Universidade de Aveiro
DETI

Professional and Social Aspects of Informatics Engineering

Assignment 3

Analysis of the challenges brought by the technology ecosystem shown in the video

2023-2024

Teacher:
Professor Rui L. Aguiar

Students:
Bárbara Nóbrega Galiza – 105937
José Miguel Costa Gameiro - 108840
Pedro Daniel Fonseca Ramos - 107348

April of 2024

Part 1: Programming Scene

1.1 Technology challenges to overcome

This initial scene spans from the beginning to the 25th second of the video. In this scene, the main actor can be seen using the help of a anthropomorphic AI to debug code. In the present time, the technologies that could be used to produce this human-like AI code assistant already exist separately, namely as AI code assistants (e.g. GitHub Copilot [3]) and as digital humans (e.g. UneeQ Digital Humans [4]). Therefore, it would already be possible to recreate the scene by combining these two technologies.

In the video, the appearance, "personality" and voice of the assistant are very realistic, unlike the digital humans we have today, making it hard to distinguish from a real person to an artificially generated human. So, for that purpose, the current technology would have to be improved.

A possible approach for the required improvement related to the appearance of these assistants would be using Deepfake techniques combined with existing humans, but that would imply a higher computational cost and would require the permission of the person being used to create the avatar. In addition, this approach could cause the already known problems related to Deepfakes, like the out-of-context usage of the video. As for the voice, it is a matter of time and resources until the current speech synthesis becomes more realistic.

For the "personality" of the AI, it depends on how it's generated. If it is chosen from a list of available personalities, it is easier to be implemented, but if it is continually crafted and adapted based on the interactions with the user, it imposes a harder level of computation. For most use cases, and for the goal of recreating what was shown in the video, the first option is enough, since the shown AI is only acting as a simple helper and motivator.

Regarding how the IDE and the code files would be accessed from the car, there are two possibilities: the car has a powerful operating system, with all the desktop computer's common functionality, or a simple OS without any real computing permissions for the user, but with an option to connect to a remote computer. This is similarly implemented nowadays with Android Auto [5] and Apple CarPlay [7] to connect a mobile phone to the inner display and peripherals of a car.

The first option, however, could create several security vulnerabilities by allowing the user to edit files related to the car itself or other core components. Although it would technically be possible to block that interference with core scripts, this option still imposes a greater risk than the second, which is also the natural evolution of what we already have in the present. Still, for the second option to be possible, a reliable network to connect to the remote computer, that could be located kilometers away from the car, would be required.

In conclusion, although many of the technologies that could be used to recreate the scene already exist, it would still be necessary to improve the overall quality of these and greatly improve supporting infrastructures such as the current wireless network.

1.2 Law and regulation blockers

As with most modern problems regarding the use of AI generated and assisted development, the main issues that arise are of credit attribution and copyright violations.

In the video, we can see that the main character is using an AI to help debug code. If we assume that this AI can also help in writing this code, which is currently possible, who takes credit for the code written by the AI? The character, the AI, the people who created the AI or the people who influenced and trained the AI through their own code and allowed it to generate his? It's also important to keep in mind that some of the code used by the AI to train itself could have been copyrighted by the respective owner and not meant for AI training or broader publication.

Currently, there is a large lawsuit against Microsoft, GitHub and OpenAI, claiming that the AI-powered tool "Github Copilot" is helping its users with copyrighted code that was published to GitHub under a license that specifically requires any use of that code to be accompanied by a credit to the original author, which does not happen [26].

In addition, the web-scrapping used by most big AI tools to generate data and training sets is not exempt from privacy and copyright laws, and currently these laws have not yet been adapted to this new technology, meaning most of the scrapped data can be considered as pirated, violating both copyright licenses and anti-piracy laws.

Ultimately, large issues such as the end of open source licenses and the fall of many community and open-source projects could occur if these issues are not resolved by new regulations. If the AI can scrape as much protected data as needed without any consequences, what barrier is there to stop larger corporations from stealing these projects by bypassing these open-source licenses for profit?

In the European Union, there are no copyright laws that specifically target AI-generated works[1], meaning that the ruling of court cases involving the problem of attributing authorship of an AI-generated software would become very subjective to the court itself, which is precisely the opposite of what should happen when the authorship of someone's personal work is questioned, since it can lead to a state of mistrust and abandonment of vital open-source projects, as well as the downfall of many careers.

Another issue that spawns from this misuse of available data, is the privacy of the code written with the help of the AI. If the AI can read the whole program that the character is writing, nothing stops the AI from uploading or using the written document for training purposes, even if the written code was meant to be private by the programmer that was using this tool.

