

**universidade de aveiro**  
theoria poiesis praxis

## Trabalho Prático 3

**Aspetos Profissionais e Sociais da Engenharia Informática**

**Tomás Brás**  
NMec - 112665

**Carolina Silva**  
NMec - 113475

**Afonso Ferreira**  
NMec - 113480

May 7, 2025

## 1 Corrigir código num carro autónomo

**Corrigir código num carro autónomo**

**Aspectos identificados no vídeo:**

- O protagonista corrige erros com a ajuda de um assistente de IA com aparência humana que interage em tempo real com o protagonista, auxiliando no processo de debugging
- O protagonista corrige erros dentro de um carro autónomo (**Condução Nível 5**)



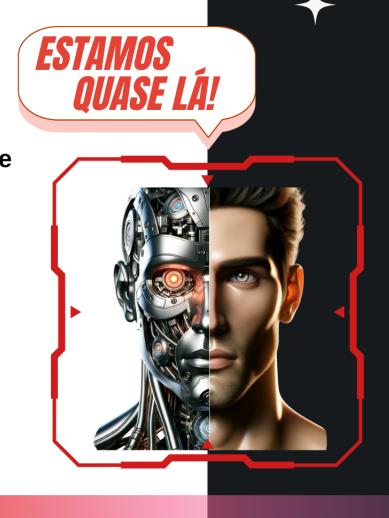
Na primeira cena, vemos o protagonista a corrigir código com erros dentro de um carro. Ele não está a fazê-lo sozinho, conta com a ajuda de um assistente de IA que se assemelha muito a uma pessoa real, e que conversa com o protagonista para o ajudar a escrever o código. O código está a ser projetado no ecrã frontal do carro, enquanto o veículo conduz-se de forma autónoma.

### 1.1 Desafios Tecnológicos

**DESAFIOS  
TECNOLÓGICOS A ULTRAPASSAR**

Quais são os principais desafios tecnológicos que identificas e que precisam de ser resolvidos?

- Dificuldade em criar avatares digitais verdadeiramente convincentes
- **Uncanny Valley**
- Ainda não existem modelos com compreensão total de contexto, intenção e timing para intervir naturalmente durante a programação.
- Decisões como travagem ou desvio exigem latências muito baixa inviável com cloud.



Vivemos atualmente num mundo onde a inteligência artificial nunca foi tão poderosa, mas integrar uma IA que nos ajude a escrever código com aparência e comportamento humano, funcionando como um parceiro de *pair-programming*, tudo isto dentro de um carro autónomo, representa um enorme desafio tecnológico.

Começando pelo facto de o agente IA ter uma aparência humana: A criação de agentes hiper-realistas tem evoluído de forma impressionante, como podemos ver na Synthesia [1], um software que permite criar avatares digitais que conseguem replicar expressões, voz e movimentos humanos, mas que ainda são facilmente identificáveis como artificiais. Pequenas imperfeições nas microexpressões faciais e a falta de naturalidade nas pausas e ritmos da fala contribuem para o fenómeno conhecido como *uncanny valley*.

Para além disso, a IA teria que demonstrar algum tipo de opinião e emoção, visto que no fim da cena o agente afirma de forma entusiasmada: "Mas, estamos tão perto!" quando o protagonista começa a desligar o dispositivo. Atualmente, os modelos de IA não oferecem este tipo de funcionalidade. As IAs modernas, como o ChatGPT ou o DeepSeek, apesar de conseguirem gerar respostas empáticas, continuam a ser sistemas sem sentimentos reais. Respondem com base em padrões de linguagem, sem qualquer consciência ou emoção genuína.

Outro aspeto importante prende-se com o facto de o agente de IA intervir proativamente, dando sugestões de correção de código sem que o utilizador tenha feito um pedido explícito. Para que isso fosse possível, o sistema teria de possuir uma capacidade avançada de compreensão de contexto e intenção, algo que hoje está longe de estar resolvido. Esta funcionalidade exigiria modelos capazes de monitorizar continuamente o ambiente de programação, detetar padrões de erro ou ineficiência, e decidir se e quando intervir. Além disso, seria necessário desenvolver mecanismos de interação social sofisticados, para que o agente soubesse como agir de forma natural, sem interromper ou incomodar o utilizador. Esta forma de assistência contínua e personalizada representa um dos maiores desafios da IA conversacional moderna.

Além dos desafios relacionados com a própria IA, existe também a complexidade da infraestrutura necessária para que toda a experiência ocorra dentro de um carro autónomo. No caso da condução autónoma, a necessidade de computação local em tempo real é absolutamente crítica. Um carro autónomo depende da rápida interpretação de dados provenientes de sensores como câmaras, radares, LIDARs e ultrassons para tomar decisões em frações de segundo. Delegar esse processamento a servidores remotos na cloud criaria atrasos fatais, mesmo uma latência de 100 milissegundos já pode comprometer a capacidade de travar ou desviar de um obstáculo a tempo. Por essa razão, os veículos autónomos seriam equipados com plataformas de *edge computing* altamente especializadas,

No contexto da interação com o programador, esta limitação de conectividade também afeta o desempenho do agente IA. Se o avatar estivesse dependente da cloud para processar linguagem natural, renderizar a fala ou gerar expressões faciais, qualquer falha de rede resultaria numa experiência frustrante ou artificial. Assim, também aqui seria essencial que os componentes mais críticos fossem processados localmente no carro, recorrendo a servidores de bordo que assegurassem um desempenho fluido, mesmo em ambientes com fraca cobertura de rede.

## 1.2 Leis e Regulação

### OBSTÁCULOS LEGAIS E REGULAMENTARES

#### A legislação atual permite os cenários apresentados?

- A legislação é bastante restritiva na União Europeia e em Portugal.
- Código da Estrada exige sempre a presença de um condutor capaz de assumir o controlo.
- Carros com autonomia total (nível 5) não podem circular legalmente em vias públicas.



#### A legislação atual permite os cenários apresentados?

- Criação de um enquadramento legal que reconheça veículos autónomos como agentes operacionais.
- Definição clara de responsabilidade em caso de acidente
- Adaptação das leis de seguros para focarem falhas técnicas em vez do comportamento humano.
- Implementação de normas éticas sobre decisões automatizadas em situações de risco.
- Existência de uma black box

#### Quais são as limitações legais e sociais a ultrapassar?

- Responsabilidade legal
- Privacidade
- Ética e aceitação social
- Seguros

Na União Europeia, incluindo Portugal, a legislação sobre veículos autónomos ainda é cautelosa. O Regulamento (UE) 2019/2144 impõe normas rigorosas de segurança para veículos com condução assistida. O AI Act (2024) classifica sistemas de condução autónoma como "IA de alto risco", exigindo certificações e monitorização contínua.

Em Portugal, o Código da Estrada exige a presença de um condutor capaz de assumir o controlo do veículo. Testes com condução autónoma teriam de ser realizados em zonas piloto sem circulação pública.

