deti

# APSEI

## Work #3

## Report

**Trabalho realizado por:**

**Matilde Teixeira (108193), Diogo Falcão(108712) e Sara Almeida (108796) – LEI**

## Introdução

Para o terceiro trabalho de APSEI, foi-nos apresentado um vídeo ao qual tínhamos que analisar e identificar os principais desafios a superar, com o intuito de viabilizar todas as cenas do filme em realidade. Existem três áreas que abordamos: os desafios tecnológicos a serem superados, obstáculos legais e regulatórios e por fim a escalabilidade e custo. Decidimos estruturar estas respostas por cena. Existem quatro cenas principais: a realização de outras atividades dentro do carro sem ser a de condução (num carro em auto piloto), a toma de controlo da condução do carro por parte do passageiro, o mandar ser parado pela polícia por excesso de velocidade/condução agressiva e por último o diálogo entre o sistema de AI de voz do carro e o condutor (que apesar de também se verificar entre a cena um e a cena dois, nesta cena, o diálogo é mais prominente). Entendemos que para a replicação deste cenário, não nos compete resolver os possíveis problemas, mas sim identificá-los e delinear estratégias para a sua eventual concretização.

## <u>Cena 1</u> - Passageiro realiza outras atividades no carro autónomo

Na primeira cena do excerto, é possível observar um passageiro que aparenta programar no para-brisas do carro. É de notar que nesta realidade, o carro deixa de ser apenas um meio de transporte que nos leva de A a B, mas sim um espaço multifuncional, propício tanto para a produtividade, como para o descanso. O passageiro tem conectado um teclado ao carro que lhe permite programar, tudo dentro de um ambiente imersivo, abstraindo-se completamente da condução. Para a realização desta cena nos dias de hoje, o maior obstáculo não seria a condução autónoma, mas sim um nível de confiança extremo por parte dos utilizadores deste meio de transporte, porém retornaremos a este tópico posteriormente.

### Desafios tecnológicos

Em primeiro lugar, abordamos os desafios tecnológicos a serem superados para esta cena ser possível. Evidentemente, a condução totalmente autónoma é um deles, isto é, uma condução que dispensa totalmente a intervenção do condutor. Como explicado nas aulas, existem seis níveis de condução autónoma, sendo zero o mais baixo - e em que tudo é controlado pelo condutor, e o nível 5 é o mais alto - onde o próprio veículo opera a 100% de forma independente, sem qualquer intervenção humana. Neste nível, o condutor continua a poder intervir na condução, mas apenas se o desejar. O nível 5 de condução autónoma é já tecnologicamente possível, mas ainda não é legal em nenhum país. No cenário apresentado, o carro percorre uma curta distância em linha reta. Essa característica facilita a realização da cena, tornando-a mais viável, especialmente quando comparada com modelos atuais. De qualquer das formas, focando-nos apenas no trajeto em carros autónomos, esta cena era exequível a nível de software do carro.

A nível de hardware, qualquer carro poderia circular nesta auto-estrada, uma vez que carros com sistema de nível 5 de condução autónoma conseguem coabitar com carros não autónomos. A União Europeia sabe que o erro humano está envolvido em cerca de 95% de todos os acidentes com veículos, de acordo com um estudo realizado em 2016. Por isto, colocar algoritmos capazes de identificar a grande maior parte das situações na estrada, seriam sempre melhores e mais seguros do que colocar um humano a conduzir. Posto isto, como permitiríamos que carros não autónomos circulassem nas mesmas estradas, deveríamos estar cientes de que mais acidentes poderiam vir a acontecer. Identificámos também no vídeo, que o carro autónomo não aparenta ter controlos manuais, por isso retornaremos a este tópico na explicação da cena dois. A linha de pensamento destes problemas levou-nos a pensar na

ideia de equipar os carros com algoritmos de auto piloto melhorados e com caixas negras, semelhante ao que a Tesla já faz com todos os seus carros e o que a UE vai tornar como medida obrigatória para todos os carros vendidos no espaço europeu a partir de junho. A caixa negra em carros funciona fundamentalmente como as caixas negras de qualquer avião: "um sistema que se destina exclusivamente ao registo e armazenamento de parâmetros e informações críticas relacionadas com uma colisão, antes, durante e imediatamente após essa mesma colisão". O objetivo deste sistema não seria "gravar as conversas que ocorrem dentro do carro", mas sim "permitir análises de segurança rodoviária e avaliar a eficácia das medidas específicas adotadas", tal como descrito no Regulamento (UE). Discutimos o acesso e a obtenção de dados deste sistema mais abaixo, na secção de obstáculos legais e regulatórios. Assim, seria possível atribuir a responsabilidade por um acidente a uma pessoa ou a um veículo, podendo o algoritmo com estes dados aprender, caso o utilizador ativasse a opção de partilha de dados. Isto porque a opção predefinida seria a não partilha destes dados em qualquer cenário, à exceção da partilha destes dados com entidades jurídicas.

Juntamente com os dados da caixa negra, também as câmaras não poderiam ser associadas ao carro e nenhum método de reconhecimento facial poderia ser usado. Em relação ao ambiente de programação imersivo que se pode visualizar ainda nesta primeira cena, nota-se que o para-brisas serve de ecrã para o passageiro. Reitera-se que a tecnologia que existe atualmente permite a realização de algo deste tipo. Fundamentalmente, estamos a falar de 4 ecrãs que se "escondem" nos quatro cantos do para-brisas quando não usados e que se juntam formando um único ecrã, quando usados. Simultaneamente, observamos duas câmaras direcionadas para o utilizador, com efeitos e sob regulações do RGPD. Mais uma vez, este tópico será discutido em mais detalhes na seção sobre legislações.

