DISCUSSION

AUTONOMOUS VEHICLES VIGILANCE SYSTEM: PROPOSAL FOR A THEORETICAL LEGAL FRAMEWORK

Veronika Žolnerčíková*[1]

Abstract: *Today's road traffic system is functional due to a complex set of rules. The key element of the system is a natural person in the driver's seat that makes decisions. These decisions may vary from driver to driver, yet all of them can still be compliant. When talking about autonomous vehicles, there is a notion that they need to be instructed on how to behave in all possible situations. However, autonomous vehicles can adopt the same variety of decisions as human drivers do. On top of that, they can communicate with other vehicles, infrastructure, and the surrounding environment. As a result, autonomous vehicles can solve tasks together in a cooperative manner. Such shift in the capabilities of vehicles is so significant that we should not be asking how to make autonomous vehicles conform to the rules, but instead how to structure the rules so that they can conform with autonomous vehicles. This paper aims to present a position on the latter question. Firstly, it describes key features of autonomous vehicles. Secondly, it takes into account relevant legal research in the field of autonomous mobility and identifies the problems that autonomous vehicles pose to the concept of liability. Finally, it provides a summary of key elements for a theoretical legal framework that can encompass autonomous vehicles. An autonomous vehicles vigilance system is proposed as a part of a solution to the liability problem.*

Keywords: *artificial intelligence, autonomous vehicle, product liability, vigilance system, standardization*

1. INTRODUCTION

Autonomous machines are commonly designated simply as "artificial intelligence" or "robots", capable of operating without further human input, therefore with a certain level of autonomy. The term "agent" can be also used because an agent is something that acts and operates autonomously, perceives its environment, creates, and pursues goals.[2] Autonomous machines are reactive. They operate independently by exercising their control over their own actions and are not directly controlled by any other agent. The programming of an autonomous machine is goal oriented.[3]

Autonomous vehicles are a type of an autonomous machine. They have additional abilities allowing them to serve their specific purpose. For example, they can be interconnected with each other and share information. Communication can be also established

[*] Mgr. Veronika Žolnerčíková, Ph.D. student, Institute of Law and Technology, Faculty of Law, Masaryk University, Brno, Czech Republic, an employee of the C4E Centre of Masaryk University, Brno, Czech Republic, and researcher at the Institute of State and Law of Czech Academy of Sciences, Prague, Czech Republic

[1] This article was supported by specific research project fund of Masaryk University No. MUNI/A/1569/2018 "Allocation of Legal Liability in Interconnected Systems".

[2] FRANKLIN, S., GRAESSER, A. Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents. In: *Proceedings of the Third International Workshop on Agent Theories, Architectures, and Languages* [online]. 1996. [2020-10-28]. Available at: <https://link.springer.com/chapter/10.1007/BFb0013570> p. 4.

[3] BROŻEK, B., JAKUBIEC, M. On the Legal Responsibility of Autonomous Machines. *Artificial Intelligence and Law*. 2017, Vol. 25, No. 3, pp. 293–304. See p. 294.

with the surrounding environment including, the road infrastructure. Depending on the type of interconnection, we differentiate between V2V (vehicle-to-vehicle) or V2X (vehicle-to-everything) communication.[4] Autonomous vehicles operate in the physical world. Therefore, they have to be capable of sensing the surrounding environment. This is done a through multitude of sensors, such as ultrasound, lidar, radar, infrared systems or cameras, complemented by high-definition digital maps.[5] This allows the vehicles to gather information about their surroundings and act on it independently without the requirement for other entity (human) to be involved in the process.[6] It navigates itself towards a designated destination. In other words, autonomous vehicles are designed to execute all critical safety functions on their own and to monitor the road for the duration of the ride.[7]

Hand in hand with the evolution of autonomous machines, smart infrastructure is developed – we are aiming towards intelligent transport systems. Cooperative intelligent transport systems (C-ITS) are such systems where users and traffic managers share information through V2V and V2X interconnection and use it to coordinate their actions.[8]

