Comment crÃ©er une IA de confiance ?
Internet
PostÃ© par : JerryG
PubliÃ©e le : 6/12/2023 14:00:00

Une Ã©tude menÃ©e par Impact AI en 2023 rÃ©vÃ¨le que malgrÃ© une perception positive en termes de productivitÃ©, gain de temps et crÃ©ativitÃ©, le potentiel de lâ□□IA est encore peu mis en Å□uvre par le grand public FranÃ§ais.

Moins dâ□□un quart des sondÃ©s lâ□□auraient dÃ©jÃ utilisÃ© dans leur vie personnelle et seulement 16% dans un cadre professionnel. Bien que la perception globale soit positive, des inquiÃ©tudes persistent.

Les prÃ©occupations majeures sont lâ□□utilisation des donnÃ©es personnelles, les pertes dâ□□emplois potentielles et le respect de la propriÃ©tÃ© intellectuelle. Les personnes interrogÃ©es ont Ã©galement des avis assez divergents quant Ã lâ□□importance et lâ□□impact de cette innovation.

Globalement, il y a une volontÃ© de mieux comprendre et dâ□□Ãªtre davantage informÃ© sur les consÃ©quences de lâ□□IA gÃ©nÃ©rative notamment au travail. De plus, 70 % des FranÃ§ais estiment que lâ□□IA gÃ©nÃ©rative devrait Ãªtre sous contrÃ´le humain, pour une relecture et une vÃ©rification aprÃ¨s intervention.

Vers une IA de confianceâ□¦

Lâ□□Ã©tude rÃ©vÃ¨le une confiance partielle des FranÃ§ais en ce qui concerne lâ□□IA : 30% expriment un besoin essentiel de dÃ©velopper une IA Â« digne de confiance Â». Cela implique dâ□□orchestrer un contrÃ´le et une rÃ©gulation adaptÃ©e en synergie avec lâ□□innovation et le progrÃ¨s pour dÃ©velopper une Intelligence Artificielle qui rÃ©pond aux attentes des citoyens avec sÃ©curitÃ©.

68 % des employÃ©s utilisent ChatGPT au travail dans le dos de leur employeur.

Sachant que ChatGPT est une application publique et non protÃ©gÃ©e, il y a un rÃ©el enjeu de contrÃ´le Ã mettre en place pour bon nombre dâ□□entreprises. La question de lâ□□Ã©thique, bien que complexe et dÃ©pendante du contexte socio-culturel, est trÃ¨s vite abordÃ©e au mÃªme titre que le sujet de responsabilitÃ© juridique.

Pour rÃ©pondre Ã des problÃ©matiques cruciales dâ□□Ã©thique et de protection des donnÃ©es, ou pour limiter le nombre de controverses et dâ□□incidents trÃ¨s nombreux liÃ©s Ã lâ□□IA GÃ©nÃ©rative, il est nÃ©cessaire de crÃ©er une IA de confiance.

2/3 des FranÃ§ais plaident pour une IA de Confiance

Selon une Ã©tude IBM, le dÃ©ploiement dâ□□une IA Ã©thique en entreprise se fait Ã©tape par Ã©tape. PremiÃ¨rement, on met en contexte son utilisation dans la vision stratÃ©gique globale de lâ□□entreprise. Ensuite on Ã©tablit une gouvernance pouvant assurer son implÃ©mentation.

Enfin, on lâ□□intÃ¨gre dans le cycle de lâ□□entreprise en engageant les parties prenantes et en organisant une structure. Il faut Ã©galement dÃ©finir une politique, en pilotant et en soutenant la culture ainsi que la formation en interne. La mise en place dâ□□une mÃ©thodologie et de processus

rigoureux est nÃ©cessaire.

RGPD et IA, quel Ã©quilibre ?

Aujourdâ□□hui, les technologies dâ□□IA se nourrissent de quantitÃ©s massives de donnÃ©es dont un grand nombre sont personnelles voire sensibles. Il est donc nÃ©cessaire de trouver un Ã©quilibre entre la protection de ces derniÃ¨res, le respect des rÃ¨gles lÃ©gales, et le dÃ©veloppement de cette technologie. Lâ□□IA vient avec son lot de complexitÃ© en matiÃ¨re de RGPD avec des risques pouvant engendrer discrimination, vol de donnÃ©es, violation de la vie privÃ©e ou gestion abusive dâ□□informations.

En rÃ©ponse Ã ces problÃ©matiques, la CNIL a mis en place un certain nombre de ressources publiques permettant de rÃ©pondre aux dÃ©fis posÃ©s par lâ□□IA. Parmi elles : Comment sÃ©curiser un systÃ¨me ou assurer une transparence, s'informer sur les enjeux liÃ©s Ã lâ□□utilisation de lâ□□IA, comment auto-Ã©valuer son systÃ¨me dâ□□IAâ□¦

Comme tÃ©moin des actions mises en place Ã grande Ã©chelle : lâ□□AI Act. Câ□□est le rÃ¨glement europÃ©en qui vise Ã rÃ©guler les utilisations de lâ□□intelligence artificielle en classant les applications en fonction de leur niveau de risque Ã©thique : minime, limitÃ©, Ã©levÃ© ou inacceptable.

