

Article

How Should Chinese Administrative Agencies Protect Data Security in Autonomous Driving?

Yajie Wang *, Haojie Tang and Chunlin Li

School of Law, Fuzhou University, Fuzhou 350108, China; lawdreamer@fzu.edu.cn (H.T.);
chunlinli@fzu.edu.cn (C.L.)

* Correspondence: fxywyj@fzu.edu.cn; Tel.: +86-180-9353-0068

Abstract

The continuous collection of road information by autonomous vehicles (AVs) has intensified regulatory pressure on data security protection. At present, the Chinese government adopts a proactive stance on protecting AV data security. Nevertheless, relevant requirements are scattered across various regulatory regimes, including data security, cybersecurity, personal information protection and AV access regulation. It has given rise to ambiguous judgement criteria and inconsistent law enforcement practices among local authorities. As a leading developed economy worldwide, the European Union has continuously refined legislation on data security protection for AVs since 2018, establishing a globally sophisticated protective framework. Against this backdrop, this paper adopts comparative analysis and normative analysis to focus on examining the characteristics of the EU's advanced rules. The research reveals that the EU has integrated risk prevention, monitoring and reporting mechanisms into a unified regulatory framework. It implements market access and safety assessment before operation, conducts ongoing safety management during operation, and launches data reporting and recall procedures after operation. After evaluating the applicability of the EU model in China, this paper suggests China adopt phased AV data security rules. Governance should focus on early detection of data breach risks before operation, real-time data monitoring during operation, and data reporting after operation. This proposal clarifies responsibilities among regulators, automakers and data service providers, improves the predictability and enforceability of relevant governance and facilitates safe, innovative and sound development of the autonomous driving industry.

Keywords: autonomous vehicles; data security; protection rules; risk regulation

Academic Editor: Grzegorz
Sierpiński

Received: 7 June 2026
Revised: 27 June 2026
Accepted: 2 July 2026
Published: 6 July 2026

Copyright: © 2026 by the authors.
Published by MDPI on behalf of the
World Electric Vehicle Association.
Licensee MDPI, Basel, Switzerland.
This article is an open access article
distributed under the terms and
conditions of the [Creative Commons
Attribution \(CC BY\) license](https://creativecommons.org/licenses/by/4.0/).

1. Introduction

With the extensive market rollout of Intelligent Connected Vehicles (ICVs), core technologies including Internet of Vehicles (IoV) have witnessed rapid development. As one core technology of ICVs, autonomous driving technologies generate massive vehicle data and personal private information. So, as autonomous vehicles (AVs) are equipped with autonomous driving technologies, their data security risks keep growing by the day. Such vehicles are confronted with diverse risks such as excessive data collection, internal data leakage and unauthorised outbound transmission of critical data. Therefore, regulating the collection and utilisation of data from AVs and standardising corresponding technological progress via legislation has become a vital research subject [1–3].

At present, academic research on data security risks of AVs mainly focuses on risk causes, risk impacts and data security protection countermeasures. In terms of risk causes, scholars generally recognise that artificial intelligence systems feature complex data processing and are vulnerable to cyberattacks throughout their full lifecycle, which necessitates the construction of end-to-end security defence mechanisms [4]. Some scholars further dissect diverse data security risks and their root causes in the autonomous driving sector, such as the inherent complexity of autonomous driving data [5,6] and failures of data protection mechanisms [7]. Regarding concrete risk impacts, certain researchers explore security assessment frameworks for underlying data algorithms and discuss various data risks, potential hazards and corresponding legal and regulatory provisions [8]. From the perspective of data security protection solutions, numerous scholars have noted divergences in national cybersecurity laws and regulations governing autonomous driving, and summarised the merits and demerits embedded in different protection regimes [9,10]. Meanwhile, driven by the rapid development of AVs in China, a body of literature targets the Chinese context and analyses distinctive traits of national unified legislation and local regional regulations across China. On legislative design, scholars point out that existing norms contain contradictory provisions to a certain extent. They argue that fundamental laws governing data security and connectivity governance for autonomous driving shall be formulated and implemented uniformly, systematically and standardly at the national level [11]. Building on this viewpoint, other researchers propose strengthening the linkage between data-related legislation and traffic regulatory laws, and establishing tiered data legislation that targets practical demands while balancing industrial innovation and personal right protection [12]. As for specific technical solutions, existing studies cover current market access mechanisms [13], improvement pathways for autonomous driving products [5,6], as well as criminal regulatory approaches [14]. Some scholars, based on the real-world cybersecurity conditions of AVs in China, hold that newly designed regulatory frameworks ought to strike a balance among national security preservation, industrial competitiveness promotion for emerging sectors and citizens' privacy protection [15].