Por fim, falta discutir se os carros autónomos usariam sistema em cloud ou sistemas do próprio carro: o ponto mais tecnologicamente complexo desta cena. A nosso ver, faria sentido usar sistemas e algoritmos que funcionassem "on device", onde os dados e processamentos poderiam ser mantidos dentro dos carros, para maior segurança e privacidade dos dados. Uma vez mais, seguiríamos o modelo da Tesla de processar todas as operações de inferência no processador do carro e treinar o modelo (rede neuronal) com dados recolhidos em tempo real. Os dados são recolhidos com sensores LiDAR juntamente com câmaras. Esta abordagem oferece diversos benefícios, como maior segurança e confiabilidade, dado que o sistema não depende de conexão externa para operar. Além disso, este incentivo à aprendizagem contínua com dados em tempo real permite que o modelo se adapte às condições reais de direção e melhore o seu desempenho.

**Legislações**

Em segundo lugar, legislações. A nosso ver, a inclusão de câmaras dentro do habitáculo do veículo é na maior parte dos casos desnecessária e não acrescenta nenhuma funcionalidade para o carro a não ser um auxílio para o sistema de AI. Atualmente, os carros são obrigados a usar sensores ou câmaras direcionadas para alertar uma possível falta de atenção do condutor, para lembrá-lo de manter os olhos na estrada. Uma vez que o carro possui nível 5 de condução autónoma, na maior parte dos cenários, as câmaras deviam permanecer desligadas e até fisicamente cobertas. Apenas seria preciso ligar as câmaras quando o condutor escolhesse conduzir manualmente o carro, para estas fazerem precisamente o que as câmaras e sensores atuais fazem. Estas câmaras, como quaisquer outras, captam informações que conseguem fazer identificar pessoas e por isso, qualificam-se como dados pessoais. Pelo princípio da minimização de dados, o condutor seria incentivado a usar o auto piloto de modo a não usar as câmaras, mas se assim o escolhesse, seria

automaticamente avisado na primeira vez que informação pessoal estaria a ser recolhida. Relembramos que estes dados, por defeito, seriam processados no carro e que ninguém à exceção de entidades jurídicas poderiam ter acesso (por exemplo em casos de acidentes), a menos que o titular do veículo decidisse ativar uma opção de partilha de dados e partilhar estes quando algum evento crítico de segurança se sucedesse. Neste caso, os dados eram partilhados com os nossos data centers, que estariam igualmente protegidos pelo RGPD a nível virtual e também fisicamente. Similarmente, o acesso a estes seria altamente controlado. Apenas referir que todos os vídeos gravados que não partilhados com os data centers, seriam apagados num prazo de 24 horas, de modo a tornar o período de retenção o mais curto possível.

Relativamente às caixas negras dos carros, estariam guardadas nestas dados como os vídeos das últimas 24 horas (quer do interior da cabine, quer do exterior) e todos os dados relativos às funções principais do carro (como falado anteriormente). Mais uma vez, quem tem acesso a estes dados seriam entidades jurídicas e pessoal autorizado e todas as leis e tratamentos de dados referidos no parágrafo acima seriam aqui também aplicadas. O auto piloto deveria adaptar-se às leis e regras de trânsito do tipo de via de circulação e deveria ter uma especial atenção a peões. O sistema de condução autónoma deve ser programado conscientemente de princípios de ética e indiscriminação: deve tratar todos os utilizadores da via pública de igual forma e evitar comportamentos que coloquem a vida ou a segurança de outras pessoas em risco. Deve também agir de forma responsável e previsível, permitindo que os outros carros e utilizadores da via pública possam antecipar as manobras.

Reiteramos que a fabricação dos veículos e dos algoritmos de auto piloto devem tomar as medidas adequadas para a proteção de dados dos aparelhos de registos de eventos contra a sua manipulação. Deve haver disponibilidade dos dados do aparelho de registo de eventos através de uma interface normalizada. Todos os dados recolhidos devem ser anonimizados e ainda complementados com requisitos adicionais para a extração de dados, privacidade e segurança dos mesmos.

**Custo e escalabilidade**

Partindo do custo, este é o fator de maior preocupação para a replicação desta cena. A tecnologia dos dias de hoje está um tanto pronta para fazer circular, num troço de uma via, carros autónomos em conjunto com carros não autónomos. Seria necessário investir no aprimoramento destes algoritmos para otimizar e aumentar a sua credibilidade. Existem já alguns modelos chineses completamente autónomos e outras marcas têm carros protótipos também capazes de circular sozinhos. Uma outra possibilidade podia ser a subcontratação destas empresas para a replicação da cena. Quer de uma ou outra forma, o custo seria relativamente alto para o auto piloto do carro (incluindo câmaras, sensores e algoritmos). Outras modificações necessárias ao carro seriam a adição de ecrãs na zona do para-brisas e a instalação de câmaras interiores.

A escalabilidade seria diretamente proporcional ao custo, em relação ao carro. Sabemos que desenvolver esta peça tecnológica seria dispendioso e por isso, para replicar o carro, seria também preciso aumentar o orçamento. Contrariando isto, está o custo e escalabilidade do resto da infraestrutura: as estradas. Tomámos a decisão no primeiro subtópico desta cena de que deveríamos usar apenas processamento “on-device” e não “cloud-based”. Para além da privacidade e segurança de dados, a decisão foi também tomada a nível da escalabilidade. Seria muito mais prático escalar para qualquer sítio do mundo (desatendendo momentaneamente às leis), porque o algoritmo do auto piloto seria capaz - na

teoria - de se ajustar a qualquer tipo de condições e tipos de estrada. Sabemos no entanto que nem todas as estradas podem ter as melhores condições para circulação de carros autónomos, mas a sua maior parte é mais do que suficiente.

