CENTRO UNIVERSITÁRIO PROCESSUS

PRÁTICA EXTENSIONISTA

TEMAS EMERGENTES

INTELIGÊNCIA ARTIFICIAL: DESAFIOS E SOLUÇÕES

Brasília
2023

TEMAS EMERGENTES

INTELIGÊNCIA ARTIFICIAL: DESAFIOS E SOLUÇÕES

Professora: Luiza Cristina de Castro Faria
Equipe: Alan Santos
Anna Claras Gomes de Macedo
Cíntia Morgana Schittler
Débora Alves
Flávio Martins Braz
Mariana Soares Oki
Paulo Japhet Sallenave de Alencar

Sumário

Conceito: **Débora**

Desafios Éticos: : **Paulo**

Desafios Práticos: **Cíntia Morgana** e **Mariana**

Buscar soluções: **Anna Clara**

Caso concreto: **Alan**

Entrevista: **Flávio Martins**

Parte Escrita do trabalho: **Flávio** e **Mariana**

INTELIGÊNCIA ARTIFICIAL

CONCEITO

É a área da ciência na qual estuda o desenvolvimento das máquinas para desempenhar ocupações da atividade humana de maneira autônoma. Suas atividades são realizadas por meio de diversos métodos, no qual funcionam de acordo com análise de dados e identificação de padrões.

Portanto, está relacionado ao desenvolvimento de sistemas de "máquinas" capazes de realizar tarefas que exigem da inteligência humana, como por exemplo: reconhecimento de voz e tradução de idiomas. No qual tem-se os mais comuns utilizados atualmente de inteligência artificial, que são ALEXA e SIRI que são assistentes virtuais que reconhecem a fala e reconhecimento facial com o "FACE ID" (que é um sistema projetado pela Apple).

DESAFIOS ÉTICOS

Viés e Discriminação: Algoritmos de IA podem perpetuar preconceitos existentes, resultando em decisões discriminatórias em áreas como recrutamento, crédito e justiça criminal.

Privacidade: A coleta massiva de dados e a análise por IA levantam questões sobre como os dados são usados, compartilhados e protegidos, ameaçando a privacidade individual.

Responsabilidade e Responsabilização: Determinar a responsabilidade em caso de erros em sistemas de IA é complexo, gerando debates sobre responsabilidade legal e moral.

Desemprego e Mudança Econômica: A automação impulsionada pela IA pode resultar na substituição de empregos humanos, exigindo requalificação e levantando preocupações sobre a segurança econômica.

Autonomia de Máquinas: À medida que a IA alcança maior autonomia, a capacidade de tomar decisões éticas em situações complexas, como carros autônomos decidindo entre salvar vidas humanas, torna-se uma preocupação.

Manipulação e Desinformação: A IA pode criar informações falsas convincentes, como deepfakes, e amplificar a disseminação de desinformação em larga escala, ameaçando a confiabilidade das informações.

Transparência e Interpretabilidade: Algoritmos complexos dificultam a compreensão de como decisões são tomadas, afetando a capacidade de explicar e justificar as ações dos sistemas de IA.

Singularidade Tecnológica: A perspectiva da "singularidade", onde a inteligência das máquinas ultrapassa a humana, traz questões sobre controle e impacto nessa eventualidade.

Autonomia Militar: O desenvolvimento de armas autônomas levanta preocupações sobre a possibilidade de ações militares sem controle humano adequado.

Propriedade Intelectual e Ética da Inovação: O rápido avanço da IA levanta questões sobre a propriedade intelectual e a ética em torno do controle e dos benefícios gerados por essas tecnologias.

DESAFIOS PRÁTICOS E SEUS RISCOS

A Inteligência Artificial (IA) surgiu como uma das maiores revoluções tecnológicas do século XXI, prometendo transformar indústrias, aperfeiçoar processos e melhorar a vida das pessoas de várias maneiras. No entanto, esse progresso não é isento de desafios, sejam eles éticos ou práticos que precisam ser abordados para aproveitar plenamente o potencial da IA.

