

APSEI Trabalho 3

Guilherme nº 107162, Rafael nº 107340, Rodrigo nº107634

April & May 2024

Índice

Contents

1	<i>Copilot Realístico</i>	3
1.1	Desafios Tecnológicos	3
1.2	Leis e Regulamentos	3
1.3	Escalabilidade e Custo	3
2	Veículos Autónomos	4
2.1	Desafios Tecnológicos	4
2.2	Leis e Regulamentos	4
2.3	Escalabilidade e Custo	4
3	Drones	5
3.1	Desafios Tecnológicos	5
3.2	Leis e Regulamentos	5
3.3	Escalabilidade e Custo	5
4	Assistente Pessoal	6
4.1	Desafios Tecnológicos	6
4.2	Leis e Regulamentos	6
4.3	Escalabilidade e Custo	6

1 *Copilot* Realístico

1.1 Desafios Tecnológicos

Na primeira cena, foi identificada uma tecnologia que se assemelha a um "copilot realístico". O *Github Copilot* é uma ferramenta de programação que tem como função auxiliar programadores durante o processo de escrita de código, fornecendo sugestões em tempo real diretamente no IDE. O que é sugerido no vídeo distingue-se dessa ferramenta, uma vez que a comunicação é feita por voz e expressões faciais, em vez de texto.

Em teoria, já existem tecnologias com IA que nos permitem algo semelhante: Como referido, o *Github Copilot* é usado para a análise de código; O *Chat-GPT* da *OpenAI* tem a capacidade de humanizar a interação com o utilizador; O *VASA-1* da *Microsoft* é uma IA desenvolvida para representação facial. Todas estas tecnologias são totalmente ou parcialmente controladas pela Microsoft, no entanto, uma vez que cada uma delas tem os seus próprios requisitos, tornaria a integração complexa.

A maior limitação atual das ferramentas de IA é o conhecimento destas se encontrar limitado no tempo, não podendo assim estar cientes de eventos ou informações posteriores a última data de treino. Este caso implicaria uma constante atualização dos dados de treinos, para permitir que o sistema possa acompanhar a evolução tecnológica das várias linguas e ferramentas de programação.

Para além disso, é também lógico que no dia de hoje, embora a IA possa reconhecer e responder a emoções, ela não tem emoções próprias e pode não entender completamente o contexto emocional.

Em termos de questões de privacidade e ética, estas são uma grande preocupação. A IA teria de ser projetada para respeitar a privacidade do programador e seguir diretrizes éticas rigorosas, mas ao mesmo tempo conseguir utilizar o código como fonte de aprendizagem.

1.2 Leis e Regulamentos

As leis e regulamentos atuais relacionados à privacidade de dados podem, de facto, ser um problema para a implementação de tecnologias de IA como um "copilot realístico". O GDPR, na Europa, exige que as empresas protejam os dados pessoais dos utilizadores, o que pode tornar-se um problema, uma vez que a qualidade e utilidade de uma IA depende proporcionalmente da quantidade de dados a que tem acesso.

Há ainda questões legais que podem levar à origem de problemas relacionados a direitos autorais, uma vez que é possível que uma IA gere um pedaço de código semelhante a conteúdo protegido de outros utilizadores.

Para além de vir a ser necessária a criação de novos regulamentos, para a implementação desta tecnologia, existem bastantes leis que teriam de ser adaptados, o que torna a implementação deste "Copilot realístico" difícil de acontecer. Assim como questões de ética e algumas tomadas de decisão, que deveriam ser impostas por lei em casos extremos.

Deveriam também serem criadas leis em torno da transparência das IA em cada empresa. Não seria uma tarefa fácil, pois os algoritmos são bastante complexos, mas seria um bem necessário para cada utilizador saber como a IA usa os seus dados, o que aumentaria a confiança na tecnologia.

1.3 Escalabilidade e Custo

Implementar um "copilot realístico" em toda a Europa teria um grande impacto pois seria necessário um grande investimento em infraestruturas, incluindo data centers e servidores, para lidar com o aumento das necessidades de processamento e armazenamento de dados.

Para além disso, as grandes preocupações desta implementação a nível europeu, estariam relacionadas com a privacidade e segurança dos dados, dadas as rigorosas leis de proteção de dados na Europa. Posto isto, as empresas precisariam de garantir que estão em conformidade com esses regulamentos, o que poderia aumentar os custos operacionais.

Escalar uma IA desde tipo faria com que o sistema precisasse de lidar com um grande volume de dados, o que poderia sobrecarregar a capacidade do servidor. Para além disso, uma vez que o sistema teria de lidar com várias entradas do utilizador, relacionadas a diversos contextos, iria exigir recursos computacionais ainda maiores. E portanto haveria ainda o problema de garantir a robustez e confiabilidade do sistema. Ainda sobre a questão do crescimento dos dados, seria uma prioridade máxima garantir a segurança e privacidade dos dados sensíveis do utilizador, para prevenir cyber-ataques.