Para além dos desafios técnicos e infraestruturais, o desenvolvimento de sistemas de condução autónoma enfrenta também barreiras significativas ao nível da proteção de dados pessoais, especialmente no contexto europeu, regulado pelo RGPD (Regulamento Geral sobre a Proteção de Dados).

O RGPD exige consentimento explícito para a utilização de dados sensíveis como imagem, voz ou biometria, o que protege a privacidade de condutores, passageiros e terceiros. No entanto, este requisito torna-se um obstáculo no treino de modelos de inteligência artificial, uma vez que os veículos autónomos necessitam de captar, de forma contínua, informações do ambiente incluindo peões, ciclistas e outros condutores para funcionarem e melhorarem.

A eficácia destes sistemas depende da análise de grandes volumes de dados reais de condução. Contudo, o RGPD impõe fortes restrições à recolha e reutilização desses dados, sobretudo quando contêm identificadores pessoais como rostos, matrículas ou padrões comportamentais. Na União Europeia, os dados usados para treino de modelos devem ser obrigatoriamente anonimizados ou devidamente filtrados para impedir a identificação de indivíduos ou de informações pessoais.

Esse processo de anonimização, embora essencial do ponto de vista legal e ético, pode reduzir significativamente a qualidade e utilidade dos dados, limitando o avanço técnico dos modelos de IA. Isto é particularmente relevante em cenários complexos, como o reconhecimento de expressões humanas ou a leitura precisa do contexto envolvente, onde detalhes identificáveis podem ser fundamentais.

Além disso, em situações de investigação de acidentes, os fabricantes podem necessitar de aceder aos registos do veículo para apurar responsabilidades. Visto que estamos a lidar com um possível crime ou infração rodoviária, a recolha e análise destes dados pode ser legalmente justificada no âmbito de interesse público.

Perante isto, torna-se evidente a necessidade de encontrar um equilíbrio entre a recolha de dados essenciais para a segurança e evolução tecnológica, e a salvaguarda dos direitos fundamentais à privacidade. Tal equilíbrio pode exigir a criação de regulamentação específica e adaptada ao setor dos veículos autónomos, capaz de garantir tanto a inovação como a proteção dos cidadãos.

Mesmo com condução assistida, o condutor, atualmente, continua legalmente responsável por quaisquer acidentes. Este facto cria um impasse jurídico para automóveis de nível 5. Nestes casos, quem seria o responsável? O condutor, o fabricante, o programador? Isto exigiria reformular todo o sistema de seguros, com base em riscos técnicos e não humanos.

Além disso, carros autónomos teriam de ser programados para tomar decisões morais em situações extremas, como proteger o condutor ou um peão. Estas decisões éticas precisariam de ser codificadas e comunicadas de forma transparente, levantando questões sociais e jurídicas complexas.

Também existe a questão de como é que o funcionamento e as regras dos carros variariam de país para país. Apesar da existência de regulamentos europeus, cada membro mantém autonomia para legislar localmente sobre a circulação rodoviária, o que cria um cenário fragmentado.

Em países como Portugal ainda exigem a presença física de um condutor com capacidade de assumir o controlo a qualquer momento, mesmo em testes experimentais.

Nos Estados Unidos, a Califórnia permite testes de veículos autónomos sem condutor presente, mas o Texas tem regras menos restritivas e incentiva empresas a desenvolver e operar veículos autónomos com maior liberdade. Esta disparidade global complica a padronização de sistemas de condução autónoma, já que os fabricantes teriam de configurar o comportamento do veículo de acordo com a legislação local de cada país (ou mesmo de cada estado, no caso dos Estados Unidos da América).

Portanto, para que o cenário de condução totalmente autônoma se torne viável a nível internacional, será necessário um esforço de harmonização regulatória, tanto ao nível da União Europeia como em cooperação com outros blocos económicos o que nos dias hoje não parece propriamente fácil. Este esforço deverá incluir acordos sobre padrões técnicos, segurança cibernética, privacidade de dados e responsabilidade civil, garantindo que os veículos possam operar legalmente e de forma segura em qualquer jurisdição.

Adicionalmente, a integração de uma caixa negra no carro tornaria-se essencial para garantir segurança, rastreabilidade e responsabilidade legal. Este dispositivo, tecnicamente conhecido como

EDR (Event Data Recorder), registaria continuamente parâmetros críticos do veículo e do sistema de IA antes, durante e após qualquer acidente. A sua função seria armazenar dados como velocidade, travagens, uso do cinto, funcionamento dos sistemas autónomos e as respetivas decisões tomadas. Em caso de acidente ou falha, esta informação seria vital para identificar com precisão se o erro foi humano, técnico ou algorítmico. Em julho de 2024, este tipo de registo tornou-se obrigatório na União Europeia para todos os veículos novos vendidos no espaço europeu, conforme definido pelo Regulamento (UE) 2019/2144.

### 1.3 Escalabilidade e Custo

#### 1.3.1 Ajudante na Correção de Código

## ESCALABILIDADE E DESAFIOS

- Latência e instabilidade da internet em movimento inviabilizam dependência exclusiva da cloud.
- Alto custo de hardware por veículo.
- Complexidade em manter atualizações frequentes dos modelos IA embarcados.
- Fragmentação legal entre países dificulta uma produção e operação padronizada.
- Elevado consumo energético dos modelos em tempo real embarcados.
- Manutenção e suporte técnico exigem infraestrutura robusta.
- **Evolução tecnológica pode reduzir custos e facilitar a adoção.**



Como já se tinha falado em integrar os modelos nos próprios veículos, a escalabilidade não seria necessariamente um problema, visto que, desde que tivéssemos a tecnologia e o processamento necessário para este modelo, não existiria problema.

Quanto aos custos, apesar dos custos de treino de modelos ser bastante elevado, dentro da casa dos milhões já vimos exemplos onde este custo pode estar a diminuir se encontrarmos as ferramentas corretas. Um exemplo disto é a DeepSeek que treinou o seu modelo R1 por apenas 5,6 milhões de dólares, utilizando chips menos potentes. Este custo é significativamente inferior aos 78 milhões de dólares estimados para o treino do GPT-4 pela OpenAI. [2]

No entanto, é importante distinguir entre o custo de treino e o custo de operação (inferência). Embora o custo de treino esteja a tornar-se mais acessível com novas abordagens, a operação em larga escala de um modelo integrado num veículo continua a implicar desafios significativos, como um consumo energético elevado, especialmente com o modelo a operar continuamente em tempo real.

Um assistente de IA embarcado precisa de atualizações frequentes para acompanhar novas linguagens de programação ou melhorias nos modelos de aprendizagem. Como a conectividade em veículos pode ser limitada, seria necessário implementar um sistema seguro de atualizações offline ou híbridas, o que aumenta os custos operacionais.

#### 1.3.2 Condução Autónoma

A nível de infraestrutura, a alternativa de realizar o processamento de dados exclusivamente na cloud não é viável em muitos contextos, devido à latência e instabilidade da ligação à internet em movimento. Assim, a solução mais eficaz passa por integrar unidades de edge computing em cada veículo. No entanto, estas unidades requerem hardware de alto desempenho, que representa um custo elevado por unidade [3].