Em relação às leis, como já exposto, não existem atualmente lugares na União Europeia que permitam a condução de nível 5 nas estradas públicas. A aceitação pública é que poderia ser mais difícil fazer escalar. Implementar este sistema em larga escala poderia trazer resistência do público devido a receios relacionados com segurança e até perda de empregos no setor. Teríamos que promover campanhas de consciencialização e demonstração da tecnologia. Por último, dado que iríamos ter uma quantidade elevada de carros autónomos a circularem, teríamos que ter medidas robustas de segurança (virtual e física) como protocolos de resposta a acidentes e crimes cibernéticos. Apesar destas preocupações, ao trazer este conceito para larga escala, haveria uma maior segurança no trânsito e uma melhoria na mobilidade.

**<u>Cena 2</u> - Passageiro assume o controlo da condução do carro.**

Esta cena começa exatamente quando o condutor desliga o ecrã e a visão do para-brisas passa a ser a estrada e o ambiente em que o carro está a movimentar-se. No início, o condutor, ao ver o local onde ainda está, parece algo aborrecido, talvez pela monotonia da condução autónoma, e pede ao carro, através da sua voz, que este limpe as lentes das suas câmaras. Quando o carro começa a limpeza, o condutor clica no botão “Delete” do teclado, desativando a inteligência artificial. De seguida, ele conecta ao carro o que aparenta ser um comando comum de videojogos e começa a controlar a sua condução com o mesmo, ultrapassando aparentemente os limites de velocidade e realizando uma condução perigosa.

Dados os acontecimentos algo extrapolantes desta cena, e tendo em conta também a cena anterior, pareceu-nos que o condutor/passageiro do vídeo terá um grande à vontade e conhecimento em tecnologia e terá provavelmente alterado algumas características sistema do carro tornando possíveis maior parte das suas ações. Ainda que tendo isto em mente, a cena foi analisada exatamente como acontece e considerando possíveis as ações do utilizador, até porque, se ele as conseguiu realizar é porque têm de ser consideradas, principalmente em termos legais e legislativos.

**Desafios tecnológicos**

Ao visualizar esta cena com atenção, algo que claramente chama a atenção quando procuramos por desafios tecnológicos que possam constituir problemas num mundo como é representado no vídeo, são as 5 entradas USB dentro do habitáculo do veículo. Tendo em conta que estamos a falar de um carro autónomo altamente tecnológico que utiliza inteligência artificial, estas entradas podem representar possíveis problemas de segurança bastante graves. Aliás, como acontece nesta cena, uma delas é utilizada pelo condutor para assumir o controlo do carro conectando o comando de videojogos à mesma. Este ato representa um risco adicional não só para o próprio condutor que realiza claramente uma condução perigosa, como também para os outros veículos e as pessoas que neles circulam. Por outro lado, e constituindo o seguinte um grave problema de segurança para o sistema, estas entradas podem facilmente ser utilizadas como meio de atos maliciosos, tais como a injeção de vírus e/ou malware. Qualquer dispositivo pode ser conectado ao carro através de um simples cabo USB, ou até, e mais simples ainda, uma pen USB comum infetada.

Mantendo a linha de pensamento acima desenvolvida, é rapidamente alcançável que talvez a falta de dualidade de sistemas de condução do carro possa ser um desafio tecnológico que dê que pensar. Isto é, o carro autónomo aparenta não estar equipado com nenhum mecanismo alternativo de condução manual, sejam estes um volante e/ou pedais, o que indica que este foi feito com o objetivo de uma condução exclusivamente autónoma, ocupando o nível 5 na escala de níveis de condução autónoma reconhecidos, já referidos na cena anterior. Este desafio não só levanta uma série de questões legais, discutidas no tópico abaixo, como também problemas relativos à segurança do passageiro, os quais podem estar interligados precisamente com a ideia analisada imediatamente acima. Imaginemos um cenário onde o carro é, nalguma ocasião, infectado com algum vírus que venha a comprometer, por exemplo, o seu sistema de deteção de obstáculos. Neste caso, se um acidente estivesse em vias de ocorrer, o condutor nada poderia fazer para se proteger na ausência de um pedal de travagem.

Numa outra vertente do vídeo, quanto ao teclado há várias questões que podem ser levantadas, começando pelo facto de este poder ser utilizado para interferir com o sistema. O condutor/passageiro, no vídeo, utilizou o botão de "Delete" do teclado para dar shutdown da AI, no entanto o carro permaneceu em andamento por alguns momentos. Primeiramente, não deveria ser possível, já que não existe forma de conduzir este carro manualmente de forma legal, que o passageiro fizesse shutdown da AI. Novamente, isto representa não só problemas legais, como também de segurança para o passageiro. Para além disso, é notório o facto de o carro continuar em andamento mesmo depois da AI ter sido desativada, o que também não faz muito sentido num carro autónomo 100% guiado através de algoritmos de inteligência artificial. Numa tentativa de encontrar uma explicação, poderíamos pensar que talvez o carro só continuou a movimentar-se devido ao balanço que já levava, dado que até o condutor assumir o controlo do carro foram apenas uns momentos em que este continuou sozinho e a estrada era reta.

**Legislações**

Nesta cena, para além de questões relacionadas com responsabilidade, podemos novamente, tal como na anterior, levantar problemas legais relacionados com as câmaras. O condutor pediu ao carro que começasse a limpeza das mesmas o que fez descer uma espécie de pala tapando a lente das câmaras. De seguida, o condutor começou então uma condução manual, depois de fazer shutdown à inteligência artificial. Por assumir o controlo do carro, perguntamo-nos imediatamente se, a partir desse momento, a responsabilidade da condução e de qualquer consequência da mesma seria do condutor. Isto é, existindo a mínima possibilidade de conduzir manualmente o carro autónomo, como poderão as autoridades legais saber se, em caso de acidente ou violação da lei, a culpa é de algum erro do sistema autónomo do carro ou se a responsabilidade é do condutor que assumiu a condução do mesmo.

