Science of Law Journal (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2023.020210
ISSN 2616-2296 Vol. 2 Num. 2

The Legal Regulation of Data Localization for Autonomous Vehicles

Hengzhe Ye*, Xinrui Tang, Ling Yang, Annuo Wei, Yaxing Zhu

Institute of Problem Solving, Hubei University, Wuchang, Wuhan, China
**Corresponding author*

Keywords: Automatic driving, data security, data localization, data cross-border mobility

Abstract: As the arrival of big data era, data resources have become more and more important in the development of international communication, and data security issues are becoming more and more prominent in various industries and fields. As a newly emerging technology that closely relies on the development of data, how to put the development of automatic driving technology industry above the safety, accelerate data supervision and data protection, and make relevant industries take the development opportunity in international competition is an urgent problem to be solved currently. Based on the current situation of the development of data localization in China, this paper systematically discusses the development dilemma of data localization, and analyzes the ways to solve it, in order to offer the possible solutions.

1. Introduction

1.1. Definition of Autonomous Vehicle Data Localization

In the era of big data, some people used to compare the data of the new era with the oil of the industrial age and call it the blood of the new era. This metaphor reflects the importance of data as a new resource for social development. Different from traditional resources, data attaches to the Internet and has strong mobility, which mobility globally through the pattern, such as transnational corporations. In 2021, the event of Didi Gate was disclosed. In the process of listing in the United States, Didi Company transferred a large number of relevant data without the approval of China's relevant data security department, and it was suspected to disclose a large amount of user information and domestic traffic map information. At the same time, the China Network Security Review Office intervened in the investigation, called Didi to stop the listing plan, removed its relevant app, ordered rectification in accordance with the "China's Internet Security Act" and "network security law". This action has raised public concerns about China's network security and data security, exposing the challenges to personal privacy and national security behind the autonomous vehicle data mobility.

"Data localization" refers to a national initiative to process data generated in the national territory and store the data in a cloud server in the domestic territory to limit the mobility of the data beyond the border. For autonomous vehicle, it means to localize the personal information data and vehicle information data of car drivers. Data mobility means communication and development. If

the autonomous technology is completely prevented from transferring to foreign countries, the domestic autonomous technology would be cut off the connection with the foreign countries, which will not only make it difficult to keep up with the development trend of the world in terms of technical innovation, but also is not conducive to the internationalization of Chinese autonomous vehicle brands. And data mobility also means risk. If a part of data is leaked, it will pose a serious threat to our national defense security and national security. Therefore, China should screen and classify the autonomous vehicle data, strictly control the data, make clear the scope of the data that should be localized, and accelerate the development of the auto industry on the premise of safety.

1.2. Types of Autonomous Vehicle Data Localization

The autonomous data can be generally classified into geographic information data, users' personal information data and vehicle usage information data. In data classification and classification protection, geographic information data is involved in national security, user personal information data is involved in personal privacy and security, and vehicle usage information is more related to legitimate rights and interests of automobile enterprises. In accordance with the importance degree and hazard degree of the data, the geographic information data in the autonomous technical vehicle, including the social information obtained by the vehicle such as three-dimensional coordinate position data, traffic signal data and geographic environment data, shall be protected with priority for national security and public interest due to its high importance and harmful degree, and high-standard localization measures shall be conducted according to the law; for the personal information of the user, the personal privacy of the vehicle owner is concerned, once the disclosure will cause a great deal of troubles to the vehicle owner, and the infringement problem is involved. If the user personal information is disclosed in a large amount in a cluster, the public safety may also be threatened. Such data shall be screened, the personal information network database shall be strictly controlled, the supervision shall be strengthened, and the data conversion measures shall be taken according to the necessary conditions; the vehicle use information refers to the legitimate rights and interests of individuals and organizations shared by the vehicle enterprise and the vehicle owner. Such data is less harmful to the public security and national security, and can be protected at a lower level based on the free choice of the vehicle enterprise and the vehicle owner, so as to facilitate the circulation of more vehicles to the market, and brings convenience to automobile enterprises and vehicle owners[1-5].

1.3. Analysis of Necessity on Localization of Autonomous Vehicle Data

The localization of autonomous vehicle data is an inevitable requirement to ensure national security and individual safety of citizens. Data mobility and development are very important for today's Internet era, but the premise of data mobility is that data security should be guaranteed first. Because of the universality of automobile and the intercommunication of data in daily application, if we don't regulate the cross-border mobility of data and store the important data outside the national border, our national security will always be a security risk. Once the cross-border data is leaked, it will cause serious consequences to our national security. In terms of citizen personal information data, if it is stored cross-border, it may cause troubles to citizens' personal information utilization; when the citizen's personal information is disclosed to the public through autonomous vehicle data, the citizen's personal privacy will no longer exist, and citizens' privacy rights will be seriously violated. If these leaked data are in the possession of lawbreakers. It will pose a danger to the personal safety of citizens.

