CHATGPT ET DONNEES PRIVEES : QUE LUI CONFIER EN TOUTES SECURITE ?

En mai dernier, OpenAI dissolvait son équipe de sécurité suite aux départs de deux de ses hauts dirigeants : le cofondateur Ilya Sutskever, et son chef scientifique, Jan Leike. Si se pose la question d'une crise temporaire ou d'une inquiétude sur le long terme, la situation n'en interroge pas moins sur les relations entre l'entreprise et la sécurité des données. Enjeu majeur lié à l'omniprésence d'internet, il n'est donc pas surprenant que l'utilisateur se demande s'il peut confier ses données aux organismes d'IA sans courir le moindre risque.

Shaked Reiner, chercheur en sécurité chez CyberArk Labs, rappelle que la politique d'OpenAI stipule que ChatGPT recueille autant d'informations que possible sur les utilisateurs et que pour tout usage de technologies ChatGPT, il faut partir du principe que ce qui est communiqué à l'outil entre dans l'espace public :

« Dans le cas d'OpenAI, les informations collectées incluent notamment les données personnelles fournies par l'utilisateur, telles que ses informations de compte et son contenu. Cela inclut également les données reçues automatiquement à partir de l'utilisation des services d'OpenAI, telles que les informations d'identification, les données de localisation, et les informations de l'appareil (ordinateur ou autre) sur lequel l'outil est utilisé (marque, nom de l'utilisateur, ou moteur de recherche employé, par exemple). OpenAI les utilise ensuite pour faire fonctionner et améliorer les services en affinant les modèles existants - l'objectif étant de rendre les réponses plus précises et plus pertinentes. Les données des utilisateurs sont également précieuses à des fins de recherche, pour aider à former de nouveaux modèles OpenAI.

Si la démarche semble honorable sur le papier, ChatGPT étant un outil complexe, et notre compréhension du fonctionnement des Large Language Models (LLMs – modèles de langage possédant plus d'un milliard de paramètres) étant limitée, il est presque impossible de déterminer à quelle fin les informations sont véritablement utilisées. Cette opacité signifie que même si OpenAI offre la possibilité aux utilisateurs d'effacer leurs données personnelles, ils ne peuvent s'assurer que l'entreprise les a déjà stockées quelque part après leur collecte. Cela leur retire ainsi tout contrôle sur leur vie privée.

C'est pourquoi, les utilisateurs de ChatGPT doivent partir du principe qu'ils ne peuvent pas confier à ces outils leurs données personnelles. Des acteurs malveillants peuvent facilement manipuler les LLM, et les utilisateurs doivent donc se montrer extrêmement prudents et ne jamais partager d'informations confidentielles telles que des mots de passe, des données sensibles ou financières. Cette recommandation s'applique également aux entreprises, lesquelles avec le temps, recourent de plus en plus à l'IA pour assurer leur sécurité informatique. De même que les hackers l'exploitent, pour leur part, de plus en plus dans le cadre de leurs attaques. Il est donc important que les utilisateurs ne téléchargent pas d'informations confidentielles sur ChatGPT, ni ne fassent aveuglément confiance aux résultats des LLM, mais plutôt qu'ils restent prudents et s'assurent de rester informés sur les politiques de confidentialité ainsi que sur les mesures de sécurité des modèles qu'ils utilisent régulièrement. »

Source : IT Channel – Aout 2024