International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 9 Issue 3, May-Jun 2025 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Evolving Data Security in Autonomous Vehicles: A Comparative Analysis of Major Manufacturers and Legal Considerations

Dilip Kumar[1], Yashwant Kumar[2]

[1]Department of Engineering, Snowflake Inc, San Mateo, CA, USA
[2]Engineering Department, Hitachi Rail, GTS, India

ABSTRACT

Increasingly, the proliferation of autonomous vehicles (AVs) presents significant demand for driving data security in transportation systems. The proposed paper aims to address current trends in AV data security, investigating data protection approaches adopted by manufacturers, including cybersecurity and threats mitigating strategies. The comparative analysis will be conducted based on industry leaders, including Tesla and Waymo. Three aspects will be central within the research framework: the comparison of threat architectures for each manufacturer, similarities and differences between data security approaches, and exploration of the legal provisions and regulatory aspects governing AV data protection in current condition. The critical analysis of the existing data protection differences and related evidence will enable to reveal the interdependencies between the driving data mechanisms of current manufacturers, vulnerabilities, and the prospects of the existing data protection legal provisions. It is expected that significant trafficking data will reveal core differences between manufacturers as well as gaps in data protection measures and related standards. Data analysis can support global approaches to AV driving data security and protection measures.

KEYWORDS: *Autonomous Vehicles; Data Security; Cybersecurity; Privacy; Legal Regulations; Tesla; Waymo; Automotive Technology; Comparative Analysis*

How to cite this paper: Dilip Kumar | Yashwant Kumar "Evolving Data Security in Autonomous Vehicles: A Comparative Analysis of Major Manufacturers and Legal Considerations" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-9 | Issue-3, June 2025, pp.838-845, URL: www.ijtsrd.com/papers/ijtsrd81164.pdf

IJTSRD81164

INTRODUCTION

The automobile industry is one of the most dynamically developing industries. Nowadays, the integration of data security tools remains a crucial factor in the production of self-driving vehicles. With the rise of increasing dependence of cars upon advanced data systems, the secure process of data handling has become the industry utmost need. To this end, the current report aims to conduct a profound overview of the self-driving car manufacturers' companies. The study objectives include a thorough analysis of the current situation among the industry players and a comparative overview of their firms' data security. In addition, the study will aim to dwell upon the development of legal guidelines with respect to the secure mechanism of personal data storage. The current issue has become a hot topic, owing to the rapid technological progress and concerns driven by it. Moreover, the report will aim to present the positive and negative aspects of self-driving cars as well as the evaluation of their methods on how automotive corporations protect the data they gather. Thus, the current report intends to portray the automobile industry status quo.

Artificial Intelligence presence in threat detection systems for autonomous vehicles can evolve to play a pivotal part in bolstering the operational security facets of self-driving cars. With AI-based threat detection systems, automobile firms would enhance their abilities in forecasting and counteracting the increasingly complex cyber threats this tech industry face. A robust commitment to data security, AI could lend itself to framing autonomous vehicle security protocols, would be essential not only to protect the private data secured from consumers patronage but also to minimize the chances of data leaks that could threaten the integrity of innovative tech in autonomous cars (Khan et al. 107054). The

establishment of laws that encourages the synchronization of security frameworks from autonomous technologies manufacturers and the recognition of consumer data privacy demands with data access limitations and validations would be crucial. Artificial intelligence can prove a functional tool in the contextualization of robust cybersecurity infrastructure for the operational rights and safety of autonomous vehicles.

How does the autonomous cars work?

Autonomous vehicles functions with the help of interconnecting sensors, actuators and powerful processors that employ complex algorithms to sense the surroundings and decide how the vehicle has to go ahead using various machine learning algorithms.

The virtual map of surroundings is created and maintained in the car by making using of various sensors that are located in different parts of the car. For example, the video cameras are used for detecting traffic lights, reading road signs and tracking other vehicles and pedestrians. The LIDAR sensors are used for measuring distances between the car and road edges, potholes or pedestrians, in short to create 3D map of the environment. RADARs are used to measure relative velocity, direction vector of the oncoming vehicles, distance to the object etc and they operate at 76-77GHz frequency. A sophisticated software that runs complex algorithms makes use of the data provided by the visual sensors and lidars and effectively decides what has to be done and signals the actuators. Actuators can be steering control, brakes, acoustic and visual warnings etc.

