Contre Attaque Surveillance de l'IA ...

CHAT GPT EN LIEN DIRECT AVEC LES FORCES DE RÉPRESSION

– **Un homme de 37 ans a été interpellé par le RAID après avoir voulu «tester la fiabilité et la surveillance de l'IA»** **–**

L'affaire est cocasse. Sans doute préoccupé par le recul des libertés publiques, un strasbourgeois a décidé de se saisir lui-même des inquiétudes qui devraient toutes et tous nous mobiliser en matière de surveillance numérique. Pour ce faire, rien de plus évident. Sur Chat GPT, l'homme de 37 ans a simplement évoqué son intention d'acheter une arme pour s'en prendre à «un agent du renseignement de la CIA, du Mossad ou de la DGSI» en vue de «tester la fiabilité et la surveillance de l'IA».

Une vaste chaîne répressive se met alors en branle. De l'autre côte de l'Atlantique, les échanges en question sont

transmis par OpenAI à des agents du FBI, qui décident à leur tour d'alerter les autorités françaises à travers la plateforme de délation en ligne PHAROS, réputée pour son inefficacité. Mais cette fois, cette étrange coopération internationale conduit au déploiement du RAID, une unité d'élite de la police nationale dédiée à l'antiterrorisme, pour procéder à l'interpellation du malheureux.
Immédiatement placé en garde vue, sa détention a finalement été levée dès le lendemain et l'affaire a été classée sans suite, des échanges numériques n'étant pas suffisamment caractéristiques d'un projet d'attentat. Il a cependant été hospitalisé d'office à l'issue de sa garde à vue en raison d'antécédents psychiatriques. S'il a effectivement obtenu la réponse à son interrogation initiale – oui, l'IA nous espionne – cette affaire soulève des préoccupations quant au monde numérique de demain.
Cette réaction en chaîne – OpenAI, FBI, PHAROS, Raid – illustre un basculement concret dans l'usage des intelligences artificielles conversationnelles. Ce qui nous est vendu comme un espace privé de dialogue fonctionne en réalité comme un environnement surveillé, capable de déclencher une cascade d'interventions d'ampleur mondiale en quelques heures. Mais c'est l'arbre qui cache la forêt : une part grandissante de la population confie sa vie aux data center. Bilan médical, fiches de paie, conseils psychologiques : en invitant l'IA dans notre intimité, nous donnons souvent sans le savoir des mines d'informations extrêmement précieuse à des entreprises privées. Le vieil adage «quand c'est gratuit, c'est que c'est toi le produit» n'a jamais semblé aussi vrai.
Chaque jour, des millions de personnes copient collent leurs résultats sanguins, leurs IRM, leurs diagnostics de cancer, leurs ordonnances ou encore leurs situations financières dans des applications comme ChatGPT pour les analyser ou demander conseil. Et de fait, ces données finissent stockées sur des serveurs californiens quasiment libre d'accès. Si non seulement les entreprises comme OpenAI se réservent le droit d'utiliser ces conversations pour entraîner leurs modèles, elles sont donc également rendues accessibles aux autorités. Autrement dit, un moteur d'IA en

sait probablement plus sur vous que votre propre famille proche ou même que votre médecin !
Alors que l'IA conversationnelle est aujourd'hui massivement utilisée à l'échelle de la planète, la concentration de données sensibles dans de telles proportions fait peser un risque immense sur la protection de la vie privée. Des entreprises tentaculaires réalisent donc un tour de passe passe vertigineux ; la dépossession massive et volontaire de toute forme de souveraineté informationnelle pour des millions d'êtres humains, le tout à des échelles qui font rêver les gouvernements les plus répressifs.
N'importe quelle police n'aura bientôt plus qu'à demander à OpenAI pour connaitre les préférences culinaires, maladies, situation amoureuse ou financière d'une personne qu'elle veut surveiller.