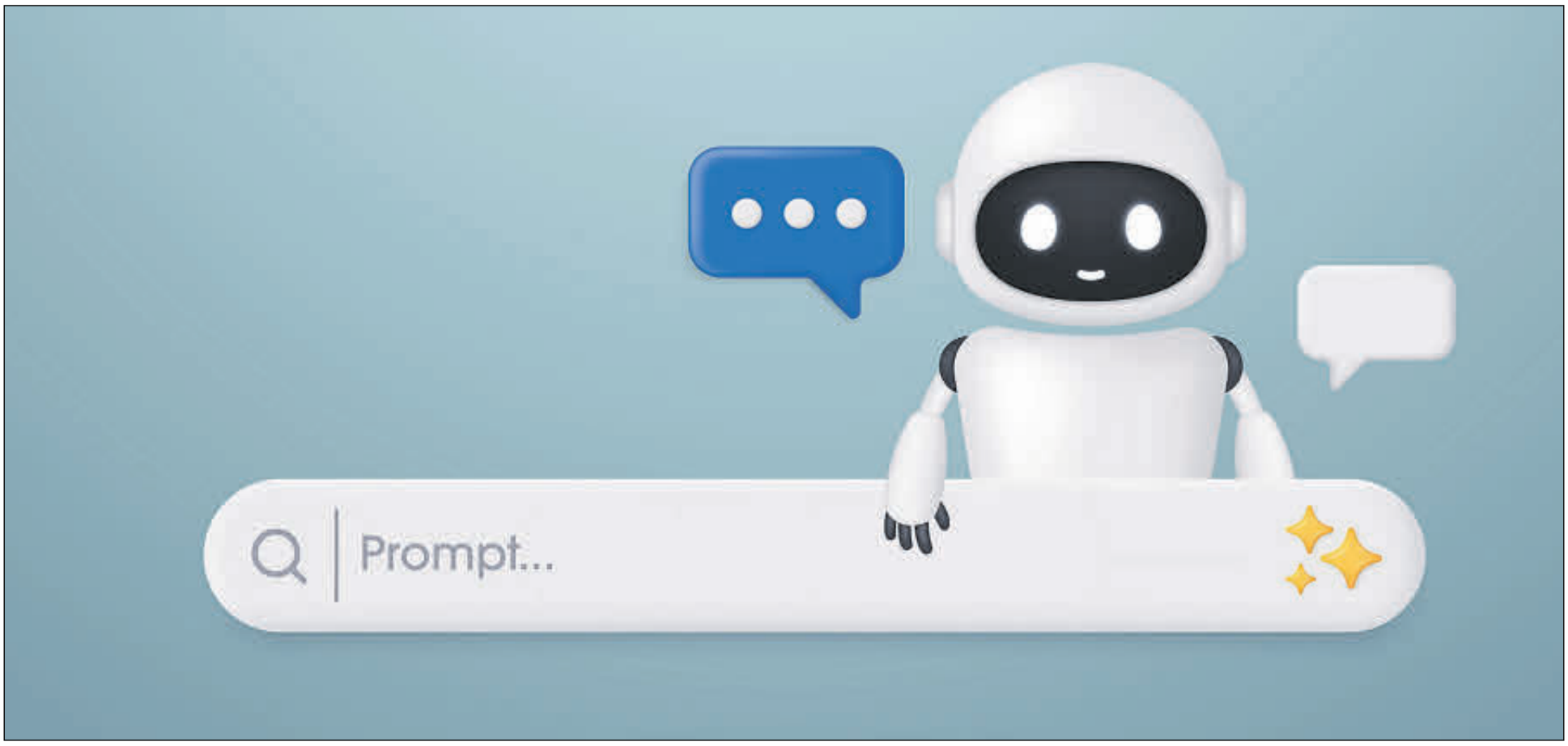
Más allá de limitadores de tiempo y aplicaciones de bloqueo, el auge de ciertos dispositivos también protege. Es el caso de los *dumbphones,* la antítesis de los *smartphones*. Se trata de teléfonos móviles que ofrecen funcionalidades básicas, realizar y recibir llamadas, enviar mensajes SMS y, en algunos modelos, usar funciones como calculadora, radio o linterna. Esto deja a un lado los problemas con la hiperconectividad al no tener acceso a Internet ni permitir que se instalen otras aplicaciones.