Tesla Vs Waymo

- Both Tesla and Waymo follow the same approach but the most important difference between their cars is Tesla operates on thousands of vehicles at real time on road and gets the real world data thereby making their vehicles more effective in real world scenarios.
- The Waymo autonomous cars are dependent mostly on the results of virtual simulations which are fed to the processor and the cars are run in the controlled environment.
- Waymo was founded in 2009 but it started to apply deep neural network algorithms for pedestrian detection in 2015 whereas Tesla started it in 2016 and by 2017, Tesla was able to deploy the 2nd gen of autopilot by using its own computer vision neural networks.
- Generally, affordable LIDARs are said to be expensive and have low resolution for seeing small details like pedestraian's nuanced body languages, detect small obstacles like plastic bags or cinder blocks. Using LIDARs doesnt prevent the use of cameras but using cameras makes it easy to distinguish the small features which can help the neural networks to predict their algorithms. But, Waymo makes use of high grade LIDARs which when placed at right position can function effectively in the dark as well.
- Waymo pilots itself without the need for any driver. But it can perform well only for small, geographically fenced environment. Wheras Tesla uses drivers for monitoring the behavior of the technology closely and take actions when absolutely necessary and then report the test observations to Tesla to correct the shortfalls.

Security issues with autonomous vehicles data

The growing autonomous vehicle industry has brought important cybersecurity issues such as data-flow regulation standardization and data law integration across multiple geographies. The important issue that arises from the aforementioned cybersecurity challenges is related to the CAVs Network Operator Centre that is responsible for the data-flow of connected and automated vehicles (Khan et al. 58–71). It is important to have a centralized and regulated control for the CAVs Network Operator Centre to prevent any data breaches towards consumers using the technology and vehicle manufacturers such as Tesla, Waymo, Ford, and General Motors operate under a standard law among other manufacturers. For example, the development of Autopilot by Tesla which is claimed to be the first commercial vehicle autonomy must be put under cybersecurity law to ensure the data protected and cannot be breached by others. Another example is Waymo who aims to offer safe, autonomous ridesharing service will need data protection regulation integration among others for their testing procedures on the road and sharing data with other manufacturers.

Comparison of Major Autonomous Car-Producing Companies

The market presence of prominent players in the autonomous development industry is associated with certain technologies and business patterns. Thus, Tesla's automated solutions are based on electric cars and the Autopilot system (Wang et al. 8867757). The inclination of Waymo (the subsidiary of Alphabet Inc.) to extensive road-testing and software development defines its place in the market connected with the fully autonomous ridesharing (Muhammad et al. 4316–36). In the case of Ford and General Motors, their autonomous technology is an addition to the existing series of cars that the company offers (Muhammad et al. 4316–36).

In addition, autonomous car producers have varying data security techniques which are mainly encryption and strict protection protocols next to personal data. Tesla uses sophisticated encryption procedures in its communication networks to avoid external interference in vehicle data demonstrating the company's reliability and customer trust in the data (Almeaibed et al. 40–46). Waymo has established strict data security measures such as key management and threats identification systems to increase the protection of autonomous cars (Nanda et al. 60–65). The autonomous car technologies of Ford and General Motors mainly focus on data encryption techniques that comply with the international requirements and standards (Nanda et al. 60–65). As these companies continue to develop their autonomous cars, there is a need to introduce new data security measures to further enhance data protection.

Finally, there is a significant divergence between the leading autonomous vehicle manufacturers' approaches to user data management in terms of transparency and control. Tesla emphasizes user engagement by establishing direct communication with its consumers, clarifying data consent protocols, and providing users with transparent information on their data usage practices, thereby supporting user trust (Yaqoob et al. 174–81). On the contrary, Waymo implements an elaborated consent management system that enables users to configure their data sharing preferences, thereby increasing perception of user control and using the related factors to enhance user confidence (Pisarov and Mester). As for Ford and General Motors, both manufacturers admit the importance of strict adherence to current privacy protection regulations and guidelines by presenting detailed disclosures on data usage practices and securing explicit consent prior to any data collection, which is perceived as the best practice for ethical data usage (Almeaibed et al. 40–46). Overall, the diverse approaches to user data management by the Autonomous Vehicle Technology manufacturers can be viewed as a part of a considerable industry-wide effort to ensure thorough privacy protection, technological advancement in the field, and user trust.

