CANADIAN RESEARCH INSIGHTS COUNCIL
LE CONSEIL DE RECHERCHE ET D'INTELLIGENCE MARKETING CANADIEN

Principes directeurs du CRIC sur l'utilisation de l'IA dans les études de marché

Introduction

L'objectif de ces principes directeurs est de fournir un cadre pour l'utilisation de l'intelligence artificielle[1] (IA) et de l'intelligence artificielle générative[2] dans les études de marché. Compte tenu de l'application et de l'utilisation croissantes de l'IA, l'objectif est d'assurer une utilisation stratégique, éthique et responsable des outils d'IA.

Principes directeurs :

1. **Transparence :** assurer la transparence et la responsabilité dans l'utilisation de l'IA (toute organisation qui utilise l'IA doit communiquer ouvertement et clairement avec les clients, les répondants et le grand public au sujet de l'intégration de l'IA dans les processus, et expliquer comment, pourquoi et quand l'IA est utilisée). Il est reconnu que l'IA est un outil qui existe dans l'industrie depuis de nombreuses années, cependant, à la suite de l'adoption généralisée des modèles d'IA générative, une révision de nos normes de transparence est nécessaire. L'approche actualisée de la transparence comprendra une communication détaillée sur la nature précise, l'application et les conséquences potentielles de ces modèles avancés d'IA générative et, s'il y a lieu, sur l'utilisation des systèmes d'IA traditionnels déjà en place.

2. **Sécurité des données :** le recours à de nombreux outils d'IA peut soulever des questions relatives à la sécurité des données. Il faut assurer le respect des normes pertinentes du CRIC, des pratiques essentielles en matière de sécurité indiquées dans la Trousse d'outils du CRIC sur la sécurité de l'information, ainsi que des contrats des clients en ce qui concerne la transmission, la conservation et la sécurité des données. Les chercheurs doivent accorder une attention particulière à la manière dont les informations saisies dans les applications d'IA seront utilisées par les applications pour l'apprentissage à partir de données ou la production d'autres résultats. Dans les situations où plusieurs normes ou contrats peuvent s'appliquer, le document de référence doit être celui qui fixe la barre la plus haute en matière de sécurité des données.

3. **Protéger les participants contre les dommages :** comme pour tous les outils de recherche, il convient d'adhérer aux principes d'un programme rigoureux de gestion de la vie privée, comme l'exigent les normes du CRIC et comme l'indique la Trousse d'outils du CRIC sur la protection de la vie privée, lorsque vous avez recours à l'IA. Il faut veiller à ce que les données et les intrants que les systèmes d'IA utilisent soient obtenus, utilisés et divulgués en toute légalité. Il faut également tenir compte de la protection de la vie privée des répondants ainsi que de leur droit à comprendre comment leurs données sont recueillies et conservées. Plus précisément,

dans le contexte des applications d'IA générative telles que les robots de conversation, l'IA modératrice ou l'IA incitative, il est essentiel d'informer clairement les répondants qu'ils interagissent avec un système d'IA et non avec un être humain.

4. **Efforts pour minimiser les préjugés :** il faut comprendre les préjugés potentiels de l'IA et accorder la priorité aux besoins des personnes et des communautés, notamment des groupes défavorisés sur le plan de l'équité. Les chercheurs doivent rester vigilants quant aux préjugés et aux limites naturelles de l'IA et prendre des mesures pour minimiser leurs conséquences tout en favorisant le principe de responsabilité. Il faut évaluer les résultats des systèmes d'IA, notamment les outils génératifs, afin de minimiser les préjugés et les inexactitudes. De plus, lorsque le contenu est principalement ou entièrement généré par l'IA, une mention claire de ce fait doit être ajoutée afin de maintenir la transparence. Ainsi, les clients sont entièrement au courant de la source et de la méthode de création du contenu.
5. **Assurer la surveillance :** les membres du CRIC doivent s'assurer que des mesures de contrôle efficaces sont en place. Ils sont encouragés à procéder régulièrement à des vérifications de la partialité de leurs systèmes d'IA, à créer des environnements de test et à mettre en place des mécanismes de surveillance humaine des systèmes d'IA afin d'assurer la responsabilité. Les équipes doivent être multidisciplinaires et comprendre des spécialistes des données, de l'éthique et du droit afin d'assurer une compréhension globale.

Définitions

Attribution : ces définitions proviennent du document « Key Terms for AI Governance », produit par l'International Association of Privacy Professionals. Elles ont été publiées à l'origine dans le centre de ressources de l'IAPP et sont utilisées avec son autorisation. Cette version a été publiée en octobre 2023.

1 : **Intelligence artificielle** : il s'agit d'un terme général utilisé pour décrire un système informatique conçu pour effectuer ou automatiser des tâches au moyen de diverses techniques de traitement de l'information. Parmi ces techniques figure l'apprentissage automatique, qui permet aux machines d'apprendre par l'expérience, de s'adapter à de nouvelles données d'entrée et d'effectuer éventuellement des tâches qui étaient auparavant effectuées par des humains. Plus précisément, il s'agit d'un domaine de l'informatique consacré à la simulation de comportements intelligents dans les ordinateurs. Les décisions automatisées peuvent faire partie de ce processus.

2 : **IA générative** : un domaine de l'IA qui utilise l'apprentissage profond à partir de grands ensembles de données pour créer du nouveau contenu, comme du texte, du code, des images, de la musique, des simulations et des vidéos. Contrairement aux modèles discriminants, l'IA générative fait des prédictions à partir de données déjà présentes et non à partir de données nouvelles. Ces modèles sont en mesure de générer de nouveaux résultats à partir de données d'entrée ou de demandes de l'utilisateur.