Adicionalmente, há custos contínuos associados à manutenção do sistema autónomo: calibração de sensores, atualizações de software, testes de segurança e suporte técnico especializado. A gestão de uma frota de veículos autónomos exige também plataformas de monitorização e controlo centralizado, o que implica investimentos em servidores, redes e equipas técnicas [4].

Outro aspecto relevante é o custo de adaptação à legislação local. Como não existe uma regulamentação global unificada, os fabricantes têm de adaptar os seus sistemas aos requisitos legais de cada país ou estado. Esta fragmentação limita a produção em massa padronizada, forçando soluções específicas por região, o que reduz a eficiência e aumenta os custos operacionais [5].

Apesar de todos estes desafios, a escalabilidade da condução autónoma tem vindo a tornar-se mais viável graças à evolução de chips especializados (como os da NVIDIA ou da Mobileye), à melhoria dos algoritmos de visão computacional e ao crescente apoio institucional a projetos-piloto. Com o tempo, espera-se que os custos desçam progressivamente, tal como aconteceu com outras inovações tecnológicas, permitindo uma adoção mais generalizada [6].

## 2 Transição de Condução Autónoma para Manual com Comando

### Transição de condução: Autónoma para Manual com comando

**Aspectos identificados no vídeo:**

- Condutor pede para limpar lente da câmara e desliga a Inteligência artificial do carro com tecla "delete".
- Conecta comando via USB e assume a condução do carro, sendo esta muito imprudente



Na segunda cena, observamos o condutor a interromper a condução autónoma do veículo através de um comando, possivelmente de videojogos. O carro, desprovido dos elementos tradicionais de controlo como volante, pedais ou travão de mão, é equipado apenas com uma câmara, um teclado sem fios e cinco entradas USB tipo B. Antes de assumir o controlo, o condutor dá ordem ao sistema para limpar a lente da câmara, impedindo assim a captação de imagens das suas ações. Em seguida, carrega na tecla “delete” do teclado, desativando por completo a condução autónoma. Conecta então o comando de videojogos a uma das entradas USB e passa a conduzir manualmente, adotando uma postura de condução claramente imprudente.

### 2.1 Desafios tecnológicos

### DESAFIOS TECNOLÓGICOS A ULTRAPASSAR

**Quais são os principais desafios tecnológicos que identificas e que precisam de ser resolvidos?**

- Desligar a IA com uma tecla é altamente improvável e inseguro.
- A condução autónoma e a IA não são separáveis nos sistemas atuais.
- Comando de videojogos ainda não garantem precisão ou segurança adequadas.
- Empresas como a Tesla testam protótipos, mas não são autorizados em vias públicas.
- Ética do florescimento humano propõe decisões baseadas no contexto e dignidade.



A condução autónoma foi concebida com o propósito de aumentar a segurança rodoviária, reduzir o número de acidentes — dos quais mais de 90% resultam de erro humano —, otimizar o tráfego e diminuir as emissões de carbono. No entanto, ao analisarmos o vídeo, identificamos duas situações que desafiam os limites da tecnologia atual: a desativação da inteligência artificial (IA) do automóvel em movimento e o controlo subsequente do veículo através de um comando de videojogos.

No mundo real, fabricantes como a Tesla permitem que o condutor assuma o controlo a qualquer momento, interrompendo o modo de condução autónoma. Contudo, o sistema de IA não é desligado: entra num estado de espera, onde continua a monitorizar o ambiente, a recolher dados e a ativar funcionalidades de segurança como travagem automática, manutenção de faixa ou alertas de colisão. Isto garante que, mesmo em modo “manual”, o veículo mantém um nível mínimo de assistência à condução, aumentando a segurança dos ocupantes e de outros utentes da estrada.

No vídeo, o condutor ordena ao veículo que limpe a lente da câmara e, em seguida, pressiona a tecla “delete” num teclado externo, aparentemente desativando a IA. Ainda assim, o carro continua em movimento, sugerindo que a condução autónoma e a inteligência artificial são sistemas operacionais distintos ou que podem ser controlados separadamente. Na realidade, tal cenário é altamente improvável. Permitir que um utilizador desligue completamente a IA durante a condução representaria um risco grave para a segurança de todos os ocupantes e demais utentes da via.

Por este motivo, os sistemas operativos dos veículos autónomos são protegidos contra alterações não autorizadas. Apenas técnicos especializados, com permissões específicas e mediante protocolos rigorosos, podem aceder à infraestrutura crítica da IA. Assim, a possibilidade de desligar a IA através de uma simples tecla física como mostrado no vídeo é incompatível com os princípios de segurança implementados na tecnologia atual. Caso tal funcionalidade fosse concebida, exigiria sistemas de autenticação avançados e múltiplos níveis de verificação de segurança.

Após a desativação da IA, o condutor conecta um comando de videojogos via porta USB-B e assume totalmente o controlo do carro. Embora este conceito pareça futurista, várias empresas já experimentam o uso de comandos em ambientes de teste, investigação e demonstração. A Tesla, por exemplo, desenvolveu o protótipo *Cybercab*, um táxi autónomo sem volante nem pedais, que pode ser controlado através de um comando semelhante ao da Xbox. Este dispositivo permite controlar a direção e a aceleração por cabo ou até remotamente, funcionando de forma semelhante a um carro de controlo remoto.

Contudo, esta abordagem ainda não é permitida em circulação real. O uso de comandos levanta sérias preocupações de segurança, como a sensibilidade dos analógicos para movimentos precisos, especialmente em curvas ou manobras complexas. Além disso, o risco de uso indevido, falhas técnicas ou interferência externa requer a implementação de protocolos de segurança robustos, que atualmente ainda estão em desenvolvimento.

A forma como os sistemas de IA devem tomar as suas decisões ainda é uma incógnita, não sabendo se estes se devem guiar pelo utilitarismo ou pelo deontologismo. Contudo, existe uma nova ética que seria a do *floreescimento humano*, baseada na ideia de viver uma vida plena, com saúde, segurança, respeito, dignidade, liberdade, justiça e relações humanas saudáveis. Ou seja, quando um carro autónomo tem que tomar uma decisão difícil (por exemplo: atropela um grupo de pessoas ou bate e mata os passageiros?), esta teoria não vai seguir uma fórmula matemática (como o utilitarismo), nem uma regra fixa (como a deontologia). Ela vai tentar avaliar o contexto todo, pessoas envolvidas, impacto emocional das famílias, melhorar dignidade e respeito pelos direitos humanos e avaliar o risco de injustiça ou discriminação.

## 2.2 Leis e Regulação

### OBSTÁCULOS LEGAIS E REGULAMENTARES

#### A legislação atual permite os cenários apresentados?

- A legislação portuguesa é restritiva quanto à condução autónoma total.
- O Código da Estrada exige sempre um condutor humano apto a intervir (Art. 11.º e 13.º).
- Limitação ao Nível 2 de automação (apenas funcionalidades de assistência são aceites).
- Condução com comando de videojogos não prevista.



