Frontiers in Business, Economics and Management
ISSN: 2766-824X | Vol. 17, No. 3, 2024

Practical Exploration of Data Security Application in Automotive Industry and Work Suggestions

Kaitian Li [1, 2], Ruiqing Zhai [1, 3], Yuning Li [1, 3, a]

[1] China Automotive Technology and Research Center Co., Ltd. Tian Jin, China

[2] China Auto Information Technology (Tianjin) Co., Ltd. China

[3] CATARC Software Testing (Tianjin) Co., Ltd. China

[a] liyuning@catarc.ac.cn

Abstract: As an important intelligent terminal in the new network world, intelligent networked vehicles have a large amount of data interactions with devices such as mobile, vehicle, roadside, and cloud servers. After large-scale commercial application, if it is not effectively controlled, it will bring great data security risks. China is gradually improving the data security regulatory system, and how to better manage automotive data security is a brand-new challenge for the automotive industry.

Keywords: Data Security, Automotive Industry, Intelligent terminal, Regulatory system.

1. Status of Automotive Data Security Standards Policy

1.1. Current Status of Laws and Regulations

China's laws and regulations on automotive data security are gradually improving. In 2017, the concept of "important data" was first introduced in the Cybersecurity Law of the People's Republic of China. In 2021, the Data Security Law of the People's Republic of China was promulgated, which for the first time defined the data processing process at the legal level. In the same year, the Personal Information Protection Law of the People's Republic of China was implemented, strengthening the protection of individual rights and interests and regulating information processing behavior. On October 1, 2021, the "Several Provisions on the Management of Automotive Data Security (Trial)" officially came into effect, clarifying the security protection requirements for personal information and vehicle information.

1.2. Current Status of Standard Policies

In terms of standards, China has gradually improved relevant standards. For example, the "General Requirements for Intelligent Connected Vehicle Data" provides guidance on security measures for data processing activities throughout the entire lifecycle of automobiles from the perspectives of personal information and important data, based on the relevant definitions and requirements of the "Several Regulations on Automotive Data Security Management (Trial)". In addition, standards such as the "Technical Requirements for Information Security of Automobile Vehicles" have stipulated the information security of the entire vehicle, and require that data processing activities first meet the relevant provisions of the "General Requirements for Data", and provide guidance on data tampering and leakage prevention.

1.3. Policy implementation status

At present, most car companies have established relatively mature data security management systems, with over 80% of vehicle manufacturers building their own data security teams and forming a management chain parallel to their business lines. However, data is distributed throughout all aspects of enterprise research and development, production, and circulation, and faces risks such as external hacker attacks and third-party data exchange, making effective data governance difficult. Facing the increasingly strict regulatory situation, it is recommended that enterprises strengthen compliance research, timely follow up on regulatory dynamics, accurately grasp policy compliance boundaries, and effectively formulate response strategies

Analysis: First of all, the basic legal framework is basically clear. The Cybersecurity Law of the People's Republic of China, the Data Security Law of the People's Republic of China, and the Personal Information Protection Law of the People's Republic of China have been promulgated one after another, giving the automotive industry a legal basis for advancing data security. Secondly, policy planning drives top-level design. A number of ministries and commissions have gradually accelerated the data safety management of intelligent networked vehicles, and implemented and improved the coordinated promotion mechanism of horizontal synergy and vertical coherence. Among them, the Several Provisions for the Administration of the Security of Automotive Data (Trial Implementation) came into effect on 1 October 2021, clarifying the scope of automotive data, the scope of automotive data processing activities, the general requirements and basic principles of automotive data processing activities, and other issues, which has promoted the effective implementation of data safety in the automotive industry. At last, multi-disciplinary coordination has accelerated the formulation of standards. The three standardization technical committees of automotive, communications and information security have strengthened coordination and system compatibility, collaborated to release the Guidelines for the Construction of the National Telematics Industry Standard System (Intelligent Networked Vehicles), and planned and designed a number of data security-related standards. Among them, GB/T 41871-2022 Safety Requirements for Information Security Technology Vehicle Data Processing is planned to be formally implemented in May 2023, and GB/T General Requirements for Intelligent Networked Vehicle Data Security has been launched in

October 2022 for public consultation.