Furthermore, the efficiency of the data security plan of the autonomous vehicle-producing companies is mostly difficult to determine in the absence of recent data mishaps and breach activities. Tesla has made an impressive leap in strengthening the encryption configuration for its data protection techniques; nevertheless, it has been the subject of various unlawful access attempts directed at its interface with its automobiles (Almeaibed et al. 40–46). Likewise, Waymo's age-old data protection mechanism has been vulnerable on occasions regarding its fringe sensors which are most potentially susceptible to adversaries, according to the examination performed by X Sun et al. (Sun et al. 6240–59). Ford and General Motors have taken a step to put pressure on their integrity for secure data storage; however, following the cyberattack, it is clearly evident that it is also susceptible, therefore, their data encryption systems require further improvement (Nanda et al. 60–65).

- Data security measures of major AV firms are discussed in this section:
- Tesla: Uses OTA updates, end-to-end encryption, and AI-based anomaly detection. Car collects data for updates and improvements. Tesla also uses encryption to enhance user privacy.
- Waymo: Uses hardware security module, encrypted storage and strict penetration testing. Waymo is applying security across both hardware and software.
- General Motors (Cruise): Multi-layer authentication, real-time threat detection, compliance with cybersecurity standards. Cruise's security model involves proactive monitoring to detect potential threats before they impact vehicle operation.

The comparison of such approaches will allow evaluating the effectiveness of each of them and defining smart practices for AV data protection.

Legal Regulations for Storing Personal Data Securely

International standards and treaties are part of the legal structure that manages the storage of personal data concerning automobile systems. One of the key examples is GDPR, which is practiced in the European Union and imposes strict data protection rules. Based on GDPR regulations, companies operating in the automobile industry are required to adhere to strict rules regarding data storage and implementation of specific data protection measures (Taeihagh & Lim, n.d.). In fact, GDPR gives instructions and recommendations regarding the localization of data storage in such a way when the specific data should be stored on certain areas and borders (Taeihagh & Lim, n.d.). On the international level, such treaties as UNECE encourage cross-border uniformity in the protection of data and cybersecurity principles and have links to the storage and usage of personal data. Among the major aims of these international laws and agreements are the minimization of cyber threats and security issues developed by automobile automobile programs. At the same time, they are directed toward standardization of the data protection process concerning automobiles and vehicle systems,

contributing to a common level of automobile data functioning.

Specifically, the regulations applicable to the autonomous vehicles focus on the data storage, user privacy, and compliance requirements. One of the clear regulations is that of the GDPR. It implements strict data storing and handling practices focusing on the user consent and the data localization (Taeihagh and Lim 103–28). The California Consumer Privacy Act (CCPA) also holds the similar burden on the manufacturers to provide the clarity regarding the data usage while providing the users with more control on their individual data. Similarly, there is a need for compliance with the ISO/ SAE 21434 standards. This standard deals with the automotive cybersecurity and risk management requirements for the vehicle data communication. These standards are essential and collectively deal with the storage and processing requirements of the data while creating trust in the consumers that the manufacturers of the autonomous vehicles are working with the privacy and security standards recognized by the different countries and jurisdictions.

Despite the referred above, the autonomous car companies face a number of barriers to comply with data security policy standards due to constant changes in these standards. The most significant obstacle is the cross-sectional character of the data made by autonomous cars. The GDPR and CCPA, for example, have different requirements regarding regional data practices (Taeihagh and Lim 103–28). Thus, companies should constantly adjust their standards to comply with the policy despite the high pace of development of technological projects. Another significant obstacle is the rapid technological development. It often happens that the development of new technologies significantly outpaces the development of existing legislative norms. Consequently, companies should adjust their legal frameworks to overcome data vulnerabilities in autonomous vehicles. The autonomous vehicle consists of a complex system of interconnected components, including various sensors. Increased incorporation inevitably leads to increased vulnerabilities as well as complicates the implementation of compliance due to the increased number of components (Sun et al. 6240–59).