GitHub openly admits that the "Copilot" AI-powered tool collects snippets of the code developed by the user[2], as well as the prompts generated and whether they are used or not, for means that they do not reveal, bringing back the problems outlined at the beginning of this section.

This can be seen in this question in the official GitHub copilot web page: **Does GitHub Copilot ever output personal data?**[2]

The answer posted by GitHub is that "While we've designed GitHub Copilot with privacy in mind, the expansive definition of personal data under legislation like the EU's General Data Protection Regulation (GDPR) means we can't guarantee it will never output such data."

In conclusion, many of the laws revolving intellectual property rights, open source licenses and overall privacy would need to be heavily changed. Laws such as the EU's aforementioned GDPR and recently passed AI act[6] still need to be adapted further to conform to the new uses of these AI tools in a way that can guarantee user privacy and a clear resolution to disputes of copyright infringements.

1.3 Scalability and cost

When a large number of people rely on AI to help them in writing code, then the codes generated will most likely be similar. This similarity could happen due to multiple factors, including the existence of certain coding patterns, the influence of popular AI models on code generation or the fact that this tools tend to give more importance to efficiency and correctness than creativity and innovation. Let's examine GitHub's Copilot, a AI code assistant that works by offering solutions that were developed by other programmers. If the entire Europe utilizes this tool to help them write code, even if the problems they are trying to be solve are different, there will always exists some similarity within the solutions.

In the scene, the AI assisting the human with coding has its own personality, appearance and voice, evident in how it interacts with the human. It appears that the human deliberately selected this options to have an ideal coworker. If we consider that everyone in Europe uses this feature for their AI partners, then there must be a large range of options available for people to select.

The shift in how we interact with computers has undergone a remarkable transformation. In the past, computer usage normally revolved around a central system with separate terminals to access. However, with remote connectivity via internet, things changed completely. Nowadays, people can access and control their computers where ever they want.

Expanding remote computing infrastructure to be able to support millions of people would have some significant implications. On one hand, it improves flexibility and accessibility, allowing them to work and access computing resources from any location with internet. However, such a large-scale deployment would pose considerable scaling challenges. As the number of users and concurrent connections grows, the demand on network bandwidth, server capacity and other resources will also start to grow. Ensuring a safe and trustworthy connectivity across vast geographical areas would be complex and expensive. Additionally, maintaining adequate security measures to store sensitive data and protecting against threats becomes more challenging in this kind of systems.

Initial setup costs, including hardware, network, infrastructure upgrades and software licensing fees would require a significant investment. Ongoing operational expenses, such as maintenance, support and data management, would also contribute to the total cost. Furthermore, the need of redundancy and fail over mechanisms to ensure high availability and reliability would add even more expenses.

Considering the scenario where multiple computers must be capable of running advanced AIs, such as the one in the video, scalability becomes a concern. As the number of computers equipped with AI capabilities increases, so does the need for powerful computational resources. Ensuring that each computer possesses necessary hardware, such as robust processors and large memory to support advanced AI algorithms is essential for maintaining optimal performance. Additionally, the distribution of computational workloads across multiple computers would require efficient load balancing mechanisms to prevent bottlenecks and ensure equal distribution.

To execute the AI algorithms, its required to have powerful hardware, such as GPUs optimized for deep learning tasks, which can constitute a significant investment. Furthermore, licensing fees for proprietary AI software, ongoing maintenance ensuring adequate training and support users to leverage AI capabilities have also high expenses.

In conclusion, the widespread adoption of AI-powered tools and remote computing across Europe offers immense potential for enhancing productivity and accessibility. However, it also brings forth challenges in terms of scalability, infrastructure costs, and maintaining diversity in coding practices. Addressing these challenges will require careful planing, investment, and collaboration among stakeholders to ensure the successful integration of advanced technologies while mitigating associated risks.

Part 2: Driving Scene

2.1 Technology challenges to overcome

The second scene that we identified is the manual driving scene, spanning from the 25th second of the video to the 1 minute and 1 second mark. In this scene, the main character can be seen taking manual control of his car by disabling the car's main AI and overriding the automatic driving capabilities of the car. The main character then drives between the other cars with some dangerous maneuvers.

In this scene, the most prominent technology challenge is clearly the wide-spread adoption of full level 5 self-driving on all the cars on this particular road.

