Village de la Justice www.village-justice.com

ChatGPT : Un risque pour les entreprises ? Par Charlotte Gerrish, Avocat et Nathalie Pouderoux, Juriste.

Parution : jeudi 22 juin 2023

Adresse de l'article original :
https://www.village-justice.com/articles/chatgpt-risque-pour-les-entreprises,46556.html
Reproduction interdite sans autorisation de l'auteur.

Open AI a mis au point un chatbot très sophistiqué appelé ChatGPT. Il s'agit d'un logiciel remarquablement intelligent permettant de collecter des informations sur les utilisateurs pour lui permettre de se développer et de s'entraîner pour devenir plus réactif. Il existe des préoccupations éthiques quant à la capacité de cette intelligence artificielle à manipuler et à tromper les individus en leur communiquant des informations biaisées ou erronées, mais il existe également des préoccupations en matière de sécurité, dans la mesure où ChatGPT peut compromettre les données à caractère personnel des utilisateurs.

I. Qu'est-ce que ChatGPT ?

ChatGPT a été lancé en novembre 2022 par Open AI. Il s'agit d'un chatbot piloté par l'intelligence artificielle (IA) et entraîné à dialoguer par écrit. Le chatbot peut répondre à des questions en utilisant le langage naturel et, lorsqu'on le lui demande, il peut imiter certains styles d'écriture. Par exemple, vous pouvez demander à ChatGPT d'écrire au sujet du temps qu'il fait comme le ferait un politicien. La technologie utilisée pour former le chatbot est la technologie des grands modèles de langage (LLM), qui recueille des données textuelles et crée des modèles en analysant les relations entre les mots et les messages-guides.

Bien que les chatbots existent depuis plusieurs années, ChatGPT est considéré comme une avancée majeure par rapport aux autres technologies de chatbot en raison de son intelligence et de sa sophistication. Vous pouvez demander à ChatGPT de parler de presque n'importe quel sujet dans n'importe quel style et il est capable de fournir des réponses détaillées et très proches de celles des humains.

II. Quelles sont les préoccupations concernant ChatGPT ?

Bien que ChatGPT soit un outil formidable pour les entreprises en raison de sa capacité à rédiger des courriels et d'autres contenus, la vitesse à laquelle cette IA se développe est préoccupante pour un certain nombre de raisons.

Contenu inexact.

ChatGPT est utilisé pour rédiger des messages, des courriels, des articles, des chansons et même des CV et des lettres de motivation. Vous pouvez demander à l'IA d'écrire sur à peu près tous les sujets et d'adapter son style d'écriture en fonction de ce que vous recherchez.

ChatGPT construit son contenu en utilisant des informations puisées dans des sources ouvertes sur Internet. Le problème est que l'exactitude des informations n'est pas garantie et qu'il n'y a aucun moyen de savoir si les informations récupérées par ChatGPT sont fiables. Contrairement à Google, qui permet de savoir si le contenu proposé provient de sources légitimes, telles que des sites gouvernementaux ou des entreprises réputées, ChatGPT se contente de fournir du contenu en réponse à des demandes d'utilisateurs. Mais ces derniers ne peuvent pas savoir d'où proviennent les informations ni si elles présentent un parti pris particulier ou si elles sont exactes.

Escroqueries.

Le Centre national de cybersécurité s'inquiète de la manière dont les logiciels de LLM tels que ChatGPT peuvent être utilisés pour rédiger des contenus malveillants qu'un cybercriminel n'aurait pas pu être en mesure d'élaborer autrement, ce qui rend les arnaques en ligne plus efficaces.

En effet, contrairement aux moteurs de recherche, ChatGPT est capable de fournir des réponses plus contextuelles et plus détaillées aux questions posées par les utilisateurs. Il est donc à craindre que les cybercriminels n'utilisent le logiciel pour rédiger des courriels de phishing convaincants et qui paraissent tout à fait réels alors que cela n'aurait pas été possible autrement. Il est dit que les auteurs de phishing n'ont pas un niveau d'anglais élevé et n'ont donc pas les compétences nécessaires pour rédiger avec soin un courrier électronique convaincant. Cela peut parfois rendre évident le fait qu'un courriel n'est pas tout à fait légitime.