Poderíamos pensar que, nestes casos, as imagens das câmaras poderiam então ser acedidas pelas autoridades para que pudessem apurar a responsabilidade dos acontecimentos através das caixas negras descritas no tópico dos desafios tecnológicos na primeira cena. No entanto, isto leva-nos ao ponto já anteriormente discutido das câmaras dentro do habitáculo do veículo, mas de um ponto de vista diferente. Nesta situação, o problema prende-se com o facto de o condutor ter o poder de, ainda que momentaneamente, fazer com que as câmaras deixem de captar imagens, por estarem a proceder à limpeza das lentes. Assim, na ocorrência de alguma infração à lei durante a condução manual, as câmaras não teriam lugar na investigação por parte das autoridades.

Voltando ao tópico das caixas negras, também nesta cena podemos comprovar a sua utilidade dado que supostamente elas poderiam determinar que a inteligência artificial foi desativada, mas apenas em caso de acidente. Isto é, no caso de violação das leis da estrada, que é precisamente a situação presente, e aliás como é mostrado na cena seguinte, a polícia não sabe que o condutor assumiu o controlo do carro e não lhe incute a responsabilidade das suas ações.

Tomando novamente em consideração a ordem dos acontecimentos nesta cena, o condutor começa por pedir ao carro que inicie a limpeza das câmaras e, só em seguida, faz shutdown do mesmo, o que indica que é claramente errado dar shutdown do carro em andamento. Novas leis e legislações teriam de ser criadas para atender a situações como esta e outras possíveis, já que, como podemos observar na totalidade do vídeo, o facto de o carro ser 100% autónomo não impediu o passageiro/condutor de infringir a lei. É de notar que, na condução autónoma de nível 5 e já que não existem mecanismos de condução manual dentro do habitáculo do veículo, o passageiro não precisaria de carta de condução. Caso o condutor da cena não tivesse carta de condução, o perigo mostra-se ser, então, ainda maior, devido à possível falta de conhecimento de regras da estrada.

**Custo e escalabilidade**

Esta é a cena que melhor demonstra como seria um ambiente onde os carros autónomos, do nível que estamos a analisar, têm lugar. Podemos observar também a forma como eles coabitam entre si e com os carros não autónomos. Como já foi referido na cena anterior, este tipo de tecnologia e a sua integração no mundo em que vivemos iria requerer custos astronómicos, principalmente na construção dos próprios carros, mas não só.

Para além destes custos iniciais, há despesas contínuas associadas à manutenção e atualização dos sistemas de AI, software e hardware dos veículos. Isto inclui correções de bugs, melhorias de desempenho, conformidade com as legislações em constante evolução, atualizações de segurança, etc. Aliás, dado o cenário problemático descrito no tópico de desafios tecnológicos desta cena a respeito das entradas USB, um exemplo de um custo consequente seria não só a constante proteção contra vírus e malware, como também o combate aos mesmos caso ocorressem.

Quanto à escalabilidade, o processamento “cloud-based” vs “on-device” também já foi discutido anteriormente, dado que no vídeo não é explícito qual destes mecanismos foi adotado. No entanto, visto o cenário desta cena onde todos os tipos de carros coabitam ao mesmo tempo perfeitamente, podemos voltar a falar dele, de outros pontos de vista. Existem obviamente vantagens e desvantagens de ambos os lados. No caso de um processamento “cloud-based”, o processo de correção de bugs, atualizações, etc. referido acima seria significativamente simplificado, o que é uma mais-valia significativa no contexto que estamos a trabalhar. As melhorias de desempenho também seriam mais facilmente aplicáveis a todos os carros simultaneamente. No entanto, este tipo de processamento, apesar de apelativo em termos de escalabilidade, pode tornar-se problemático quando queremos expandir a tecnologia, por exemplo, para toda a Europa. O facto de existirem milhares de carros a comunicar com um servidor central significa obviamente uma imensidão de mensagens a circular ao mesmo tempo para o mesmo local. Ora, isto pode gerar latência, ou seja, um atraso entre o envio da mensagem e a sua receção, resultando em possíveis riscos de segurança rodoviária.

Tendo em conta ainda o impacto deste cenário na Europa, o processamento "on-device" seria provavelmente o mais acertado no que toca, por exemplo, às áreas rurais bastante presentes pela mesma. Este tipo de processamento traria confiabilidade da conectividade onde a cobertura de rede é limitada, permitindo que este cenário fosse de facto expandido a todos os locais possíveis.

Para além disso, este tipo de processamento apresentaria vantagens em termos legislativos já que seria mais fácil cumprir não só com todas as regulamentações europeias, como também com todas as regras de cada país individualmente. Em termos de cibersegurança e prevenção de ataques como os já descritos nesta cena, o processamento "on-device" evitaria ataques de larga escala ao servidor central, o que poderia ser fatal para o sistema, para além do perigo que representaria.

**<u>Cena 3</u> - Carro é parado pela polícia por excesso de velocidade/condução agressiva.**

Na seguinte cena conseguimos ver o utilizador a conduzir o carro de um forma violenta e perigosa, devido ao excesso de velocidade e ultrapassagens rápidas que faz, e a ser parado por um drone polícia. De facto, começa-se a ouvir as sirenes e o carro quase que para autonomamente, e o utilizador liga novamente a inteligência artificial do carro, que até àquele momento estava desligada, permitindo uma condução perigosa. No drone polícia, este apresenta um ecrã do tamanho de um tablet, que é retrátil, onde se pode ver uma polícia que começa a questionar o utilizador sobre os comportamentos abusivos que o carro estava a ter. O utilizador desculpa-se por ter sido o carro a ter estes comportamentos abusivos, ao que após a polícia inquisiona o carro. Este responde que perdeu consciência momentaneamente, e que vai fazer o update do antivírus. Isto significa que o update é relativamente rápido, pois caso não o fosse o carro não poderia continuar em circulação - sendo o contrário do que a cena induz, ou que a polícia manda. Após este momento, o utilizador faz um comentário mais inusitado à polícia ao que a AI do carro lhe responde com dados pessoais deste, facultando fazer uma chamada relativa a dados pessoais e privados que outrora facultou. Deste modo, nesta cena, temos vários desafios face ao que disponibilizamos atualmente em termos de tecnologias, em termos de legislações pouco permissivas e acima de tudo custo e estabilidade.