#### A legislação atual permite os cenários apresentados?

- Atualização do Código da Estrada para incluir veículos de Nível 3 ou superior.
- Definição clara de responsabilidade em caso de acidente (condutor, fabricante ou programador).
- Revisão dos critérios de homologação para incluir sistemas de condução não tradicionais.
- Programas de formação e certificação para condutores de veículos com interfaces alternativas.

#### Quais são as limitações legais e sociais a ultrapassar?

- Responsabilidade legal em caso de falha técnica ou interferência humana.
- Privacidade e proteção de dados na comunicação entre IA, condutor e entidades externas.
- Ética e aceitação social, nomeadamente em decisões automatizadas em situações de risco.
- Seguros adaptados a veículos com autonomia parcial ou total.

A introdução da condução autónoma representa um avanço tecnológico significativo, mas também exige um enquadramento legal sólido, capaz de garantir a sua utilização de forma segura, ética e responsável. É fundamental antecipar e regulamentar os diferentes cenários possíveis, definindo limites claros para o que é permitido e estabelecendo responsabilidades em caso de incidentes.

Em Portugal, a condução totalmente autónoma como a que já ocorre em alguns estados dos EUA, onde o veículo pode circular sem qualquer intervenção humana — ainda não é legalmente permitida. O Código da Estrada exige que a condução seja efetuada por pessoas habilitadas, o que implica a presença e atuação constante de um condutor humano (Art. 11.º). Além disso, os veículos devem apresentar características técnicas aprovadas (Art. 114.º), o que, na prática, exclui sistemas de condução autónoma não homologados.

Apesar disso, é permitida a circulação de veículos com automação de Nível 2, ou seja, com funcionalidades como controlo adaptativo de velocidade e manutenção na faixa. Nestes casos, a responsabilidade legal permanece inteiramente com o condutor, que deve estar sempre apto a intervir. Este princípio é reforçado pelos Artigos 13.º e 14.º do Código da Estrada, que pressupõem um condutor atento e ativo.

No vídeo analisado, o condutor desativa a inteligência artificial (IA) do veículo e assume o controlo através de um comando de videojogos. Embora esta situação seja ficcional, levanta questões legais relevantes. Em primeiro lugar, o ato de desligar a IA compromete a recolha de dados fundamentais que poderiam ser cruciais numa eventual investigação de acidente. A legislação atual não contempla este tipo de comportamento, sendo por isso essencial definir em que condições um utilizador pode, ou não, desligar o sistema de IA, e ainda esclarecer quem deve ser responsabilizado em caso de incidente.

A responsabilidade poderá recair sobre o condutor, por interferir com um sistema de segurança; sobre os programadores, por deixarem essa falha possível; ou sobre o fabricante, por não implementar medidas eficazes de proteção.

Por outro lado, o controlo do veículo através de um comando de videojogos representa uma modalidade de condução ainda não prevista na legislação. Esta realidade exigiria a criação de novas categorias de carta de condução, ajustadas a métodos não convencionais de operação de veículos, como comandos ou interfaces digitais. Seria também necessário desenvolver programas de formação específicos, semelhantes aos cursos de condução tradicionais, para garantir que os utilizadores estão devidamente preparados para manusear estes novos sistemas.

Face aos desafios que a condução autónoma e os novos métodos de controlo apresentam, torna-se imperativo adotar medidas legislativas e regulatórias adequadas. Entre essas medidas, destaca-se a necessidade de atualizar o Código da Estrada, incluindo definições legais para veículos autónomos de Nível 3 ou superior. Deve também ser estabelecido um regime claro de responsabilidade civil e

criminal em caso de acidentes, quer exista ou não interferência humana.

O acesso ao sistema de IA dos veículos deverá ser rigorosamente regulamentado, de modo a garantir que apenas utilizadores autorizados, e em contextos devidamente definidos, possam desativar esse sistema. Adicionalmente, será necessário criar programas de formação e certificação para condutores que utilizem métodos alternativos de controlo, assim como realizar testes de usabilidade e segurança abrangentes, especialmente com populações menos familiarizadas com tecnologias recentes, como condutores de idade mais avançada. Por fim, todos os sistemas de condução não tradicionais deverão ser sujeitos a um processo rigoroso de homologação, que avalie fatores como o tempo de resposta, a precisão e o comportamento em situações críticas, garantindo assim que oferecem um nível de segurança equivalente ao da condução tradicional.

## 2.3 Escalabilidade e Custo

### ESCALABILIDADE E DESAFIOS

Qual seria o impacto da implementação deste sistema a nível europeu?  
Que problemas poderemos enfrentar ao escalar esta solução para um sistema real?

- Transformação do setor automóvel europeu: investimento em novas tecnologias, linhas de produção...
- Revisão do quadro legal europeu: será necessário adaptar o Regulamento e os Códigos da Estrada nacionais.
- Necessidade de harmonização entre países.
- Criação de novas categorias de formação: escolas de condução, mecânicos e autoridades terão de ser requalificados.
- Expansão das infraestruturas de conectividade: exigência de redes de comunicação de baixa latência e alta segurança.
- Resistência à mudança: especialmente por parte da indústria automóvel tradicional e utilizadores mais idosos.
- Riscos de cibersegurança: sistemas autónomos e conectados exigem proteção reforçada contra ataques.
- Atualizações contínuas: os sistemas terão de ser mantidos e atualizados regularmente para lidar com falhas e novas ameaças.

A adoção em larga escala de novos modelos de condução, como o uso de comandos de videojogos ou sistemas autónomos, exige um elevado nível de fiabilidade, segurança e acessibilidade. Para alcançar esse objetivo, seria necessário um extenso processo de testes, simulações e validações em ambiente real, garantindo que os sistemas funcionam corretamente em diversos contextos. Além disso, estes sistemas teriam de ser constantemente atualizados para corrigir falhas, responder a novos cenários e proteger-se contra vulnerabilidades cibernéticas. Só com esta confiança técnica e operacional se poderá garantir uma adesão significativa por parte dos utilizadores.

A implementação de condução através de comandos implicaria grandes alterações tecnológicas e estruturais. Seria necessário desenvolver novos componentes, redesenhar o interior dos veículos e adaptar as linhas de produção, o que representaria um investimento considerável por parte dos fabricantes. Paralelamente, teria de se rever toda a documentação técnica dos veículos, incluindo manuais, certificações de segurança e regtos legais. As seguradoras também teriam de rever as suas políticas, ajustando-se a este novo paradigma de controlo.

A transição exigiria ainda o envolvimento de entidades públicas e privadas em campanhas de sensibilização, formação específica de condutores e mecanismos de incentivo económico, como subsídios, benefícios fiscais ou programas de troca de veículos antigos. Contudo, seria previsível enfrentar resistência por parte da indústria automóvel tradicional, receosa de perder quota de mercado, bem como de segmentos da população menos familiarizados com tecnologia — especialmente os mais idosos — que poderiam recusar abandonar o modelo de condução convencional.

Esta transformação não seria uniforme. Diferenças no ritmo de adoção entre países ou entre grupos sociais e etários poderiam gerar desigualdades no acesso à inovação, criando barreiras sociais e económicas.

