LA TRIBUNE
L'ESSENTIEL DE L'ACTUALITÉ ÉCONOMIQUE ET FINANCIÈRE

PAYS : France
PAGE(S) :88;89
SURFACE :150 %
PERIODICITE : Quotidien

RUBRIQUE : Numérique
DIFFUSION :192749
JOURNALISTE : Guillaume Renouard

► **29 septembre 2023 - N°7715**

NUMÉRIQUE

IA : « La politique cyber française s'est montrée prévoyante et pragmatique » (James Hodge, Splunk)

(Crédits : Splunk)

Guillaume Renouard, à Londres.

ENTRETIEN. Que changent les progrès de l'IA, et en particulier de l'IA générative, dans la cybersécurité ? Comment les régulations en place doivent-elles évoluer pour s'adapter ? Quels pays sont en avance sur la question ? Eléments de réponse auprès de James Hodge, vice-président général de la stratégie chez Splunk, une plateforme de gestion de données générées par les machines. Il siège également au conseil du comité de l'intelligence artificielle (IA) chez TechUK, une association professionnelle qui cherche à créer des ponts entre l'industrie britannique des nouvelles technologies et les décideurs politiques.

LA TRIBUNE - Le Premier ministre britannique Rishi Sunak a affirmé à plusieurs reprises sa volonté de faire de son pays un champion international de l'intelligence artificielle. Il organise cet automne un grand sommet autour de la technologie, là où a été inventée la machine Enigma. Où en est la régulation de l'IA au Royaume-Uni aujourd'hui ?

JAMES HODGE - Un livre blanc a été publié cet été, afin de proposer une approche « *pro-innovation* » de la régulation de l'IA, qui pourrait ouvrir la voie à une loi, l'an prochain. Y figure notamment l'idée de raisonner par industrie, plutôt que de traiter la technologie de manière monolithique. Il s'agit de tirer les enseignements de certaines erreurs commises par le RGPD, avec chaque site qui demande vos préférences en matière de cookies, alors que ce n'est pas toujours important pour l'internaute.

C'est la même chose pour l'IA : prenons d'un côté un chatbot avec lequel j'interagis pour obtenir un rendez-vous médical,

LA TRIBUNE
L'ESSENTIEL DE L'ACTUALITÉ ÉCONOMIQUE ET FINANCIÈRE

PAYS : France
PAGE(S) :88;89
SURFACE :150 %
PERIODICITE : Quotidien

RUBRIQUE : Numérique
DIFFUSION :192749
JOURNALISTE : Guillaume Renouard

► **29 septembre 2023 - N°7715**

à qui je transmets donc des informations de santé personnelles, et de l'autre un second chatbot auquel je pose quelques questions sur le site d'un fabricant d'électroménager, car j'essaie de comprendre pourquoi ma machine à laver ne marche plus. Il s'agit de la même technologie, mais les implications en matière de **protection de la vie privée** sont totalement différentes.

Idem pour la **reconnaissance faciale.** On ne parle pas de la même chose, selon qu'il s'agisse de contrôler l'identité des passagers qui prennent le train ou pour une cellule antiterroriste de repérer un homme suspecté de vouloir commettre un attentat.

L'approche prônée par le livre blanc est donc à mon sens très pragmatique. Elle se distingue toutefois de celle adoptée par l'**AI Act européen**, qui fait reposer la majorité des obligations de conformité sur les fournisseurs de la technologie, plutôt que sur les différentes industries qui l'utilisent. Une approche par industrie est à mon sens plus pertinente, dans la mesure où l'on se retrouve autrement avec une législation très générale qui, en s'attaquant à un trop grand nombre de cas possibles, risque de ne pas fonctionner, d'entraver l'innovation ou encore de manquer certains risques. On le voit avec l'approche du **RGPD** sur les cookies : la plupart des internautes se contentent de cliquer sans lire les détails.

On a récemment beaucoup parlé des dommages que la vague de l'IA générative pouvait causer entre les mains des hackers. Comment évaluez-vous le risque posé par l'IA en matière de cybersécurité ?

À partir du moment où un programme comme ChatGPT est capable d'écrire des lignes de code, il semble tout naturel qu'il soit également capable d'écrire des logiciels malveillants, et ainsi de donner un coup de pouce aux acteurs les plus mal intentionnés. Et en effet, l'entreprise de cybersécurité CyberArk a récemment démontré qu'elle avait réussi à faire coder un virus polymorphe par ChatGPT en tournant habilement sa requête.

Cependant, le virus en question était plus une expérience qu'autre chose. Le simple fait qu'une IA ait réussi à le coder ne signifie pas pour autant qu'il soit efficace. Il faut aussi se demander s'il fonctionne correctement une fois déployé, s'il est capable de déjouer les antivirus et autres barrières de protection. Il faut une large quantité de savoirs pour parvenir à cocher toutes ces cases, et l'IA générative n'en est, pour l'heure, pas encore là.

Mon point de vue, ainsi que celui de nombreux autres acteurs du secteur, est que le principal risque posé par l'IA générative repose plutôt sur la manipulation : en permettant aux hackers de s'exprimer aisément, et sans fautes, dans un langage qui n'est pas le leur, elle peut leur permettre de plus facilement endormir la vigilance des victimes et conduire à des erreurs humaines qui demeurent aujourd'hui la source de la grande majorité des cyberattaques.

La bonne nouvelle, c'est que les entreprises sont de plus en plus efficaces pour repérer les logiciels malveillants. Une récente étude de Splunk montre qu'il faut aujourd'hui en moyenne deux mois pour qu'une entreprise détecte un tel logiciel dans son système : il y a cinq ans, on parlait de neuf mois. Les entreprises françaises sont particulièrement bien positionnées : 29% des organisations françaises signalent des violations au cours des deux dernières années, contre 61% dans le reste de l'Europe.

Qu'est-ce qui explique cette réussite française, selon vous ?

La France dispose d'une population plus qualifiée dans le domaine de la cybersécurité que le reste de l'Europe. 10% des entreprises françaises évoquent ainsi des difficultés pour recruter du personnel qualifié en cybersécurité, contre 23% à l'échelle européenne. Dans l'ensemble, la politique cyber française s'est montrée prévoyante et pragmatique. Nous avons notamment observé la mise en place de grandes initiatives telles que le « **Campus Cyber** » qui rassemble toute la communauté de cybersécurité française, des entreprises privées aux institutions publiques, en passant par les enseignants et les étudiants.

Le manque de talents constitue l'un des principaux obstacles sur lesquels butent aujourd'hui les politiques et les entreprises de cybersécurité. Nous pensons toutefois que l'IA générative peut ici apporter des solutions en permettant à davantage de travailleurs de manipuler des outils de cyberdéfense complexes. C'est pourquoi chez Splunk nous avons récemment lancé un « AI assistant », qui permet de formuler des requêtes cyber en langage articulé, par exemple « Y a-t-il eu des brèches sécuritaires dans mon pare-feu aujourd'hui ? ». On réduit ainsi le niveau minimum pour pouvoir poser des questions et obtenir des réponses concernant la sécurité de l'organisation.