2. THE PROBLEM WITH LIABILITY IN AUTONOMOUS VEHICLES

I identified three main problems with attribution of liability for the conduct of autonomous vehicles. Firstly, we do not know who the responsible party for the conduct of artificial intelligence should be. Secondly, current liability concepts might prove to be ineffective because of the amount of data transfers in interconnected cooperative systems of autonomous vehicles. This kind of data exchange makes proving causality between a conduct and an incurred damage very difficult. Thirdly, the application of product safety rules will not work on intelligent software because defects will be impossible to prove from a legal standpoint. These are my three arguments why there is a liability problem with autonomous vehicles. This chapter analyses them one by one in more detail.

2.1 ATTRIBUTION TO A SPECIFIC PERSON

The key element of today's road traffic system is a natural person in the driver's seat responsible for decision-making. The current bar is set to fit the abilities of a human driver. Desirable attributes in a vehicle with a human driver are crash avoidance, crashworthiness and post-crash survivability.[9] These are without a doubt attributes desirable in an au-

[4] EUROPEAN COMMISSION. Cooperative, connected and automated mobility (C-ITS). In: *European Commission* [online]. 2020 [2020-10-28]. Available at: <https://ec.europa.eu/transport/themes/its/c-its_en>.

[5] LIM, H. Y. *Autonomous Vehicles and the Law: Technology, Algorithms and Ethics.* Cheltenham: Edward Elgar Publishing, 2018. pp. 7–13.

[6] KRAUSOVÁ, A. Legal Regulation of Artificial Beings. *Masaryk University Journal of Law and Technology.* 2007, Vol. 1, No. 1, pp. 155-185, [2020-10-28]. Available at: <https://journals.muni.cz/mujlt/article/view/2451>. p. 187.

[7] MINISTRY OF TRANSPORTATION OF THE CZECH REPUBLIC. Vize autonomní mobility. In: *Ministry of Transportation of the Czech Republic* [online]. 2017 [2019-05-28]. Available at: <https://www.czechspaceportal.cz/3-sekce/its—-inteligentni-dopravni-systemy/strategicke-dokumety/vize-rozvoje-autonomni-mobility/>. p. 14.

[8] Ibid.

[9] MARTIN, J. et al. Certification for Autonomous Vehicles. In: *University of North Carolina at Chapel Hill* [online]. 2015 [2020-10-28]. Available at: <https://www.cs.unc.edu/~anderson/teach/comp790a/certification.pdf>. p. 2.

tonomous vehicle as well. Nevertheless, an autonomous vehicle and therefore its manufacturer will be fully responsible for all the decision making, whereas currently the responsibility and subsequent legal liability is shared with the driver. In the ecosystem of intelligent transportation the driver will be absent.

Traffic safety relies on traffic rules, which are also directed at the driver. However, we do not test the capabilities of the driver. We presume that every human has certain capabilities, and in certain countries the driver has to obtain a driving license by passing a mandatory examination. This again, the shows how liability has always been tied to a conduct of a certain person, natural or legal.

In most European countries, liability is attributed to a specific person based on who caused the damage while following these criteria: a) whose conduct constituting fault has caused it, b) whose abnormally dangerous activity has caused it, or c) whose auxiliary has caused it within the scope of its functions.[10] According to these criteria, we might attribute liability for an accident involving an autonomous vehicle to one of these following persons: Manufacturer, distributor, internet service provider, operator or driver (depending on the liability regime). There is an ongoing debate on this topic, but so far not heading towards a definitive answer. That said, most agree that the party, which has the most information, resources, and over-all capabilities to mitigate potential risks, should be the one to carry the legal consequences of a system failure.[11]

2.2 PROVING CAUSALITY

To hold a party liable, four criteria must be met: a) an illegal action occurs, b) damage is caused and c) causal nexus is established between a) and b). The fourth criterion, fault, is necessary for the attribution of liability only if the law requires it. In extracontractual liability, the criterion of fault must be met only in fault-based liability, not strict-based. However, the criterion of causal nexus (causation) must be fulfilled in all types of liability.[12] This principle is applied in many states, although there are differences in how causation works and how is it proven in court from country to country.