2 Veículos Autónomos

2.1 Desafios Tecnológicos

Na segunda cena, somos confrontados com um carro elétrico, que se movimenta no trânsito, lado a lado tanto de carros homólogos, como também de carros "normais". Esta é a tecnologia que apresenta o maior número de desafios. Desde a tomada de decisões, à remoção de condutores humanos, passando pela condição das estradas e até mesmo assuntos mais divisórios como a mineração de lítio para as baterias dos carros.

Enfrentamos também várias limitações neste processo: por exemplo, a presença de condutores humanos apresenta uma vulnerabilidade ao sistema, devido à natureza imprevisível. A tomada de decisões dos veículos autónomos é outro desafio crucial, pois envolve a criação de algoritmos complexos que devem considerar uma variedade de variáveis em tempo real para garantir a segurança dos passageiros e peões que se encontrem na estrada.

2.2 Leis e Regulamentos

A lei permite a circulação dos automóveis autónomos. Segundo a Society of Automotive Engineers (SAE), estes veículos encontram-se atualmente no nível 2 (Exemplo: Tesla) de condução autónoma - *o condutor é obrigado a detetar objetos ou ocorrências e reagir se o sistema automatizado falhar*. o nível máximo é o 5 - *para além de definir o destino e ligar o sistema, não é necessária a intervenção humana na condução*, que é o que é visualizado no clipe.

Atualmente o carro de maior nível é carro Waymo (nível 4)

Sobre a legislação relativo a culpabilidade em caso de acidentes, os fabricantes têm diferentes entendimentos quanto à responsabilidade que pretendem assumir. (*A Volvo afirma que se irá responsabilizar pelos danos causados pelos seus veículos*. *A Tesla afirma que devem ser as seguradoras do condutor a assumir a responsabilidade*)

É essencial definir leis sobre a culpa em caso de acidentes. no cenário futuro, em que os carros se encontram no nível 5, não havendo intervenção humana na condução, é essencial que a culpa não seja sua.

De relembrar também que um veículo autónomo enquadra-se na categoria de *High Risk* do *European AI Act*. Assim sendo, tem de corresponder às seguintes regras: existência de sistemas de mitigação e avaliação de riscos, databases de alta qualidade para reduzir os riscos de resultados discriminatórios, *logging* da atividade, documentação extensa, supervisão humana e um bom nível de robustez, segurança e precisão.

2.3 Escalabilidade e Custo

A implementação de veículos autónomos em toda a Europa teria um impacto significativo em termos de escalabilidade e custo. Logo à partida, mais veículos autónomos nas estradas significariam menos ação humana no tráfego, que mitigaria acidentes, aumentando a segurança na estrada.

No entanto, os custos económicos e ambientais de fabricação desses veículos seriam bastante altos, devido à dependência de lítio para as baterias, uma vez que a mineração de lítio é dispendiosa, além ainda dos impactos ambientais significativos, desde a contribuição para o aumento do aquecimento global à perda de biodiversidade, devido à degradação de solos.

Além disso, a manutenção das estradas teria que ser rigorosa para garantir que todas estejam em condições de satisfazer a navegação segura dos carros. Em termos de escalabilidade, este sistema enfrentaria desafios como a integração de sistemas de trânsito já existentes e a garantia de que houvesse uma correta coordenação e comunicação entre os diversos veículos.

3 Drones

3.1 Desafios Tecnológicos

No vídeo, é apresentada a ideia de um cidadão a ser abordado por um "drone polícia": essa pessoa está a comunicar com um polícia, não presencialmente na estrada, mas sim, através de um ecrã, que se encontra no drone.

Assume-se que esse drone é controlado à distância pelo polícia. Podemos desde logo, encontrar possíveis limitações ao uso desta tecnologia, como a autonomia do drone (quanto tempo aguenta o drone a circular, antes de carregar) e o alcance do mesmo (em relação ao seu controlador)

3.2 Leis e Regulamentos

Segundo a legislação portuguesa, qualquer pessoa que possua um drone com menos de 25kg, pode sobrevoá-lo até uma altitude de 120m, com a condicionante de não poder sobrevoar concentrações de pessoas ou transportes de mercadorias perigosas.

Para utilizar um drone com dimensões superiores às referidas anteriormente, é obrigatório apresentar um manual de operações e um ERP (Plano de Resposta a Emergências), podendo com isso, e, solicitando autorização à ANAC (Autoridade Nacional de Aviação Civil) ultrapassar os 120m de altitude e sobrevoar concentrações de pessoas e transporte de mercadorias perigosas.