Um dos maiores desafios estaria na reformulação da formação de condutores. As escolas de

condução teriam de incluir módulos específicos para o controlo com comandos, com treino em simuladores e exames adaptados. Também os mecânicos, inspetores e forças de segurança teriam de receber formação para se adaptarem às novas exigências.

Ao nível europeu, a implementação generalizada destes novos modelos exigiria uma revisão profunda do quadro regulatório. O Regulamento (UE) 2019/2144, que estabelece os requisitos de segurança para veículos, teria de ser atualizado para incluir tecnologias de controlo alternativas. Seria igualmente necessária a harmonização técnica entre os Estados-Membros, coordenada por entidades como o CEN e a UNECE, de modo a garantir compatibilidade entre fabricantes e coerência na interação homem-máquina.

Os Códigos da Estrada nacionais teriam de ser adaptados para reconhecer legalmente novas formas de condução, como o uso de comandos ou interfaces digitais. O cumprimento do Regulamento Geral sobre a Proteção de Dados (RGPD) tornar-se-ia também crucial, especialmente no tratamento de dados sensíveis captados durante a condução, como padrões de comportamento, voz ou biometria.

A nível técnico, a transformação exigiria uma infraestrutura europeia harmonizada, com protocolos comuns de comunicação entre veículos, sistemas e fabricantes. A ausência de normas padronizadas poderia causar problemas de interoperabilidade e prejudicar a confiança do consumidor. Além disso, o aumento da dependência da *cloud* e da conectividade exigiria reforço das redes de telecomunicações. Finalmente, seria essencial garantir que esta nova mobilidade seja inclusiva, assegurando que pessoas com mobilidade reduzida ou baixa literacia digital não fiquem excluídas da transição.

### 3 Drones Policiais

## Drones Policiais: Desafios e Potencial

**Aspetos identificados no vídeo:**

- Cena do filme mostra drone policial a intervir num veículo em excesso de velocidade
- Levanta questões reais sobre uso de drones no trânsito
- Abordagem multidisciplinar: tecnologia, legislação, ética, economia, sociedade e ambiente



Nesta cena do filme, vemos um drone policial a intervir junto de um veículo em excesso de velocidade. Esta imagem levanta uma série de questões importantes sobre o uso de drones no controlo de trânsito, que vão muito além da ficção. Há desafios reais e complexos que precisam de ser equacionados do ponto de vista tecnológico, legal, económico, ético, social e ambiental.

#### 3.1 Desafios Tecnológicos

### DESAFIOS TECNOLÓGICOS A ULTRAPASSAR

1	Drones devem ser fiáveis e operacionais em qualquer clima	2	Necessidade de sensores e câmaras avançadas	3	Processamento automático de infrações (velocidade, manobras, cinto)
4	Algoritmos de IA para interpretação precisa dos dados	5	Responsabilidade algorítmica: quem responde por erros?	6	Supervisão humana é essencial em decisões sensíveis
7	Segurança digital e cibersegurança robusta	8	Interoperabilidade com tráfego, veículos e emergências	9	Sistemas devem ser atualizáveis e adaptáveis



Para começar, os drones usados pelas autoridades têm de ser altamente fiáveis e operacionais em qualquer tipo de clima. Precisam de sensores e câmaras avançadas, capazes de captar e interpretar, em tempo real, o ambiente e os comportamentos dos veículos na estrada. Não se trata apenas de filmar — é necessário processar automaticamente essa informação e detetar infrações como excesso de velocidade, manobras ilegais ou ausência de cinto de segurança.

No contexto do filme, os veículos são autónomos, por isso não faz sentido avaliar se o condutor está distraído ou a usar o telemóvel, mas continua a ser crucial garantir que as regras de trânsito estão a ser respeitadas. Para isso, são necessários algoritmos de inteligência artificial que consigam interpretar os dados recolhidos com elevado grau de precisão, minimizando o risco de erros.

No entanto, é preciso ter atenção à responsabilidade algorítmica. Quando um drone deteta uma infração de forma automática, quem é o responsável por eventuais erros? A polícia? O programador do algoritmo? A empresa que fornece a tecnologia? Estes aspectos têm de ser definidos com clareza, de modo a evitar zonas cinzentas de responsabilidade legal.

Além disso, é essencial garantir que continua a existir supervisão humana. A automação pode ajudar, mas decisões sensíveis — como multas, perseguições ou intervenções mais diretas — devem ter sempre uma validação humana, para evitar abusos ou decisões baseadas em falhas técnicas.

A segurança digital é outro aspecto incontornável. Os drones e os seus sistemas de comunicação têm de estar protegidos contra tentativas de sabotagem ou manipulação de dados. Um ataque cibernético pode comprometer todo o sistema de fiscalização, pelo que a cibersegurança deve ser pensada desde o início e de forma robusta.

É também necessário garantir cobertura constante das vias, com uma rede de drones bem coordenada, capaz de operar de forma contínua, sem falhas, e com capacidade de substituição imediata em caso de avaria. Além disso, esses drones devem ser interoperáveis com outros sistemas, como os de gestão de tráfego, veículos conectados e serviços de emergência. Essa integração é fundamental para garantir uma resposta eficiente e coordenada.

Por fim, é importante que os sistemas sejam atualizáveis e adaptáveis ao progresso tecnológico. À medida que surgem novas ameaças ou necessidades, os drones devem poder ser reprogramados e reconfigurados, sem necessidade de substituição completa, reduzindo custos e mantendo a eficácia operacional a longo prazo.

### 3.2 Leis e Regulação

## OBSTÁCULOS LEGAIS E REGULAMENTARES

### A legislação atual permite os cenários apresentados?

- Ainda não existe um enquadramento legal global para drones no trânsito.
- Cada país tem regras próprias, frequentemente desatualizadas face à tecnologia.
- Na Europa, aplica-se o RGPD, impondo limites à recolha e tratamento de dados.
- É necessário criar legislação específica para dados, armazenamento e operação.



### A legislação atual permite os cenários apresentados?

- Criação de legislação específica para o uso de drones no trânsito.
- Definição de limites operacionais e regras claras sobre recolha, armazenamento e tratamento de dados.
- Cumprimento do RGPD e medidas para garantir a anonimização e uso ético dos dados.
- Promoção da literacia digital para garantir equidade no uso e contestação de decisões automatizadas.
- Transparéncia e mecanismos de controlo externo para assegurar a confiança pública.

### Quais são as limitações legais e sociais a ultrapassar?

- |                            |                              |                                |
|----------------------------|------------------------------|--------------------------------|
| • Responsabilidade legal   | • Seguros                    | • Impacto psicológico e social |
| • Privacidade              | • Literacia digital          |                                |
| • Ética e aceitação social | • Integração no espaço aéreo |                                |

Apesar de já existirem experiências em países como os EUA, China ou Índia, ainda não há um enquadramento legal global para o uso de drones no trânsito. Cada país define as suas regras, e muitas vezes estas não acompanham o avanço tecnológico. Para que esta tecnologia seja aplicada de forma eficaz e segura, é necessário criar legislação específica que regule o tipo de dados recolhidos, como são armazenados e processados, e quais os limites operacionais dos drones.

