Les navigateurs dopés à l'IA pourraient mettre les utilisateurs face à de sérieux risques

TECHNOLOGIE Alors qu'OpenAI a lancé Atlas, un navigateur web fusionné avec ChatGPT, Microsoft l'a immédiatement imité. Les alternatives se multiplient, mais de nombreux problèmes de sécurité et de protection des données sont déjà présents

ANOUCH SEYDTAGHIA

C'est une bataille qui démarre à peine, mais qui est déjà très intense: celle des navigateurs web. Depuis des années, Google règne en maître quasi absolu, son logiciel Chrome détenant quelque 70% du marché mondial. Mais il y a du nouveau, avec l'arrivée de navigateurs centrés autour de l'intelligence artificielle (IA). Ces programmes d'un nouveau genre se multiplient brutalement, promettant monts et merveilles aux utilisateurs. Les spécialistes avertissent: il faut employer ces navigateurs IA avec la plus grande prudence, tant les risques de sécurité sont importants.

Revenons d'abord quelques jours en arrière. Mardi 21 octobre, OpenAI lançait soudainement Atlas, un navigateur dans lequel ChatGPT est totalement intégré. Le chatbot est omniprésent, assurant la navigation sur le web, promettant de réserver lui-même une table dans un restaurant ou une chambre dans un hôtel, de rédiger des e-mails ou d'automatiser des tâches. Quasi simultanément, mais sans que les médias y accordent le même intérêt, Microsoft insufflait de l'IA dans son navigateur Edge. Celui-ci devient capable de comparer des informations, d'effectuer aussi des réservations et des résumés de pages. Il peut aussi fusionner des onglets pour en synthétiser les informations.

Ce n'est pas tout. En parallèle, Perplexity, autre géant de l'IA, poursuit le développement de son navigateur Comet, capable selon la firme américaine de faire du shopping, de créer des sites web ou encore de gérer les onglets. Des acteurs plus petits tentent aussi de se faire une place, comme Neon, créé par Opera, ou Dia, conçu par The Browser Company. Et bien sûr, Google, qui vient de lancer son AI Mode, va certainement rapidement transformer Chrome en navigateur IA.

Les promesses sont immenses, les éditeurs de ces navigateurs faisant miroiter des systèmes complets, capables d'effectuer des tâches complexes à la place de l'utilisateur, qui n'a qu'à regarder le service agir et déplacer la souris. Mais de nombreux spécialistes avertissent ces jours des risques.

Problème architectural

«Je recommande de n'utiliser aucun de ces navigateurs jusqu'à ce que des garanties de sécurité suffisantes existent. Et celles-ci doivent être fournies par des professionnels de la sécurité, et non des ingénieurs en IA. Cela peut prendre des années, car c'est un problème architectural et non pas un «bug» logiciel», lance ainsi Grégory Mermoud, professeur associé à l'Institut d'informatique de la HES-SO Valais.

Selon l'expert, il y a d'abord un risque pour la confidentialité des données. «Le modèle observe tous les faits et gestes de l'utilisateur, ainsi que le contenu des sites visités. Ces données sont toutes transmises à l'éditeur du navigateur, comme OpenAI. Une partie de ces données peut être utilisée pour entraîner de futures versions du modèle. Cela dépend de la licence utilisateur et de la configuration du logiciel. Cependant, le risque ici n'est pas beaucoup plus grand que dans l'utilisation extensive et aveugle de ChatGPT ou d'un autre modèle d'IA.»

«L'idée même de donner à un agent IA un accès omniscient à notre navigateur [...] est vraiment effrayante»

GRÉGORY MERMOUD, PROFESSEUR ASSOCIÉ À L'INSTITUT D'INFORMATIQUE DE LA HES-SO VALAIS

Grégory Mermoud cite ensuite un autre risque qu'il qualifie d'«immense»: «L'idée même de donner à un agent IA un accès omniscient à notre navigateur, avec la possibilité d'effectuer des actions, tout cela en étant identifié auprès des services, est vraiment effrayante. Cela va à l'encontre de tous les mécanismes de sécurité qui ont été introduits dans les navigateurs depuis deux décennies.»

Longtemps sous-estimé, le navigateur web est un logiciel à la complexité et à la sophistication insoupçonnées du grand public, poursuit le professeur associé. Or il occupe une fonction à la fois critique et extrêmement sensible car il passe son temps à exécuter du code tiers qui ne peut pas être considéré comme fiable. Grégory Mermoud donne un exemple, souvent cité par ses pairs: «Un attaquant peut en principe utiliser une technique d'«injection d'instructions» dans un site web qu'il contrôle ou qu'il peut modifier afin de demander à l'agent de lui transmettre des données sensibles ou exécuter des actions non désirées (comme virer de l'argent sur un compte) sur un autre site auquel il est connecté.»

«Lent, fragile et pénible»

Certes, certains mécanismes sont en place pour protéger l'utilisateur, notamment la confirmation des actions sensibles, comme remplir un formulaire ou envoyer un e-mail. «Mais la nature même de ces outils tend à leur donner une autonomie dont on ne soupçonne pas les conséquences», alerte Grégory Mermoud.

Sur les réseaux sociaux, on voit certains internautes mettre en avant les actions déléguées à leurs navigateurs IA. «Il existe bien sûr des cas d'usage pour lesquels cela apporte beaucoup de valeur, mais ils ne sont pas aussi nombreux que ce qu'on veut bien nous vendre. Les premiers retours d'utilisateurs montrent que cela reste lent, fragile et pénible, du fait que l'agent automatise des tâches finalement assez communes et peu complexes (réserver un hôtel) et qu'il nécessite toujours de nombreuses interventions manuelles. Tout cela au prix d'énormes risques de sécurité supplémentaires malgré tout», conclut Grégory Mermoud. Une prudence absolue est ainsi de mise.