universidade de aveiro
departamento de electrónica,
telecomunicações e informática

Aspetos Profissionais e Sociais da Engenharia Informática

Work no. 3

Diana Miranda
NMec: 107457

Miguel Pinto
NMec: 107449

Rúben Garrido
NMec: 107927

June 8, 2024

Contents

1 Fixing broken code in a self-driving car **2**
1.1 Technology challenges . . . 2
1.2 Laws and regulations . . . 3
1.3 Scalability and cost . . . 4
1.3.1 Code editing . . . 4
1.3.2 Self-driving . . . 4

2 Disabling self-driving for a manual high-speed driving **5**
2.1 Technology challenges . . . 5
2.1.1 Cars not having the concept of a human driver . . . 5
2.1.2 Overriding self-driving using a console controller . . . 5
2.2 Laws and regulations . . . 6
2.3 Scalability and cost . . . 7

3 Police drone **8**
3.1 Technology challenges . . . 8
3.2 Laws and regulations . . . 9
3.3 Scalability and cost . . . 10

4 Human-like interaction through AI **11**
4.1 Technology challenges . . . 11
4.2 Laws and regulations . . . 12
4.3 Scalability and cost . . . 13

5 References **14**

1 Fixing broken code in a self-driving car

1.1 Technology challenges

Even though the world is now in the era of AI, the integration of a code editor with a human-like AI pair programmer in a self-driving car presents a unique challenge.

- **Recreating one with a real human appearance is still in its early days**. Take Apple Vision Pro's Persona feature as an example: It creates a 3D model of a person purely based on a few scannings and a bunch of AI, but everyone can notice that its representation is very unnatural. This AI would also have to **be more proactive and to have a wider context span** than it has as of today, offering suggestions, identifying errors, and writing code, without requiring a human's prompt. An example of this kind of AI is GitHub Copilot, however, its context is very short so it sometimes fails to understand the whole project, which is not something a real pair programmer would do.
- Furthermore, the AI would have to **express some sort of feelings**, as we can see in the end of this scene, where the AI-powered pair programmer says "But, dude, we are so close!" when the main character starts to turn it off. Current AI models do not offer such "feature", being devoid of feelings, simply answering what humans ask them without any expression.
- The AI integration and the immersive code editor **requires low latency and high processing capabilities**. While the former immediately suggests on-device processing, the latter implies a data center with a distributed grid computing system, like AWS or Azure. In cases where the IDE is running locally, a powerful CPU and/or GPU is needed to be running in the car, as well as a huge amount of RAM memory.

  However, if the IDE is running in the cloud, connectivity issues arise. Latency and speed are a major problem with current wireless communication infrastructures, where a no-lag experience is inversely proportional to the distance from the host. This way, either this can be replicated only on a single kilometer, or a big set of antennas would have to be implemented on the road, which is extremely expensive.
- Another challenge would be **the operating system the car is running**. It should support several displays, and it should be decoupled from the self-driving system. Also, it should support keyboards, for both the IDE and the car controls. The IDE must be compatible with this operating system, so using Linux seems to be a great idea due to being open-source and having large app compatibility.

This scene also shows a self-driving car, which isn't mature yet with current systems, so a few technological challenges will be faced.

- Right now, AI-based driving (like the Tesla's Autopilot feature) **still requires the driver's attention**, because it's not capable enough to take all decisions by itself.
- The self-driving software **should be decoupled** from any other car features, because any external interaction is a backdoor for hacking, exceptions, failures and more. It should also be resilient and have as few bugs as possible, because every driving decision can take a big impact on other people around.
- **Latency is expected when using external services**, and dealing with lags and missed packets can delay the action time, causing accidents or other types of problems, due to no response from the server. Also, the bandwidth required to send all sensor data to the cloud is much higher than a simple local connection, which brings infrastructure costs. Because of this, the self-driving model should be **run locally in the car** in an independent way, yet sending stats data to a centralized infrastructure.