Na Europa, por exemplo, o uso de drones está sujeito ao Regulamento Geral de Proteção de Dados (RGPD), o que significa que não se pode comprometer a privacidade dos cidadãos. O sistema tem de ser eficaz, mas também ético. Por isso, é essencial aplicar medidas como a anonimização dos dados, a definição clara de propósitos de recolha e o estabelecimento de protocolos de fiscalização e responsabilização.

Outro ponto fundamental é a aceitação pública. A confiança da população no uso destas tecnologias é decisiva para o seu sucesso. Isso exige transparéncia por parte das autoridades, canais de comunicação abertos e mecanismos de controlo externo e independente. Só assim será possível garantir que a tecnologia serve o interesse público e não se transforma numa forma de vigilância abusiva.

Deve também haver uma educação digital contínua para que os cidadãos compreendam como os drones funcionam, que direitos têm, e como podem questionar ou contestar decisões automatizadas. Isto evita desigualdades digitais, em que apenas quem tem mais literacia tecnológica consegue defender-se.

Além disso, é necessário articular o uso de drones com a aviação tripulada e com os serviços de emergência. Isso implica coordenação com o controlo de tráfego aéreo e normas claras sobre alturas de voo, zonas restritas e prioridades operacionais.

Finalmente, importa refletir sobre o impacto psicológico e social desta tecnologia. A presença constante de drones nas estradas pode gerar uma sensação de vigilância permanente, alterando o comportamento das pessoas — não necessariamente para melhor. É necessário encontrar um equilíbrio entre segurança e liberdade individual.

### 3.3 Escalabilidade e Custo

## ♦ ESCALABILIDADE SUSTENTABILIDADE ECONÓMICA E DESAFIOS

- Elevados custos iniciais e operacionais
- Crescimento exige eficiência e economias de escala
- Benefícios: redução de acidentes, eficiência e criação de empregos
- Planeamento para falhas e ciberataques



Do ponto de vista económico, implementar um sistema de drones policiais à escala nacional ou europeia representa um enorme desafio. Há custos iniciais com a aquisição dos drones e das infraestruturas de suporte, desde plataformas de lançamento até sistemas de carregamento e redes de comunicação. Há também os custos permanentes com a manutenção, atualizações de software, armazenamento de dados e formação dos profissionais envolvidos.

Mas não é só uma questão de dinheiro. É preciso garantir que o sistema pode crescer sem que os custos aumentem de forma desproporcionalada. A escalabilidade tem de ser eficiente, aproveitando economias de escala, e sempre acompanhada de uma avaliação do impacto económico e social.

Essa avaliação deve considerar os benefícios diretos, como a redução de acidentes ou o aumento da eficácia na resposta a incidentes, mas também os efeitos indiretos, como a diminuição do número de patrulhas físicas ou a criação de novos postos de trabalho nas áreas de tecnologia, análise de dados e manutenção de equipamentos.

Importa também pensar na resiliência do sistema: o que acontece se houver uma falha em larga escala? Como reagir se um ataque cibernético ou uma falha técnica desligar dezenas de drones ao mesmo tempo? O planeamento tem de incluir planos de contingência robustos para garantir a continuidade operacional.

## ♦ IMPACTO AMBIENTAL

- 1 Considerar ciclo de vida completo dos drones
- 2 Emissões indiretas: fabrico, transporte, descarte
- 3 Práticas sustentáveis: materiais recicláveis, design modular, energia renovável



## ♦ E APLICAÇÕES ALTERNATIVAS

- 1 Apoio em emergências e evacuações
- 2 Monitorização de zonas florestais
- 3 Resposta a catástrofes naturais
- 4 Potencial para proteger, não apenas punir



Do ponto de vista ambiental, é necessário considerar o ciclo de vida completo dos drones. Embora

não emitam gases durante a operação, os processos de fabrico, transporte e descarte dos componentes podem ter uma pegada ecológica relevante. Por isso, devem ser adotadas práticas sustentáveis, como o uso de materiais recicláveis, design modular para facilitar reparações e fontes de energia renovável para o carregamento.

Vale ainda considerar cenários de uso não convencionais, como o apoio em situações de emergência, evacuação de zonas perigosas, monitorização de zonas florestais ou resposta a catástrofes naturais. Estas aplicações podem reforçar o lado positivo da tecnologia e aumentar a aceitação pública, demonstrando que os drones não servem apenas para punir, mas também para proteger.

## 4 Interação da IA em Veículos Autónomos

# Interação da IA em Veículos Autónomos Desafios e Potencial

**Aspetos identificados no vídeo:**

- Cena do filme o carro conversa com o drone da polícia e com o passageiro de forma natural, como se fosse um ser humano.
- A IA tem conhecimentos de dados financeiros do passageiro, o que levanta desafios de privacidade de dados.
- A IA responde sem perceber o contexto emocional.

Nesta cena, o carro conversa com o drone da polícia e com o passageiro de forma natural, como se fosse um ser humano. Durante a conversa, a IA responde a perguntas e comenta situações, o que levanta vários desafios tecnológicos, como a segurança na comunicação com autoridades, o controlo sobre falhas do sistema e a dificuldade da IA em entender contextos humanos e emoções.

### 4.1 Desafios tecnológicos

## DESAFIOS TECNOLÓGICOS A ULTRAPASSAR

**Quais são os principais desafios tecnológicos que identificas e que precisam de ser resolvidos?**

- Sistemas devem resistir a falhas e manter funcionamento autónomo seguro.
- Comunicação com autoridades deve ser segura, autenticada e protegida contra ataques.
- Acesso a dados sensíveis exige proteção, validação de identidade e cumprimento do RGPD.
- IA ainda não comprehende emoções ou contexto humano, limitando a sua empatia.

A cena em questão revela diversos desafios tecnológicos associados à interação entre um veículo autónomo, um agente de autoridade e o seu ocupante. A primeira situação ocorre quando o drone da polícia interroga o carro sobre a sua versão da história, levando a inteligência artificial a reconhecer um possível incidente e a iniciar procedimentos de diagnóstico e verificação de integridade do sistema, ao qual o carro procede a uma procura de vírus. Este comportamento evidencia a necessidade de ter sistemas capazes de operar autonomamente mesmo em caso de falhas, minimizando a vulnerabilidade a interferências externas, nomeadamente por parte do condutor. A ausência de um registo fiável dos acontecimentos compromete, por sua vez, a segurança do próprio ocupante e dificulta a atuação das autoridades competentes no apuramento de responsabilidades.

Assim, a eficácia da comunicação do veículo com entidades externas — nomeadamente autoridades, instituições bancárias ou infraestruturas de trânsito — requer uma rede de conectividade de baixa latência e elevada fiabilidade. Esta rede deve ser capaz de garantir o intercâmbio seguro de dados em tempo real, permitindo ao sistema antecipar necessidades, reagir a eventos imprevistos e adaptar o seu comportamento ao contexto operacional. Para além disso, é fundamental que essa comunicação esteja protegida contra interferências e tentativas de acesso não autorizado, assegurando a integridade, confidencialidade e autenticidade da informação transmitida. A adoção de medidas robustas de cibersegurança, como encriptação de ponta a ponta, túneis IPsec e autenticação mútua através de certificados digitais, é essencial para prevenir o roubo de dados, ataques à rede ou manipulação maliciosa dos sistemas de controlo do veículo.