> Los 'dumbphones' controlan la hiperconectividad al no permitir Internet ni la instalación de aplicaciones

El *Estudio Generación SPCial sobre hábitos de desconexión digital de los jóvenes españoles,* de SPC, confirmó el auge de esta opción en nuestro país, ya que un 12,2% de la población ha optado por cambiar su *smartphone* por un teléfono sin Internet y un 19,5% conoce a alguien que lo ha hecho.

Verónica Catediano, PR Manager de SPC, apunta que en España "el mercado libre de teléfonos móviles básicos mueve alrededor de 300.000 unidades al año, de las que SPC comercializa cerca del 60% del total. En la actualidad, se está ampliando el tipo de persona que lo elige". Por un lado, Catediano menciona "el público sénior como uno de los principales usuarios de este formato, porque valora la sencillez y la facilidad de uso. La categoría ha evolucionado. Hoy un teléfono sencillo ofrece un diseño cuidado, buena autonomía, materiales resistentes y funciones adicionales útiles para cada perfil".

Sin embargo, se suman ahora otros consumidores. "Hoy muchas personas lo usan como segundo dispositivo para desconectar sin dejar de estar localizables", apunta Catediano y es que "el détox digital ya forma parte del día a día, por lo que hay quien se pasa al teléfono básico los fines de semana o en determinadas franjas para recuperar tiempo y atención". Por otro lado, puede ser el primer móvil, tal y como señala la PR Manager de SPC: "Las familias lo eligen cada vez más como paso previo al *smartphone*".



El porcentaje de usuarios que hacen clic en un enlace de Google pasa del 15% al 8% si aparece un resumen de IA. ISTOCK

Los 'bots' ganan terreno en Internet y protagonizan el 31% de las búsquedas

Se trata de programas de motores de búsqueda, como Googlebot, que recorren la red constantemente para leer, copiar e indexar páginas web y agentes de inteligencia artificial y rastreadores de IA que recopilan datos masivos

Judith Arrillaga Pérez

Vista creada con IA. Estas cuatro palabras ya forman parte de la historia de Internet. Es lo primero que aparece cuando alguien hace una búsqueda a través de Google. Esta función hace resúmenes de lo que se está buscando y los acompaña de enlaces con la fuente original y, de esta manera, se reducen las visitas a las páginas web tradicionales.

Este último punto está suponiendo un cambio de paradigma y está transformando Internet tal y como lo conocemos. "El 31% del tráfico de Internet ya no es humano y esto nos hace reflexionar, porque la gente ya no busca un producto, sino cubrir una necesidad", explica Jaime Villanueva, director general del área Audiovisual de Econocom, a *elEconomista.es*. Entonces, ¿cómo se realizan estas búsquedas? Se trata de programas de motores de búsqueda, como Googlebot, que recorren la red constantemente para leer, copiar e indexar páginas web y agentes de inteligencia artificial y rastreadores de IA que recopilan datos masivos de foros, noticias y sitios web para entrenar algoritmos o responder consultas sintéticas. Y esto, ¿en qué se traduce? Según datos que recoge Econocom, el porcentaje de usuarios que hacen clic en un enlace de Google pasa del 15% al 8% si aparece un resumen de IA.

> El 9% de los usuarios dejaría a la IA realizar las compras de poco valor, como las que se hacen en el supermercado

Esta realidad está impactando especialmente en el mundo del *retail*. "El 9% de los usuarios le dejaría a la IA realizar las compras de poco valor, como, por ejemplo, aquellas que se realizan en el supermercado", añade el experto. A esto hay que añadirle que el 13% de los compradores online en España usan la IA para informarse antes de comprar, según se recoge en el *Estudio Ecommerce*, elaborado por IAB Spain.