Proving causation between the conduct of AI and damage poses difficulties. Mainly because of the inherent uncontrollability and unpredictability of the machine's software.[13] The issue of causal nexus gets further complicated with the interconnection of autonomous vehicles. A complex environment is created by interconnection. Cooperative

[10] EUROPEAN GROUP ON TORT LAW. Principles of European Tort Law. In: *European Group on Tort Law* [online]. 2005. [2020-10-28]. Available at: <http://www.egtl.org/petl.html>. Art 1.

[11] KRAUSOVÁ, A. et al. Výzkum potenciálu rozvoje umělé inteligence v České republice – Analýza právně-etických aspektů rozvoje umělé inteligence a jejích aplikací v ČR [Analysis of the Development Potential of Artificial Intelligence in the Czech Republic]. In: *Úřad vlády ČR* [online]. 10. 12. 2018. [2020-10-28]. Available at: <https://www.vlada.cz/assets/evropske-zalezitosti/aktualne/AI-pravne-eticka-zprava-2018_final.pdf>.

[12] MELZER, F. Corpus delicti aneb obrana úpravy deliktního práva v návrhu občanského zákoníku. *Bulletin advokacie*. 2011, Vol. 3. pp. 24-27, [2020-10-28]. Available at: <http://obcanskyzakonik.justice.cz/images/pdf/Melzer_Corpus%20delicti_aneb%20obrana_upravy_deliktniho_prava.pdf>.

[13] LIM, H. Y. *Autonomous Vehicles and the Law: Technology, Algorithms and Ethics*. Cheltenham: Edward Elgar Publishing, 2018. pp. 82–98.

system is not bound to a certain number of machines. Vehicles can leave and join any time. Their role in the system is interchangeable. Every vehicle is processing in real time. Imagine a highway where all the cars are in autonomous mode and they leave or join the system by entering the highway territory. Other parties are involved, such as telecommunication and geolocation services providers. All these parties feed data to the system. For example, when an error in data on traffic congestion occurs, it is misinterpreted by the traffic infrastructure and as a result, a car crashes into the lane of other cars. The cause of the event lies somewhere in the system. Determining which unit erred and is responsible might prove to be difficult in a cooperative environment.

2.3 APPLICATION OF PRODUCT LIABILITY RULES ON SOFTWARE

Current legislation ensures the safe conduct of products through product liability rules. These can be accompanied by technical norms. In some products, legislation only tells us that they need to be safe. Technical norms instruct the manufactures on how to comply with that requirement. Specific standards usually take place if the product is deemed to be more dangerous and/or its target user more vulnerable (children for example). Specific standards are also used in technical fields, where it is necessary for products to be compatible to achieve proper function. Without a doubt, artificial intelligence falls under these criteria and therefore, specific standards should be created.[14]

However, product liability rules were not made to conform with software. Product liability lawsuits are based on of these situations: a) product was defective by design, b) inadequate instructions or warnings were given, or c) defect occurred during the manufacturing process.[15] But proving that software is defective is much more complicated than with a tangible product. Let alone with goal-oriented software. In hard-coded software, it shall be, from the technical standpoint, possible to follow the programming step by step. Therefore, it is verifiable if the software met the required standard of care or not.[16] In comparison, intelligent software changes with every iteration and, presumably, it will require further updates and maintenance to ensure its prolonged compatibility and function. The programming choices cannot be traced as easily as in hard-coded software. Additionally, it is yet unclear how to prove if a defect was present when the vehicle left the manufacturing process or, much later, when the product was already in use. Although the vehicle is a machine in the physical world, its functionality relies for the most part on its software. Ergo, the attempt to apply product liability rules on autonomous vehicles will prove to be ineffective.

[14] ŽOLNERČÍKOVÁ, V. Homologation of Autonomous Machines from a Legal Perspective. In: *Proceedings of the EXplainable AI in Law Workshop co-located with the 31st International Conference on Legal Knowledge and Information Systems (JURIX 2018)* [online]. 2019 [2020-10-28]. Available at <http://ceur-ws.org/Vol-2381/xaila 2018_paper_4.pdf>. See pp. 51–52.