1.2 Laws and regulations

With current laws, if an accident happens, the person that is sitting on the driver's seat will answer for the respective situation. Also, it's illegal to let a car drive by itself without any human surveillance.

In a fully self-driving environment, regulations will need to follow the evolution, however, there are a few questions that need some discussion. When should laws change? Is there a metric that evaluates a car's ability to fully self-drive? And which country will be the first to take the step?

Furthermore, in the hypothetical case where a self-driving car kills someone in an accident, who's to blame and take consequences against? The car owner trusted the car algorithm, which is said to be trustable. Should the car manufacturer and its software developers be responsible for this murder? How can a judge decide which person has the fault?

Although a special authorization can be issued for recreating a scene like this, there isn't enough information yet that answers these questions. Also, different countries have different regulations, so the implementation a fully autonomous car can be divergent among them.

Another issue regarding regulations is the data collection. For example, in the European Union, the GDPR enforces some data protection rules that limit the tracking companies can do. AI's way of deciding things is essentially based on already-known training data, which means that car manufacturers need to continuously collect data from their cars to keep improving their AI systems. In countries with such laws, the training data must be filtered, so that tracking people (or anything else that represents them) is harder or even impossible.

Besides data training, tracking can also be done when assessing responsibilities. Car manufacturers can get access to data, to check if a specific situation is a car's fault or not [1]. This means that privacy can be violated if security measures are not taken in place, like blurring faces.

Regarding audio, regulations must define that it's illegal to record and store conversations that happen inside the car, especially when that's used for ads or other commercial purposes.

However, despite the country's data protection rules, any data protection can be bypassed when a lawful interception is used. In this case, the car should share as much data as possible, so that responsibilities can be taken against. This means that, although most tracking data should not be sent to the car manufacturer, the car should still store it, so that it can be checked when needed.

1.3 Scalability and cost

1.3.1 Code editing

Regarding the IDE features, where the code editing environment has a human-like AI with a on-device processing, scalability is non-applicable, because the pair programming AI model expectations are the same, whether it is run on a 100-meter driving, a 1-kilometer driving or any other distance.

Talking about the costs, developing this AI takes now less money and time than it would 10 years ago. With the innovation that arises every day in the AI area, it's now more possible than ever to create a virtual human-like 3D model of a person cheaply.

However, AI models are also getting more resource-intensive in terms of training. GPT-4, for example, takes more time, resources and energy to be trained when compared to the standard GPT-3.5 Turbo. This means that, although running it is not very expensive, training the model would need thousands of GPUs, which increases the cost exponentially.

1.3.2 Self-driving

If everything is running on the cloud (and thus there are no actions taken by the car itself), scalability and costs are deeply connected to the communication infrastructure. In the case a new long-distance communication protocol is developed, the number of antennas can be significantly reduced, otherwise proper redundancy and coverage should be assured. This brings some scalability problems: assuring a connection in a single kilometer (even if not in the same road) is different from doing it in an entire city or country. Also, the number of cars directly impact the infrastructure bandwidth needed, which means that scaling cloud-based self-driving cars is difficult and very expensive.

Because of this, a local-powered model should be deployed, where each car has its own processing unit, and there is no need to communicate, send and receive data from a cloud server. This is perfect for scalability, not only in a geographical way but also in a multiplicity one. Also, costs reduce significantly, since the required infrastructure is much smaller than the one with a cloud environment.

Regardless of being local or not, scaling self-driving vehicles can incur more costs in some places. Not all roads or "decision points" fit a stereotypical shape. There are situations where the AI model is more fail-prone due to greater complexity than it was expected. Modifying roads to align with training expectations can incur additional expenses.

2 Disabling self-driving for a manual high-speed driving

2.1 Technology challenges

The cars in the video were clearly self-driven and some components which we are used to see in almost any vehicle were missing, such as a steering wheel, pedals and a hand-brake. This involves engineering the concept of the car without even considering the driver to be a human entity.

