LAS INVESTIGACIONES A OPENAI, PROPIETARIA DE CHATGPT, EN LA UNIÓN EUROPEA, PERO TAMBIEN EN ESPAÑA.

Seguro que todo el mundo ha escuchado hablar en los últimos meses acerca de ChatGPT, el sistema de chat con inteligencia artificial que ha irrumpido con fuerza sorprendiéndonos a todos.

ChatGPT emplea el modelo de lenguaje GPT (*Generative Pre-trained Transformer*) que es una herramienta de inteligencia artificial que genera texto a partir de una entrada de texto dada.

ChatGPT, beneficios y límites

Esta nueva y disruptiva herramienta se encuentra entrenada, para mantener conversaciones que entenderá tras formularle la correspondiente pregunta, dándonos respuesta a las mismas y generar un texto coherente y preciso que puede llegar a ser indistinguible de un texto escrito por humanos.

En principio, ChatGPT a través de sus algoritmos debería responder, siendo capaz de entender lo que le estamos preguntando con bastante precisión y es realmente sorprendente las respuestas acertadas y completas que es capaz de expresar.

Todo esto puede ser de gran de utilidad en nuestro día a día si se emplea correctamente. Pero, ¿qué limitaciones o puntos negativos tiene esta herramienta? Debemos tener en cuenta que, el hecho de que ChatGPT sea una herramienta tan nueva, hace que el nivel de errores que pueda cometer sea más alto.

Como riesgos operativos y de importancia, se han detectado algunos como la generación de textos con información errónea, combinando información veraz con otra falsa. Pero además, el hecho de usar determinada información con ChatGPT, implica que estamos nutriendo al sistema y a la herramienta con dicha información, siendo fundamental no compartir dicha información sensible o confidencial, así como datos personales con la misma. De hecho, esto es algo que se avisa ya por la propia herramienta.

En todo este asunto, es conveniente recordar que OpenAI (la empresa detrás de ChatGPT) es una compañía que se encuentra ubicada en San Francisco, Estados Unidos. Este país, no se ajusta a las exigencias en materia de protección de datos que exige la Unión Europea, por lo que las transferencias de datos que se estén produciendo a dicho país no garantizan la seguridad de los datos de los usuarios de, en este caso, ChatGPT.

Pero, todo esto ¿cómo afecta a la privacidad?

Especialmente en Europa, preocupa el impacto en la privacidad que puede producir esta herramienta, teniendo en cuenta el Reglamento General de Protección de Datos (RGPD)

En concreto, fue **Italia** el primer país que se pronunció al respecto, llegando a prohibir su uso por tratar datos de los usuarios de forma masiva e injustificada y sin cumplir la normativa europea. Esto es debido a que ChatGPT, para continuar entrenando su

sistema, sigue empleando y tratando datos de los usuarios para ir depurando su experiencia.

Adicionalmente, la falta de transparencia y la dificultad de acceso a la información recopilada, es otra de las razones en las que se basó la autoridad italiana para tomar dicha decisión. Es decir, OpenAI no informaba a sus usuarios de la información que recopilaba, incumpliendo directamente con el RGPD.

Tampoco permite ChatGPT la verificación de la edad de los usuarios que se registran. Aunque la herramienta indica en sus condiciones de uso que se dirige a mayores de 13 años, no hay manera de verificarlo, lo cual permite a menores de esa edad usar la herramienta. Hay que tener en cuenta, que, en la Unión Europea, conforme a RGPD, los menores de 16 años no pueden dar por sí mismos el consentimiento para el tratamiento de sus datos, aunque esta edad puede diferir de un país a otro, como es el caso de España, que rebaja hasta los 14 años la validez del consentimiento en menores.

Esta prohibición temporal por parte de Italia, ha marcado la hoja de ruta a seguir en Europa, que si bien se encuentra trabajando en una ley que regule la inteligencia artificial, la misma no estará lista para su entrada en vigor a corto plazo, por lo que tendremos que esperar algún tiempo, es posible que años, en que dicha normativa se aplique y comience a regular este asunto.

¿Prohibición definitiva?

