LE COURRIER | LA LIBERTÉ | **INTERNATIONAL** | MARDI 4 AVRIL 2023 | pg. 8

L'Italie interdit ChatGPT

Les autorités accusent le robot conversationnel de ne pas respecter la loi sur les données personnelles

ChatGPT est apparu en novembre 2022 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 ou même à réussir des examens. KEYSTONE

ARIEL F. DUMONT, ROME

Intelligence artificielle – Les Etats-Unis et l'Europe s'interrogent sur les difficultés de réguler l'utilisation de l'intelligence artificielle (IA) en ce qui concerne la protection des données personnelles.
La semaine dernière, dans une pétition adressée aux entreprises et aux gouvernements, un groupe composé de 1000 experts mené par le milliardaire Elon Musk a réclamé le gel du développement de l'IA pendant six mois, en évoquant «des risques majeurs pour l'humanité sur le plan économique et politique». Pour les auteurs de cet appel, ce délai devrait servir à réorienter la recherche afin de développer des systèmes de sécurité et de fiabilité au niveau de la protection des données personnelles. Justement ce qui manquerait à l'interface d'IA générative créée et développée par la start-up américaine OpenAI selon les autorités italiennes.

Danger pour les mineurs

Rome a donc décidé de bloquer ChatGPT, dont la première version a été lancée en novembre 2022 et qui affiche aujourd'hui plus de 100 millions de comptes, au prétexte que la start-up américaine n'a pas respecté le règlement général européen sur la protection des données personnelles (RGPD). Ces mesures ont été adoptées en 2016 par la Commission européenne et transcrites dans le droit italien. Une décision identique avait été prise il y a deux mois pour bloquer l'app Replika, un autre programme commercialisé comme un «ami virtuel» et qualifié de dangereux pour les mineurs.
Retour sur les faits. Le 20 mars dernier, ChatGPT subit une perte de données importante concernant les conversations des utilisateurs et les informations relatives au payement des abonnés au service payant. L'autorité nationale italienne de protection des données personnelles (Garante della privacy) est rapidement alertée. Cet organisme note que l'entreprise américaine OpenAI qui a créé et développé cet outil conversationnel, capable d'échanger et de suivre un véritable dialogue avec son interlocuteur sous forme de messages écrits, n'a pas jugé utile d'informer ses utilisateurs de cette perte. Vendredi, l'autorité décide d'intervenir et de bloquer l'algorithme.

L'âge pas vérifié

Dans un communiqué, elle indique que cette décision «avec effet immédiat» implique la limitation provisoire du traitement des données des utilisateurs italiens vis-à-vis d'OpenAI, la société américaine qui a développé et gère la plate-forme. Selon l'autorité italienne, la start-up OpenAI n'a donné aucune information aux utilisateurs sur la procédure concernant le traitement de leurs données personnelles.
Cet organisme reproche aussi à OpenAI l'absence d'une base juridique justifiant le recueil et la conservation en masse des données dans le but d'entraîner les algorithmes qui font tourner la plate-forme. Il soulève également le problème des réponses inexactes souvent données par ChatGPT, une pratique qui laisse envisager «un traitement des données inexact».
Enfin, l'Autorité pose la question des mineurs. Bien que l'utilisation de ce robot soit destinée aux plus de 13 ans, la start-up n'a pas développé de filtres permettant de vérifier l'âge de l'utilisateur. Ce vide expose par conséquent les mineurs à des réponses non conformes à leur niveau de développement et de prise de conscience, affirme cet organisme. En parallèle, l'autorité a ouvert une enquête sur la perte des données du 20 mars dernier.

Version plus puissante

L'équivalent italien du Préposé à la protection des données a demandé à OpenAI, dont le siège est situé à San Francisco (USA), mais qui a désigné un représentant dans l'espace économique européen, de lui communiquer dans un délai de vingt jours les mesures entreprises pour respecter le règlement général européen. Faute de quoi, la start-up devra payer une amende allant jusqu'à 20 millions d'euros ou jusqu'à 4% de son chiffre d'affaires mondial annuel.
Toutefois, l'autorité italienne n'a pas précisé si le blocage de ChatGPT concernera également les versions Plus ou gratuites. Toutefois, le choc est sacrément rude pour la start-up américaine, qui est en train de développer une version encore plus puissante. Selon le développeur américain Siqi Chen, spécialisé dans l'IA, le robot ChatGPT5, qui devrait être lancé d'ici à la fin de l'année, pourrait penser et agir exactement comme un être humain. «Pour la première fois, nous sommes capables de créer l'intelligence elle-même, c'est une arme à double tranchant, mais si ça se passe bien, elle pourra résoudre de nombreux problèmes comme le réchauffement climatique», prophétise Siqi Chen.
I