Level 5 self-driving refers to the 6 levels of autonomous driving[8], with level 5 meaning that the car can drive completely autonomously without any human interaction on all scenarios and is the only level where no human attention on the road is required. The beginning of this scene demonstrates that the main character is not even able to see out of the windows while the car is driving itself, indicating this level of self driving.

The highest level of self driving currently achieved by road-legal cars (production vehicles) has recently been beaten by Mercedes[9], reaching a level 3. Currently, there are level 4 cars being tested in the streets for the purpose of ride sharing, and prototype cars that have begun testing to achieve a level 5, but they are still far from being road-worthy [8].

This level of self driving might appear as the biggest problem in this scene, but it is overshadowed by another problem seen in the video, the adaptation of older cars to be self-driving.

In the video we can clearly see ”regular” cars that conform to the same standards and shapes as the cars from the present day, with the only difference being a black half-sphere on top of the roof.

Since these cars can drive along with the new autonomous vehicles, it clearly indicates that they have been adapted in some way to be able to drive autonomously, which tackles the problem of making older cars obsolete and the general population not being able to afford the purchase of a new one. The black half-sphere likely houses the sensors and processing power required to fully transition these cars into the full self-driving world, and would likely be the largest task shown in this scene, since adapting old technologies to work along side new ones always leads to large problems and unexpected compatibility problems.

Another evident technological issue in this scene is the use of another AI that represents the car itself, and is used to control its features.

Although no humanoid character is displayed like in the first scene's AI, this new AI seems to provide much more functionality, allowing the complete control of the car's available functions exclusively through voice commands. In this scene, this AI is not seen doing any particular activity that cannot be done with current voice-assistants, so we conclude that it is simply an evolution of the current existing systems (for now).

The final problem that we identify from this scene is the communication between all the different cars and models on the road.

All the different cars are seen grouped together, leaving very little space between them in case any emergency action needs to be taken, whether because one car had to evade another or a car had a simple blown tire.

This means that the data and signal transfers between cars have to be much faster, reliable and available than any public network currently in use, meaning that, once again, a large leap in network communications needs to be achieved in order to make this scene feasible in the real world.

2.2 Law and regulation blockers

The laws and regulations regarding autonomous driving vary across the globe, with different countries having different levels of permission. For example, Germany was the first country to regulate level 4 autonomous driving, in 2022, and has currently a few operating shuttles on the streets, but with the condition of traveling at a low speed, on fixed routes and with safety drivers [14]. In the United States of America, there are some states that also allow level 4, and ride-hailing services, like the ones provided by Waymo, are already available [15]. Moreover, the first sale of a level 3 self-driving car was made there, in April of 2024 [16].

In an international level, the European Commission has adopted technical legislation for fully driverless, but still on level 4 due to geographic limitations, vehicles (e.g. shutters and robotaxis), and aligns with the United Nations legislation for level 3 automation [17]. Additionally, there are two main regulations that apply to the autonomous vehicles (AVs): the Type-Approval Framework Regulation (TAFR) and General Safety Regulation (GSR), which specify the technical, environmental and safety requirements that need to be met by manufacturers. However, it's important to note some changes might happen upon the full application of the EU AI Act, since it may categorize the AI used in AVs as "high-risk". Even though the EU AI Act recognizes the already existent regulation such as TAFR and GSR, the AI systems that don't fall into that category will be determined by the standard risk level approach [18].

Given this scenario, the existent laws do not allow in any country what is seen in the video, which would be level 5 of autonomous driving. Another aspect that is not well established by some regulations (e.g. European legislation) is the liability factor, that is, who takes the blame when an accident occurs in a fully automated vehicle. In Germany, some of these issues have been clarified by national legislation, in which the owner of the vehicle, being it driverless at the moment or not, takes the responsibility, and the fault of the accident is analyzed individually [19].

So, in order to achieve a fully automated reality, both of the concerns would have to be addressed, and while the level 4 to level 5 improvement relies on the advance of technology, the liability issues pose a more ethical and social aspect that could take longer to get into an agreement. Also, by being an ethical issue, it could vary between countries, what could make the adoption of international regulations a harder task.

Apart from the mentioned regulatory issues, there are some other secondary, but equally as important concerns. In the video, all the cars seem to be fully automated and communicating with each other, as it would make sense in order to create a higher cohesion and avoid accidents between manual and automated cars. So, for that to be possible, either all roads would demand only automated cars to be used, or there would be a separation, where there would be manual-only, or manual-majority roads and autonomous-only roads. That specification would have to be determined by law, and so would have the corresponding punishment in case of infringement. For example, the hacking of the car that happened in the scene, would have to be listed as a felony.

