«Le déploiement des systèmes d'IA va beaucoup trop vite»

TECHNOLOGIE Meredith Whittaker, présidente de la messagerie Signal, partage ses craintes sur les futurs développements de l'intelligence artificielle. L'Américaine estime que les agents soulèvent des questions majeures sur la confidentialité des données et les droits humains

PROPOS RECUEILLIS PAR GRÉGOIRE BARBEY

«Nous faisons face à des acteurs technologiques qui sont devenus plus puissants que bon nombre d'Etats»

INTERVIEW

C'est une voix qui compte en matière de respect de la vie et d'intelligence artificielle. Meredith Whittaker, présidente de la Fondation Signal, basée en Californie, qui gère la messagerie du même nom, était de passage à Genève dans le cadre du sommet international AI for Good organisé cette semaine à Palexpo par les Nations unies. *Le Temps* l'a rencontrée dans son hôtel, peu avant son départ. L'occasion d'approfondir avec cette spécialiste de l'éthique de l'intelligence artificielle, ancienne employée de Google, les enjeux que cette technologie soulève en matière de confidentialité des données. Elle met en garde l'industrie contre un développement trop rapide et non maîtrisé, et critique aussi la volonté du Conseil fédéral d'étendre la surveillance des télécommunications.

Quels défis l'intelligence artificielle pose-t-elle en termes de respect de la vie privée? C'est une notion vague ayant de multiples définitions. Chez Signal, nous sommes surtout préoccupés par l'essor de l'intelligence artificielle dite agentique, qui promet de réaliser des tâches à notre place pour autant qu'elle puisse avoir accès à nos appareils et à nos données, ce qui porterait atteinte à la confidentialité de nos communications ainsi qu'à leur sécurité.

C'est-à-dire? Pour l'instant, c'est encore très théorique et nous nous basons essentiellement sur la façon dont les entreprises qui conçoivent ces outils les présentent. En tenant compte de leurs promesses, si vous souhaitez déléguer la réservation d'un restaurant à un tel système, et qu'il doit en plus se coordonner avec vos amis pour trouver la bonne date, alors il lui faudra accéder à de nombreux éléments sensibles de votre appareil. D'abord, votre agenda, pour vérifier vos disponibilités. Ensuite, votre plateforme de messagerie, pour se coordonner avec vos amis. Il aura probablement aussi besoin de votre navigateur web, pour chercher le restaurant. Et enfin, il lui faudra bien entendu utiliser votre carte de crédit, pour valider la réservation de l'établissement. Bref, il va requérir des autorisations étendues au sein de vos applications pour mener à bien sa mission. Et puisque les grands modèles de langage seront probablement trop volumineux pour être embarqués, les données qu'ils vont utiliser seront extraites de votre smartphone et traitées sur les serveurs de leurs éditeurs.

Et pourquoi cela pourrait-il affecter Signal? Parce que cela pourrait créer une perméabilité entre le système d'exploitation des appareils et les applications elles-mêmes. C'est regrettable car les utilisateurs ne sont pas avertis de ce risque. Il y a un manque de transparence de la part des entreprises qui conçoivent ces outils. Notre messagerie est utilisée par des millions de personnes à travers le monde parce qu'elle offre une confidentialité robuste. Notre protocole cryptographique est testé et éprouvé depuis plus de dix ans. Notre code source est ouvert et si un utilisateur ne nous fait pas confiance, il peut vérifier lui-même comment l'application fonctionne. Or, si cette perméabilité devait se concrétiser, alors cela créerait une vulnérabilité au sein de Signal qui pourrait compromettre sa fiabilité. Ce qui n'aurait pas seulement pour effet de menacer les gens qui développent cette messagerie, mais aussi les personnes qui comptent sur eux pour protéger leurs communications, parfois au péril de leur vie.

Que pouvez-vous faire pour empêcher cela? Nous devons être très clairs sur les implications que pourraient avoir ces agents sur l'avenir de Signal. Beaucoup de gens utilisent notre messagerie, y compris au sein des géants de la tech ou de l'administration américaine. Toutes ces personnes ont un intérêt à ce que nous puissions continuer notre travail. Nous devons aussi exiger une plus grande transparence de la part des entreprises qui conçoivent ces systèmes, que ce soit sur les données qui seront collectées et traitées, mais aussi sur les options qui seront accessibles aux développeurs d'application pour qu'ils puissent désactiver certains accès.