**Desafios tecnológicos**

Primeiramente vamos avaliar as tecnologias existentes e quais as possíveis melhorias a serem implementadas para estas cenas serem possíveis, tais como os desafios que têm de ser ultrapassados para que isso seja viável.

Em relação aos drones, estes são constituídos por 6 hélices, o corpo do drone tem um motor e as sirenes da polícia. Possui também um tablet retráctil onde aparece a imagem de uma polícia em "real-time" e o que parece ser uma lanterna, que por ser de dia não está acesa. Simultâneamente, um dos desafios implícitos na construção de um drone desses seria o peso que este teria de levantar. De acordo com a aparência do drone este parece pesar mais do que 250 gramas, mas menos do que 25 kg inserindo-se na categoria de drones médios, e sendo assim podendo transportar até 5 kg, dependendo do modelo. Hoje em dia, o peso normal para um tablet é de 500 gramas, mais o peso da luz que seria normal das 100 gramas, por isso tal seria possível. O maior problema neste dispositivo é o facto de este dobrar quando não se encontra perante um carro, mas também o de estar constantemente em video-chamada com a polícia prova-se um aspeto desafiante. Deveria-se usar uma comunicação resiliente e rápida,

como o 5G. Cada drone poderia dispor de um hotspot portátil de internet rápida para comunicar rapidamente com os polícias de trânsito em trabalho remoto. Regressando ao tópico do drone desdobrar o tablet e ligar as luzes de emergência ao verificar uma infração, para isto acontecer, teria que haver um sensor para detetar a proximidade do carro e acionar o mecanismo de mostrar o tablet, e quando a polícia saísse do espaço, acionar o mecanismo de retração do tablet, tal como é mostrado no final deste excerto. O nosso grupo fez uma reflexão ao nível da polícia no drone ser uma figura gerada por AI. Mais tarde na cena, foi possível perceber que a polícia demonstrou emoções, inclusive cortando a conversa. Por isso, esta hipótese foi descartada.

Para combater o excesso de velocidade e garantir a segurança nas estradas, o drone, equipado com sensores e software avançado, seria capaz de detectar veículos que ultrapassarem o limite de velocidade. Ao identificar uma infração, o drone acionaria sirenes para alertar o condutor e calcularia a sua localização futura, considerando a desaceleração esperada após a ativação do aviso sonoro. Com base nesta previsão, o drone ajustaria a sua trajetória para interceptar o veículo de forma eficiente, traçando uma linha reta que o levaria do ponto atual ao ponto de interceptação. Note-se que se usam drones para sobrevoar as estradas, o que já é feito em vários países e por isso não existem quaisquer desafios tecnológicos a serem ultrapassados. Constata-se que quando as sirenes do drone-polícia são acionadas a velocidade do carro começa a diminuir até parar. Para isto acontecer o carro teria que receber algum sinal por parte do drone, para diminuir a velocidade. Este faria com que o motor abrandasse quando lhe mandasse esse sinal. Teríamos de ter uma integração entre o carro e o sistema de drones da polícia, para a identificação de drones e obedecer às autoridades. Em outra nota, a integração de dados como localização e coordenadas em tempo real do veículo não seria precisa, pois, na atualidade, os policiais já dispõem de sensores para medir a velocidade.

Já dentro do carro, observamos um ecrã no habitáculo do carro referente ao assistente pessoal de AI embutido com as funções do carro. Retornaremos a este ponto mais adiante, na última cena. Este sistema de AI dispõe de informações relativas ao passageiro, fazendo com que este assistente pessoal lide com dados pessoais - iremos tratar este tópico na secção das legislações. O sistema aparenta ter um microfone sempre ligado e responde a comandos de voz naturalmente. Um destes comandos é o pedido de histórico por parte do polícia, ao que o sistema de AI responde que perdeu consciência e que irá fazer atualizações antivírus disponíveis. Podemos assim concluir que o carro também tem controlo sobre o próprio software, a nível das atualizações.

**Legislações**

Relativamente a esta cena, existem alguns problemas de legislação que têm que ser ultrapassados, muitos deles relacionados com a utilização de drones, mas também relativamente à inteligência artificial usada, nomeadamente em termos legais.

De acordo com a legislação vigente, um drone de porte médio, até 25 kg, da categoria OPEN, o drone que se enquadra nesta categoria, só pode sobrevoar até 120 metros acima do terreno, e nunca acima do piloto remoto 120 metros. Se este encontrar alguma ponte, estes podem sobrevoar 15 m acima de um obstáculo. Sendo assim, relativamente a alturas, não haveria problemas relativamente aos drone polícia, pois estes estariam sempre a mais ao menos esta altura a monitorizar o terreno.No entanto, o principal problema surge da área que está a ser monitorizada, que se trata de uma estrada com carros a passar.

Efetivamente, de acordo com a EASA, European Union Aviation Safety Agency, um ajuntamento de pessoas pode ser num evento ou em ruas com lojas, no horário de funcionamento destas, bem como automóveis a circular em estradas, dessa forma teria que haver alguma alteração na legislação para que fosse permitido o controlo da velocidade por drones, porque senão a área de atuação deste seria reduzida, e estaria constantemente a infringir regulamentações. Além disso, relativamente à condução independente teria que se estudar o possível cenário de aplicação caso algum drone caísse em cima de algum carro ou pessoa, e como proceder caso isso aconteça mesmo que a probabilidade disso acontecer fosse ínfima.