Another concern would be the privacy issues related to the data collected by the sensors and the outside and inside cameras. The outdoor data is used to feed the machine learning algorithm so it can make the automated decisions, which makes it undoubtedly the most important part of the autonomous driving system, but, if not in compliance with data protection's regulations, such as the EU General Data Protection Regulation (GDPR), it can pose a huge threat to the driver. In this scenario, a non-compliant manufacturer would have enough data to know the driver location at all times, and to know their usual routes.

Moreover, the cameras kept inside the car also have to comply to the GDPR (in Europe) or it's equivalents from each country, since it would also record personal data, this case being more critical. In the present, some incidents regarding both internal [20] and external [21] cameras already happened with Tesla cars, which indicates a need for a reinforcement of the current laws.

In conclusion, the current laws and regulations don't allow what is shown in the video to happen yet, and several changes related would have to be made to make it possible. These changes include not only the technical aspects related to the autonomous driving levels permitted, but also the accidents' liability, the manual/automated coexistence road definitions and privacy related issues.

2.3 Scalability and cost

In this scene, we can see a whole new world in terms of autonomous vehicles. A new vehicle model is introduced, with a brand new design, and although vehicles that are more common nowadays are also present, they possess a device on top of them to allow self-driving.

Currently, in Europe, only autonomous cars that fulfill the requirements defined for the 3rd level of the 6 levels of vehicle autonomy, which states that the vehicle has capabilities for environmental detection, and can perform most of the driving shores, but the human can override its command if required, are allowed[8]. Now, in this scene, as mentioned in this report earlier, the level identified for the autonomous vehicles is level 5. So, to allow the whole Europe to start driving level 5 autonomous vehicles, it would be required to change the level permitted, but this would also mean that the production and development of autonomous vehicles would have to increase in a drastic way.

One of the security issues that is presented to us in this scene, is when the human disables the self-driving functionalities, assumes control of it and performs dangerous maneuvers. When it comes to millions of people using autonomous vehicles, its required that the vehicle system does not get compromised or that it has security measures to fix the system automatically in case the system gets corrupted. When this situation occurs, we can see that it doesn't affect the other autonomous vehicles in the road. In order other words, no accidents happen or traffic jamming, because all vehicles have always the notion of whats surrounding them.

In 2017, according to this article [10], the average cost of developing a fully functional automated vehicle could reach about $ 250,000. Carmakers and research industries affirm self-driving equipment could reach up to $ 8,000 - $ 10,000, so this means that a person who owns a $ 25,000 car would have to pay 33 % of the original car's price to turn their vehicle more or less self-driving. On top of all of this, the ongoing maintenance and evaluation of the car and self-driving equipment's condition will also have an impact in the expenses of owning it.

Currently, there are some cars that are not totally self-driving, but have some functionalities, like lane-departure warning, lane-keep assist, adaptive cruise control, autopilot, etc. An example would be Tesla Model S [22], with a price of $ 80,990, and it may include some of the features mentioned above with a price of $ 6,000 or have more enhanced features for $ 12,000 like an enhanced Auto Pilot. If this car that isn't completely autonomous still has a high price associated, then we can expect that when fully autonomous vehicles get in the market for sale, they will be a lot more expensive.

Another important aspect to have in consideration is the network that will handle the communication between all the autonomous vehicles. This network needs to allow the transmission of large amounts of data, because each level 5 autonomous vehicle will send about 25 gigabytes of data per hour [11]. It also requires advanced safety mechanisms to be considered a very safe and protected network, with the purpose of avoiding possible attacks that will affect the communications between the vehicles and, consequently, cause road accidents. The performance can't also be influenced by environment conditions, like fog, snow, ice, rain, lightning, etc.

The network that will allow communication between autonomous vehicles also needs to be able to scale horizontally, meaning that it must allow millions of vehicles to send and receive data so that they can overcome dangerous situations without putting a human being life at risk. It should also always have a very low latency to permit very fast communications and to allow the vehicles to always be aware of the environment surrounding them to determine the next action.

All these requirements for the network, the expenses to develop, maintain, secure and test are extremely high, so this innovation must be very carefully planned to avoid possible mistakes and additional expenses.

Part 3: Police Dialog Scene

3.1 Technology challenges to overcome

The third scene that we identified is the traffic stop scene, spanning from the 1 minute and 1 second mark to the 1 minute and 29 second mark. In this scene, the main character is caught dangerously driving by a policewoman that is communicating via a drone. Additionally, a conversation happens between the main character, the policewoman and the car's representative AI.