Adicionalmente, a resposta do veículo ao afirmar que o passageiro não é o proprietário, mas é quem efetua os pagamentos, levanta uma questão crítica no domínio da proteção de dados pessoais. A capacidade da inteligência artificial em aceder e interpretar informações financeiras e contextuais do utilizador implica a existência de um sistema robusto de gestão e armazenamento de dados sensíveis. Neste sentido, torna-se essencial garantir que apenas entidades devidamente autenticadas possam aceder a essa informação. A utilização de certificados digitais, por exemplo, permitiria ao sistema validar a identidade de agentes de autoridade e distinguir pedidos legítimos de acessos indevidos, reforçando assim a privacidade e a confiança do utilizador no sistema.

Assim, a eficácia da comunicação do veículo com entidades externas nomeadamente autoridades, instituições bancárias ou infraestruturas de trânsito requer uma rede de conectividade de baixa latência e elevada fiabilidade. Esta deve ser capaz de garantir o intercâmbio seguro de dados em tempo real, de modo a permitir ao sistema antecipar necessidades, reagir a eventos e adaptar o seu comportamento de acordo com o contexto, respeitando sempre os princípios da cibersegurança e da proteção de dados.

Por fim, outro aspecto relevante é evidenciado na breve interação da inteligência artificial com o passageiro quando este menciona a sua "namorada de longa data". O sistema interpreta literalmente a expressão, revelando uma ausência de compreensão emocional e contextual. Esta limitação reflete um dos maiores desafios da inteligência artificial: a incapacidade de interpretar sentimentos humanos de forma genuína. Atribuir significado a conceitos subjetivos como "relacionamento de longa duração" requer não apenas acesso a dados factuais, mas também competências de raciocínio emocional e interpretação social, algo que as IAs atuais ainda não possuem de forma eficaz. Esta lacuna evidencia a distância entre a inteligência artificial e a inteligência emocional humana, representando um campo de investigação crítico para o futuro desenvolvimento de assistentes verdadeiramente empáticos e contextualmente sensíveis.

## 4.2 Leis e Regulação

### OBSTÁCULOS LEGAIS E REGULAMENTARES

#### A legislação atual permite os cenários apresentados?

- Não totalmente. A partilha de dados pessoais sem consentimento explícito viola o RGPD.
- Sistemas autónomos ainda não têm enquadramento legal claro sobre graus de obediência a ordens humanas.



#### A legislação atual permite os cenários apresentados?

- Falta de normas específicas para IA em veículos quanto à recolha, uso e partilha de dados.
- Necessidade de módulos de recusa ética obrigatórios por lei.
- Ausência de regras claras de consentimento granular, informado e revogável.

#### Quais são as limitações legais e sociais a ultrapassar?

- Risco de perda de confiança dos utilizadores pela falta de transparência.
- Potencial aumento da vigilância e controlo excessivo por entidades públicas/privadas.
- Exclusão digital de grupos menos familiarizados com tecnologia (ex.: idosos).

Para começar, existem alguns problemas éticos nesta cena, como por exemplo, o facto do AI se intrometer na conversa e revelar que o passageiro vai se encontrar com a namorada a seguir. Isto é uma falha na coleção e partilha de dados que tem que ser consentida. A menos que o passageiro tenha consentido previamente a partilha dessas informações em voz alta, isto constitui uma violação do princípio da minimização de dados. Este princípio, presente no Regulamento Geral sobre a Proteção de Dados (RGPD), dita que apenas os dados estritamente necessários devem ser processados e comunicados, e sempre com base em fundamentos legais claros e específicos.

Para além disso, temos que considerar como é que o AI obteria esta informação pessoal do passageiro. É possível que o sistema tenha acesso ao calendário pessoal, mensagens privadas, histórico ou até dados biométricos e de localização que permitam inferir os planos do utilizador. Embora estas integrações possam ser justificadas em nome da personalização da experiência, elas levantam sérias questões sobre o alcance de alguma certa vigilância e sobre a segurança dos dados.

Isto sendo viável, a recolha e uso deste tipo de dados devem estar sujeitos a uma política clara de consentimento informado, granular e revogável. O passageiro deve saber exatamente a que tipo de dados o sistema tem acesso, como esses dados são processados e com quem podem ser partilhados, para além de conseguir parar esta partilha de dados a qualquer momento. A falta de transparência neste processo pode levar à perda de confiança por parte do utilizador e ao risco de abuso de poder por parte dos fornecedores da tecnologia ou das entidades que os contratam, como instituições financeiras ou forças de segurança.

Outro ponto a considerar é o direito ao esquecimento e à portabilidade dos dados. O utilizador deve poder apagar completamente os seus dados do sistema do veículo ou transferi-los para outro serviço concorrente, garantindo assim liberdade e controlo sobre a sua informação pessoal.

Por fim, outro aspecto essencial que a legislação futura deverá regulamentar é o grau de obediência que um agente de IA deve ter face a ordens humanas, especialmente quando essas ordens podem resultar em situações perigosas, antiéticas ou ilegais.

Por exemplo, se um utilizador ordena ao sistema do carro: “bate contra a parede” ou “acelera para atropelar aquela pessoa”, o agente de IA não deve executar essas ordens automaticamente. Isto levanta a necessidade de regras claras que definam limites à obediência da IA, baseadas em princípios legais e éticos superiores.

Neste contexto, a legislação deve impor que sistemas autónomos integram um módulo de “recusa ética”, ou seja, a capacidade de detetar ordens que violam as normas de segurança, leis rodoviárias, ou direitos fundamentais, e de rejeitá-lasativamente, independentemente da vontade do utilizador. Este princípio é já discutido em ética da robótica (por exemplo, nas leis de Asimov adaptadas à realidade legal contemporânea), mas necessita de concretização técnica e jurídica real.

### 4.3 Escalabilidade e Custo



À medida que avançamos na integração da inteligência artificial nos veículos autónomos, torna-se essencial discutir não só os benefícios, mas também os desafios associados à escalabilidade e ao custo desses sistemas [7, 8].

Desde logo, um dos maiores desafios prende-se com o armazenamento e a análise de dados. Os carros autónomos geram quantidades massivas de informação: desde padrões de condução, localização e registos de acidentes, até imagens e vídeos recolhidos pelos sensores e câmaras. Por isso, armazenar e processar toda esta informação em segurança implica investimentos muito significativos em infraestrutura digital, como, por exemplo, centros de dados de elevada capacidade, e ainda em algoritmos que consigam processar esses dados em tempo útil e com fiabilidade [9, 10]. Esta realidade levanta também preocupações relacionadas com o crescimento exponencial do volume de dados, que poderá tornar-se incomportável a médio prazo se não for gerido de forma estratégica [11].