2. The Automotive Industry Data Security Industry Development Issues

In recent years, China's intelligent networked automobile data security in reference to mobile phones, the Internet field and other data security protection technology based on the relevant work has been carried out, but overall automotive enterprises in the data security management system, security protection technology and other aspects of the data security management system, security protection technology and other aspects of the development of the industry there are many problems.

2.1. Automotive Data Interaction Scenarios Are Complex and Involve a Wide Range of Data Types

Intelligent Internet-connected vehicles are gradually extending to travel, entertainment, life and other services, and with the increase in application scenarios the types of automotive data are constantly enriched. For example, more and more mass-produced cars are beginning to carry new technologies such as autonomous driving, intelligent cockpit, high-precision maps, etc., and trying to introduce new functions such as sentry mode, remote photo taking, high-precision positioning and V2X. However, the interaction scenarios of automotive data involve vehicle-cloud communication, vehicle-device communication, vehicle-vehicle/vehicle-road communication, etc., in which data security risks and pitfalls have become more prominent.

2.2. The High Complexity of The Automotive Environment Makes Protection Difficult and Costly

Automobile high-speed movement, limited space, complex environment and other characteristics of the security protection technology to put forward higher requirements. Firstly, the network nodes will switch at high speed during the process of automobile movement, and it is necessary to meet the integrity of data transmission, security and link stability at the same time, which has higher requirements on technology. Secondly, automobiles are limited by cost and space, the high cost of chips makes it difficult to continuously superimpose the arithmetic power and storage space at the car end, and technologies such as face/plate anonymization outside the car require high arithmetic power at the car end, which puts forward higher technical difficulties and costs to enterprises.

2.3. Longer Automotive Industry Chain, Large Volume of Upstream and Downstream Data Sharing and Circulation

The large volume of data application interfaces between the upstream and downstream of the automotive industry chain and the existence of overlapping areas between various data processing systems make the data boundaries fuzzy and the scope of responsibility for data processing difficult to clarify. Vehicle manufacturers usually share information such as vehicle operating status, in-vehicle information services, and fault conditions with third parties to assist in vehicle maintenance and diagnosis, optimize intelligent driving algorithms, and monitor battery status, etc. Some joint ventures may also share relevant information with third-party enterprises abroad, and in order to safeguard the safety of the data sharing process, the upstream and downstream of the industry chain should establish a unified security concept.

2.4. Enterprise Data Security Is Not Effectively Integrated with The Vehicle Development Process

Automotive data security is different from traditional Internet security, it is a combination of systems, processes and products, and it is a control process to optimize the risk visible, so it is crucial to guarantee the safety of the research and development process. At present, most enterprises consider personnel, capital, technology investment and other issues, and there is a serious lack of motivation to build an effective data security protection system and other issues. For vehicle production enterprises, except for a few enterprises from the whole supply chain, the whole R&D process links to effective control of data security, the majority of enterprises have not yet data security into the vehicle R&D procedures.

3. Status of Automotive Data Safety Regulation

The current situation of automobile data security supervision is mainly reflected in the following aspects.

3.1. At the National Level

in 2021, five ministries including the Ministry of Industry and Information Technology issued the "Regulations on the Management of Automotive Data Security (Trial)", which clarified the basic requirements for data classification, processing, and cross-border transmission. At the local level, Zhejiang Province issued the "Zhejiang Province Automotive Data Processing Management Regulations" in 2023, further refining the rules of data processing, clarifying the definition and processing requirements of important data, emphasizing specific requirements for personal information and important data processing, and strict supervision of cross-border data transmission.

3.2. Regulatory Trends

From national to local, the trend of automotive data security regulation is becoming more specific and practical. The definition of important data is clearer, the requirements for processing personal information and important data are more specific, and the supervision of cross-border data transmission is stricter. For example, Zhejiang Province has stipulated that cars default to not collecting cabin data, increasing the protection of privacy inside the car.