2. Analysis on Current Legislation of Autonomous Vehicle Data in China

Our country is still in the initial stage for the security legislation of autonomous vehicle data. There is a shortage of relevant professional centralized legislation in the industry, and the number of relevant laws and regulations is limited, which is reflected in the “Regulations on the Safety Management of Automobile Data (Trial)” and the “Measures for the Exit Security Assessment of Personal Information and Important Data (Trial)” and other laws. Moreover, these provisions still need to be completed in the aspects of detailed legislative rules, standards and definitions, which is embodied in the following points.

2.1. Clear Legislative Direction

At present, China has taken a lot of measures against the whole legislation of data localization. Article 10 of the “Data Security Law of the People’s Republic of China” stipulates: “The relevant industry organizations shall, in accordance with the Constitution, formulate the data security code on conduct and group standards in accordance with the law, strengthen the self-discipline of the industry, guide the members to strengthen the data security protection, improve the data security protection level, and promote the healthy development of the industry." This law provides a programmatic law for the development of data security regulations for the autonomous vehicle industry. The Article 21 within it stipulates that: the State shall establish a data classification and hierarchical protection system, based on the importance of the data and the degree of harm caused to the national security, public interests or the legitimate rights and interests of individuals and organizations after the data is tampered, destroyed, leaked or illegally obtained or used. The data shall be protected by classification and hierarchical system. This provision establishes an important protection direction for data protection.

2.2. Lack of Specific Provisions

Relevant laws and regulations are relatively general and lack of specific provisions. For example, in the “Measures on Security Assessment of the Cross-border Transfer of Personal Information (Trial)”, the situation that the data shall not be exported may infringe upon personal interests, may affect national security and harm social and public interests. Such ambiguous provisions are difficult to grasp in actual operation and the data definition is unclear. There may be cases of double legal evaluation protection and omission of protection. Finally, the burden of judge's discretion is too heavy, and it is difficult to protect the data in an all-round way [6].

2.3. The Judgment and Punishment are Not Unified

Relevant laws and regulations determine that the punishment is not uniform and there are contradictions. For example, if Article 66 of the “Cyber security Law” and Article 45 of the “Data Security Law” stipulate that, those who provide important data overseas shall be ordered to make corrections and given a warning by the relevant competent authorities. After giving a warning, the penalties of these two laws are to confiscate the illegal income and impose a fine of 50,000 to 500,000 yuan and a fine of 100,000 to 1 million yuan respectively. The inconsistent punishment of the two laws for the same problem will cause confusion in the applicable laws and make the problem difficult to solve. The credibility of the law is greatly diminished.

3. International Perspective of Data Localization and China's Legislative Attitude

3.1. International Perspective

From the perspective of international field, the United States is the representative of active opponents of data localization. On March 25, 2019, the draft Joint Statement on Electronic Commerce Initiative submitted by the United States in the negotiation of WTO digital trade rules explicitly stated that "the cross-border mobility of data should not be restricted". As the economic leader of the world's Internet, the United States has made a series of efforts for the free mobility of data in order to create a favorable business environment and consolidate its dominant position in international trade. On the other hand, Russia, India and other countries are committed to promoting data localization, adopting strict control on cross-border data mobility, creating data barriers in international trade, and striving to protect their own data sovereignty. Due to its political and economic status and trade policy in the world, EU has taken a neutral attitude towards data localization[7].

3.2. China's Legislative Attitude

China's legislative attitude to the current localization of data is eclecticism, which is similar to that of the European Union. That is to say, under the premise of protecting the national network security and digital sovereignty, China will guarantee more competitive advantages of relevant enterprises in the international market and improve the international competitiveness[8,9]. On the one hand, China guarantees national security and data security through a large number of legislation. For example, the “Network Security Law”, the “Data Security Law” and the “Personal Information Protection Law”, etc. On the other hand, China has issued a large number of encouragement policies to support the international development of enterprises, and to control and release the cross-border data mobility of enterprises. Article 11 of the Data Security Law indicates that, China actively conducts international communications and cooperation, takes data security governance and data development and utilization as key areas, participates in the formulation of international rules and standards related to data security, and promotes the cross-border security and free mobility of data.