Additionally, during the video the protagonist is able to turn off the self-driving through a button in a wireless keyboard and connect a video-game controller to an USB port available in the car, thus allowing him to be the new driver and proceed driving recklessly.

2.1.1 Cars not having the concept of a human driver

- Replacing a human driver - In order to be aware of its surroundings, this new driver entity would need to rely on cameras and sensors all around the car just to have an idea of what actions can and should be performed on any given situation and mainly in real time. For the latter to happen, there is the need for local processing, though the AI itself could be trained in larger computers at the factory with better capabilities before being implemented in each vehicle.
- Human imperfection - Human drivers are not perfect, thus training data would have flaws that would require filtering said data or correcting the model while testing it. This means the switch to self-driving would not be an immediate process, but instead would have a learning curve for both humans and the new driver entities.
- People have needs - The cars will still be intended to carry people from point A to B and we, humans, are unpredictable. The need for a stop, being for leisure, emergency or simply a routine will come up, and the driver entity needs to correspond to this, likely by voice commands and verification of a safe environment when coming to a full-stop.
- Occupants vs Pedestrians - Any maneuver performed must be safe for everyone around the car, we can't just ask it to run over someone, for example as it would bring legal consequences to the human (command giver) and possibly the car manufacturer for allowing such behavior. Therefore, priorities need to be defined through a driving style, either it being more aggressive (close to speed limit, crossing yellow lights, not full stopping upon a stop sign) or, contrarily, a more responsible one.

2.1.2 Overriding self-driving using a console controller

Even though the video protagonist shows joy while overriding the car's controls it appears that this action was not originally intended by the manufacturer, therefore an exploit to the vehicle's software security. This brings a whole new set of worries about cars and would imply that all vehicles require systematic security patches to prevent this behavior.

The newly created driver entities would also need to adapt to this kind of reckless behavior in real-time, as they would likely need to follow the laws of robotics [2] and protect their own occupants (those in different vehicles) from this reckless driver, while minimizing collateral damages to other people's integrity.

2.2 Laws and regulations

Figuring out the legal side of self-driving cars involves addressing key issues like speed limits, accident liabilities, standardizing communication, and data privacy. These regulations shape how autonomous vehicles operate, who's responsible in case of accidents, and how they handle passenger data. As technology advances, these rules will play a vital role in ensuring safe and ethical self-driving experiences on the road.

- Speed limitations - In the movie scenario speed limitations could be temporarily bypassed, mainly due to the road most likely being closed for the effects of the production. In the normal road usage this would certainly not be allowed, as speed limits are defined for every type of road, such information would need to be passed along to the corresponding software so that the new driver entities could comply with it.
- Legal responsibilities - Now that human would not be expected to be the driver of any vehicle, there would be the need to define new rules when it comes to what entity is responsible for an accident, is it the manufacturer, the software developers (of the self-driving system) or the human drivers? [3] When it comes to the override most likely it would fall upon the driver, due to it being an intentional way to break a system and partially on the software developer for allowing such exploit.
- Standardization - In the current world, there is trouble defining standards (in some parts of the world) for the simple act of charging a vehicle, let alone the necessity of a full self-driving traffic on a highway with software on both centralized and on each car, creating new regulations for communication and interoperability standards would be crucial.
- Data privacy concerns - Given that most self-driving vehicles are operated by private companies and collect location information, images of people on the street, there are significant concerns about privacy and data security. [4] Regulations would need to be established and/or improved to ensure that vehicle occupants have control over their personal data and that this data is collected, stored, and used in accordance with ethical and legal standards. This could include requirements for obtaining explicit consent from users for the collection and use of data, anonymization of personal data whenever possible, and the implementation of robust security measures to protect this data against unauthorized access.