«Si nous voulons vraiment préserver les droits fondamentaux, nous devons défendre un monde dans lequel la confidentialité est la norme et la collecte de données l'exception»

Le modèle d'affaires des entreprises qui développent ces agents repose en grande partie sur les données. Croyez-vous vraiment qu'elles renonceront à de tels accès? C'est vrai, ça ne va pas de soi. Mais le développement de ces systèmes menace aussi des entreprises qui génèrent du profit grâce aux données. Regardez Spotify. Je doute vraiment qu'ils verraient d'un bon œil qu'un agent de Microsoft ou de Google puisse accéder à leur application en profondeur pour créer une liste musicale de manière automatisée tout en extrayant des données au passage. Je pense qu'il y a beaucoup d'entreprises qui ont tout intérêt à créer des frontières beaucoup plus claires entre les systèmes d'intelligence artificielle et leurs applications. Et les géants de la tech devraient en tenir compte, car si des applications disparaissent parce qu'elles ne peuvent plus générer d'argent, alors leurs écosystèmes perdront également de la valeur. Tout ce développement va beaucoup trop vite. C'est préoccupant de voir que des systèmes qui n'ont pas été audités ni validés et qui demeurent opaques sont aujourd'hui déployés à grande échelle, y compris dans des domaines sensibles au cœur des gouvernements et de l'économie mondiale.

Est-ce que des sommets comme AI for Good, en réunissant les différentes parties prenantes, peuvent contribuer à faire évoluer la situation? Nous faisons face aujourd'hui à des acteurs technologiques qui sont devenus plus puissants que bon nombre d'Etats. Ces processus de discussion entre les Etats, les entreprises et la société civile sont importants, mais ils ont surtout pour effet de produire plus de documentation. Nous devons aujourd'hui réfléchir à la manière dont nous pouvons imposer à cette industrie l'adoption de normes et de standards réellement ouverts. Si nous avions été intelligents, nous l'aurions déjà fait, car ce sont des règles d'hygiène élémentaires. Mais nous avons laissé le battage médiatique et le désir de profits rapides prendre le dessus.

Comment se porte Signal? Nous sommes une organisation à but non lucratif et nous pouvons compter sur un large soutien, ce qui nous permet de continuer à investir dans la recherche pour renforcer la confidentialité des communications. Une cinquantaine de personnes travaillent pour Signal, et nous pouvons compter sur un budget annuel d'environ 50 millions de dollars. Un tiers de ce montant provient de petites contributions de l'ordre de 5 à 20 dollars. Le reste est issu de dons plus importants.

Au-delà de l'intelligence artificielle, il y a aussi la question du chiffrement. Celui-ci est de plus en plus souvent attaqué par les législateurs. Ça vous inquiète? Oui, bien sûr. Nous avons d'ailleurs été choqués de voir que la Suisse envisageait de renforcer la surveillance de masse par ordonnance, ce qui aurait pour effet de contourner la loi et le parlement. Ce pays est connu pour son engagement en matière de confidentialité, nous avons donc été surpris qu'une démarche aussi extrémiste et contraire au respect de la vie privée ait pu être portée par les autorités suisses. Aujourd'hui, si nous voulons vraiment préserver les droits fondamentaux des êtres humains, nous devons défendre un monde dans lequel la confidentialité est la norme et la collecte de données l'exception.

Que faites-vous pour convaincre les gens d'utiliser votre application plutôt que WhatsApp ou Telegram? Nous faisons en sorte de proposer la meilleure expérience aux utilisateurs en matière de communication, y compris en respectant leur vie privée.

Lorsque Meta revient sur sa promesse de ne pas monétiser les données de WhatsApp à des fins publicitaires, ça vous réjouit? Je pense que la multinationale a commis beaucoup d'erreurs ces derniers temps qui remettent en cause son engagement en matière de confidentialité des communications. La publicité en est une, mais il y a aussi eu l'intégration de Meta AI, son intelligence artificielle générative.

Combien d'utilisateurs revendiquez-vous? Nous n'avons pas ce chiffre, mais notre application a été téléchargée des centaines de millions de fois. Cela donne un ordre d'idée.