O surgimento e o avanço das IAs (Inteligências Artificiais) estão trazendo uma série de desafios práticos para a sociedade, entre eles: Perda de empregos, Prejuízos sociais, Vícios em tecnologia com efeitos na saúde mental, Discriminação e Controle.

As IAs estão sendo usadas para automatizar cada vez mais tarefas, o que pode levar à perda de empregos em alguns setores, como por exemplo, as tarefas de atendimento ao cliente, de manufatura e de transporte.

Podem ser utilizadas para criar conteúdo prejudicial, como discurso de ódio, desinformação e propaganda, gerando um impacto negativo na sociedade, levando à polarização política, à violência e à instabilidade social.

Se forem treinadas em dados que refletem preconceitos humanos, as IAs podem ser discriminatórias. Por exemplo, podem ser usadas para prever a probabilidade de uma pessoa ser presa ou ser aprovada para um empréstimo, o que pode levar a discriminação racial, de gênero ou socioeconômica.

E por fim, como já foi dito, as IAs representam uma tecnologia de grande potencial, contudo, sua aplicação também tem sido aproveitada para a prática de atos maliciosos, como ataques cibernéticos ou espionagem. Observa-se um aumento na utilização dessa tecnologia por criminosos na criação de estratégias mais orgânicas e difíceis de detectar.

Aqui estão alguns dos riscos do uso da IA de forma errada e por pessoas maliciosas e que querem tirar vantagem ou aplicar golpes:

Sofisticação e Realismo Aprimorados: A IA pode ser usada para criar conteúdo cada vez mais realista e convincente. Golpistas podem desenvolver textos, imagens e até mesmo vídeos que se assemelham muito ao material legítimo, tornando os golpes mais difíceis de detectar.

Ataques Personalizados: A IA permite a análise de grandes volumes de dados para criar perfis detalhados das vítimas em potencial. Isso permite que os golpistas adaptem seus ataques para parecerem mais autênticos e relevantes para cada vítima, aumentando a probabilidade de sucesso.

Automatização e Escala: A IA pode automatizar tarefas de criação e distribuição de golpes em grande escala. Isso significa que os golpistas podem atingir um número maior de pessoas em menos tempo, aumentando suas chances de sucesso.

Geração de Conteúdo Enganoso: A IA pode criar notícias falsas, avaliações falsas de produtos e avaliações enganosas, o que pode levar as pessoas a tomar decisões com base em informações falsas.

Alguns exemplos específicos de como a IA está sendo usada para golpes incluem:

Golpes de engenharia social: Os criminosos usam a IA para manipular as vítimas para que elas realizem ações que beneficiem os criminosos. Por exemplo, os criminosos podem usar a IA para criar anúncios ou postagens de mídia social que são projetados para induzir as vítimas a clicar em links maliciosos ou fazer doações de caridade falsas.

Golpes de deepfake: Esse é um dos mais perigosos golpes, onde os criminosos usam a IA para criar vídeos e áudios falsos que parecem ser reais. Esses deepfakes podem ser usados para difamar indivíduos, espalhar desinformação ou enganar as pessoas para que elas realizem ações que beneficiem os criminosos.

Aqui estão algumas dicas para lidar com esses desafios:

a) Desenvolver políticas e regulamentações para garantir que as IAs sejam usadas de forma responsável e ética.
b) Educar o público sobre os riscos e benefícios das IAs.
c) Desenvolver IAs que sejam mais transparentes e auditáveis.
d) Investir em pesquisa para desenvolver novos métodos de controle das IAs.