The easiest technological challenge to first identify is the way that the police officer is presented in this scene: a drone with a tablet-like screen that has the capacity to fully interact with the occupants of a vehicle in the middle of a highway.

This technology does not pose a serious technological problem by itself, since all of the required functionality for such an interaction has been possible for some years now, apart from the near silent drone fans, which have been tried by many engineers before but were never successfully designed with a silence as good as the one shown in the video.

However this interaction quickly brings back the same challenge that most of the other scenes of this video have, the need for faster, extremely reliable and highly available wireless connectivity.

We also assume that the drone is piloted by an AI, which would need to either be fully contained inside the small drone, or would need to be controlled by a central computer, which then again would require a massive advance in the wireless communication system.

The use of drones also requires the creation of drone charging and maintenance stations. Since we don't know if the drones just regularly patrol the area or if the drones are called, for example, when a radar detects a speeding car, we can assume that these drones have to spend a lot of time in the air, meaning that they have to be very reliable and charge fast, or else it would be necessary for a large amount of drones to make sure that the police service is available when needed.

Another problem we can identify from this scene is when the AI responds to the questions that the police officer asks, even if they reveal personal information of the occupants in the car.

Considering only the technological issues that such a feature would bring, it would mean that the AI would need to have the capacity of correctly identifying the authority of whoever is asking it questions. This would be very hard to achieve, and would require some sort of tagging or central database where the AI could securely retrieve the identity or confirm the authority of the person speaking to it.

Furthermore, the car would need to know exactly what information it can provide to the officer without leaking any of the confidential data from its owner, and be able to register this interaction in case being useful, for example, in court.

Concluding, in this scene, the major technological issue shown is the requirement for a massive improvement of the wireless communications field, where the AI pilot's commands, video, voice, camera and microphone would all need to be able to wirelessly communicate with minimal delay between the different locations and remote parts of the road, in order to effectively deploy these ”virtual officers” without causing problems with the availability of the police force.

The maintenance, charging and range of drones would also need to be considerable improved, which could involve a big leap in the production of batteries and supporting technologies.

Finally the existing AIs would need to be able to correctly identify authority figures and know what data is relevant to them and which pieces of private information they can show or not.

3.2 Law and regulation blockers

In this scene, we're presented with a dialog between 3 main characters, a human being, a police officer talking through a drone and an AI assistant. In terms of laws and regulation blockers some issues were identified, like the footage gathered by the police drone, which the police can use if the AI assistant reveals something about its owner, the virtual police officers and some laws about the use of drones.

The GDPR in Europe imposes several laws and regulations that can be applied to footage gathered by entities, in this case police authorities. For the police officer to be able to see the human being, the tablet used by the drone to transmit needs to record what's in front of it, and if the images recorded are stored somewhere, then it must comply with the GDPR requirements to protect this data from unauthorized access, alteration or disclosure. The human being that's being recorded by the tablet must also be informed, if the footage recorded is being stored in some place, that he's being filmed, the purpose and the retention period of the footage. If we assume that the footage obtained by the tablet is going to be stored, then the entity responsible for saving it should have technical and organizational measures to ensure the security of the personal data present and it should only be retained for no longer than necessary with the purpose of why it was collected [23].

According to the European Union Aviation Safety Agency (EASA),[24] operating a drone in any country in Europe is legal as long as it complies with the regulations defined by it. For example, to control a drone, the person must maintain a visual line of sight or the remote pilot must be assisted by a UA observer [24] (another human being that's watching the drone's track). However, in this scene, the drone isn't being supervised by anyone, since we assumed that an AI is piloting the drone, so for this scenario to become true, it would be required to change this law. Some other points that need to be followed, in order to control a drone legally, is to assure that the drone keeps a safe distance away from any person, or that it doesn't exceeds the 120 meters in terms of altitude, or that it doesn't carry any dangerous goods and will not drop any material [24]. All this topics are functionalities that the drone should have integrate in its system.

Since there isn't any laws or regulations regarding the drone in the scenario presented to us in this scene, then it would be required to create new laws that would make this scenario safe and that it wouldn't cause any legal problems.

Another aspect present in this scene is the virtual police, who is presented in a tablet through a video call. Currently, in Europe, there isn't any law that forbids a police officer to approach a citizen in public and question him/her via an online video call, however, for this situation to be real, it would also be necessary to evaluate every risk, legal problem or dangerous situation and create new laws to make it a safe situation.