[15] KELLER, P. Autonomous Vehicles, Artificial Intelligence, and the Law. *The Journal of Robotics, Artificial Intelligence & the Law*. 2018, Vol. 1, No. 2, [2020-10-28]. Available at: <https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/imported/20180206—autonomous-vehicles-artificial-intelligence-and-the-law.pdf?la=en&revision=5b0de312-a58a-4e77-b5a4-f0fddf16c423>. p. 104.

[16] LIM, H. Y. *Autonomous Vehicles and the Law: Technology, Algorithms and Ethics*. Cheltenham: Edward Elgar Publishing, 2018. p. 82

3. PROPOSAL FOR A THEORETICAL LEGAL FRAMEWORK

To summarize, safety issues surrounding artificial intelligence are specific given that all the capabilities, actions and potential errors of the technology depend on how it is programmed in the first place, since there are limited possibilities of intervention afterward and the human-supervision is absent.[17] Every time the software of the autonomous vehicle processes information, the code itself changes. Because of that, it is not possible to subsequently determine why the machine acted in a certain way, leading to an inherent level of unpredictability.[18]

This paper proposes that the main tool ensuring the safety of artificial intelligence is through the following steps:

1. Creating technical standards usable for goal-oriented programming that will allow to verify compliance with standards of care.
2. Adopting sector-specific legislation that will enable the creation of tailor-made regulation for each sector where AI machines will operate and may present higher safety risks.
3. Including newly made vigilance system allowing periodical testing of AI products during their entire lifecycle.

3.1 TECHNICAL STANDARDS

The key elements are standards and availability of testing methods ensuring that a product is safe and behaves in a desirable manner. Draft provisions on civil rules for robotics[19] indicate that standardization is a key element for artificial intelligence, providing a guarantee for high-level product safety and consumer protection.

The creation of technical standards is required for three reasons. Firstly, to exploit the potential of autonomous vehicles, they need to be interconnected, which requires compatible equipment. Secondly, to properly ensure minimal safety standards, technical parameters of the system of devices and the driving software are needed to be established with caution, therefore they cannot be solely in the hands of the manufacturer. Third, if standards are not available, it can possibly lead to major discrepancies between available products, resulting in safety risk.

We currently do not have technical standards suitable for autonomous vehicles for various reasons: a) missing role-model for their creation, b) unpredictability of the future road traffic-system, c) necessity to determine the threshold for acceptable error rate, d) absence of criteria on the learning data, e) absence of a reliable method for compliance testing – we do not have explainable AI.[20]

[17] See MAURER, M., GERDER, J. CH., LENZ, B. and WINNER, H. (eds.). *Autonomous Driving. Autonomous Driving: Technical, Legal and Societal Aspects*. Germany: Springer, 2016. Available at: <https://link.springer.com/book/10.1007%2F978-3-662-48847-8> p. 446

[18] LIM, H. Y. *Autonomous Vehicles and the Law: Technology, Algorithms and Ethics*. pp. 5–87.

[19] EUROPEAN PARLIAMENT. Report with recommendations to the Commission on Civil Law Rules on Robotics. In: *European Parliament* [online]. 27. 1. 2017. [2020-10-28]. Available at: <http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_CS.html>. Art. 22.

[20] ŽOLNERČÍKOVÁ, V. *Homologation of Autonomous Machines from a Legal Perspective*. pp. 51–52.

3.2 SECTOR-SPECIFIC REGULATION

On 21 July 2017, the European Parliament published a *Report with Recommendations to the Commission on Civil Law Rules on Robotics.*[21] The report comprehensively addresses legal issues related to the development and operations of AI, including: a) liability and fault; b) protection of privacy; c) security and protection; and d) creation of an ethical code for manufacturers.[22] Although the effort is being made in the European Union to provide a basic regulatory framework for all the types of artificial intelligence for civil usage, it is unlikely that rules for AI liability can be uniform, including product safety regulation.