Para que consigamos nos proteger contra os diversos tipos de golpes que fazem uso da Inteligência Artificial é necessário vigilância, conhecimento e algumas práticas de segurança. Aqui estão algumas dicas de segurança que devemos tomar, individualmente, para nos protegermos desses ataques:

1. Desconfie de Fontes Desconhecidas: Esteja atento a e-mails, mensagens e comunicações de fontes desconhecidas. Evite clicar em links ou baixar anexos de remetentes não confiáveis.
2. Verifique a Autenticidade: Sempre verifique a informação de um e-mail ou mensagem antes de tomar qualquer ação. Entre em contato diretamente com a empresa ou pessoa, utilizando informações de contato confiável, para confirmar a solicitação.
3. Use Senhas Fortes: Utilize senhas complexas e únicas para suas contas. Considere o uso de gerenciadores de senhas para ajudar a criar e armazenar senhas seguras.
4. Faça backup de seus dados regularmente.
5. Desenvolva um código com seus familiares. Se você receber uma ligação ou mensagem de áudio que o deixar em dúvida, basta mencionar o código para determinar se se trata de um golpe ou não.

Em resumo, a utilização crescente da Inteligência Artificial (IA) para a realização de golpes representa um desafio significativo para a segurança cibernética. Essa tecnologia possibilita a criação de estratagemas mais elaborados, personalizados e difíceis de detectar, colocando em risco a privacidade e a confiança das pessoas. Para se proteger contra esses riscos, é fundamental adotar práticas de segurança sólidas, como a verificação de fontes, o uso de senhas robustas e a conscientização sobre as táticas empregadas pelos golpistas. A vigilância constante e a educação são essenciais.

SOLUÇÕES

A Inteligência Artificial é realmente fascinante em vários sentidos. Pode facilitar a vida das pessoas em alguns aspectos, e até ajudar a dar asas à nossa imaginação. Contudo, ela também representa novos riscos aos quais precisamos ficar atentos.

Para evitar cair em golpes envolvendo inteligência artificial, é importante estar ciente das táticas usadas pelos golpistas e adotar medidas de segurança adequadas.

Há novas categorias de golpes que já estão sendo aplicados com o apoio das ferramentas de IA.

A proteção contra golpes aplicados com inteligência artificial (IA) envolve estar ciente das táticas usadas pelos golpistas e adotar medidas para se proteger. Aqui estão algumas dicas específicas para se proteger contra golpes que fazem uso da IA:

Desconfie de Comunicações Suspeitas: Esteja atento a mensagens, emails, chamadas telefônicas ou solicitações de contato que pareçam estranhas ou fora do comum. Fique alerta para mensagens automáticas que pareçam não serem geradas por seres humanos.

Verifique a Identidade do Remetente: Verifique a identidade do remetente antes de responder a qualquer mensagem ou fornecer informações pessoais ou financeiras.

Use Soluções de Segurança Online: Utilize software antivírus e antimalware confiáveis em seus dispositivos para protegêlos contra ameaças online, incluindo malwares baseados em IA.

Atualize Regularmente Seu Software: Mantenha seu sistema operacional, navegadores e aplicativos atualizados para se proteger contra vulnerabilidades conhecidas.

Use Autenticação de Dois Fatores (2FA): Sempre que possível, ative a autenticação de dois fatores para suas contas online. Isso adiciona uma camada extra de segurança.

Tenha Cuidado com Links e Anexos: Evite clicar em links ou abrir anexos de fontes desconhecidas ou suspeitas. Golpistas muitas vezes usam links maliciosos para infectar dispositivos com malware.

Verifique a Validade de Sites e Serviços Online: Certifique-se de que está usando sites e serviços legítimos, verificando a autenticidade dos sites antes de inserir informações pessoais ou financeiras.

Tenha Consciência de Chatbots Maliciosos: Esteja ciente de chatbots e assistentes virtuais que podem tentar enganá-lo. Verifique se você está interagindo com um serviço legítimo.

Aprenda sobre Detecção de Deepfakes: Familiarize-se com as tecnologias de detecção de deepfakes para identificar vídeos e imagens falsificados.

Proteja Suas Informações Pessoais: Evite compartilhar informações pessoais e financeiras sensíveis em conversas online ou com fontes não confiáveis.

Relate Golpes: Denuncie qualquer atividade suspeita às autoridades locais e às plataformas onde ocorreu o golpe.