Moreover, international institutions and government organizations are significantly involved in the enforcement of data safety regulations for autonomous vehicles, thereby enhancing cohesive compliance throughout the industry. Institutions such as the European Union and regulations like the General Data Protection Regulation (GDPR) impose strict measures and compliance privacy and data safety daters, thereby compelling automobile industries to enhance the dependability of their data practices (Taeihagh and Lim 103–28). Besides, they partner with automotive industries for standardization of procedures that foster accountability and transparency across diverse stakeholders. In the USA, Federal agencies unit with star authorities to define the nature of the impact of technology, considering the trade between innovation and strict non-negotiable safety requirements. The engagement aims to address the cybersecurity threats and maintain data privacy, which remain essential during the evolving technological developments of autonomous vehicles (Sun et al. 6240–59).

- AVs data security falls under the certain regulations, such as:
- The General Data Protection Regulation (GDPR): Provides requirements for processing personal data in autonomous vehicles (AVs) in the European Union (EU).
- California Consumer Privacy Act (CCPA): Ties data rights and protections to consumers of AVs in California.
- The National Highway Traffic Safety Administration (NHTSA) Guidelines: Established guideline for cybersecurity best practices for AV manufacturers.
- ISO/SAE 21434: A worldwide standard for the risk management of cybersecurity in automobiles.

Pros and Cons of Using Autonomous Cars

The benefits of using autonomous cars are many. Automating vehicles promises safer roads since human error is considered to be one of the main causes of traffic accidents. With the usage of autonomous vehicles, it will rely heavily on the use of technologies such as sensors and algorithms that will constantly assess the surroundings - leading to more organized and accidents free roads (Ahangar et al., 2020) (Ahangar et al. 706). On the other hand, they are factors that optimize traffic - meaning less congestion especially in the city, and reduced time of being idle in traffic which will lead to a more efficient system and is also less harmful to the environment compared to before with high fuel consumptions. All these will contribute to the overall improvement that is offered wherein transportation is much safer and friendly thanks due the automation that is employed in this aspect (Wang et al. 8867757).

Meanwhile, autonomous vehicles have also been associated with drawbacks. One concern is the technological limitations wherein the network of sensors and processors that allow the vehicle to operate autonomously are still prone to errors and

malfunctions (Parekh et al. 2162). Another concern relates to ethics which involves the decision-making ability of the vehicle in critical situations such as choosing between the safety of its passengers and the risks imposed to other entities. Lastly, the advancement of autonomous vehicles may lead to employment loss for drivers of various transports (Pisarov and Mester). Therefore, if the implementation of autonomous vehicles is to be considered, the aforementioned drawbacks should also be accounted for aside from its benefits.

The pros of self-driving vehicles includes the improvement it brings in road safety as it will removed human error in driving. Human error is considered one of the causes of road accidents and according to the study by Ahangar et al., autonomous vehicles are equipped with sensors and algorithms to analyze on the road and hence, will continue to decrease traffic accidents (Ahangar et al. 706). Next, self-driving vehicles can improve traffic condition as its algorithms will follow specific set of rules to drive continuously. Expectedly, there will be lesser traffic jams in particularly in urban areas where its gridded structure causes traffic (Wang et al. 8867757). Time wasting activities such as waiting on traffic can be decreased and leads towards a system which directs vehicles better while also remaining green as it requested less burning fuel. In conclusion, the expected advantages result in a better automobile system where transition towards self-driving cars results in improved safety and greener vehicles. Automation is a regime change in the automobile industry so far (Ahangar et al. 706).

Autonomous cars development also have major economic impacts, positive and negative. Economically, autonomy will greatly increase productivity since in a society where autonomous cars are the norm, time spent commuting would be remolded into a time usable for working or having leisure activities, further increasing GDP output. Also, the economic costs of logistics would be reduced highly thanks to minimization of traffic jams and accidents, making transport more efficient and cheap for companies. On the downside, autonomous cars put many jobs relying on classic driving at stake, meaning that the workforce will have to be retrained and the affected economy diversified and adjusted (Pisarov and Mester). Nonetheless, despite the autonomous development showing a promising future economically for society as a whole, the consequent challenges arise have to be coped successfully in order to maintain a productive balance as this technology gets improved.