2.3 Scalability and cost

When it comes to making self-driving cars work smoothly and affordably, there's a lot to consider. From dealing with heavy traffic to ensuring backup plans are in place for emergencies, and keeping the systems secure from cyber threats. Plus, there's the challenge of getting different systems to be inter-compatible and managing the costs, like insurance and privacy regulations.

- High traffic flow - In a scenario of heavy traffic, the presence of multiple cars at high speeds will significantly increase the probability of accidents. To mitigate this risk, it would be necessary to develop a centralized system to coordinate the actions of all vehicles in real-time. This would involve implementing a vehicle-to-everything (V2X) [5] communication technology to facilitate communication between vehicles and coordinate maneuvers, such as lane changes and speed reduction, safely and efficiently.
- Redundancy - Even with a central system, it is still essential to have redundancy to ensure the safety and reliability of operations. This would include implementing backup strategies for the central system as well as local redundancy systems in each vehicle (multiple censors, communication systems, etc). These backup systems would ensure that in case of central system failure or loss of communication, vehicles would still be able to operate autonomously and safely.
- Security updates - With the increasing complexity of autonomous vehicle control systems and the constant threat of cyber attacks, the implementation of regular security updates is essential to protect vehicles against potential threats. This would involve developing and distributing security patches to fix software vulnerabilities and ensure the integrity and security of vehicle control systems.
- Compatibility - Integrating various systems from different companies will not be easy and will likely demand for government regulation of to follow regarding implementations which could also lead to the delay of the previously mentioned updates.
- Indirect costs - In addition there are other costs associated with the development of these systems, such as impact on insurance costs (the accident risk will change, but now the driving skills are not dependent on the human driver), also the compliance costs with safety and data privacy regulations (the vehicle knows common destinations and hears conversations).

3 Police drone

3.1 Technology challenges

This scene represents a police drone, which is approaching a driver who happens to be overspeeding. Deployment of this technology on the streets bring us a bunch of tech challenges that must be addressed:

- Effective and strong police drones to regulate traffic - The drones should be highly robust and durable since they shall withstand all weathers and should not have the tendency to malfunction easily. Moreover, these drones should be fitted with state-of-the-art sensors and cameras that can interpret their surroundings in real time, almost instantly. They should, therefore, be able to detect any infringement and notify the police stations to which they are connected. This will alert on-duty officers at the police stations, through which the drones can instantly move to the car that has committed the infringement. After that, the police will take over the situation and take the necessary action regarding the vehicle and its occupants.
- Artificial intelligence algorithms to identify dangerous or illegal driving behaviors - Drones will need to be fitted with artificial intelligence algorithms that will process the information in real time and derive the correct conclusion. The AI should be able to discern between dangerous or illegal driving behaviors, such as determining whether one is doing a legal overtake or an illegal overtake. Exists, already, algorithms capable to detect whether passengers wear seat belts, if a driver is using a cellphone or if the driver is distracted [6]. However, for the case seen in the movie scenario these existing algorithms will need to be adapted to the particular needs, because, for example, in the video, the cars are 100% autonomous, so there is no need to check if the driver is distracted. Still, the algorithm should be able to check for compliance with traffic rules, like speed limits and overtaking rules, and its accuracy should be such that there are no false negatives
- Protection from cyber attacks or manipulations - The integrity of the data and the operational safety must be protected at all costs to stop them from being hacked or manipulated, which may result in accidents or abuses. There will always be malicious individuals who may try to hack the system in some way to stop it from detecting their vehicles, and this must be highly made difficult to achieve, ideally impossible. This risk, then, demands that methods be highly secure to stop any kind of attack, be they from external parties or internal members of the police force, which makes them employ highly advanced cybersecurity measures. The network that connects the drones to the police stations must also be highly guarded to avoid any kind of attack that could lead to disruption or delay of the connection between them.
- Highway coverage - Ensuring total coverage ensures that drones can monitor all areas of interest effectively. This includes not only the technical capacity to cover a large area but also the logistic element of maintenance, recharging, and coordination of several drones. Since no area can be left uncovered, ensuring that upon failure of one drone, another one is immediately available to take over the area of the first one is essential. This means that perhaps there should be a drone monitoring the same area simultaneously to ensure that the system is always available and quickly responsive to any incident. Besides covering all the roadways, it is important that the link between the drones and the police station they are connected to is always functional and with very low latency. Communication failure between the drones and the police station should not occur since this is necessary to ensure that on-duty officers receive alerts in real time.