3.3. Enterprise Response Measures

Most car companies have formed relatively mature data security management systems, and more than 80% of vehicle companies have built their own data security teams, forming a management chain parallel to their business lines. However, data is distributed throughout all aspects of enterprise research and development, production, and circulation, facing risks such as external hacker attacks and third-party data exchange, making effective data governance difficult. Enterprises need to establish comprehensive and proactive digital security capabilities from various dimensions such as boundaries, endpoints, application development, security operations, and data security governance.

3.4. Future Challenge

With the development of intelligent connected vehicles, data security issues are becoming increasingly prominent. The multiple data breaches that occurred in 2023 indicate that car companies face significant challenges in data classification and grading, data encryption and decryption, and leak prevention. In the future, AI technology innovation represented by large models will bring new risks and challenges to automotive data security, which need to be prevented and laid out in advance.

4. The Main Problems Currently Existing

At present, the top-level design work of data security for intelligent networked vehicles is being carried out steadily at three levels, namely, national laws, policy planning, and industry standards, but there are still three aspects of problems in practice.

4.1. Uneven Enterprise Data Security Practices Due to Standards, Regulatory Efforts, Etc.

At present, the annual report on automotive data safety management is still in the exploratory period, and the evaluation of enterprises in various places is different. For example, the Beijing Internet Information Office and the Shanghai Internet Information Office have centrally reviewed the annual reports of enterprises to find out the problems and urge them to make targeted rectifications. However, there are still some places that have not yet formed the review mechanism for the annual reports, and some enterprises are still taking chances. As a result, except for a few headline enterprises that effectively control data from the entire supply chain and R&D process, most enterprises have not yet incorporated it into their vehicle R&D procedures. In the mapping tests conducted by third-party testing organizations, most automotive products were found to be in non-compliance with excessive collection of personal information and illegal sharing of data.

4.2. Lack of Industry Consensus on the Scope of Important Data and Lack of An Industry Catalogue of Important Automotive Data

The Several Provisions for the Administration of the Security of Automotive Data (Trial Implementation) clearly defines important data in automobiles and the requirements for the regulation of important data. Vehicles are commonly equipped with satellite navigation signal receivers, cameras, radar and other sensors used to collect the surrounding road environment and geographic information, and involves a large number of personal information such as the vehicle VIN code and the owner's account number. Therefore, there is important data in automobiles, and involves complex and diverse scenarios. However, at this stage, the industry has not formed a catalogue of important data, and in practice, automotive data processors are unable to specify the types of important data, take appropriate preventive measures, or supervisory agencies monitor the safety of important data.

4.3. The Automotive Mapping Data Policy System Has Been Gradually Improved, But the Boundaries of Corporate Responsibility Have Yet to Be Clarified

At present, with the rapid development of intelligent networked vehicles, the importance of mapping geo-environmental information data security continues to rise, and presents a trend of tightening regulation. Regulators have issued a number of regulations and standards on mapping geo-environmental information for smart connected cars to further regulate mapping data, mapping behaviors and mapping activities in the automotive industry, and to promote the development and utilization of mapping geo-environmental information data under the premise of safety and compliance. In this context, how to balance data safety and compliance with utilization efficiency, define the scope of openness of mapping geo-environmental information data to the industry, and how to cooperate with multiple industries and sectors are becoming new challenges for automotive mapping geo-environmental information data management.

5. Proposals for Work

5.1. Regularly Carrying Out Data Safety Inspections and Assessments

Relying on the review of the annual data security report situation of enterprises, regularly organize and carry out automotive data security inspection and assessment, map out the compliance situation of the actual data security system and products of automotive enterprises, verify the principle of in-vehicle processing of vehicle cockpit data, anonymization of faces/plate numbers outside the vehicle, notable notification of the processing of personal information, and the exit of vehicle data through the results of the inspection and assessment, and promote the automotive data processors to continuously improve their safety awareness.