Mantenha-se Atualizado: Esteja atento às notícias e informações sobre novas táticas de golpes envolvendo IA. Lembre-se de que a tecnologia está sempre evoluindo, incluindo a IA usada por golpistas. Portanto, é essencial permanecer vigilante e educado sobre as ameaças em constante mudança e adotar as melhores práticas de segurança digital para se proteger contra golpes aplicados com IA.

CASO CONCRETO

Golpistas estão cada vez mais empenhados em confundir vítimas usando recursos da inteligência artificial IA. O novo golpe consiste na manipulação da voz por meio de programas que imitam respiração, pausas e tom de fala, gerando frases que são enviadas por áudio ou ligação a pessoas que possam reconhecer os sons, como amigos e familiares. O objetivo é enganar e extorquir. Esse foi o caso do pai do influenciador Dario Centurione que publica vídeos com dicas e curiosidades nas redes sociais. Após receber uma ligação que supostamente seria do filho que pedia dinheiro, o homem, de 71 anos, fez um Pix de R$ 600 para o golpista. "Meu pai não desconfiou porque, segundo ele, a voz era muito parecida. Ele

falou: 'Dario, eu tinha certeza de que era a sua voz. Era o mesmo tom'", contou o influenciador. O pai de Dario só se deu conta de que havia caído em um golpe quando conversou de fato com o filho, que disse que não tinha pedido dinheiro. Fonte: https://www.r7.com/T7sj

---

ENTREVISTA

Entrevista feita com o Desenvolvedor de Smart Contracts Samuel Barbosa (https://www.linkedin.com/in/samuel-barbosa-599859244)

[entrevista realizada por Flávio Martins Braz, via Skype e editada para maior clareza]

Fale um pouco sobre você, por gentileza.

Sou Samuel Barbosa dos Santos, um desenvolvedor de software de 33 anos nascido no Rio de Janeiro, Brasil, e atualmente residindo em Medellín, Colômbia. Sou especializado em tecnologias de ponta, como apps para Android, blockchains e inteligência artificial.

Nestes últimos anos, temos visto avanços assombrosos nas possibilidades das tecnologias de Inteligência Artificial. Com isto, alguns setores da Sociedade tem manifestado grandes receios sobre os possíveis impactos desta tecnologia. Você acredita que estes medos têm fundamento?

Sim e não (risos). Veja: uma tecnologia transformadora como a Inteligência Artificial certamente não trará apenas malefícios, tampouco apenas benefícios. A pergunta mais difícil é: o saldo final será positivo o suficiente para justificar o uso desta tecnologia? Eu tenho a tendência a acreditar que sim.

Em sua opinião: quais as áreas que podem ser mais radicalmente impactadas pelos avanços na Inteligência Artificial?

É mais fácil você me perguntar quais áreas não seriam impactadas! (risos) O avanço da tecnologia de Inteligência Artificial pode simplesmente mudar os horizontes da humanidade como os conhecemos hoje em dia: desde os serviços de Saúde Pública, passando pelo impacto em Programas de Bem-Estar Social, Sustentabilidade Energética e, até mesmo,

avanços significativos em programas de Exploração Espacial. As possibilidades são diversas e praticamente infinitas.

Mas e quanto à dissolução de empregos? A automatização impulsionada pela IA não tem grandes chances de afetar os empregos e aumentar a desigualdade de rendimentos?

Com certeza, estas são preocupações válidas e, de certa forma, até inevitáveis. Para enfrentar estes desafios, deve haver investimentos em programas de educação e formação que preparem os trabalhadores para mercados de trabalho em evolução quanto a este quesito tecnológico. Além disso, em minha opinião, num futuro próximo pode ser necessário explorar modelos econômicos alternativos, como a renda básica universal, para garantir a estabilidade social. Cidades como Tacoma, em Washington, já estão realizando experiências neste sentido.

Você falou sobre os possíveis impactos positivos da I.A. na Saúde Pública, na Sustentabilidade Energética, dentre outros. Você pode elaborar um pouco mais sobre estas possibilidades?

