

Ética & Inteligência Artificial

Marcelo Fantini
Rubens de Castro Pereira

RA 108341
RA 217146

24 de março de 2023

1. Defina Ética em Inteligência Artificial.

A ética em Inteligência Artificial (IA) representa um conjunto de valores e princípios que devem ser respeitados por todos os atores envolvidos no ciclo de vida de sistemas de IA com destaque ao respeito, proteção e promoção dos direitos humanos, liberdades fundamentais e dignidade humana, diversidade e inclusão [1].

2. Apresente uma notícia recente de um problema de Ética em IA.

Escreva sua resposta aqui!

3. Apresente um artigo científico recente de uma solução para um problema de Ética em IA.

Escreva sua resposta aqui! O artigo [2] tem como propósito tratar dos riscos potenciais e uso indevido de geração de conteúdo por IA (GCIA), auxiliar na eliminação de obstáculos e promover entregas seguras e éticas de conteúdos gerados por IA. Os tipos de conteúdos podem ser bastante variados podendo ser imagens, textos, áudios e vídeos.

Com o uso extensivo da GCIA tem surgido preocupações relativas à privacidade, preconceito, toxicidade, desinformação, propriedade intelectual e potencial uso indevido diante das pessoas. Uma questão relevante surgiu recentemente com a disponibilização de novas funcionalidades no ChatGPT as quais permitem fazer a depuração de código fonte de programas de computador ou elaborar trabalhos escolares/acadêmicos. Esses resultados podem gerar riscos potenciais, pois os modelos de GCIA produzem trabalhos replicando conteúdos com os quais foram treinados devido à elevada capacidade de memorização. O conjunto de dados utilizados para treinamento frequentemente tem origem e direitos autorais desconhecidos, muitas das vezes não passam por uma análise de curadoria cuidadosa. A maioria dos modelos de GCIA decodificadores de textos são treinados com grandes quantidades de dados obtidos da internet, os quais podem conter desvios (bias) relacionados a temas sociais, podem ser tóxicos, e outras limitações inerentes aos grandes modelos de linguagens.

Para que os modelos de GCIA sejam responsáveis, estes devem considerar o seguinte escopo: privacidade, vies (tendências), toxicidade, desinformação, proteção da propriedade intelectual. Além disso, deve contemplar também a robustez dos sistemas, explicabilidade (feedback), código fonte aberto, consentimento, créditos e compensação, e ambiente amigável para o seu uso.

Privacidade Os modelos base e os modelos generativos de conteúdo possuem a vulnerabilidade de ataques de privacidade, a qual pode ser decorrente de dados duplicados nos datasets de treinamento. Esse comportamento de replicação tem sido extensivamente estudado nesses modelos, podendo levar a resultados de imagens como a combinação de fundo e de objetos de imagens reais do conjunto de imagens de treinamento. Esses resultados levantam questões sobre memorização de dados, propriedade das imagens difundidas, imagens de pessoas reais, reproduzindo dados do treinamento e não novas imagens criadas pelos modelos.

As questões de privacidade ainda não possuem solução definitiva, mas ações vem sendo tomadas para minimizar tais questões. As companhias tem disponibilizado website para fornecer identificação de imagens já treinadas/memorizadas. Outra ação para evitar a duplicação de dados é o uso de técnicas de deduplicação removendo de forma ampla dados duplicados utilizados em treinamento. Além disso, companhias tem adotado medidas para prevenir o compartilhamento de dados sensíveis pelos seus empregados, evitando o uso desses dados em futuras versões de modelos de GCIA. Atualmente as

medidas para evitar o vazamento de dados privados são insuficientes e ainda faz-se necessário explorar sistemas confiáveis para a detecção de dados duplicados em modelos generativos e maior investigação na memorização e generalização em sistemas de aprendizado profundo.

Viés/Tendências/Bias - Toxicidade - Desinformação

Os dados de treinamento utilizados nos modelos de Inteligência Artificial (IA) são obtidos do mundo real, os quais, sem a intenção, podem reforçar estereótipos indesejáveis, excluir ou marginalizar certos grupos de indivíduos, conter dados tóxicos, levando à incitação ao ódio ou violência a a ofender indivíduos.

O uso de filtros nos dados é uma possibilidade de minimizar tais problemas, contudo eles podem introduzir vieses nos dados de treinamento que podem se propagar nos modelos. A fim de minimizar esses vieses, técnicas de pré-treinamento são utilizadas nos dados antes do treinamento. Outra estratégia adotada é o contínuo treinamento dos modelos de GCIa com as informações mais recentes evitando o surgimento de lacunas de informação e garantindo que os modelos permanecem atualizados, relevantes e benéficos para a sociedade. Ainda existem lacunas para investigação mais profunda desses vieses, toxicidade e desinformação em todo o ciclo de vida de desenvolvimento dos modelos, apesar de ser uma tarefa desafiadora.

Proteção da propriedade intelectual

Discussão

Conclusão

Referências

- [1] Scientific United Nations Educational and Cultural Organization (UNESCO). Recommendation on the ethics of artificial intelligence, 2022.
- [2] Chen Chen, Jie Fu, and Lingjuan Lyu. A pathway towards responsible ai generated content, 2023.