Lundi 16 septembre 2024  
  
Microsoft Copilot semble être la solution la plus adaptée aux besoins d’intelligence artificielle dans l’entreprise. Sa fonctionnalité « knowledge », équivalent de base de données de retrieval (RAG), permet de créer des chatbots sur mesures basés sur des fichiers Sharepoint spécifique.  
  
Problème : Chaque personne au sein des différentes équipes/ départements de l’entreprise possède des droits d’accès différents aux différents fichiers présents sur le sharepoint.

* Question : **Est-ce que les droits paramétrés sur le Sharepoint sont constant dans le Copilot ?**

Cela soulève un problème fondamental : l’accès à l’information.  
  
J’ai commencé mes recherches concernant le sujet Copilot en lisant la documentation fournie par Microsoft. En feuilletant la documentation je soulève les potentiels challenges auxquels nous allons faire face et parallèlement je cherche des solutions, quelles proviennent de Microsoft ou de tiers.  
  
Aujourd’hui nous avons soulevé 2 challenges :  
  
1. L’option « own general knowledge » qui permet à un copilot d’utiliser les données d’entraînement du modèle utilisé par le Copilot dans la composition de ses réponses (Ex : ChatGPT et sa base d’entraînement -> une question sur Napoléon).

* **Challenge soulevé** : Est-ce que le knowledge vient interférer dans la réponse du Copilot ? Est-ce cela augmente la possibilité d’hallucination ou hors sujets (dans le sens où plutôt que de répondre précisément sur le knowledge du Sharepoint, le Copilot répond à la question en se basant sur sa base de données d’entraînement).
* **Potentielle solution**: Test Q/A.

2. Le prompting : La plupart des collaborateurs ne savent pas correctement utiliser l’IA et ne savent pas ce qu’est le prompt engineering, or la fructification de l’IA réside dans sa correcte utilisation.

* **Challenge soulevé** : Est-ce que la qualité du prompt d’entrée a un effet sur le résultat fourni par le Copilot ? Est-ce que Microsoft Copilot Studio a des solutions pré-intégrées on-premise ? Fonctionnent-elles correctement ?
* **Potentielle solution** : Création d’une loop d’amélioration de prompt en utilisant des méthodes telles que MONOPARA (Modèles de NLP permettant de baisser la perplexité d’un prompt). Intégration d’un tunnel d’utilisation intégrant des templates de prompt, une validation par user feedback, contexte, etc…

Suite : Nous avons prévu de caler un point pour m’octroyer l’accès à la modification d’un Copilot afin de commencer une série de test. Voici une brève description de l’environnement de test :  
  
Je serais admin et Jérôme sera un utilisateur lambda. Nous allons créer 2 fichiers fictifs : en tant qu’admin j’aurais les droits aux 2 fichiers tandis que Jérôme n’aura accès à qu’un fichier. Ensuite nous testerons du prompt hacking de manière à vérifier si les droits sharepoint sont transverses à l’utilisation d’un Copilot Microsoft.