Em relação à Saúde, a IA pode melhorar e muito o acesso dos pacientes, graças à monitoração remota e a telemedicina, uma vez que a precisão e a velocidade do diagnóstico analisando imagens médicas e dados de pacientes irá avançar enormemente. Além disso, a tendência é da análise preventiva identificar com grande antecedência os surtos de doenças e recomendar medidas de prevenção, auxiliando inclusive na elaboração de políticas públicas. Neste cenário, dificilmente teríamos chegado ao caos coletivo que se instaurou durante a pandemia.

No quesito da Sustentabilidade Energética e Ambiental, a IA deverá otimizar o consumo de energia em edifícios e indústrias; ajudar na implementação de uma agricultura de precisão que melhore o rendimento das colheitas; os modelos de previsão climáticas devem se aperfeiçoar imensamente, dentre dezenas de outras possibilidades que ajudem na conservação ambiental e climática do planeta.

Mas estes são meros exemplos. Temos possibilidades da I.A. auxiliar em avanços na Educação, no Transporte Público, na vida Financeira das pessoas, dentre dezenas e, talvez, centenas de outras áreas da vida individual e em sociedade.

Você certamente transmite muito otimismo em suas opiniões sobre I.A. Mas e quanto aos riscos? Em sua opinião, quais são os pontos em que a humanidade deve ter mais atenção e cuidado no desenvolvimento e implementação em larga escala destas tecnologias?

As preocupações éticas são fundamentais. À medida que os sistemas de IA se tornam mais independentes, as questões relacionadas com o preconceito, a transparência e a

responsabilização se tornam infinitamente complexas. A sociedade precisa estabelecer diretrizes e padrões éticos claros para esta implantação da IA, de maneira preventiva, para evitar ao máximo cenários imprevistos.

Certamente, ataques cibernéticos e campanhas de desinformação poderão representar ameaças consideráveis à sociedade. Melhorar a segurança e a responsabilização da IA é essencial, e isto exige inovação contínua nas medidas de segurança cibernética, regulamentações mais rigorosas e, sobretudo, cooperação internacional para combater estas ameaças, que muito provavelmente irão transpor os limites de fronteiras regionais.

Você acredita na possibilidade de um evento catastrófico facilitado pela implementação destas tecnologias de Inteligência Artificial?

Apesar de, pessoalmente, não ter muito receio deste tipo de "hecatombe", a preocupação de vários setores da sociedade com estes eventos catastróficos é essencial, pois acaba requerendo planejamento e vigilância a longuíssimo prazo. E isto é ótimo. À medida que os sistemas de IA se tornam mais interligados e independentes, aumenta o potencial de falhas em grande escala ou de consequências indesejadas. Então, este tipo de preocupação ajuda a criar esforços de investigação contínua, de testes rigorosos e medidas proativas para detectar e responder a potenciais catástrofes.

Para finalizar: como você imagina que a Sociedade poderá estar em 20 anos, graças à adoção em larga escala destas tecnologias que discutimos?

Seria mais fácil você me perguntar os números da loteria de fim de ano (risos). Mas acredito que é seguro afirmar que veremos experiências altamente personalizadas em saúde, educação e entretenimento, impulsionadas pela capacidade da IA de compreender e atender às necessidades individuais. A automação irá remodelar as indústrias, com maior foco em profissões criativas e baseadas no conhecimento, enquanto as ferramentas e a robótica alimentadas pela IA irão auxiliar nas tarefas repetitivas. Os transportes serão mais seguros e eficientes, graças a veículos autônomo. Os desafios globais, como as alterações climáticas, serão abordados de forma mais proativa com soluções baseadas na IA.
No entanto, considerações éticas, como a privacidade dos dados e o acesso igualitário aos benefícios da IA continuarão a ser preocupações sociais críticas, e provavelmente iremos necessitar de regulamentações robustas e discussões contínuas sobre o papel da IA nas nossas vidas.

Obrigado pela entrevista!

Obrigado pela atenção e sucesso em seu trabalho.