Outro tópico que é preciso ver, é o facto de que quando o carro é encontrado a andar a velocidades perigosas a culpa desta ação recai para a AI do carro, ao invés do condutor. Isto implicaria algumas alterações na lei atual, onde o maior problema seria como lesar o culpado, dado que esta ação não seria praticada por uma pessoa. A inteligência artificial pode ter tido melhorias sucessivas, no entanto, mesmo que esta consiga responder e executar diversas tarefas, esta não apresenta ainda consciência moral ou sequer é capaz de fazer deliberações éticas. Esta consciência moral, implica a capacidade de distinguir entre o certo e o errado e de agir de acordo com esses valores. Desta forma, haveria um problema na culpabilização da AI por algum crime, dado que esta não apresenta esta denominada consciência moral. Além do mais, existiria um problema em aferir a responsabilidade do crime e como é que a AI tomaria responsabilidade dos seus atos. Daí surgiram problemas éticos na utilização desta e na replicação de uma consciência moral utilizada por uma inteligência artificial.

Outro problema que surge no contexto deste vídeo é o facto do microfone estar sempre ligado, isto comprovando-se pelo facto da IA ter respondido ao comentário mais atrevido feito por parte do utilizador à polícia. Isto já é feito por múltiplos sistemas hoje em dia, e estes têm que respeitar as regulamentações impostas pelos RGPD's, tendo que aplicar um filtro para não reconhecer sons exteriores, que não sejam a voz do utilizador. Para além disto, nota-se que a voz dos utilizadores não pode ser gravada.

Relativamente à AI, no decorrer desta cena conseguimos ver que a certa altura a AI acede a informações pessoais como se nada fosse, inferindo relações e sugerindo ligar à namorada do utilizador. Note-se que, este tipo de sistemas já está disponível no mercado, logo o problema identificado aqui seria como guardar os dados do utilizador de forma segura e sem denunciar a sua identidade, e assim cumprindo as recomendações e obrigações dos RGPD's.

**Custo e escalabilidade**

Relativamente a custos e escalabilidade, considerando primeiramente os drones, teríamos que ver a extensão que estes atuariam no controlo de velocidade, dado que se estes estiverem em todos os locais, ou se estiverem somente em alguns locais, o custo de implementação destes seria mais dispendioso. Esta realidade já existe, onde é feito o controlo de velocidade em sítios específicos na Europa, no entanto mobilizar drones específicos para determinadas zonas, de modo a haver um maior controlo ia ser algo muito caro, além de que iria poluir, de certa forma, o espaço aéreo onde estão as estradas. Se a segurança dos utilizadores dependesse da segurança dos carros, este último cenário seria essencial, no entanto o preço de cada drone, bem como identificar as áreas de abrangência de cada um, seria algo custoso também e a escalabilidade seria também um problema.

Outro problema a resolver neste vídeo, que se relaciona com um um problema de tecnologia a utilizar, seria o facto do carro parar autonomamente com a presença do drone polícia. Para que isto fosse realmente eficiente, isto teria que ser implementado em todos os carros, e ser um requisito de segurança para estes, logo todos os carros que circulavam na estrada teriam que ter isto, sendo um default de fabrico.

Relativamente à AI, teríamos aqui dois problemas. Um deles tem a ver com a AI responder consoante o tom de voz, induzindo diferentes expressões e respondendo tal e qual a uma pessoa. Temos que ver que a medição de emoções baseado no tom de voz, seria algo caro, dado que as emoções não são assim tão fáceis de detetar consoante o tom de voz, dado que na linguagem comum existe sempre as ironias e outras expressões, logo esta AI teria que ser treinada com muitos modelos, para que fosse minimamente eficiente. Outro fator seria que se todos os carros tivessem uma AI personalizada que respondesse consoante o tom de voz com as suas informações pessoais, necessitar-se-ia de muito espaço de armazenamento destas informações.

**<u>Cena 4</u> - Diálogo entre o sistema de IA de voz do carro e o condutor.**

Na cena seguinte, podemos observar que, após o diálogo com a polícia, o condutor fica descontente com a atitude que a inteligência artificial do carro teve durante a sua conversa com o drone polícia, Na sequência deste descontentamento o utilizador faz-lhe duas perguntas às quais o carro responde com diferentes tempos de resposta. Após esta pequena conversa o carro retoma o caminho, mas só quando o utilizador pede especificamente por isso. Mais uma vez, notamos a integração de todo o sistema, ao qual o sistema de AI do carro possui controlo total.

**Desafios Tecnológicos**

Um sistema de AI no carro não é algo inédito, aliás, a partir de 2022 surgiu uma tendência de integrar o ChatGPT em vários dispositivos e em 2024, a Volkswagen passou a ter um sistema assistente híbrido com o ChatGPT. Os desafios tecnológicos começam quando se nota que para se ter acesso a respostas do sistema de voz de inteligência artificial, o pedido tem que ir à cloud e percorrer os servidores do fornecedor deste serviço. Deveríamos ter este ponto em atenção e manter a certeza de que ninguém conseguisse obter acesso a dados do veículo e do passageiro, mas iremos falar noutra possível forma mais adiante.

