Available at
https://ejournal.ubibanyuwangi.ac.id/index.php/jurnal_tinsika
(Desember 2025)
DOI:-

Jurnal Teknik industri, Sistem informasi dan Teknik informatika,
10(x), 2022, 18-28

A Review: Exploring data protection challenges of automated driving

As autonomous driving advances, data privacy is urgent. Modern vehicles collect immense data streams—from location to biometrics—which are essential for safety but pose serious security risks.

Luqman Hakim[1)]

[1)]*Program Studi Teknik Informatika, Fakultas Teknik, Universitas Bakti Indonesia*
Jalan Kampus Bumi Cempokosari No.40, Cluring - Banyuwangi 68482

mailto:luqman@ubibanyuwangi.ac.id

Introduction

This review will look at how important it is to explore data protection for automated vehicles. The subtopics that will be reviewed include:

1. Exploratory reasons.
2. The idea proposed.
3. Suggestions or conclusions on exploration.

As automated driving technology continues to evolve, the question of data protection has never been more pressing. Modern autonomous vehicles are equipped with a suite of sensors, cameras, and connectivity features that collect vast amounts of data every second—ranging from location and speed to passenger preferences and even biometric information. While this data is essential for ensuring safety, navigation accuracy, and personalized in-car experiences, it also introduces significant challenges regarding privacy and security.

One major concern is the risk of unauthorized access. With so much sensitive information being transmitted between vehicles, cloud servers, and third-party service providers, robust cybersecurity measures must be implemented at every stage. Without stringent safeguards, personal data could be vulnerable to hacking or misuse.

Moreover, questions arise over who truly owns the data generated by these vehicles—the manufacturer, the software provider, or the driver? Clear regulations must be established to define ownership rights and responsibilities. Transparency is key: users should always know what data is being collected about them and how it will be used.

In conclusion, while automated driving promises safer roads and greater convenience for all users, we cannot overlook its profound implications for data protection. Addressing these challenges head-on will ensure that technological progress does not come at the expense of individual privacy rights.

Mission to have Vision Zero by 2050 of road safety facing a challenge of EU data protection framework. The right to data protection is not an absolute right, it must be balanced with other rights. The author is proposed a three-steps approach to ensuring the data protection in automated vehicles at the European level. The possibilities and restrictions of the processing and the use of data under European Union GDPR (General Data Protection Regulation). The author makes a limitation which are to collect and use data related to the physical condition of automatic vehicle users. The automation level using SAE (the Society of Automotive Engineers) which is consist of SAE level 0 – SAE level 5.

Description summary

T. Mulder and N. E. Vellinga paper's is categorized as the controlled research because it's comparing two or more rules and it's also having a limitation of research scope. The author making a good explanation in the beginning about how the data protection is

important and how the health data is also important.

T. Mulder and N. E. Vellinga explain their hypothesis by the role of GDPR which is depending on different circumstances. The definitions of personal data in data concerning health are met when:

a) The data are clearly medical data
b) The data are raw sensor data that can be used in itself or in com- bination with other data to draw a conclusion about the actual health status or health risk of a person
c) Conclusions are drawn about a person's health status or health risk

The scientific method of their research is using use case which are divided into several sections:

1. Types of data
2. Collecting the data
3. Sharing the data
4. Buying the data

Each of those section is having a specific issue which will be recommend for some output and the controller could use below approach:

1. Step 1: Data Protection Impact Assessment (DPIA)
   According to the GPDR and the fourth criterion of the Article 29 Work-ing Party's criteria, DPIA is mandatory. A DPIA must take place prior to the processing, according to Article 35 (1) GDPR.
2. Step 2: Data Protection by Design
   Article 25 paragraph 1 of the GDPR stipulates obligations for data protection by design which is require data protection established from the outset of the earliest design phase, in this case, systems for automated vehicles.
3. Step 3: Data Protection by Default
   Data protection by default refers to the implementation of safeguards that protect the right to data protection as the default setting.

Strict requirements, especially those relating to data on health, add complexity to the implementation of GDPR. Within the GDPR there is the possibility of activities to collect, share and sell personal data and data about health, which in turn can contribute to road safety.

Evaluation summary

T. Mulder and N. E. Vellinga paper's is having a systematic explanation by giving citation which are related to the GPDR issues in regard with data protection for AI (Artificial Intelligence). They also have a clear reason why is the legal implication is needed. The possibilities and restrictions of using and processing personal data is discussed very well, especially when the data is gathered by the AI – in this case is Automated Vehicle.

However, there is a weakness in terms of the use of ISO 27018-2019. They mention about cloud-services but however they did not mention about anything about code of practice for protection data in public clouds. ISO 27018-2019 provide information processing services as PII processors through cloud computing under contract with other organizations. PII is stands for protection of personally identifiable information[1].

Road safety is a public interest and that should have the right to data protection – they said. GPDR is good and DPIA is mandatory but however this is need for a strict requirement for AI to collect the data from the user. However, they did not mention about the regulatory of AI in regards of healthcare. AI could be help and having a good impact for patients and perhaps the providers but however, bad application of AI could be a dangerous for them[2].

Conclusion

In the case of automatic vehicle users, strict requirements must be applied to protect the freedoms and basic rights of data subjects. This contribution has explored some of the possibilities and requirements. Although there are more options regarding the collection of (personal) data via automated vehicles, the processing of data, and further the

requirements that apply to processing. from this data, the GDPR not only sets the requirements, but also offers guidance on how to meet these requirements.

In the healthcare, the relationship between data protection and having a better service regarding Automated Vehicles is demanded. Both have a different perspective.

Taking a deep review on the privacy concerns regarding the data on health of Automated Vehicles users is need more elaboration and supporting documents as well as the related institutions, government, and the AI producers. If the reason is to protect the user's data, while the AI is need for the patient data (the AI users health activity) then the AI algorithm should use Deep Learning or DL to provide patients' data without saving their personally identifiable information[2]. That could be classified as anonymization process. Anonymization is a data processing technique that deletes or changes personally identifiable information[3].

References

[1] 14:00-17:00, "ISO/IEC 27018:2019," ISO. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/65/76559.html (accessed Dec. 10, 2021).

[2] F. Pesapane et al., "Legal and Regulatory Framework for AI Solutions in Healthcare in EU, US, China, and Russia: New Scenarios after a Pandemic," Radiation, vol. 1, no. 4, Art. no. 4, Dec. 2021, doi: 10.3390/radiation1040022.

[3] "How Google anonymizes data – Privacy & Terms – Google." https://policies.google.com/technologies/anonymization?hl=en-US (accessed Dec. 10, 2021).