Artificial Intelligence is a multidimensional phenomenon encompassing software operating in cyberspace, autonomous machines operating in the physical world, as well as human-like robots. Even with autonomous cyber-physical machines it is hard to find common ground for regulation. There is no final list including all the types of autonomous machines, but current discussion revolves around autonomous cars, autonomous trains, drones (unmanned aerial vehicles), medical robots and robot caregivers, industrial and agricultural equipment, repair robots,[23] but these are just examples of usage of the technology. Although all these examples are based on AI programming, they do not operate the same. They operate in a different environment, use a variety of sensors, does not learn on the same datasets, and serve a different purpose.

The only thing that the operation of AI devices may have in common is the necessity to determine that the software responsible for the operation of autonomous machines meets the required standard of care and that compliance is ensured through the whole lifecycle of the product. The author of this article perceives this as the key element of future AI regulation framework.

3.3 VIGILANCE SYSTEM

We need a system that can periodically test the abilities of the car's software, confirm that its abilities to perform critical driving functions are intact and that it is still compatible with other units (for example by installing issued updates). This will ensure compliance during the whole lifecycle of autonomous vehicles. Lifelong safety is required also by the proposed cybersecurity regulation. Therefore, it will probably apply to AI technologies anyway.[24]

This is not a new idea and already exists in certain fields. It is called a vigilance system. It is used for example in the field of medicine in the European Union[25] as well as in third

[21] EUROPEAN PARLIAMENT. *Report with recommendations to the Commission on Civil Law Rules on Robotics.*

[22] BASCHOVÁ, D. (ed.). Umělá inteligence a příležitosti v ČR [Artificial Intelligence and Opportunities in the Czech Republic]. In: *The Aspen Institut Central Europe* [online]. 2019. [2020-10-28]. Available at: <https://www.aspeninstitutece.org/news-article/expertni-studie-umela-inteligence-prilezitosti-v-cr/>. p. 21.

[23] These types are also subject to draft provisions of European Parliament, see ibid.

[24] NAUDTS, L. *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure* Security. Leuven: Intersentia, 2019. pp. 196–198.

[25] See EU Council Directive 93/42/EEC of 14 June 1993 concerning medical devices.

countries[26]. With medical devices, it is expected that their quality and safety is ensured not only when they leave the manufacture, but during their whole lifecycle. Surely this makes sense. Under the Czech Medical Devices Act[27] medical devices are tested, whether they consist of hardware, software, or both. The system of incident reporting is a part of the vigilance system. Only certified professionals can perform specified actions with the devices. A supervisory body is established, keeping track of every certified device on the market and reported incidents.

4. CONCLUSION

To sum it up, when an error occurs in intelligent, cooperative transportation systems, it is difficult to identify the responsible party. The burden of proof of causality is on the victim, and there is very limited possibility to do so for an average user. Also, the legal requirements for the proof will be different in each country even if the technology will be regulated on EU level. It is yet unclear which party should be liable for the conduct of AI. Because a variety of AI technologies is in development, it is not possible to adopt one-size-fit-all legislation.

This article presents an argument that we should focus primarily on preventive liability, ensuring product safety. Three steps are proposed for achieving this goal. Firstly, we must create technical standards and verifiable standards of care. Secondly, the work must be done to identify potential risks in each sector where autonomous machines will operate and adopt a tailor-made legislation. Thirdly, vigilance systems should be set in place in those sectors where ensuring safety through the whole lifecycle of a device is necessary. The vigilance system for medical devices can serve as a role model.

[26] See GUPTA, P. et al. Medical device vigilance systems: India, US, UK, and Australia. In: *Medical Devices: Evidence and Research*. 2010, Vol. 3, pp. 67–79, [2020-10-28]. Available at: <https://www.researchgate.net/publication/230723400_Medical_device_vigilance_systems_India_US_UK_and_Australia>.

[27] Czech Act no. 268/2014 Coll., on Medical Devices as amended.