Data Collection Safety by Automobile Companies

Autonomous vehicles collect their data through a network of connected sensors. The established V2V radiant systems enable communication between different vehicles. The vehicle's infrastructure is also composed of sensors such as LiDAR, radar, cameras, etc., to gather more extensive data features and ensure safe navigating (Ignatious and Khan 736–41). Aside from the collected data from the sensors, vehicle connectivity through efficient communication is also crucial in decision-making. With the consideration of real-time data computation on the road(Hudea et al., 2018)(Nanda et al. 60–65), data security can also be questioned with the introduction of such technologies. Thus, further improvements are needed if breaches could potentially damage the entire functionality of vehicles or infringe user privacy. Also, it is difficult to secure these connections as the network environment is dynamic (Sun et al. 6240–59).

In addition to this, data protection while gathering and transferring information, also plays a crucial role in the autonomous vehicle system, it is important to possess the data with respect to its integrity and privacy. The primary way of data protection is through the encryption technology where the data will be protected using encryption technique as information transfer through vehicle communication network. State-of-the-art encryption algorithms are used to protect the unauthorized access of vehicles' onboard and transmission network data, as per newly published research on communication security for autonomous platform (Nanda et al. 60–65). Besides encryption, secure networking protocols are also influential in data protection to build strong protective measures against unsolicited cyber-attacks. Together, these practices provide a strong mechanism to mitigate the threats, and also synchronize with the growing cybersecurity revolution in the automobile industry, thereby enhancing the users' faith in autonomous vehicles technology.

Nonetheless, it remains undeniable that data collection processes behind AVs carry certain risks regarding privacy and security vulnerabilities. The reliance of these systems on highly sophisticated sensing and networking technologies creates potential for inadvertent exposure of sensitive data, which is susceptible to access from peripheral sensors through unauthorized network connections (Sun et al. 6240–59). The implementation of autonomous data collection processes exposes potential privacy risks due to the huge volume of personal data collected such as geographical location and driving habits, which are vulnerable due to certain weaknesses in their implementation and securing protocols. In addition, the complexity of AV systems pose security

vulnerabilities, particularly in insecure environments due to uncertainties regarding the integrity of collective connected systems (Nanda et al. 60–65). In this regard, these vulnerabilities highlight an immediate need for the establishment of adequate encryption protocols and access restrictions required in ensuring the security and trust of personal user data against breaches in autonomous and intelligent vehicular technologies.

Furthermore, the use of artificial intelligence (AI) represents both opportunities and challenges for the enhancement of data collection safety in autonomous vehicles. Through the use of AI algorithms, the accuracy of data processing is further optimized, as these algorithms are capable of learning from large datasets and improving the reliability of the information received by the vehicle's systems (Bathla et al. 7632892). However, the complexity of AI platforms may also create new vulnerabilities that adversaries may seek to exploit, further necessitating the need for cybersecurity of critical vehicles (Bathla et al. 7632892). Additionally, AI's ability for real-time decision-making will require additional processing capabilities, which, while beneficial for data processing, may also present unique challenges related to energy consumption and hardware requirements (Bathla et al. 7632892). Therefore, as the use of AI in autonomous vehicles evolves, the task of balancing enhanced data safety with unique security challenges will be a priority for manufacturers that continue to hope for public adoption and adherence to existing regulatory measures.

Nevertheless, the data gathering systems that are essential for the operation of autonomous vehicles represent critical risks associated with unauthorized access or the exploitation of data collected by the vehicle. The utilization of advanced sensing and communication technologies in autonomous vehicles renders these systems vulnerable to cyberattacks, as unauthorized users may exploit vulnerabilities in auxiliary vehicle sensors to gain access to protected information (Reference-erbc-UH3iVAJ). The risk is exacerbated by the wealth of sensitive data collected by the vehicle, including personal details such as location and driving habits, contributing to privacy breaches or data misuse, and the complexity of operations, which hinders the implementation of reliable security, as demonstrated by concerns about secure network retention in different operational scenarios (Reference-QYMMAqIJjeAJ). It is critical to mitigate these threats through strong encryption and access restrictions.