4. Dilemma of China's Autonomous Vehicle Data Localization

4.1. Data Classification is Unclear and Lack of Industry Standards

So far, the relevant legal and normative documents issued by China on the road test of unmanned vehicles emphasize the functional safety of vehicles, but seldom involve the safety of data, and lack of the demarcation and distinction of the level, type, quantity and range of data. In 2017, the Chinese government issued the final Guidelines for the Guidance on Constructing National Standards System for Internet of Vehicles Industry (Smart Transport), but its articles are more general and abstract, and there are no concrete rules, so it is difficult to use it to guide and solve the problems related to the data risks of autonomous vehicles. Industry standards related to personal information security and national security of autonomous vehicle data are still in vacancy. There is no standard basis, and it is difficult to complete the jurisdiction of domestic autonomous vehicle data.

4.2. Transfer of Data by the Enterprise

Autonomous vehicle data is of great commercial value, and the process of storing data locally may increase the cost of operation for the enterprises. Meanwhile, the implementation of a country's strategy of data localization is often accompanied by the strengthening of administrative supervision and criminal punishment, which also increases the cost for operators to prevent legal risks [10]. In pursuit of self-interest, enterprises may violate their own country's strategy of data localization and try to transfer data abroad, so as to reduce operating cost or evade legal liability.

4.3. Difficulty in Supervision and Review

The Internet has boundary less property. Users and network service providers do not need to be in the same country to complete the process of providing data services [6]. Remote transmission makes it difficult to define the geographical location of data storage, processing and transmission. In addition, the data itself has virtual characteristics, whether it is transmitted to foreign countries through the Internet or stored in physical media such as USB flash disk, it is difficult to carry out dynamic real-time monitoring on it [10]. It is very difficult for the network supervision department and customs department to supervise and examine.

4.4. Incomplete Data Security Assessment Mechanism

According to the National Security Law and the Data Security Law, cross-border data transmission by key information infrastructure operators shall be submitted to the Internet Information Office and relevant departments of the State Council for evaluation. However, the Measures on Security Assessment of the Cross-border Transfer of Personal Information do not issue the evaluation standard which is still relatively vague. There is still no clear demarcation between "personal privacy", "social and public interests" and "national security" for what kind, level and quantity of data. Even if the regulators are in possession of the real-time dynamics of data transmission, it is difficult to find the basis for their evaluation or judgment in the review process.

5. Specific Path of Autonomous Vehicle Data Localization

In view of the development goal and realistic dilemma of the localization of autonomous vehicle data in China, it is necessary to regulate the localization of data by law, giving consideration both on efficiency and safety. It is not only considered to fully release the industrial development activities to promote the vigorous development of relevant domestic industries, but also take into account the data security issues, and attach great importance to data security prevention while developing the autonomous technology. Ensure the healthy development of autonomous technology within the scope of personal privacy, public interest and national security.

5.1. Formulate Complete Industry Standards

Relevant administrative departments under the State Council shall, in conjunction with the technical personnel of autonomous vehicle data, conduct investigation and research, formulate detailed and complete autonomous vehicle data industry standards. take data classification and hierarchical management, data desensitization, database audit, data abnormal behavior identification, interface security, digital watermark, data destruction, data security management and control platform as the conventional means for data processing, do a good job in delimiting and distinguishing the data types, levels, quantities and scopes, and establish and perfect a complete

data classification and protection mechanism [11]. On the one hand, help enterprises to implement differentiated data security protection capability, promote further enrichment and perfection of relevant data security products on the basis of meeting basic requirements, and create high-quality data security product services; On the other hand, provide the corresponding basis and evidence for data localization legislation and law enforcement[12].

5.2. Establishment of a Sound Accountability Mechanism

Relevant responsible departments shall establish a sound accountability mechanism. The Notice on Strengthening the Network Security and Data Security of Internet of Vehicles issued by the Ministry of Industry and Information Technology in September 2021 requires that intelligent connected vehicle (ICV) manufacturing enterprises and Internet of Vehicles service platform operation enterprises to establish data management ledger in accordance with the principle of "who is in charge, who is responsible, who is responsible for operation and who is responsible for it", to conduct classified and hierarchical management on the data and divide the management responsibilities[13,14]. On the one hand, the hierarchical classification of data strictly controls the release of personal information, reduces the risk of personal information leakage, and prevents enterprises or individuals from abusing their personal information, renting or selling. On the other hand, the legislation pays more attention to the national security, aiming at the autonomous transnational data and the local important strategic resource information, strictly prevent the leakage and theft, and escort for the national defense and the localization of the data. Establish and improve the data security protection and punishment mechanism for data leakage. With the clear punishment of legislation, enterprises are compelled to abide by laws and regulations, abide by the industrial norms, and supervise and urge the managers to strengthen the data security protection and pay more attention to the data security through the perfection of legislation, so as to enhance the data security guarantee capability of China's autonomous vehicles.

