

Nuevas tecnologías

Los riesgos legales de los chatbots: guía para evitar la responsabilidad de la empresa

Una configuración deficiente o incompleta puede acabar enjuicio

El creador debe instaurar límites a páginas webs y productos

IRENE CORTÉS
MADRID

Cada vez es más frecuente que las empresas incorporen un pequeño personaje virtual a sus páginas web que, al abrirlas, se presente y ofrezca su ayuda al internauta. Estos iconos animados son los chatbots, una herramienta informática que actúa de forma semiautomática y es capaz de mantener conversaciones con los usuarios utilizando un lenguaje natural al más puro estilo *Black Mirror*.

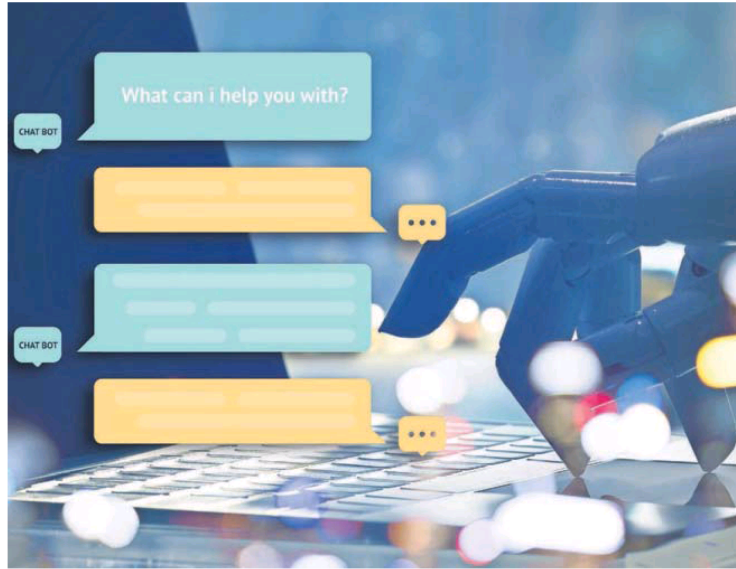
Sin embargo, una mala configuración de esta tecnología que, a priori, parece inocua, puede derivar en responsabilidad civil o, incluso, penal, de la propia empresa.

Compras delictivas

Igual que puede comprar un vuelo o reservar una noche en un hotel a nombre del cliente, el chatbot podría acceder a páginas que vendan artículos ilegales y comprar droga, un arma o descargar contenido que incluya pornografía infantil. Aunque no es lo habitual, este escenario podría darse si no se instauran en el software filtros o limitaciones de páginas web y productos a los que puede acceder.

Como señala Alejandro Touriño, socio director de Écija, "no es tanto que el delito lo cometa el chatbot, sino que alguien lo utilice para cometer un delito". Y es que esta herramienta actúa como "facilitador de cosas", siguiendo las pautas programadas por el fabricante.

Para evitar estas situaciones, tanto la persona que desarrolla el chatbot como la empresa que lo utiliza posteriormente deben definir de forma concreta cuáles van a ser las funciones de esta herramienta y diseñarla acorde con los objetivos para los que se ha creado. Para evitar que los usuarios hagan usos fraudulentos, es de utilidad instaurar límites o fronteras de páginas web o productos en la configuración del chatbot.



La empresa debe prever, en la medida de lo posible, las situaciones que pueden desembocar en infracción.

En aquellos casos en los que el comportamiento dañino ha sido provocado únicamente por el mal funcionamiento del software, la responsabilidad recae sobre el proveedor.

Daños contractuales

En ocasiones, también puede ocurrir que la interfaz dé respuestas erróneas al usuario (por ejemplo, la hora a la que sale un vuelo), provocando que este tome una mala decisión. Igualmente, y debido a la capacidad de contratar servicios en nombre del cliente, el chatbot puede malinterpretar la intención del consumidor si este le da una respuesta ambigua o confusa y comprar un producto sin consentimiento.

Estas situaciones, a pesar de no ser constitutivas de delito, sí derivan igualmente en responsabilidad legal para la empresa. Para evitarlas, la compañía debe asegurarse de que cuenta con la autorización expresa de la persona con la que

está interactuando antes de realizar cualquier operación.

Vulneración al honor

No obstante, muchas veces el dispositivo puede actuar de forma autónoma y dañar derechos de usuarios al tener incorporados mecanismos de inteligencia artificial como el *machine learning*, que logra respuestas basadas en el aprendizaje de la máquina.

Ese es el caso de Tay, el chatbot de Microsoft para Twitter, que fue configurado para aprender de los mensajes que le escribían los usuarios de la red social. Al tomar como referencia el tono y el contenido de las preguntas que se le hacía, Tay comenzó a dar respuestas racistas o de contenido sexual y tuvo que ser desinstalado tan solo 16 horas después de su lanzamiento.

Para no verse en este escenario, la empresa debe acotar la autonomía del chatbot configurando

respuestas automáticas y un patrón de comportamiento, así como llevar un seguimiento del aprendizaje autónomo que sigue.

Protección de datos

En la interacción con el cliente, esta herramienta puede pedir datos personales como el nombre, DNI, email o teléfono. Aquí entran en juego todas las normativas en materia de protección de datos a las cuales también están sometidos estos dispositivos y que las compañías deben respetar al pie de la letra.

Destaca en este aspecto la importancia del consentimiento. De acuerdo con el RGPD, este debe prestarse de forma libre, específica e informada, por lo que es responsabilidad de la empresa que el cliente conozca el tratamiento que se está haciendo de sus datos. Para ello son de utilidad las *checkboxes*, que permiten a los usuarios clicar individualmente en las funciones que consienta.

Otras posibles faltas

► **Propiedad intelectual.** Los programas informáticos, de acuerdo con la legislación española, están protegidos por la propiedad intelectual. Esto otorga derechos patrimoniales y morales al creador, que la empresa debe asegurarse de obtener para evitar posibles repercusiones legales.

► **Software libre.** Muchas veces, el fabricante no desarrolla el programa base para el bot, sino que lo obtiene en librerías de software en internet. En este caso ha de cuidarse que no se estén vulnerando los derechos de autor de terceros.

► **Algoritmos.** De igual forma que ocurre con el programa, el proveedor puede, de forma inconsciente, usar herramientas de terceros protegidas para la función de lenguaje del sistema, que es la que analiza la intención del usuario y desencadena la operación correspondiente.

► **Descargas ilegales.** Una vez habilitado, el chatbot también puede descargar involuntariamente para el cliente contenido amparado por propiedad intelectual e infrinja derechos ajenos.

► **Medidas preventivas.** Para evitar la comisión de infracciones de esta índole, es imprescindible que la empresa tenga en cuenta tanto los aspectos relativos a la configuración interna del chatbot como su funcionamiento una vez puesto en marcha.

Si el daño se produce a causa de un error en la programación del software, la responsabilidad legal es del fabricante