Dans ce contexte, il est important que les entreprises disposent d'un logiciel de détection des menaces à jour afin d'identifier les attaques plus avancées. En outre, les organisations devraient former leurs employés à la détection des courriels malveillants, notamment en élaborant un protocole d'entreprise clair en cas de demande de divulgation d'informations sensibles.

Protection de la vie privée.

La politique de confidentialité d'Open AI indique qu'elle recueille les données à caractère personnel des utilisateurs, les téléchargements de fichiers et les commentaires fournis au chatbot. Elle précise également que les données à

caractère personnel seront utilisées « pour développer de nouveaux programmes et services » et qu'elles peuvent être communiquées à des tiers tels que des fournisseurs de services, des sociétés affiliées et lors de transferts d'activités.

Ce qui est problématique, c'est que le ChatGPT fonctionne en apprenant à partir des demandes et des informations qui lui sont fournies. Par conséquent, si les utilisateurs fournissent des données à caractère personnel et téléchargent des fichiers contenant des données sensibles, ces données seront toutes capturées et stockées. En outre, si des questions sensibles concernant la santé, les finances ou des questions juridiques sont posées, qui sont personnelles et spécifiques à l'individu qui les pose, ces questions seront enregistrées et utilisées par le chatbot dans son processus d'apprentissage. Cela signifie que ChatGPT peut détenir des données très personnelles sur n'importe qui et peut également les divulguer à des tiers (comme indiqué dans la politique de confidentialité). Si ces données sont ensuite piratées, les utilisateurs risquent de voir leurs informations sensibles exposées et potentiellement volées et utilisées pour commettre des délits tels que la fraude.

Les entreprises doivent donc être très vigilantes quant aux informations qu'elles saisissent dans ChatGPT et veiller à ne pas fournir de données à caractère personnel qui pourraient leur être attribuées et être utilisées contre elles, ou qui pourraient mettre des personnes en danger. Par exemple, si une entreprise demande au chatbot de rédiger un courriel contenant la date de naissance, le nom et le numéro de passeport d'un employé, ChatGPT conservera ces informations et, en cas de fuite, les données à caractère personnel de l'employé pourraient être en péril.

Par ailleurs, au début de l'année, un dysfonctionnement temporaire de ChatGPT a permis à certains utilisateurs de voir le titre des conversations d'autres utilisateurs. Bien que ce problème ait été résolu depuis, il démontre que ce logiciel d'IA n'est pas entièrement sûr et que nous ne savons pas dans quelle mesure notre vie privée est menacée. L'autorité de protection de données britannique (l'Information Commissioner's Office (ICO)) a déclaré que les entreprises qui utilisent des chatbots doivent respecter la vie privée et les données à caractère personnel de leurs utilisateurs, en particulier lorsque le logiciel utilise le LLM, qui est spécifiquement formé pour comprendre et répondre à un grand nombre de données sensibles.

Conclusion.

Les risques ont été reconnus. ChatGPT est bloqué dans certains pays, dont la Chine, l'Iran, la Corée du Nord et la Russie. L'Italie a été le premier pays occidental à bloquer ChatGPT pour des raisons de protection de la vie privée. Cette décision s'explique en partie par le fait qu'une violation de données avait été signalée le 20 mars 2023 et que des conversations d'utilisateurs et des informations de paiement avaient été divulguées.

L'autorité de protection de données italienne (Garante) a déclaré qu'il n'existait aucune base légale pour la collecte et le stockage massifs de données à caractère personnel en vue de l'entraînement d'algorithmes. En outre, il n'existe aucun moyen d'identifier les utilisateurs, ce qui expose les mineurs à recevoir des contenus inappropriés ou inadaptés. Nous attendons de voir la réaction des autorités françaises sur la légalité de ChatGPT en France.

Charlotte Gerrish, Avocat associée Fondatrice du Cabinet Gerrish Legal Barreau de Paris et Nathalie Pouderoux, Paralegal Paris - Londres - Stockholm

---