3.2 Laws and regulations

The use of drones for traffic control on roads is already implemented in some countries such as the United States, Canada, China, Russia, and India, however, there is still no standard policy for their use. This is something that is being tested and researched in order to try to overcome several challenges and concerns, such as privacy, security, and public acceptance. And although in some countries the use of drones by the police is already regulated, there are still no specific laws for their use in traffic control as seen in this movie scene [8].

Several benefits are available in implementing drones for traffic control, as, with a proper implementation, it is possible to have complete control of everything happening in a road, something that would be a bit more difficult to be controlled only by human police on-site [7]. Drones can also help in the assessment of accidents, since all images are stored for a period of time, thus allowing the police to review the footage and assess the parties responsible for the accident and the circumstances of the incident.

However, regarding laws and regulations, there must be caution in using these drones so that they do not invade the privacy of citizens, especially in member countries of the European Union, where they are under the General Data Protection Regulation (GDPR), drone usage for monitoring citizens may face serious restrictions unless it complies with privacy laws. Another area where laws and regulations must be well defined is air safety, since the integration of drones in the air space, especially in urban environments and highways, requires coordination with civil aviation authorities to ensure air safety. This implies the avoidance of collision with other aircraft and the avoidance of drones interfering with emergency operations or controlled air traffic.

There is a need to modify and change the law to make the use of drones by the police in air traffic control effective and proper work out in several areas of concern:

- Security and Privacy Policies Development - It would be of paramount importance to develop stringent security and privacy standards to protect the data saved by drones so that the monitoring was done ethically and legally. This would also involve measures such as anonymization of data, as far as possible, and robust security protocols so that there is no unauthorized access or cyber attacks.
- Coordination with Air Traffic Control - There will be a need to develop coordination mechanisms that facilitate interaction between the operations of the drone and the air traffic control so that the premise of avoiding collisions and ensuring the safety of operations will be considered.
- Specific Legislation for Drones in Traffic Control - Specific legislation should be developed and implemented that clearly defines the parameters of the use of drones for traffic control, including the technologies that can be used, how data is collected, stored, and used, and the rights of citizens.

3.3 Scalability and cost

The use of police drones for traffic control across Europe can be quite complex in terms of logistics and finance, and therefore some very important factors need to be considered.

- Initial and Ongoing Costs - Initial costs involved in the purchase of police drones include establishment costs, such as the launch and landing platform infrastructures, integration into traffic management and emergency response systems. There is also costs involved in the training of personal to operate and manage the drone, therefore maintaining efficiency and safety in that role. And the drones require maintenance at regular intervals to ensure they will work and last long, witch involve normal checks and repairs. Another area of consideration is the cost incurred in the energy needed to recharge these machines during frequent use in monitoring and control activities.
- Technological Infrastructure - Effective drone operations need complex control systems that include the costs of software licensing and data storage, along with cutting-edge processing capabilities. Such a system not only has to deal with massive data loads but also provide fast reaction time and availability of the system.
- Costs of regulatory and compliance - Working within local and international drone operating regulations, costs include audits, compliance checks, and system updates to satisfy legal requirements. Non-compliance may be subject to large financial penalties and operation limitations, increasing the overall cost. The drones and their data must be protected with huge investment in advanced cybersecurity measuresthis includes securing communications, implementing encryption technologies, and updating security continuously with training.
- Scalability considerations - The infrastructure that is deployed in the initial drone deployments must be scalable proportionate to the number of drones but, at the same time, should not incur proportional increases in expenses. This means planning for economies of scale such that an increase in the number of drones does not lead to an increase in expenses proportionally. Such an assessment must therefore be done through a conducted economic impact study to understand the return on investment of deploying drones. This includes direct financial benefits of reduction in manpower cost and other indirect benefits in the form of enhanced traffic safety and quicker response to incidents.