Em relação à captura de imagens, através desde dispositivo, legislação remete para a Comissão Nacional de Proteção de Dados e para a Força Aérea Portuguesa, sendo mandatório comunicar a intenção de tirar fotografias ou gravar vídeos com o drone.

Posto isto, aplicando o cenário mostrado no vídeo, não seriam necessárias grandes mudanças na lei, uma vez que a polícia facilmente teria as autorizações necessárias, para sobrevoar os espaços que desejasse e capturar as imagens que necessitasse.

3.3 Escalabilidade e Custo

Primeiramente, seria necessário estabelecer políticas e legislações relacionadas com privacidade e segurança, abrangíveis a todos os países europeus.

Além disso, seria essencial investir no treino dos agentes da polícia que estariam responsáveis por controlar os drones.

Em relação à implementação, esta teria de ser feita sobre uma infraestrutura de comunicação robusta e distribuída, de modo a coordenar o maior número possível de drones na maior área possível e, além disso, e uma vez que os drones seriam usados pelos serviços de segurança pública, seria necessário uma interoperabilidade entre os sistemas de comunicação do aparelho com os serviços de emergência existentes

4 Assistente Pessoal

4.1 Desafios Tecnológicos

O desenvolvimento de um Assistente Pessoal baseado em inteligência artificial enfrenta vários desafios tecnológicos. Em primeiro lugar, é crucial garantir uma compreensão precisa e contínua da linguagem natural, para que o assistente possa interpretar com precisão os comandos e perguntas dos utilizadores. Além disso, a capacidade de aprender e adaptar-se às preferências e padrões de uso de cada utilizador é essencial para fornecer uma experiência personalizada e eficaz.

A integração de várias tecnologias de IA, como processamento de linguagem natural (NLP), reconhecimento de voz e aprendizado de máquina, é necessária para criar um assistente robusto e versátil. A coordenação eficiente entre essas tecnologias é fundamental para garantir um desempenho suave e uma interação natural com o utilizador.

Garantir a privacidade e a segurança dos dados do utilizador é uma preocupação central. O assistente deve ser projetado para proteger as informações pessoais dos utilizadores e cumprir os regulamentos de privacidade de dados, como o GDPR, para evitar violações de privacidade e fuga de dados.

4.2 Leis e Regulamentos

As leis e regulamentos atuais podem apresentar desafios significativos para a implementação de um Assistente Pessoal de IA. Regulamentações como o GDPR estabelecem padrões rigorosos para a proteção de dados pessoais dos utilizadores, o que requer medidas robustas de segurança e privacidade por parte dos desenvolvedores do assistente.

Além disso, questões relacionadas à propriedade intelectual e direitos de autor podem surgir, especialmente no caso de assistentes que fornecem informações protegidas por direitos de autor ou criam conteúdo original, como música ou literatura.

Para implementar um Assistente Pessoal de IA dentro dos limites legais e regulatórios, é necessário garantir a conformidade com as leis de proteção de dados e privacidade, implementando medidas adequadas de segurança e consentimento do utilizador. Isso pode envolver a anonimização de dados pessoais sempre que possível e fornecer aos utilizadores controle sobre suas informações.

Além disso, as questões de propriedade intelectual devem ser cuidadosamente consideradas, e os desenvolvedores do assistente devem garantir que o conteúdo fornecido não infrinja os direitos de autor ou outras leis de propriedade intelectual.

4.3 Escalabilidade e Custo

Implementar um Assistente Pessoal de IA em toda a Europa teria implicações significativas em termos de escalabilidade e custo. Seria necessário um investimento substancial em infraestrutura de servidores e capacidade de processamento para lidar com o aumento da demanda e garantir uma resposta rápida e confiável em toda a região.

Além disso, questões relacionadas à privacidade e conformidade regulatória exigiriam recursos adicionais para garantir que o assistente esteja em conformidade com as leis de proteção de dados em todos os países europeus.

Escalar um Assistente Pessoal de IA para uma implementação em toda a Europa pode enfrentar desafios significativos de escalabilidade. O aumento do volume de utilizadores e solicitações pode sobrecarregar a infraestrutura de servidores e resultar em tempos de resposta mais lentos e instabilidade do sistema.

Além disso, a personalização e adaptação do assistente para atender às preferências e necessidades de uma base de utilizadores diversificada em toda a Europa pode exigir recursos computacionais consideráveis e técnicas avançadas de aprendizado de máquina.

Garantir a segurança e privacidade dos dados dos utilizadores em uma escala tão ampla seria também um desafio significativo, exigindo medidas robustas de segurança cibernética e conformidade regulatória em todos os níveis do sistema.