Outra característica problemática dos modelos de AI são que estes, uma vez que se baseiam em probabilidades, podem responder de forma “alucinada”, isto é, não correta. Confiar um sistema de um carro, juntamente com alguns dados pessoais, pode levar a confiar no sistema de AI em cenários onde responde incorretamente. Seria necessário separar este sistema de voz em dois, como os carros de hoje em dia: o primeiro sistema, mais simplista, que responde a comandos como “abre as janelas”, “liga as luzes” ou “limpa as câmaras” ou “começa a andar”. Este sistema identifica as respostas e procura-as dentro do sistema do próprio carro. Os sistemas precisam de ser resilientes contra possíveis ataques, caso o carro seja roubado. O último comando não é possível atualmente, pelo que se trata de um desafio tecnológico. O carro não pode simplesmente começar a andar sem nenhuma outra verificação, como a voz do carro e a inexistência de pessoas ou outros obstáculos na via. Para uma segurança acrescida, o carro trancaria as portas sempre que estivesse parado. O segundo sistema, este sim de AI, funcionaria como funciona o “Apple CarPlay” e “Android Auto”, ou seja, o telemóvel serve de processador e efetua todas as pesquisas a dados pessoais como contactos, titular de contas do pagamento do carro, etc. Deste modo, todos os dados privados

circulariam com o cliente/dono do carro e não com o carro em si. O acesso a estes dados teriam de ser formados por ligações seguras e guardados conforme as opções do utilizador no seu telemóvel. Desta forma, o carro em si não tem guardado quaisquer dados protegidos por legislações. O assistente de AI, na cena, parece responder a qualquer pergunta, mesmo sem lhe ser pedido diretamente, o que envolve ter pelo menos um microfone sempre ligado a ouvir conversas, o que se deve reger por legislações (voltaremos a falar neste tópico mais adiante).

Um problema relacionado com este tópico é o facto de quando o carro está conectado com o telemóvel, qualquer pessoa pode fazer perguntas ao sistema relacionadas com a pessoa que tem o telemóvel conectado. A própria polícia soube utilizar essa função para pedir uma espécie de logs do carro, que acediam a todos estes dados (aceder à caixa negra do dispositivo). Apenas a polícia, juntamente com os sensores do carro que identificaram o drone, poderia ter acesso a estes dados por questões judiciais (neste caso, pedir os acontecimentos durante a condução excessiva do condutor). Outros problemas acrescentados seriam a disponibilidade do passageiro para providenciar estas informações. A polícia por vezes pode abusar do poder e pedir informações que não sejam necessárias à situação atual do caso.

É de notar que nesta cena, os tempos de resposta a várias questões são diferentes, quando por exemplo o dono do carro pergunta de uma forma retórica quem é que faz os pagamentos. O sistema de AI demora algum tempo a responder, não porque demora mais tempo a procurar a informação, mas porque provavelmente identificou a partir da voz, tom de voz e gestos do passageiro, a resposta concordante com esse comportamento. Os desafios tecnológicos passavam por juntar o reconhecimento destas emoções e modo de falar no mesmo "prompt" e calcular a resposta mais provável com o tempo esperado.

**Legislação**

Relativamente a esta cena existem alguns aspetos que necessitariam de ser mudados de forma a cumprir a legislação vigente. Um destes prendia-se com o facto da AI interagir com a polícia sem o utilizador querer. Segundo a nossa abordagem, como explicado acima, qualquer pessoa poderia fazer perguntas à inteligência artificial do carro, e esta só teria informações básicas sobre o carro e contactos. Desta forma, isto poderia introduzir algumas violações de RGPD's, devido à divulgação de informação sensível sobre o utilizador, nomeadamente os nomes das pessoas, contactos telefónicos mas também o tipo de relação com o utilizador, dado que através desta se poderia inferir indiretamente a identidade do utilizador.

Outro fator a notar é o facto dos microfones estarem sempre ligados, o que já acontece hoje em dia. No entanto, existe um problema quando esta guardasse informações pessoais, vozes do utilizador ou outros indivíduos ou sons exteriores, que permitam reconhecer o local. Teria que haver algum mecanismo que impossibilitasse a divulgação destas, por forma a não infringir as regulamentações impostas.Todos os dados usados e processados do carro, tais como gravações das câmaras e dos áudios, nunca poderiam ser acedidos, pois tornar-se-iam em problemas.

No que diz respeito à resposta à polícia, relativamente à namorada de longa duração, a resposta parece quase humana. Sendo assim, haveria um problema grande no desenvolvimento deste "**sentido humano"**, ou de uma "consciência moral" como indicado anteriormente. O desenvolvimento desta seria algo particularmente difícil, em termos de

regime jurídico associado devido a que se uma AI tivesse algum sentido de responsabilidade esta teria que ser julgada da mesma forma que um ser humano, quando cometesse qualquer tipo de ato prejudicial à sociedade, e na divulgação de dados pessoais, que iria contra os RGPD's.

Outro problema que encontramos nesta cena, trata-se do facto de um utilizador conseguir iniciar a marcha do carro, com um comando de voz. Efetivamente para avançar o carro teria que ver se não tinha nenhum carro, pessoa ou objeto em frente para o fazer em segurança, o que nesta cena não acontece, avançando somente em frente. Sendo assim, teria que haver um mecanismo de controlo, por forma a que o carro não andasse sozinho se tivesse objetos em frente, e se o carro andasse em frente a culpa recairia sobre o carro, pois cada carro estaria equipado com este mecanismo.

**Custo e Escalabilidade**

Nesta cena, é importante discutir a escalabilidade do sistema de AI, bem como os custos a si associados. Quanto aos custos, já foi referido anteriormente, mas novamente, não só a produção e treino como também a manutenção e atualização deste sistema têm custos elevadíssimos associados. Quanto à escalabilidade, é importante que este sistema consiga lidar com diversas interações simultâneas e complexas.

Outro grande problema seria a parte legislativa relativamente às possíveis ações que o carro poderia desempenhar através dos comandos de voz do utilizador. De modo a que isto fosse possível, este tornar-se-ia bastante caro, devido a ter de estudar todos os possíveis movimentos de obstáculos circundantes para realizar as ações apropriadas, e não comprometer a segurança do utilizador. Para além disto, de modo a que este sistema fosse o mais seguro possível teríamos de assegurar que a maioria dos carros teria este tipo de sistema, o que implicaria um custo ainda maior na implementação destes serviços de forma a que estes fossem o mais previsíveis e seguros possíveis.