The AI assistant present in the vehicle's system can't provide any personal information about the owner of the vehicle without his/her consent, because that would result in an incorrect use of personal data and it would violate the data protection laws defined in Europe. In this scene, the AI gives information to the officer without asking for permission to the owner of the car. Of course that since she's considered an agent of the law, the AI must have some identification mechanisms to identify specific entities and provide only allowed information.

In conclusion, the scenario presents a complex interaction between technology, law an privacy. The current laws in Europe do not allow the scenario to be fully real, and for that not only some laws would have to be changed, but new laws would also have to be created.

3.3 Scalability and cost

The reproduction of this scene in real life would pose big scalability issues. The first one that can be noted relates to amount of drones needed to conduct traffic surveillance. In that sense, there are two paths that could be followed: similar to what is done today with on-site police officers, the drones could be stored in stations placed in strategic places, and if some driver was caught by radars or cameras while infringing the law, the drone would go to the car's location; or the drones could be distributed equally across the road to cover every section of it.

While the first one would be easier to implement and to scale, the second one would create a safer traffic environment, which is particularly important in a full automated cars scenario with the possibility of rogue manual vehicles disrupting the natural flow, like the one shown in the video. The higher safety would come from the quicker action, but that would also mean much more drones and charging stations would be necessary. If it can be guaranteed the speed of drones is high enough to make the delay insignificant, the first option becomes the best one.

Another aspect related to the number of drones needed is the amount of cars on the road. That statistic is highly variable, and so the number of drones available at each moment should follow this proportion, in order to reduce the costs of having an unnecessary large number of machines when not needed and to be able to increase the coverage when most needed.

In terms of how this new scenario would impact the whole Europe, the main concerns would be building the drone stations (where they would charge and wait for any infringement alert) alongside all highways and roads, what would be a huge infrastructure change and not only would cost a lot of money, but would cause a huge disturbance while they were being built. The building of more antennas to support the extremely reliable wireless communication needed for the drones could also contribute to this scalability problem.

The physical security of the drones and their stations is also a critical issue, given the power held by the police upon citizens. In the video, the mounting of drone and tablet does not seem very secure, what could lead to the destruction or split up of the devices by the person being approached. That should be fixed, as it should be harder to interfere with the drones, and would be achieved with a security improvement like using bulletproof glass and stronger attachments. The stations would also have to be equipped with physical security technology, and all of these changes would greatly increase the costs of implementation.

Since the tablets would communicate via network, it would also be very important to guarantee the cybersecurity of those machines and of the communication, so no third party could interfere with the police approach. Also, the amount of drones connected would also pose a scalability problem.

In conclusion, to achieve this innovative scenario across the whole Europe, we would have to deal with the scalability and monetary issues such as deploying and maintaining a large number of drones, building several drone stations across the roads, improving the network infrastructure and guaranteeing the physical and digital security of those machines.

Part 4: AI Dialog Scene

4.1 Technology challenges to overcome

The last scene we identified spans from the 1 minute and 29 seconds mark to the end of the video. In this scene, the character ends the conversation between him, the police officer and the AI assistant and then proceeds to talking only with the assistant.

Although no humanoid character is displayed like in the first scene, the AI assistant provides much more functionality, like informing contacts, gathering payment information and making suggestions based on the context (e.g. when it realizes the man will be late and asks if it should let his girlfriend know about it). While most of this functionality already exists, one of the differences is how the AI answers the man naturally, without much delay, what isn't something we have today with assistants like Alexa or Siri.

In addition, the assistant is fully integrated with the car, which is already possible and has been done by Microsoft [25], with the difference of using not only voice commands, but also video feed trough internal cameras. The combined usage of these two different sources of data wouldn't be hard to achieve with the present technology, and would very likely increase the model's precision.

Another important aspect of the assistant is the data it has access to. In the scene, it can be seen it not only knows the location and destination, but the driver's contacts, appointments and payment history. For that to be possible, it has either to store all that information on the car operating system itself, or to have integration with other devices, like a computer and/or cellphone. The latter seems to be the better option and the natural evolution of what we have with technologies like Android Auto and Apple CarPlay, as mentioned in the first scene. Therefore, there aren't much limitations if the connection is made with a cellphone, but the case of a remote computer connection would require a reliable wireless network.