5.2. Studying and Sorting Out a Catalogue of Important Automotive Data

Under the guidance of the Office of the Internet Information Office, setting up an automotive important data catalogue research working group jointly with the industry to identify important data in the automotive industry from various perspectives, including confidentiality, integrity, availability, authenticity and accuracy, based on different factors such as the use of the data and the threats it faces; and combine the technical protection measures deployed by the enterprises with their costs, the management system and process for the protection of important data, and the amount of important data collected and its specific use, to sort out and form a list of important data in the automotive industry.

5.3. Regulate the Technical Authentication System for The Anonymization of Human Faces and License Plates Outside the Vehicle

At present, some companies are forced to downgrade intelligent functions such as sentry mode and remote photo taking in order to cope with data security regulatory requirements. At this stage, the automotive industry is carrying out the exploration and research of off-vehicle facial license plate anonymization technology, and in the future, the

industry can be organized to jointly explore the effectiveness of off-vehicle end-protection in different scenarios, overcome the technology's consumption of hardware resources, communication delays, and other pain-points, and form a standardized technical authentication system, so as to promote off-vehicle facial license plate anonymization technology to achieve industrialized application.

6. The Future Prospects of Automotive Data Security

Automotive Data Security can be said to be a vast world full of challenges and opportunities. With the rapid development of intelligent car technology, cars have become important terminals for information collection and data exchange. It is expected that by 2025, the penetration rate of new L2 level and above assisted driving passenger cars will exceed 70%, with a huge amount of data uploaded to the cloud every year.

If these data are used properly, they will drive the iteration of intelligent technology, improve enterprise management level, and even give birth to new formats and services. However, risks such as unauthorized access, data leakage, and malicious tampering cannot be ignored. In recent years, malicious attacks and data breaches targeting vehicle manufacturers, vehicle networking information service providers, and other related enterprises have occurred frequently, posing severe challenges to automotive data security. In the future, the development of automotive data security will present the following trends:

6.1. Regulations and Policies Are Increasingly Improving

With the increasingly prominent issue of automotive data security, governments and relevant institutions around the world will continuously improve relevant regulations and policies, clarify standards and requirements for data collection, storage, use, and transmission, and provide legal protection for enterprises and individuals.

6.2. Technological Means Continue to Advance

With the continuous development of technologies such as big data, cloud computing, and artificial intelligence, automotive data security protection measures will also continue to innovate and upgrade. For example, by using techniques such as data encryption, access control, and risk assessment, the security and privacy of data can be improved.

6.3. Strengthening Industry Chain Collaboration

Automotive data security involves various links in the entire industry chain, requiring cooperation between upstream and downstream enterprises in the industry chain to form a joint force. In the future, we will strengthen the collaboration between upstream and downstream of the industrial chain, establish a shared responsibility mechanism for automotive data security, and ensure the sustainability of the security management mechanism in the supply chain.

6.4. Increased Awareness of User Privacy Protection

With the continuous improvement of consumers' awareness of personal privacy protection, automotive companies will pay more attention to user privacy protection, strengthen data security management, and enhance user trust.

In short, the future prospects of automotive data security are full of hope and challenges. Only through the joint efforts of relevant departments, enterprises, and industries can we build a solid defense line for data security and promote the healthy, stable, and orderly development of the entire automotive industry.

References

[1] Li Xiaoling. Shenzhen takes the lead in legislating intelligent networked vehicles. Economic information daily, p. 006, August 23rd, 2022.

[2] Wu Haiyan, Chen Pu, Chen Yaliang, et al. Research on domestic and foreign governance mechanisms and policies for data security of intelligent networked vehicles. Telecommunications Information, no. 9, pp. 27-33, September 2022.

[3] Deng Yaoyue. A Brief Analysis of the Data Risks and Measures of Intelligent and Connected Vehicles. Auto Time, no. 24, pp. 10-12, November 2022.

[4] Wang Rong. Construction and evaluation practice of automobile data safety compliance with intelligent network connection. Intelligent Connected Vehicles, no. 1, pp. 57-59, January 2023.

[5] Huang Daoli. Review and Prospect of the Five-year Implementation of the Cybersecurity Law of the People's Republic of China. China Information Security, no. 2, pp.61-64, February 2023.