A escalabilidade de sistemas de Inteligência Artificial e o seu custo é, de longe, o maior problema deste terceiro ponto em qualquer uma das quatro cenas faladas neste trabalho. A Inteligência Artificial é, só por si, um conjunto de algoritmos com milhares de milhões de parâmetros e o seu processo de treino exige elevados custos computacionais. Formar um novo algoritmo para os carros iria ser demorado e dispendioso. Para além disto treinar um algoritmo para avaliar o tom de voz do utilizador, bem como conhecer expressões coloquiais o que introduziria uma nova dificuldade, principalmente na percepção de possíveis figuras de estilo, praticadas pelo utilizador, tais como possíveis ironias.

**Referências:**


Caetano Retail. (s.d.). Condução autónoma. Recuperado de https://caetanoretail.pt/blog/conducao-autonoma/

EUR-Lex. (2019). Regulamento (UE) 2019/2144 do Parlamento Europeu e do Conselho de 27 de novembro de 2019 relativo aos requisitos aplicáveis à homologação de veículos autónomos e veículos automatizados. Recuperado de https://eur-lex.europa.eu/legal-content/pt/ALL/?uri=CELEX:32019R2144

Razão Automóvel. (s.d.). Autopedia: Caixa negra automóvel, acesso a dados e privacidade. Recuperado de https://www.razaoautomovel.com/autopedia/caixa-negra-automovel-acesso-a-dados-e-privacidade/

Comissão Europeia. (s.d.). Regras técnicas de segurança dos veículos: Procedimentos de teste para características de segurança avançadas. Recuperado de https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12224-Vehicle-safety-technical-rules-test-procedures-for-advanced-safety-features_en

Autoridade Europeia para a Proteção de Dados. (s.d.). Vigilância por vídeo. Recuperado de https://www.edps.europa.eu/data-protection/data-protection/reference-library/video-surveillance_en

Diário da República Eletrónico. (2019). Lei n.º 58/2019 de 8 de agosto de 2019. Recuperado de https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982

Tecnoblog. (s.d.). Volkswagen vai colocar ChatGPT em seus carros. Recuperado de https://tecnoblog.net/noticias/volkswagen-vai-colocar-chatgpt-em-seus-carros/

Diário da República Eletrónico. (1989). Decreto-Lei n.º 153/89 de 10 de maio de 1989. Recuperado de https://dre.tretas.org/dre/36265/decreto-lei-153-89-de-10-de-maio

LGPD UFSC. (s.d.). Dúvidas frequentes. Recuperado de https://lgpd.ufsc.br/duvidas-frequentes/

Comissão Europeia. (s.d.). O que são dados pessoais? Recuperado de https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_pt

Ghosty Sky. (2024, fevereiro 23). Legislação europeia na utilização de drones: Tudo o que precisa de saber. Recuperado de https://www.ghostysky.com/2024/02/23/legislacao-europeia-na-utilizacao-de-drones-tudo-o-que-precisa-de-saber/

Autoridade Europeia para a Proteção de Dados. (2022). Diretrizes 02/2021 sobre a aplicação do Regulamento (UE) 2016/679 relativo à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais em sistemas de videovigilância. Recuperado de https://www.edpb.europa.eu/system/files/2022-02/edpb_guidelines_202102_on_vva_v2.0_adopted_pt.pdf

Pinheiro, E. (s.d.). Consciência da IA: O dilema moral. Recuperado de https://www.linkedin.com/pulse/consci%C3%AAncia-da-ia-o-dilema-moral-edson-pinheiro-tquqf/

Pereira, L. G. V. R. (s.d.). [Tese de mestrado, Universidade de Coimbra]. Recuperado de https://estudogeral.uc.pt/retrieve/266115/Tese%20Final%202%20-%20Lu%c3%ads%20Gabriel%20Vicente%20Ribeiro%20Pereira.pdf

Diário da República Eletrónico. (1998). Lei n.º 67/98 de 26 de outubro de 1998. Recuperado de https://diariodarepublica.pt/dr/legislacao-consolidada/lei/1998-34450175

Vox Pop Lisboa. (s.d.). Política de privacidade. Recuperado de https://www.voxpoplisboa.pt/politica-de-privacidade.html

Autoridade Nacional de Aviação Civil. (s.d.). Proposta de regulamento para o Regulamento Europeu de Aeronaves Pilotadas à Distância (RPA) - Consulta pública. Recuperado de https://www.anac.pt/SiteCollectionDocuments/legislacao/reg_rpa_consulta_publica.pdf

Agência Europeia para a Segurança da Aviação. (s.d.). Regulamentos de UAS (drones) explicados. Recuperado de https://www.easa.europa.eu/en/the-agency/faqs/regulations-uas-drone-explained

Drone Insights. (s.d.). Perguntas frequentes. Recuperado de https://droneinsights.pt/perguntas-frequentes/qual-e-peso-que-um-drone-pode-carregar/

Pplware. (s.d.). Helicópteros e drones vão controlar velocidade nas estradas. Recuperado de https://pplware.sapo.pt/informacao/helicopteros-drones-controlar-velocidade/

Nordic Steel. (s.d.). Classes de corrosão C1, C2, C3, C4, C5. Recuperado de https://en.nordicsteel.no/fagartikler/korrosjonsklasse-c1-c2-c3-c4-c5

Agência Europeia para a Segurança da Aviação. (s.d.). Voo de drones perto de pessoas. Recuperado de https://www.easa.europa.eu/pt/light/topics/flying-drones-close-people