4 Human-like interaction through AI

4.1 Technology challenges

This scene shows the AI assistant interacting with the police drone and the car passenger in a similar way human beings do. And even thought there are already AIs that can do much the same thing, the development of a system similar to the one shown in the video would involve at least some technological challenges.

As mentioned in section 1.1, the voice assistant should be decoupled from the self-driving system, because hacking or failures in the former will negatively impact the latter, which can cause several problems.

After the police asked the car its “version of the story”, the car says it “lost consciousness”. This means that the car, although not knowing exactly what happened, has some sort of logging that its system had been unhealthy for a while, and thus makes a security check for some potential viruses. The technological challenge is to have a secondary system that is resilient to failures and keeps track of other component’s health. As stated in section 2.3, that system is a centralized one, that connects multiple vehicles to guarantee redundancy and connectivity between them.

The AI knows whom it is talking with, and it is aware that it is a law enforcement officer, which is a big technological challenge because it furnished the records of the car to the police agent. The important thing is that the AI must be aware that it is having the conversation with the law enforcement agent and shouldn’t provide such information to an ordinary person requesting the same.

This can be done by providing the police’s digital certificate to the car system for verification of the authenticity of communications between the devices. This certificate allows the car to give identification to the police drone as a law enforcement agent. Once this is accomplished, the car’s system can be assured that it is communicating with a law enforcement entity and therefore has the authorization to provide vehicle records in accordance with the current regulations.

Regarding the "long-term girlfriend" interaction, the moment where the AI voice assistant starts speaking is purely a coincidence, since there is no conversation awareness. However, as mentioned in section 1.1, current AIs cannot take judgments or feelings about their surroundings. Associating the adjective "long-term" to the main character’s girlfriend is a judgment of their relationship: how can the AI decide whether a relationship is short or long? There is no metric that evaluates it. This is a technological challenge since AI doesn’t understand emotions, but rather mimics them.

4.2 Laws and regulations

- Personal data access - There are ethical and legal issues related to the privacy of individuals inside the car and access to their personal data by the car's AI system which imply sharing said data with the company responsible for developing said software and likely the car manufacturer as well. **Every collection of data needs to be consented, justified and necessary for the task to perform**. In the video, the value judgment on the occupant's relationship status would not be a valid access, but the data fetching to determine who is making the payments would be.
- Certificate standardization and authenticity - There are already trusted organizations capable of emitting certificates, though **regulations towards said certificates would now need to be reinforced as they will have impact upon accidents involving lives** instead of being a useful tool to navigate in websites, due to the AI system in the car revealing to the police officer what happened from its *own* perspective.
- Reliability as witnesses and defendants - This new driver entity was questioned by the police officer while the car was stopped, which means that upon illegal activity these entities *point of view* could be considered in court. This necessitates a whole **new set of regulations outlining when and to what extent the testimony of such entities could be deemed relevant in legal proceedings**. Additionally, procedures could be established to verify the authenticity of the information provided by autonomous cars and investigate any suspicions of data manipulation or misuse.
- Cross-border considerations - As self-driving vehicles may operate across different jurisdictions with varying regulations, there is a need to address the challenges of regulatory compliance in a global context. Namely, if a car is registered in the United States but meant to be driven in China, it must comply with both U.S. and Chinese regulations, which may differ significantly. A more concrete example of this is Tesla's struggles to export their cars to China, in which the presence of cameras all around is still a barrier to overpass [9]. That being said, **clear guidelines and mechanisms for cross-border regulatory compliance are essential** to ensure the safe and legal operation of self-driving vehicles in diverse geographical areas.