En el caso de Italia, esta prohibición tenía un carácter temporal, en tanto que OpenAI facilitara toda la información requerida por la autoridad de control italiana garantizando el cumplimiento de la normativa europea.

Principalmente, lo exigido conlleva garantizar, entre otras cuestiones **(i)** la transparencia de los datos y métodos empleados para el tratamiento, **(ii)** la existencia de una base jurídica aplicable que justifique el tratamiento como el consentimiento o en su caso el interés legítimo como elemento indispensable para el tratamiento, **(iii)** la posibilidad de los usuarios de ejercitar sus derechos tal y como permite la normativa en la UE, o **(iv)** la protección de los menores de edad implementando el correspondiente sistema de verificación.

Y, ¿en España?

Siguiendo los pasos de Italia en lo que respecta a la investigación de OpenAI y su herramienta, también la Agencia Española de Protección de Datos (AEPD) ha iniciado una investigación a la empresa propietaria de ChatGPT, de cara a esclarecer cómo afecta a la privacidad y el tratamiento de datos de los usuarios.

A través de un comunicado, la AEPD manifestó el inicio de oficio de las actuaciones de investigación pertinentes a la empresa estadounidense.

La AEPD, exigió al Comité Europeo de Protección de Datos (EDPB, por sus siglas en inglés), abordar y considerar este asunto ya que los tratamientos globales que se realizan mediante el uso de ChatGPT pueden suponer un impacto importante en los derechos de las personas. Todo esto hace necesario, según considera la AEPD, que se lleven a cabo acciones coordinadas y armonizadas a nivel europeo para garantizar el cumplimiento de las exigencias del RGPD.

Tras esta petición por parte de la AEPD, también se ha acordado por parte del Comité, lanzar un grupo de trabajo para que las diferentes autoridades de control puedan intercambiar información sobre las acciones que vengan realizando, de forma que se fomente la cooperación entre las mismas.

En paralelo con este grupo de trabajo europeo, la AEPD continuará con sus investigaciones para determinar si el uso de ChatGPT supone un peligro para la privacidad de los usuarios, debiendo implementar medidas como las indicadas por la autoridad de control en Italia, o bien esperará a las conclusiones que se obtengan del grupo de trabajo europeo sobre este asunto.

Por tanto, se prevé que el uso de esta herramienta en Europa deba realizar cambios sustanciales en el tratamiento de datos de los usuarios para garantizar que dicho tratamiento se realiza de forma lícita y cumpliendo con los requisitos de la norma.

¿Qué pasa con su uso a nivel corporativo?

Las organizaciones ya están analizando los usos de ChatGPT y herramientas similares a nivel corporativo y más allá de aquellas que prohíben su uso ante la incertidumbre que supone, lo cierto es, que se convierte en una asignatura pendiente de analizar por equipos legales, de gestión de riesgos y de ciberseguridad, entre otros.

La regulación de este tipo de herramientas a nivel interno se hace imprescindible, junto con la concienciación de los empleados, para evitar riesgos de incumplimiento normativo, de fuga de información confidencial, o incluso de seguridad.

Además, como ya es sabido, los resultados arrojados por dicha herramienta presentan errores, lo que puede suponer riesgos de cara a su uso sin analizarlos previamente por expertos en el tema que se esté tratando.

En definitiva, se debe realizar un análisis exhaustivo de los usos a nivel corporativo previo a incorporarlo en procesos internos de la organización.

¿Qué opina ChatGPT?

Hemos preguntado a la herramienta que ofrezca un resumen de los riesgos de uso de ChatGPT a nivel organizativo y esto es lo que nos responde:

"El uso de ChatGPT a nivel organizativo presenta riesgos significativos, como la privacidad y seguridad de los datos, la reproducción de sesgos y la difusión de información incorrecta, posibles implicaciones legales y regulatorias, la falta de transparencia y explicabilidad del modelo, y la dependencia tecnológica. Estos riesgos requieren una gestión cuidadosa para minimizar impactos negativos en la organización." (Resultado literal ofrecido por ChatGPT).

Cristina Martínez

Departamento Legal

Áudea Seguridad de la Información