Peligros del Chat GPT: IA y Privacidad.

Carmen Natera

Aunque los chatbots basados en Inteligencia Artificial pueden ser una fuente de valor añadido, también ponen en riesgo la privacidad de los usuarios y titulares de los datos que se tratan para entrenar los sistemas. Además, contravienen importantes obligaciones y principios de protección de datos. Por ello, urge la creación de un marco regulatorio europeo que regule el funcionamiento de la tecnología IA. Sin embargo, resulta difícil diseñar un marco normativo que no quede obsoleto incluso antes de que vea la luz.

La proliferación del uso de sistemas de chat –*chatbots*– basados en modelos de lenguaje de Inteligencia Artificial (IA), como el popular *Chat GPT*, es una tendencia en auge que, sin perjuicio de ser una potencial fuente de valor añadido para el usuario, puede, a su vez, entrañar importantes riesgos para su privacidad y para la de los sujetos cuyos datos se tratan con el fin de alimentar y entrenar el algoritmo que rige el funcionamiento de los sistemas.

El quid de la cuestión reside en que los chatbots se nutren, entre otros, de nuestros datos personales. Son modelos que se abastecen y funcionan a partir de cantidades ingentes de datos. Cuantos más datos mejor y más precisa será la capacidad del sistema, no sólo para detectar patrones, sino para anticiparse a los mismos y generar respuestas; aunque cuantos más datos, mayores serán también los riesgos derivados de la utilización de los mismos. Pero ¿de dónde se obtienen los datos que proveen los sistemas de IA y qué dicen las autoridades al respecto?

La información que se emplea para entrenar y nutrir a modelos de lenguaje de IA, como Chat GPT, se obtiene sistemáticamente de Internet (artículos, libros, páginas web, foros, blogs, periódicos), incluyendo datos personales, en su mayoría, recabados sin el consentimiento previo de sus titulares. A este respecto, cada vez son más las autoridades de protección de datos que ponen en tela de juicio la licitud de este tipo de sistemas ya que su funcionamiento no es, en muchos casos, conforme a la normativa de privacidad. Un ejemplo de ello lo encontramos en el comunicado promulgado el pasado 31 de marzo de 2023 por la autoridad italiana de protección de datos *(Il Garante per la Protezione dei Dati Personali)*, en el que instó al bloqueo inmediato y temporal del Chat GPT, alegando que el sistema recopilaba datos personales de manera ilícita y que, además, no contaba con sistemas de verificación de edad de menores.

A la decisión del garante italiano se han sumado numerosos expertos que han solicitado la paralización del entrenamiento de los sistemas de IA

de los mismos es lícito y seguro para los usuarios e interesados. De hecho, esto último fue planteado en la Carta abierta formulada por Elon Musk, Steve Wozniak y otros empresarios, inversores y analistas para la suspensión temporal del entrenamiento de los sistemas de IA más potentes.

El quid de la cuestión reside en que los chatbots se nutren, entre otros, de nuestros datos personales.

Entonces, ¿qué significa que el tratamiento de datos realizado por los sistemas de chats basados en IA no sea conforme a la privacidad y qué puede hacerse para revertir esta situación?

Son varios los preceptos del *Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos* (RGPD) que se ven comprometidos por el tratamiento que de los datos realizan estos sistemas, sin perjuicio de otras disposiciones legales que también puedan resultar infringidas.

En primer lugar, se incumple el deber de información ya que, generalmente, no se proporciona información completa y transparente a los usuarios e interesados sobre el tratamiento que de sus datos hacen estos sistemas. Además, el incumplimiento de los principios que deben regir el tratamiento de datos personales, entre ellos, el principio de exactitud, puesto que muchos de los datos introducidos en los sistemas son inexactos, no reales, produciéndose, en consecuencia, una desinformación a gran escala. En este sentido, una de las grandes preocupaciones derivadas del uso de sistemas como Chat GPT es la tendencia a "maquillar" la información y aumentar, por ende, los sesgos en las respuestas proporcionadas al usuario, las cuales, posteriormente se introducen en el tráfico jurídico.

Al margen de lo anterior, otra de las infracciones destacables en materia de privacidad tiene que ver con la ausencia de base legitimadora que ampare el tratamiento masivo de datos personales con la finalidad de abastecer y entrenar los algoritmos que rigen el funcionamiento de los chatbots. También se destaca la contravención del principio de confidencialidad y la falta de medidas de seguridad, lo cual incrementa enormemente la posibilidad de brechas y ciberataques.

La gestión irresponsable de los datos que pueden realizar estos sistemas da lugar a resultados poco fiables, de baja calidad y que, sin duda, pueden dañar el bienestar de la ciudadanía y la seguridad en el tráfico jurídico.

Por ello, podemos concluir que, si bien la IA tiene el potencial de transformar sectores, solucionar problemas, simplificar respuestas o ser una gran fuente de información, también puede, como se expone en el documento *"General-purpose artificial intelligence"* publicado por el Parlamento Europeo, representar grandes riesgos éticos y sociales para la ciudadanía. Es importante resaltar que los sistemas de chatbots pueden reproducir, reforzar y amplificar patrones de discriminación, desigualdad o de algún otro modo contrarios a derecho, a partir de la información que se emplea para entrenar sus algoritmos. En consecuencia, la gestión irresponsable de los datos que pueden realizar estos sistemas da lugar a resultados poco fiables, de baja calidad y que, sin duda, pueden dañar el bienestar de la ciudadanía y la seguridad en el tráfico jurídico.

Los sistemas de chats basados en IA son sistemas opacos, cuya falta de transparencia supone que muchos de sus resultados sean difíciles de explicar y que la responsabilidad derivada del uso de los mismos sea difícil de atribuir. Esto puede, además,

contribuir a la desinformación, divulgación de noticias falsas, así como a fomentar el plagio y la infracción de derechos de propiedad intelectual, entre otros perjuicios.

Resulta de imperiosa necesidad realizar un llamamiento a la creación de un marco regulatorio sólido y homogéneo, a nivel europeo y mundial, que regule el uso y funcionamiento de los sistemas de IA.

Llegados a este punto, resulta de imperiosa necesidad realizar un llamamiento a la creación de un marco regulatorio sólido y homogéneo, a nivel europeo y mundial, que regule el uso y funcionamiento de los sistemas de IA. En el contexto europeo, este proyecto ya se puso en marcha hace aproximadamente dos años con la propuesta de Reglamento de IA por el que se establecen normas armonizadas en materia de inteligencia artificial -AI Act-. Sin embargo, dado que el campo de la IA y sus aplicaciones avanzan a una velocidad imparable, resulta difícil que la norma no quede obsoleta incluso antes de que nazca.