4.3 Scalability and cost

- Data storage and analysis - Costs associated with storing and analyzing large amounts of personal data are already a growing problem with alarming annual growth rates [10] and will increase even more as vehicles get to be self-driven and take advantage of existing systems to store driving data, such as patterns, location history, accidents report, other vehicle and pedestrian movement (through videos).
- Regulatory Compliance and Cybersecurity - Adopting AI in all cars across the Europe is more than just integrating the technology, compliance with the data protection laws, such as GDPR, adds to the costs involved. The regulations mandate protection pf personal data, which requires the integration of the best cybersecurity mechanisms to safeguard against unauthorized access and data breaches. In addition, the expanded use of AI can facilitate cyber-attacks and this attacks on autonomous vehicles, are potential threats that could cause severe real life consequences. Therefore, it is necessary to invest a lot in cybersecurity infrastructure not just for safety but also to improve the trust of the public in the safety and reliability in this type of vehicles.
- Judicial investigation impact - With the introduction of these new entities in legal cases, there would be costs to consider, mainly to the bigger amount of time and resources spent judging this additional information source (to validate its integrity, regulatory compliance and decision impact) in each case.

5 References

[1] CBS News. "Self-Driving Car Ticketed; Company Disputes Violation", at 27 March 2018. https://www.cbsnews.com/sanfrancisco/news/self-driving-car-ticketed-san-francisco/, Last access: April 30 2024.

[2] Wikipedia. "Three Laws of Robotics", at 9 April 2024. https://en.wikipedia.org/wiki/Three_Laws_of_Robotics, Last access: April 28, 2024.

[3] Wikipedia. "Regulation of self-driving cars", at April 22, 2024. https://en.wikipedia.org/wiki/Regulation_of_self-driving_cars, Last access: April 28, 2024.

[4] Matthew Guariglia. "The Impending Privacy Threat of Self-Driving Cars", at August 4, 2023. https://www.eff.org/deeplinks/2023/08/impending-privacy-threat-self-driving-cars, Last access: April 28, 2024.

[5] Kevin Aries. "What Is V2V Technology?: V2V vs V2I vs V2X Technology Systems", at June 4, 2021. https://www.verizonconnect.com/resources/article/connected-vehicle-technology-v2v-v2i-v2x/, Last access: April 28, 2024.

[6] Gareth Roberts. "AI cameras that can spot mobile phone use prove successful in trials", at August 18, 2023. https://www.fleetnews.co.uk/news/car-industry-news/2023/08/17/ai-cameras-that-can-spot-mobile-phone-use-prove-successful-in-trials, Last access: April 26, 2024.

[7] Eleanor Noyce. "Police catch 300 drivers breaking law in three days using AI system", at August 16, 2023. https://www.independent.co.uk/news/uk/crime/devon-cornwall-police-drivers-artificial-intelligence-b2394118.html, Last access: April 26, 2024.

[8] Lexipol Content Development Team. "Key considerations for a law enforcement drone policy", at March 11, 2024. https://www.police1.com/police-products/police-drones/key-considerations-for-a-law-enforcement-drone-policy, Last access: April 29, 2024.

[9] Reuters. "Tesla clears key regulatory hurdles for self-driving in China during Musk visit", at April 29, 2024. https://www.voanews.com/a/tesla-clears-key-regulatory-hurdles-for-self-driving-in-china-during-musk-visit/7588990.html, Last access: April 30, 2024.

[10] Melvin M. Vopson. "The worlds data explained: how much were producing and where its all stored", at May 4, 2021. https://theconversation.com/the-worlds-data-explained-how-much-were-producing-and-where-its-all-stored-159964, Last Access: April 30, 2024.