5.3. Implementation of Hierarchical Management and Real-time Supervision

Administrative organs at all levels shall clearly define the current arrangement, manage the geographic information data, personal information data of users and vehicle information data with hierarchical system, confirm the management authority of supervision departments according to the data security mechanism of different levels, jointly sign the offices of different supervision departments, strengthen the supervision on the cross-border mobility of autonomous data at all levels, innovate and establish dynamic and scientific real-time supervision mode, improve the working mechanisms of information communication, monitoring and early warning, emergency treatment and contingency plan management, promote the integration and systematization of the links between departments, and strictly control the importance and hazard of data and prevent the risk of data leakage from many aspects.

5.4. Optimize the Safety Assessment Mechanism

The National Internet Information Office and other relevant departments shall optimize the data security assessment mechanism, further complete the "Measures of Data Cross-Border Transfer Security Assessment", and shall, in particular, address the provisions of Clause 1 and Clause 2 of Article 5. "legality, legitimacy and necessity of the purpose, scope and method of data processing by the data outbound and overseas receivers", "the scale, scope, type and sensitivity of cross-border data, and the potential of data outbound for national security, public interests, risks arising from the legitimate rights and interests of individuals or organizations" shall be clarified. Strictly control the

release of personal information to reduce the risk of personal information disclosure; strictly prevent the data related to national security and the information leakage and theft of important local strategic resources, escort for the national defense and the landing of data localization, and enhance the data security guarantee capability.

6. Conclusion

The vitality of data lies in mobility, but the mobility must be built on the basis of security, especially across borders. If the cross-border mobility of autonomous vehicles data is not regulated and protected, it will not only lose the meaning of the mobility itself, but also bring great hidden dangers to the privacy of citizens and the national security. In the face of the era of information globalization, the management strategy of cross-border mobility of autonomous vehicle data needs to be determined according to the current situation of our country. In the present stage, we still need to adhere to the strategy of data localization, and promote the sound development of the autonomous vehicle industry on the basis of protecting citizen's privacy and safeguarding national security.

References

[1] Zheng Ge. Data Rule of Law and Future Transportation: A Preliminary Discussion - Data Governance of Autonomous Vehicles. China Law Review, 2022(01):202-214.

[2] Lu Juan. The localization construction of the right to be forgotten in the era of big data. Yantai University, 2021. 000422.

[3] Tang Binbin. Research on Cross-border Data Collection in Criminal Justice. The Jurist, 2020(04):156-170. 1005-0221. 202.04.012.

[4] Fu Xinhua. European Union and American Legal Practice of the Right to Data Portability and Its Localization System Design. Hebei Law Science, 2019, 37(08) 102-3933.2019.08.013.

[5] Yang Nan. The Functions and Applicable Rules of the "Blank-Regulations" against the Crime of Infringing on Personal Information. Journal of East China University of Political Science and Law, 2021, 24(06):73-85.

[6] Tang Binbin. Reflection and Improvement of Legal Regulation of Data Localization. Journal of Intelligence, 2022, 41(05).

[7] Wang Meili, Chen Yu. Research on the Docking between China's Cross-Border Data Transfer Rules and the CPTPP. International trade, April 7, 2022.0.

[8] Zhang Taolue, Qian Rong. The German Road Traffic Act in the Age of Autonomous Driving: the Law on Autonomous Driving and Its Exploration and Enlightenment. Deutschland Studien, 2022, 27(01)

[9] Ardi Kolah. The GDPR Handbook: A Guide to Implementing the EU General Data Protection Regulation. Journal of Data Protection & Privacy, 2018(1).

[10] Chen Yuheng. Classification, Preservation and Compliance of Autonomous Driving Algorithm Data under the "Data Security Act". Science and Technology and Law Chinese-English Version, 2022(03).

[11] Zhang Feng, Jiang Weiqiang, Wang Guangtao. Current Situation and Thinking of Data Security Standard System in Telecommunication Field. China Information Security, 2022(04):36-39.

[12] Li Shuo. Research on the Legislation of Self-driving Cars. Administrative Law Review, 2019(02):104-113.

[13] Jiang Su. The Challenges of Self-driving Cars to the Law. China Law Review, 2018(02):180-189.

[14] Yang Shan, Zhang Sasha. Legal Barriers and Countermeasures to the Development of Intelligent Connected Vehicles. Journal of Southwest Jiaotong University (Social Science): 1-11 [2023-03-05].