Moreover, it's important to note this AI assistant still has some limitations. The first one is how it gives out personal information, namely about the man's girlfriend, at the wrong moment (in the man's view). The AI didn't understand the flirting context, and gave out information that disrupted the man's intention. The other limitation is seen when the AI takes a little longer to answer the man's question about who is making the payments. Although that's natural and probably caused by the larger search needed to retrieve that information, it still can be seem as a limitation for disturbing the natural conversation flow.

Overcoming these limitations would pose a great challenge. In the flirting context example, the AI would have the capacity to judge in which situation to reveal certain information, solely based on the tone and context of the conversation, which is highly subjective. As for the second one, it's a matter of computing and network capabilities, and although it's possible to reduce the response time, it's impossible to reduce it to zero.

In conclusion, to achieve this technology, the main challenges would be developing a more precise and natural AI assistant, the integration with remote computers, which depends on a reliable wireless network, and the combined usage of video and audio feed for the assistant. To obtain an even better AI than the one shown in the video, with better context awareness and lower response time, an even better AI would have to be developed and computing and networking resources would have to be greatly improved.

4.2 Law and regulation blockers

In this scene, the main focus for potential law and regulation issues is the access of private data such as bank payments, contacts and calendar by the car's AI.

Similarly to the first scene, the car's AI is shown to have a deep understanding of the activities of its users, for example, here the car knows where the main character is driving, when it wants to arrive and who is waiting for him at the destination.

This means that the same privacy issues from before arise. Currently, in the EU, the private knowledge of an AI is governed by similar GDPR laws that govern the use of other applications, and for an AI to have the level of collected information that was show in this scene, these laws would need to be heavily altered in favor of these AIs.

This would be one of the largest problems with the implementation of this technology, as most countries would have to make exceptions for these AI in order to allow them to collect as much of its user's data as possible.

Currently, AIs and virtual personal assistants such Google Assistant, Samsung's Bixby or Apple's Siri require the use of the developer's own apps, as they lack the legal permissions to acquire data from other apps (although exceptions, such as Spotify or YouTube exists, where the developers of the companies involved have allowed the integration of their apps by these AI).

In the video we can see the AI access the bank statements of Citibank, and since we can assume that Citibank did not develop this AI, the law would clearly need to be changed to accommodate this level of data acquisition.

More specifically, the articles regarding the collection and processing of user data would need to be revised in order to allow AI companies to develop ways of accessing more sources of information, since the current Data Privacy section in the European Union's AI Act[12] does not easily allow for the collection of such data, as quoted in "(...) (the GDPR) requires a valid basis for the collection of personal data (per article 6) and as applicable an additional basis per article 9 for special categories of personal data"[13].

4.3 Scalability and cost

The remake of this scene in real life would also bring important scalability and cost issues. In terms of scalability, the most important one is related to, once again, the wireless network necessary to connect the AI to remote devices. As mentioned in 4.1, if the AI is connected only to the phone and the driver is caring it inside the car, it would be easy to connect via Bluetooth, but other functionality and information that couldn't be achieved via mobile integration would be missing. Therefore, supporting connection to remote computers would be preferred. However, that choice would require a reliable network, that would be able to support a high number of users simultaneously.

Another scalability problem related to the network would be the connectivity to internet at all times, so that the AI could pull information from online sources. That is specially necessary when answering questions such as ”who owns the car” and ”who is making the payments”, like the ones that appear in the video. That connectivity would require a extremely high coverage in all roads, which is not something we have today, and would require a big infrastructure change like the building of more antennas across the whole Europe. Additionally, supporting this connectivity from all cars in Europe would require an extremely reliable network, able to scale as the number of users connected grows.

Regarding the costs of this solution, the integration of the AI assistant to cars would imply a rise of the vehicles manufacturing prices and, subsequently, a rise in the purchasing prices. That would be caused not only by the high cost of adding a powerful computer to the cars, but also by the addition of the cameras used to support the AI. In the video, two of these cameras can been seen. In addition, the costs of building the network infrastructure needed would also be high.

In conclusion, the introduction of AI assistants to vehicles bring some scalability and cost problems such as the number of cars connected to the network, the high cost of fabricating cars with embedded computers of such high processing capabilities and the maintaining of remote access to computers or devices.