Esto va a suponer un cambio de 180 grados de Internet tal y como lo conocemos. De hecho, son muchas las voces que alertan de que este cambio ya se está produciendo. "Ya no son buscadores, es algo que cumple las satisfacciones", destaca Villanueva. Sin embargo, lo que a simple vista es un beneficio para el usuario, no lo es tanto para los portales de venta. Amazon, sin ir más lejos, ha bloqueado desde el mes de octubre Muse, el agente de compras de Meta. Este nuevo servicio tiene acceso al correo, al calendario y a los pagos, y compra y reserva por ti cualquier cosa en Internet. "Una parte muy relevante del negocio de plataformas como Amazon depende de la atención: publicidad en resultados, productos patrocinados, recomendaciones propias, datos de comportamiento. Es decir, viven en buena medida de la experiencia publicitaria, la recomendación cruzada y las compras por impulso", explica Josep Curto, profesor de los Estudios de Informática, Multimedia y Telecomunicación de la Universitat Oberta de Catalunya (UOC). "Un agente que compara y decide por el usuario se salta justo esa capa, y la plataforma pierde el control sobre la relación con el cliente", añade.

En una línea muy similar se pronuncia el experto de Econocom. "A ti como usuario, los *bots* te van a racionalizar mucho las compras, pero Amazon se tiene que proteger si quiere subsistir", señala Villanueva.

Pese a las reticencias del gigante del comercio electrónico a que *bots* de terceros naveguen entre sus entrañas, nada parece indicar que esta tendencia se vaya a frenar en el corto y largo plazo. Es más, las previsiones de Morgan Stanley apuntan a que las compras hechas por agentes en Estados Unidos en 2030 oscilarán entre los 190.000 millones de dólares y los 385.000 millones de dólares, lo que supondrá entre el 10% y el 20% del comercio electrónico.

La IA, también en las tiendas físicas

La irrupción de la inteligencia artificial y los *bots* no solo va a suponer un cambio de 180 grados en Internet, también va a golpear de lleno a las tiendas físicas tal y como se conocen. De hecho, para el director general del área Audiovisual de Econocom existe una importante brecha entre el mundo *online* y el mundo *offline*.

"Hay una brecha enorme entre la racionalización del mundo *online* con el espacio físico. Cuando haces una compra *online*, el algoritmo te conoce, sabe lo que estás buscando, te persigue por todos los sitios, te personaliza el servicio... Cuando llegas a un concesionario de coches, por ejemplo, eres uno más, *eres café para todos*, te pones tú a buscar y mirar entre los coches... No puede ser que se pierda esa personalización", alega.

"Hemos detectado también un uso cada vez mayor del móvil dentro de los espacios físicos, para la comparación de precios, por ejemplo. La tienda tiene que hacer la reconversión total y absoluta", sentencia el experto de Econocom. A pesar de que es necesario que los espacios físicos lleven a cabo una importante transformación, Villanueva no pone en duda el futuro de estos espacios: "A veces somos muy dramáticos. Yo creo que el espacio en físico va a seguir teniendo su lugar. Pero también porque tiene un componente de ocio, por lo menos en España".

Recarga tu ahorro con Smart Mobility de Iberdrola



DENTRO DE CASA >

Carga **100 km por tan sólo 1 €** con el Plan Recarga Inteligente.

Disfruta de **500 € de dto. en tus facturas de luz** al instalar tu cargador con Iberdrola.

FUERA DE CASA >

Viaja con **la red de recarga pública más grande y potente** de España.

Y si tienes la luz con nosotros, consigue hasta un **60% de ahorro para tus recargas** con la **Tarjeta Iberdrola y nuestras Suscripciones.**



UNIVERSO MUJER

900 24 24 24
iberdrola.es
Puntos de Atención

125 Iberdrola