

¿Dejarías que una IA compre por ti? Experto alerta sobre desafíos de seguridad ante innovador sistema

Santander y Visa realizaron recientemente una prueba en la que agentes de inteligencia artificial (IA) completaron compras en distintos países de la región, incluyendo Chile. Los sistemas adquirieron libros y bombones, mostrando la posibilidad de ejecutar pagos automatizados en distintos mercados.

Para Claudio Álvarez, experto en ciberseguridad y académico de la Facultad de Ingeniería y Ciencias Aplicadas de la Universidad de los Andes (Uandes), este tipo de herramientas representa una evolución de la automatización que ya existe en el comercio digital.

En ese sentido, el especialista señala que estos sistemas podrían

actuar como asistentes de compra capaces de buscar productos, comparar precios y ejecutar transacciones dentro de límites definidos por los usuarios, ampliando el rol que hoy cumplen los asistentes virtuales.

Los desafíos de delegar decisiones de compra

Sin duda este modo de comercialización es toda una innovación, pero el avance también debe contar con ítems que no pueden ser ignorados. Sobre todo, porque modelos así pueden introducir nuevos riesgos de ciberseguridad y a la protección de datos de los usuarios.

“El principal cambio es que la decisión económica deja de ser ejecutada directamente por una persona y pasa a ser delegada a

un sistema autónomo. Eso abre varios vectores de riesgo”, dice Álvarez.

Uno de ellos es la posibilidad de manipulación durante la navegación de la inteligencia artificial en Internet. “Si un agente de IA interactúa con plataformas para decidir qué comprar, podría ser influido por contenido malicioso o promociones engañosas diseñadas para inducir decisiones incorrectas”, señala.

Otro escenario es el eventual compromiso del sistema que controla al agente o de sus credenciales de acceso. En ese caso, un atacante podría realizar transacciones en nombre del usuario, convirtiendo a estos sistemas en un nuevo objetivo para el fraude digital.

El académico Uandes agrega que estas herramientas también requerirán acceder a grandes volúmenes de información personal -como hábitos de consumo, historial financiero o preferencias-, lo que aumenta el impacto potencial de filtraciones o usos indebidos de datos.

Al respecto, Álvarez plantea que el avance de este tipo de tecnologías abre preguntas sobre responsabilidad en caso de errores o manipulaciones. “No siempre está claro quién debería responder: el proveedor del agente, el banco, el comercio o el propio usuario”, afirma.

También, menciona que existe un riesgo sistémico interesante: “Si en el futuro millones de agentes automatizados comienzan

a tomar decisiones de compra simultáneamente, por ejemplo, reaccionando a promociones o variaciones de precio, podrían producirse comportamientos colectivos inesperados en los mercados digitales”.

En síntesis, el comercio gestionado por agentes de IA tiene el potencial de hacer el consumo digital más eficiente y personalizado, pero también introduce una nueva superficie de ataque en el sistema financiero, dice Álvarez. “Por eso es importante que estas tecnologías se desplieguen gradualmente, con fuertes mecanismos de seguridad, límites claros de operación y sistemas de auditoría que permitan entender y revisar las decisiones que toman estos agentes”, concluye.