

ChatGPT : l'Italie bloque le robot conversationnel, accusé de ne pas assez protéger les données

Dans son communiqué, l'Autorité italienne souligne que ChatGPT « a subi le 20 mars une perte de données (data breach) concernant les conversations des utilisateurs et les informations relatives au paiement des abonnés au service payant ».

Les reproches que l'Italie fait au robot sont multiples. Les autorités du pays ont annoncé ce vendredi leur décision de bloquer le robot conversationnel ChatGPT, accusé de ne pas respecter la législation sur les données personnelles et de ne pas avoir de système pour vérifier l'âge des usagers mineurs.

Cette décision « avec effet immédiat » aura pour conséquence « la limitation provisoire du traitement des données des utilisateurs italiens vis-à-vis d'OpenAI », créateur de ChatGPT, a indiqué dans un communiqué l'Autorité nationale de protection des données personnelles. Ce robot est apparu en novembre et a rapidement été pris d'assaut par des utilisateurs impressionnés par sa capacité à répondre clairement à des questions difficiles, à écrire des sonnets et même à réussir des examens.

ChatGPT peut également être utilisé pour écrire du code informatique, sans avoir les connaissances techniques. Dans son communiqué, l'Autorité italienne souligne qu'il « a subi le 20 mars une perte de données (data breach) concernant les conversations des utilisateurs et les informations relatives au paiement des abonnés au service payant ».

Pas de filtre pour les moins de 13 ans

L'Autorité reproche aussi à ChatGPT « l'absence d'une note d'information aux utilisateurs dont les données sont récoltées par OpenAI, mais surtout l'absence d'une base juridique justifiant le recueil et la conservation en masse des données personnelles, dans le but d'entraîner les algorithmes faisant fonctionner la plateforme ».

En outre, alors que le robot est destiné aux personnes de plus de 13 ans, « l'Autorité met l'accent sur le fait que l'absence de tout filtre pour vérifier l'âge des utilisateurs expose les mineurs à des réponses absolument non conformes par rapport à leur niveau de développement ».

L'Autorité demande à OpenAI de « communiquer d'ici 20 jours les mesures entreprises » pour remédier à cette situation, « sous peine d'une sanction allant jusqu'à 20 millions d'euros ou jusqu'à 4 % du chiffre d'affaires mondial annuel ».

Cette annonce intervient alors que l'agence de police européenne Europol a averti lundi que les criminels étaient prêts à tirer parti de l'intelligence artificielle comme le robot conversationnel ChatGPT pour commettre des fraudes et d'autres cybercrimes.

Du phishing à la désinformation et aux logiciels malveillants, les capacités en évolution rapide des robots de conversation (chatbots) sont susceptibles d'être rapidement exploitées par des personnes mal intentionnées, a estimé Europol dans un rapport.

Elon Musk et des centaines d'experts mondiaux ont signé mercredi un appel à une pause de six mois dans la recherche sur les intelligences artificielles plus puissantes que ChatGPT 4, le modèle d'OpenAI lancé mi-mars, en évoquant « des risques majeurs pour l'humanité ».

Lien	https://www.ledevoir.com/societe/justice/787593/intelligence-artificielle-l-avocat-chatgpt-pour-le-meilleur-ou-pour-le-pire
Auteur	Le Parisien avec AFP
Date	31/03/2023