References

[1] **Navigating the legal landscape of AI copyright: a comparative analysis of EU, US, and Chinese approaches**

Accessed in: 26/4/2024

`https://link.springer.com/article/10.1007/s43681-023-00299-0`

[2] **GitHub Copilot "FAQ - privacy for individuals "**

Accessed in: 25/4/2024

`https://github.com/features/copilot/#faq-privacy-copilot-for-individuals`

[3] **GitHub Copilot**

Accessed in: 28/4/2024

`https://github.com/features/copilot/`

[4] **UneeQ Digital Humans**

Accessed in: 28/4/2024

`https://www.digitalhumans.com/`

[5] **Android Auto | Android**

Accessed in: 30/4/2024

`https://www.android.com/intl/pt_pt/auto/`

[6] **The EU AI Act's relationship with data protection law**

Accessed in: 30/4/2024

`https://privacymatters.dlapiper.com/2024/04/europe-the-eu-ai-acts-relationship-with-data-protection`

[7] **iOS - CarPlay - Apple**

Accessed in: 30/4/2024

`https://www.apple.com/ios/carplay/`

[8] **The 6 Levels of Vehicle Autonomy Explained**

Accessed in: 30/4/2024

`https://www.synopsys.com/automotive/autonomous-driving-levels.html`

[9] **2024 Mercedes-Benz EQS Sedan and S-Class Will Debut Drive Pilot in the U.S**

Accessed in: 30/4/2024

`https://www.caranddriver.com/news/a42672470/2024-mercedes-benz-eqs-s-class-drive-pilot-autonomous-u`

[10] **What it really costs to turn a car into a self-driving vehicle**

Accessed in: 2/5/2024

`https://qz.com/924212/what-it-really-costs-to-turn-a-car-into-a-self-driving-vehicle`

[11] **6 Key Connectivity Requirements of Autonomous Driving**

Accessed in: 2/5/2024

`https://spectrum.ieee.org/6-key-connectivity-requirements-of-autonomous-driving`

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive

Accessed in: 3/5/2024

https://eur-lex.europa.eu/eli/reg/2016/679/oj

[13] AI Act Explained: Navigating Data Governance in the Age of Artificial Intelligence

Accessed in: 3/5/2024

https://matrixreq.com/blog/ai-act-explained-navigating-data-governance-in-the-age-of-artificial-int

[14] Autonomous vehicles: turning point in European public transport

Accessed in: 4/5/2024

https://ioki.com/en/autonomous-vehicles-turning-point-in-european-regional-and-local-transport/

[15] Autonomous Driving Technology - Learn more about us - Waymo

Accessed in: 4/5/2024

https://waymo.com/about/#blog

[16] 1st self-driving car that 'lets you take your eyes off the road' goes on sale in the US — and it's not a Tesla | Live Science

Accessed in: 4/5/2024

https://www.livescience.com/technology/electric-vehicles/1st-self-driving-car-that-lets-you-take-yo

[17] Vehicle Safety and automated/connected vehicles - European Commission

Accessed in: 4/5/2024

https://single-market-economy.ec.europa.eu/sectors/automotive-industry/vehicle-safety-and-automatedconnected-vehicles_en

[18] Driving Innovation: Navigating the EU AI Act's Impact on Autonomous Vehicles

Accessed in: 4/5/2024

https://www.holisticai.com/blog/driving-innovation-navigating-eu-ai-acts-impact-on-autonomous-vehic

[19] EU: Green light to self-driving vehicles | TRATON

Accessed in: 4/5/2024

https://traton.com/en/newsroom/stories/legal-framework-in-the-eu-driverless-through-europe.html

[20] Tesla workers shared sensitive images recorded by customer cars | Reuters

Accessed in: 4/5/2024

https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-

[21] Tesla Makes Camera Settings More Privacy-Friendly · Dataetisk Tænkehandletank

Accessed in: 4/5/2024

https://dataethics.eu/tesla-makes-camera-settings-more-privacy-friendly/

[22] 10 Cars That Are Almost Self-Driving

Accessed in: 4/5/2024

https://cars.usnews.com/cars-trucks/advice/cars-that-are-almost-self-driving?slide=2

[23] European Data Protection Supervisor - Video Surveillance

Accessed in: 4/5/2024

https://www.edps.europa.eu/data-protection/data-protection/reference-library/video-surveillance_en

[24] European Union Drone Regulations

Accessed in: 5/5/2024

https://uavcoach.com/drone-laws-in-the-european-union/

[25] **Meet TomTom's in-car AI assistant | TomTom Newsroom**
Accessed in: 5/5/2024
https://www.tomtom.com/newsroom/product-focus/meet-tomtom-in-car-ai-assistant/

[26] **Insights from the Pending Copilot Class Action Lawsuit | Articles | Finnegan | Leading IP+ Law Firm**
Accessed in: 25/4/2024
https://www.finnegan.com/en/insights/articles/insights-from-the-pending-copilot-class-action-lawsui
html