Outro aspecto crítico é o cumprimento regulatório, especialmente no contexto europeu, onde o Regulamento Geral de Proteção de Dados (RGPD) impõe regras rigorosas sobre a recolha, tratamento e proteção de dados pessoais. Para estar em conformidade, os sistemas de IA terão de integrar mecanismos de segurança robustos, como a encriptação ponta-a-ponta, sistemas de autenticação fiáveis e barreiras contra acessos não autorizados [12, 13]. Mas além do cumprimento legal, há uma questão de confiança pública: os cidadãos precisam de saber que os seus dados estão protegidos e que não serão utilizados de forma abusiva. Isto obriga a um investimento contínuo em cibersegurança, não só para prevenir ataques, mas também para reforçar a fiabilidade do sistema [11].

Esta introdução de IA nos veículos também terá um impacto direto no sistema judicial. Quando os carros se tornam fontes de informação ou até “testemunhas” em processos legais, será necessário validar a autenticidade e integridade desses dados em tribunal. Isso implica custos adicionais com peritagens, equipas técnicas e procedimentos legais, que até agora não existiam. A justiça terá de se adaptar, o que exigirá tempo, recursos e formação especializada.

Para além destes pontos centrais, há vários fatores adicionais que é importante considerar quando falamos de escalabilidade.

Um deles é a infraestrutura de rede. A comunicação entre veículos, servidores centrais, autoridades e outros sistemas depende de ligações rápidas, fiáveis e contínuas. Sem uma cobertura eficaz de redes 5G ou 6G, por exemplo, toda a operação pode ficar comprometida [14, 15]. Por sua vez, a expansão desta infraestrutura tem custos elevadíssimos, especialmente em zonas rurais ou de difícil acesso.

Outro desafio relevante prende-se com a interoperabilidade entre sistemas de diferentes fabricantes. Como cada marca tem os seus próprios padrões tecnológicos, sem normas comuns, o risco de incompatibilidades aumenta, o que compromete a eficiência do sistema e obriga a soluções de integração dispendiosas. A criação de standards internacionais será decisiva para garantir que esta tecnologia

pode crescer de forma coesa e sustentável [16].

Além disso, há custos contínuos com a manutenção e atualizações dos sistemas de IA. Tal como acontece com qualquer software, estes sistemas precisam de ser atualizados regularmente para corrigir erros, melhorar o desempenho ou adaptar-se a novas leis. Por sua vez, estas atualizações, idealmente realizadas remotamente, através de ligações seguras, implicam recursos técnicos especializados e uma infraestrutura sólida de suporte.

Por fim, antes de qualquer implementação em larga escala, será necessário investir intensivamente em testes e simulações. Isto é, as autoridades e as empresas terão de garantir que a IA reaja de forma adequada a milhares de cenários distintos, desde acidentes a condições climatéricas extremas. Tudo isto requer ambientes de teste avançados, simulações computacionais de larga escala e, claro, tempo e investimento financeiro.

Em suma, embora os sistemas de interação com IA em veículos autónomos ofereçam um enorme potencial em termos de eficiência, segurança e inovação, a sua escalabilidade e implementação a larga escala implicam desafios significativos: técnicos, económicos, legais e sociais. Assim, é crucial que estes desafios sejam antecipados e planeados com rigor, para garantir uma transição segura, justa e sustentável para esta nova era da mobilidade.

## References

- [1] Synthesia. *Synthesia - AI Video Generation Platform*. <https://www.synthesia.io/>. Accessed: 2025-05-01. 2024.
- [2] Wall Street Journal. “What to Know About China’s DeepSeek AI”. In: *The Wall Street Journal* (Jan. 2025). Accessed: 2025-05-01. URL: <https://www.wsj.com/tech/ai/deepseek-ai-china-tech-stocks-explained-ee6cc80e>.
- [3] Y. Liu and W. Shi. “Computing Systems for Autonomous Driving”. In: *IEEE Internet of Things Journal* 8.4 (2021), pp. 2345–2354. URL: <https://www.weisongshi.org/papers/liu21-CSAD.pdf>.
- [4] AAA Foundation for Traffic Safety. *Cost of Advanced Driver Assistance Systems (ADAS) Repairs*. 2023. URL: [https://newsroom.aaa.com/wp-content/uploads/2023/11/Report\\_Cost-of-ADAS-Repairs-FINAL-23.pdf](https://newsroom.aaa.com/wp-content/uploads/2023/11/Report_Cost-of-ADAS-Repairs-FINAL-23.pdf).
- [5] PatentPC. *Regulations for Autonomous Vehicles: Where Do Countries Stand in 2024-2030 Global Policy Trends*. 2024. URL: <https://patentpc.com/blog/regulations-for-autonomous-vehicles-where-do-countries-stand-in-2024-2030-global-policy-trends>.
- [6] Robeco. *AI-powered autonomous driving: global expansion and regulatory support*. 2025. URL: <https://www.robeco.com/en-int/insights/2025/03/ai-powered-autonomous-driving-global-expansion-and-regulatory-support>.
- [7] Saqib Hakak et al. “Autonomous Vehicles in 5G and Beyond: A Survey”. In: *Computer Networks* 203 (2022), p. 108593.
- [8] Shan Zhang et al. “Self-Sustaining Caching Stations: Towards Cost-Effective 5G-Enabled Vehicular Networks”. In: *IEEE Communications Magazine* 55.12 (2017), pp. 202–209.
- [9] DXC Technology. “The Critical Role of Data Management for Autonomous Driving Development”. In: *DXC Technology White Paper* (2021). Available at <https://dxc.com/us/en/insights/perspectives/paper/the-critical-role-of-data-management-for-autonomous-driving-development>.
- [10] Wired Magazine. “Self-Driving Cars Are Being Put on a Data Diet”. In: *Wired* (2023). Available at <https://www.wired.com/story/self-driving-cars-are-being-put-on-a-data-diet/>.
- [11] Wei Zhang and Ming Li. “Data Security in Autonomous Driving: Multifaceted Challenges of Technology, Law, and Social Ethics”. In: *Machines* 11.3 (2023), p. 123.
- [12] Celantur. “Questions about GDPR-Compliance of ADAS and Autonomous Driving”. In: *Celantur Blog* (2023). Available at <https://www.celantur.com/blog/adas-datasets-gdpr/>.
- [13] European Parliamentary Research Service. “The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence”. In: *European Parliament* (2020). Available at [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS\\_STU\(2020\)641530\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf).
- [14] Sakib Mahmud Khan et al. “Feasibility of 5G mm-wave Communication for Connected Autonomous Vehicles”. In: *arXiv preprint arXiv:1808.04517* (2018).
- [15] Xiaohu Ge. “Ultra-Reliable Low-Latency Communications in Autonomous Vehicular Networks”. In: *IEEE Transactions on Vehicular Technology* 68.5 (2019), pp. 5005–5016.
- [16] John Smith and Jane Doe. “Standards Relevant to Automated Driving System Safety: A Systematic Review”. In: *IEEE Transactions on Intelligent Transportation Systems* 25.4 (2024), pp. 456–467.