Son objectif est de veiller Ã ce que les systÃ¨mes dâ□□IA mis sur le marchÃ© europÃ©en soient sÃ»rs et respectent les droits fondamentaux des citoyens et les valeurs de lâ□□UE. Tout cela en garantissant la sÃ©curitÃ© juridique et en renforÃ§ant les exigences en matiÃ¨re de sÃ©curitÃ©.

Protection des donnÃ©es et chiffrement bout Ã bout

Pour ne pas porter atteinte aux droits des utilisateurs, il est nÃ©cessaire de respecter certaines rÃ¨gles fondamentales du RGPD Ã savoir :

-ConformitÃ© des donnÃ©es et lÃ©gitimitÃ© dâ□□utilisation
-Collecte et Respect du consentement
-Limitation dâ□□utilisation des donnÃ©es Ã ce qui est nÃ©cessaire
-Assurance de la sÃ©curitÃ© des donnÃ©es
-NÃ©cessitÃ© dâ□□information et de Transparence

Pour se conformer au RGPD, les entreprises peuvent opter pour le chiffrement bout Ã bout. Câ□□est une technique de sÃ©curitÃ© qui garantit que seuls lâ□□Ã©metteur et le destinataire peuvent accÃ©der au contenu des donnÃ©es Ã©changÃ©es. Cela mÃªme lorsque celles-ci transitent par des rÃ©seaux tiers.

En matiÃ¨re dâ□□intelligence artificielle et de protection des donnÃ©es, le chiffrement bout Ã bout joue un rÃ´le crucial. Il permet dâ□□assurer la confidentialitÃ© et la sÃ©curitÃ© des informations sensibles utilisÃ©es dans les systÃ¨mes dâ□□IA.

Mettre en place des audits de sÃ©curitÃ©

Lâ□□enjeu qui gravite autour des audits de sÃ©curitÃ© est consÃ©quent. Les entreprises sont aujourdâ□□hui plus que jamais exposÃ©es Ã des cyber-attaques. Il est donc essentiel de mettre en place rÃ©guliÃ¨rement un processus dynamique permettant de sâ□□assurer de la fiabilitÃ© et de la rÃ©cence des mesures de protection des donnÃ©es en vigueur.

Dans le cas contraire, les entreprises sâ□□exposent Ã des pertes de donnÃ©es confidentielles pouvant mener Ã des consÃ©quences financiÃ¨res, humaines ou morales plus ou moins graves.

Avec des Ã©changes de quantitÃ©s massives de donnÃ©es liÃ©es Ã lâ□□IA, il est essentiel pour les entreprises de protÃ©ger efficacement leurs SystÃ¨mes dâ□□Informations. Il est donc judicieux pour le dÃ©veloppement dâ□□une IA de Confiance de passer par la mise en place ces audits afin de dÃ©tecter et prÃ©venir des failles potentielles de sÃ©curitÃ©.

Ils pourront prendre diverses formes en fonction des objectifs et des besoins propres Ã lâ□□entreprise :

-Diagnostic technique
-Test de vulnÃ©rabilitÃ©
-Audit stratÃ©gique
-Test de rÃ©sistance
-Test dâ□□ingÃ©nierie sociale

5 actions directes pour votre entreprise

Transparence et traÃ§abilitÃ© : Offrez des explications claires Ã vos utilisateurs sur la maniÃ¨re dont les donnÃ©es sont utilisÃ©es, collectÃ©es ou traitÃ©es ainsi que sur les dÃ©cisions prises par les systÃ¨mes dâ□□IA.

Protection des donnÃ©es : Assurez-vous que la sÃ©curitÃ© des donnÃ©es soit une prioritÃ© dÃ¨s le dÃ©veloppement des algorithmes et des modÃ¨les dâ□□IA. Veillez Ã Ãªtre au fait de lâ□□actualitÃ© concernant le RGPD, lâ□□AI Act et toute loi en vigueur.

Gestion responsable des donnÃ©es : Mettez en place une mÃ©thodologie et des protocoles de gouvernance robustes en ce qui concerne la gestion des donnÃ©es.

SÃ©curitÃ© et Ã©valuation continue : Effectuez des protocoles rÃ©guliers pour Ã©valuer les risques et lâ□□efficacitÃ© des mesures dÃ©jÃ en place. Soyez Ã jour et certifiÃ©s par des tiers professionnels.

Formation et sensibilisation : Formez vos Ã©quipes sur les enjeux Ã©thiques et les bonnes pratiques en termes de protection des donnÃ©es. Encouragez une culture axÃ©e sur la sÃ©curitÃ© au sein de votre organisation en recrutant si nÃ©cessaire un Chief Ethics Officer, dixit Patrick SÃ©guÃ©la, CEO de Synapse DÃ©veloppement