Looking forward, anticipated developments in autonomous vehicles data gathering safety will greatly change with modernization and progressive rules and regulations. With the modernization of the autonomous vehicle industry, technologies such as artificial intelligence will become more advanced and integrated the data gathering system in autonomous vehicles allowing for safer measures that will not hinder productivity and efficiency (Bathla et al. 7632892). Moreover, machine learning will also develop and assist in analyzing data of autonomous vehicles being utilized to be more aware of the circumstance and conditions that will affect safety records. With these developments, better safety practices can be integrated along the data-gathering process to ensure proper use of information. The laws and regulations that will be related to data security and related issues are expected to be increasingly involved internationally as autonomous data-harvesting vehicles gain popularity and usage in various countries (Taeihagh and Lim 103–28). Data owners will be more aware of their rights regarding data access. These developments and changes will influence autonomous vehicle users to further innovate data collection systems to ensure safety, effectiveness, and security of consumer data rights and privacy internationally.

Industry Best Practices and Recommendations

Learning from best practices concerning data security in the autonomous vehicle industry is possible through a couple of case studies. Tesla where data security has been achieved through end-to-end encryption best practice is one of them. The company's commitment to this practice has proven its worth in implementing secure communication among vehicles and subsequently preserving network data integrity (Nanda et al. 60–65). Another case study is that of Waymo, which achieved significant data privacy and security through the use of intrusion detection systems. The company bases its intrusion detection methodology on an overview of the entire communication infrastructure where potential breaches are monitored and dealt with (Almeaibed et al. 40–46). The auto manufacturer also employs standard intrusion detection technology academy to the autonomous car industry. Other case studies that can be evaluated include Ford, which employs multi-layered encryption practices to conform to best practice security standards (Sun et al. 6240–59). In essence, the united practices illustrate that multi-faceted security practices are necessary to ensuring user data privacy in autonomous standardized connections.

Moreover, in order to further the data security development in autonomous vehicle-related companies, it is necessary to innovate without losing focus on the legal context. The first recommendation

would be the implementation of dynamic encryption technologies, which increases data security by using a continuously changing cryptographic key, helping to further reduce unauthorized access (Sun et al. 6240–59). The second recommendation is to have a robust data governance framework, which is in accordance with the standards followed globally, like the General Data Protection Regulation (GDPR) (Taeihagh and Lim 103–28). Also, companies should invest in Artificial Intelligence to further improve the threat detection system and response and train the AI to be able to identify and act before exposure to any vulnerabilities (Bathla et al. 7632892). These are a few recommendations that could further improve the data security in the autonomous vehicle-related companies, not only to secure important data but also to build the trust of consumers through protecting their private data and gain advantage over competitors.

In addition , it is important that the autonomous vehicle companies work in collaboration with the regulatory authorities and other stakeholders of the industry to enhance the data security efforts . By collaborating with each other , the different companies in the industry can share knowledge and best practices in dealing with the cybersecurity problems prevalent in an industry .Besides , regulatory can also engage in fruitful collaboration with the autonomous vehicles companies to provide certain guidelines and frameworks regulating policies for securing data standards at all levels worldwide , to build even more customer trust and compliance (Sun et al. 6240–59).Other industry stakeholders , can equally engage with the data security efforts of autonomous vehicle companies from other industries to help in the identification of existing potentials and vulnerabilities in the industry through diverse perspectives while also providing for the innovation of unique solutions that foster technological development along with the protection of user data of the autonomous vehicle companies (Taeihagh and Lim 103–28). Therefore , this collaborative effort will help secure the user data of autonomous vehicles as the level of complexity increases , as companies will be able to establish unified plans to solve the emerging problems .

For the creation of consistent and all-encompassing patterns of regulatory law, the implementation of cross-border compliance, and its further adaptation for various risks and challenges, is formed into a compulsory legal and organizational regulation for making automobile data security more reliable and protected. With the introduction of strict guidelines as envisaged in General Data Protection Regulation (GDPR), which plays among the integral components in effective regulation compliance and persistent legislation in providing recognized and definite data protection standards worldwide, automobile manufacturers store personal databases safely and efficaciously, with cross-border compliance ensuring stable borders of security traditions to gain consumer reliance on autonomous technologies and drive innovations. To implement this measure, the strategy is needed to be definite enough in scope to keep and secure the particularities of distinct international legislations and norms, diligently adapted to eliminate posed legal threats, which can be observed in China, where data localization laws are effectively imposed and adhered to (Taeihagh and Lim 103–28). Ultimately, cross-border compliance with adaptive promotion measures is aimed to protect consumer data, simultaneously playing an incentive role in the industry moving forward by keeping the secure autonomous driving environment for building up the future.