«Pour la première fois, nous sommes capables de créer l'intelligence elle-même»

Siqi Chen

Blocage en Suisse compliqué

Est-ce qu'un blocage de ChatGPT en Suisse par décision du Préposé fédéral à la protection des données serait envisageable ?

En Suisse, les risques que l'algorithme ChatGPT conçu par la firme californienne OpenAI fait peser sur les données personnelles et pour les mineurs ne sont pas différents de ceux mis en évidence en Italie par l'Autorité nationale de protection des données personnelles. Ce robot conversationnel peut aider à rédiger un sonnet, composer une dissertation ou contribuer à la réussite d'un examen, mais il peut aussi diffuser à large échelle des conversations ou des données personnelles des utilisateurs. Et quand ceux-ci sont mineurs, il y a carrément infraction, selon l'autorité italienne, qui a demandé à OpenAI des corrections immédiates dans les 20 jours sous peine d'une forte amende.
«Actuellement, la loi suisse sur la protection des données ne permet pas d'agir comme l'a fait l'Autorité italienne de protection des données personnelles», explique Jean-Philippe Walter, commissaire à la protection des données du Conseil de l'Europe. «On ne peut pas infliger d'amendes

par exemple qui, avec la législation européenne, peuvent être salées: jusqu'à 4% du chiffre d'affaires de la société.»
La loi suisse ne permet que d'adresser des recommandations ou alors l'autorité peut requérir des mesures provisoires par exemple s'il y a un danger imminent pour le public.«La révision de la loi en Suisse sur la protection des données autorisera certaines restrictions d'utilisation mais ne permettra pas d'introduire une interdiction totale», ajoute Jean-Philippe Walter. «Ce qui a cours comme pratique actuellement est une demande à l'entreprise de se mettre en règle. Demander un blocage d'un outil comme ChatGPT pourrait être en tout cas beaucoup plus compliqué que dans l'Union européenne. Il faudrait entre autres que l'entreprise ait une représentation en Suisse.»
Selon Jean-Philippe Walter, qui était également préposé fédéral suppléant à la protection des données, les dangers sont bien réels. «Ce robot conversationnel peut répondre à des questions qui touchent des pratiques et des données personnelles voire intimes de certaines personnes comme des demandes relatives à la santé», ajoute le spécialiste. «Une personne peut donner à ChatGPT un curriculum vitae à reformuler, ce qui fournit des données personnelles qui par la suite peuvent être réutilisées par un autre utilisateur sans que celle-ci en soit informée. En plus, le robot peut identifier l'utilisateur ou plus précisément qu'il s'agit d'une personne bien précise sans connaître son nom mais uniquement par le recoupement d'informations notamment de trafic, comme la localisation.»

PIERRE-ANDRÉ SIEBER

LA POLICE EUROPÉENNE MET EN GARDE

Dans un récent rapport, l'agence de police européenne Europol a signalé les dangers pour la sécurité représentés par ChatGPT. Ce robot conversationnel peut aider des gens mal intentionnés à rédiger des courriers imitant le style d'entreprises comme des banques pour soutirer de l'argent à certaines personnes. Il peut aussi rédiger des tutoriels expliquant comment réaliser un larcin. Enfin, il peut élaborer des malwares ou virus pour infecter des systèmes informatiques.
Europol voit dans ce robot un risque évident. On en veut pour preuve l'appel signé par un millier de chercheurs en intelligence artificielle (IA) qui demandent une pause de six mois dans la recherche sur l'IA car la régulation ne va pas assez vite pour garantir un outil qui «représente un risque majeur pour l'humanité» s'il n'est pas maîtrisé.
Jusqu'à présent, la ville de Montpellier, en France, a interdit l'utilisation de ChatGPT à ses agents. A Paris, Sciences PO a également interdit le robot conversationnel à ses étudiants. PAS