Las preguntas “prohibidas” en la era de la IA: por qué consultar salud o leyes a un chatbot es un peligro

ChatGPT, Gemini y Copilot operan bajo estrictos límites de privacidad y seguridad. Conoce los temas tabú que bloquean a los asistentes virtuales y los riesgos de cruzarlos.

La inteligencia artificial se ha integrado por completo en nuestra rutina diaria. Sin embargo, el avance acelerado de asistentes como ChatGPT, Gemini y Copilot obliga a los usuarios a conocer no sólo su potencial, sino también sus límites éticos y legales.

Saber qué preguntas no deben hacerse a la IA es fundamental para evitar riesgos de seguridad, problemas legales y malentendidos sobre el verdadero alcance de estas plataformas. Aunque la confianza en los asistentes virtuales crece cada día, la IA es una herramienta poderosa, pero no una fuente de verdad universal para consultas de alta sensibilidad.

1. El límite profesional: Salud, finanzas y asesoría legal

Uno de los errores más comunes y peligrosos es recurrir a la inteligencia artificial para obtener diagnósticos médicos, tratamientos, estrategias financieras o asesoría legal personalizada.

Aunque los chatbots pueden ofrecer información general y educativa, carecen de la capacidad de sustitución profesional. Un error en estas áreas puede acarrear consecuencias graves para la salud o el patrimonio, por lo que la consulta con expertos cualificados sigue siendo insustituible.

2. Privacidad blindada: Datos personales y acceso a cuentas

El principio que rige el funcionamiento de la IA es la protección absoluta de la privacidad. Según expertos en ciberseguridad de Eset, estas plataformas tienen prohibido proporcionar datos personales (como direcciones, teléfonos o información bancaria), incluso si estos son de carácter público en internet.

Asimismo, intentar obtener contraseñas, mensajes privados o accesos a cuentas ajenas está completamente fuera de su alcance. Más allá de ser un límite ético, esta restricción previene fraudes, robos de identidad y delitos informáticos sancionados por la ley.

3. Tolerancia cero a la ilegalidad y el hackeo

Solicitar instrucciones a la IA para vulnerar sistemas informáticos, fabricar sustancias prohibidas, acceder a contenido restringido o planificar cualquier acto delictivo genera un bloqueo inmediato. Los desarrolladores han implementado barreras técnicas infranqueables para garantizar que la tecnología no sea utilizada como un manual de instrucciones para causar daño a individuos o instituciones.

4. Filtros éticos: Odio, discriminación y contenido explícito

Los sistemas de moderación de los grandes modelos de lenguaje están programados para rechazar la generación de discursos de odio, mensajes ofensivos, violentos, discriminatorios o sexualmente explícitos. El objetivo principal de los desarrolladores es mantener un entorno digital seguro, ético y respetuoso para todos los usuarios.

5. Sin futuro ni emociones: Predicciones y opiniones subjetivas

Aunque la IA es excelente analizando datos históricos y ofreciendo estimaciones, los asistentes virtuales no pueden predecir el futuro, resultados deportivos exactos, elecciones políticas ni movimientos bursátiles individuales. Además, al carecer de conciencia y experiencias propias, el terreno de las opiniones personales y los juicios subjetivos les está completamente vedado.