Conclusion

The report highlighted that data protection is a consideration in the autonomous car market, and it is essential in establishing compliance and a trust factor amongst users. The current market is mainly penetrated by such companies as Tesla, Waymo, Ford, and General Motors, among other players, but the development of data protection standards needs to be consistent. It is determined that autonomous vehicles provide numerous advantages with increased safety and efficiency, challenges with respect to technology and ethics, with legislation and common laws adaptations needed in a dynamic environment. Data protection in the autonomous car market is a necessity in a scenario when the progress is evident not only in technologies and devices functionalities but also in the way there is an adaptation with the levels and methods of legislation and regulation in this area, for both developers and ordinary users.

Works Cited

[1] Ahangar, M. N., et al. “A Survey of Autonomous Vehicles: Enabling Communication Technologies and Challenges.” *Sensors*, vol. 21, no. 3, 2021, p. 706, https://www.mdpi.com/1424-8220/21/3/706.

[2] Almeaibed, S., et al. “Digital Twin Analysis to Promote Safety and Security in Autonomous Vehicles.” *IEEE Communications Standards Magazine*, vol. 5, no. 1, 2021, pp. 40–46, https://ieeexplore.ieee.org/abstract/document/9392784/.

[3] Bathla, G., et al. “Autonomous Vehicles and Intelligent Automation: Applications, Challenges, and Opportunities.” *Mobile Information Systems*, vol. 2022, no. 1, 2022, p.

7632892, https://onlinelibrary.wiley.com/doi/abs/10.1155/2022/7632892.

[4] Ignatious, H. A., and M. Khan. "An Overview of Sensors in Autonomous Vehicles." *Procedia Computer Science*, vol. 198, 2022, pp. 736–41, https://www.sciencedirect.com/science/article/pii/S1877050921025540.

[5] Khan, S. K., et al. "Cybersecurity Regulatory Challenges for Connected and Automated Vehicles–State-of-the-Art and Future Directions." *Transport Policy*, vol. 143, 2023, pp. 58–71, https://www.sciencedirect.com/science/article/pii/S0967070X23002330.

[6] ---. "Modelling Cybersecurity Regulations for Automated Vehicles." *Accident Analysis & Prevention*, vol. 186, 2023, p. 107054, https://www.sciencedirect.com/science/article/pii/S000145752300101X.

[7] Muhammad, K., et al. "Deep Learning for Safe Autonomous Driving: Current Challenges and Future Directions." *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, 2020, pp. 4316–36, https://ieeexplore.ieee.org/abstract/document/9284628/.

[8] Nanda, A., et al. "Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions." *IEEE Wireless Communications*, vol. 26, no. 4, 2019, pp. 60–65, https://ieeexplore.ieee.org/abstract/document/8809661/.

[9] Parekh, D., et al. "A Review on Autonomous Vehicles: Progress, Methods and Challenges." *Electronics*, vol. 11, no. 14, 2022, p. 2162, https://www.mdpi.com/2079-9292/11/14/2162.

[10] Pisarov, J., and G. Mester. "The Future of Autonomous Vehicles." *FME Transactions*, vol. 49, no. 1, 2021, https://www.academia.edu/download/84528917/1451-20922101029P.pdf.

[11] Sun, X., et al. "A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs)." *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, 2021, pp. 6240–59, https://ieeexplore.ieee.org/abstract/document/9447840/.

[12] Taeihagh, A., and H. S. M. Lim. "Governing Autonomous Vehicles: Emerging Responses for Safety, Liability, Privacy, Cybersecurity, and Industry Risks." *Transport Reviews*, vol. 39, no. 1, 2019, pp. 103–28, https://www.tandfonline.com/doi/abs/10.1080/01441647.2018.1494640%4010.1080/tfocoll.2022.0.issue-best-paper-moshe-givoni-prize.

[13] Wang, J., et al. "Safety of Autonomous Vehicles." *Journal of Advanced Transportation*, vol. 2020, no. 1, 2020, p. 8867757, https://onlinelibrary.wiley.com/doi/abs/10.1155/2020/8867757.

[14] Yaqoob, I., et al. "Autonomous Driving Cars in Smart Cities: Recent Advances, Requirements, and Challenges." *IEEE Network*, vol. 34, no. 1, 2019, pp. 174–81, https://ieeexplore.ieee.org/abstract/document/8809568/.