Nevertheless, few scholars have systematically examined disparities in the core priorities of data security protection rules for AVs across distinct operational phases. Such an analysis carries great significance for clarifying regulatory priorities of data protection in each phase and coordinating legislation and industrial policies from various fields. Summarising and sorting risk sources by operational phase enables targeted adjustment of protection priorities and clarification of the application sequence of regulatory norms. This paper takes risk governance theory as its theoretical foundation and integrates full-lifecycle management requirements for both AV data security and artificial intelligence supervision. It intends to address the complex, uncertain and systematic technical risks brought by autonomous driving through a continuous governance workflow consisting of risk identification, risk assessment, risk management, risk communication and corrective feedback. Different from existing studies, this paper draws on the mature legislative experience of the EU and proposes localised regulatory solutions tailored to China's current legal system and industrial development realities. It consolidates scattered obligations stipulated in separate regulations into an integrated full-process risk governance chain covering prevention before operation, monitoring during operation and remediation after operation and translates these general obligations into concrete requirements for administrative authorities, manufacturers and system developers.

Accordingly, to address the above research gaps, this paper first sorts out current national laws, policies and local regulatory documents issued by Chinese authorities concerning data security protection for AVs, and identifies prominent defects within China's practical governance system. These defects include vague judgement standards for sensitive data and fragmented local implementation practices across regions. Afterwards, nor-

mative analysis and comparative analysis are adopted to examine the EU's legal framework for AV data security protection, as well as regulated stakeholders and specific regulatory measures embedded in its phased protection mechanism. Taking both innovations and limitations of the EU framework into consideration, this paper discusses the adaptability and feasible transplantation paths of such a regulatory structure in China and constructs a three-tier protection framework covering prevention before operation, monitoring during operation and remediation after operation for AV data security in China. Meanwhile, this study fills the research gap of phased AV data security protection based on vehicle operational states. The derived conclusions can offer normative references for China to optimise its domestic AV data security regime and deliver empirical insights for other countries to improve their corresponding regulatory systems.

2. Practical Deficiencies in AV Data Security Protection

Under current regulatory provisions in China, ICVs refer to new-type vehicles equipped with sensors, on-board computing modules and IoV communication devices. They enable information interaction among vehicles, humans, roads and the cloud, and are capable of environmental perception and intelligent control, covering all levels of driving automation ranging from L0 to L5. Autonomous driving technologies represent a complete technical system that supports vehicles to perform dynamic driving tasks independently. In this paper, AVs are defined as ICVs equipped with autonomous driving technologies in light of China's current industrial development context. Such vehicles allow driving operations to be jointly completed by human drivers and automated systems within restricted or full operational scenarios [16]. With the deepening global layout of China's AV industry, China exported 4.91 million automobiles in 2024 [17]. Nevertheless, due to the unique attributes of AVs, growing challenges and risks have emerged in their data security [18,19]. China's current legal system has constructed multiple mechanisms for data security protection. However, there is a lack of coordinated rules concerning autonomous driving, especially regarding the identification, application and protection of vehicle data. Local legislation has laid practical foundations for institutional innovation, but the data requirements and regulatory connections remain inconsistent across different regions. Therefore, it has become an urgent legal issue to coordinate various laws and policies and prevent potential risks in autonomous driving data security.

2.1. AV Data Security Protection Built by Central and Local Governments

Unlike traditional automobiles, AVs are not merely transportation tools relying on mechanical systems. Rather, they are mobile digital terminals integrating sensors, onboard communication modules, cloud platform services, remote upgrade systems, and continuous data feedback mechanisms. During operation, vehicles continuously collect multiple types of information, including location data, driving trajectories, driving behaviours, and in-vehicle interaction data. They typically maintain constant connections with manufacturers' servers through cellular communications and vehicle-to-everything platforms. Consequently, the entire process—from data collection and generation to transmission and processing—involves data handling by different entities (See Figure 1).

From an engineering perspective, AV data architecture is highly heterogeneous, meaning different data categories face fundamentally distinct technical failure modes [20]. For instance, raw perception and High-Definition (HD) map data are vulnerable to physical sensor spoofing and unauthorised data extraction. V2X (Vehicle-to-Everything) communication data, which is critical for vehicle-road-cloud interaction, is highly susceptible to Man-in-the-Middle (MITM) attacks and compromised node injections [21]. Furthermore, even after anonymisation, driver behaviour and trajectory data retain a high risk of re-identification attacks based on spatial-temporal correlations [22]. Finally, cloud-based

training data and Over-the-Air (OTA) system update logs face risks of model manipulation. Thus, uniform legal regulation is insufficient without addressing these specific technical attack vectors. UNECE Regulation No. 155, Annex 5 categorises AV cybersecurity threats into seven major categories comprising 69 specific attack vectors [23]. This technological complexity inevitably subjects AVs to coordinated regulation and protection under multiple laws and policies.

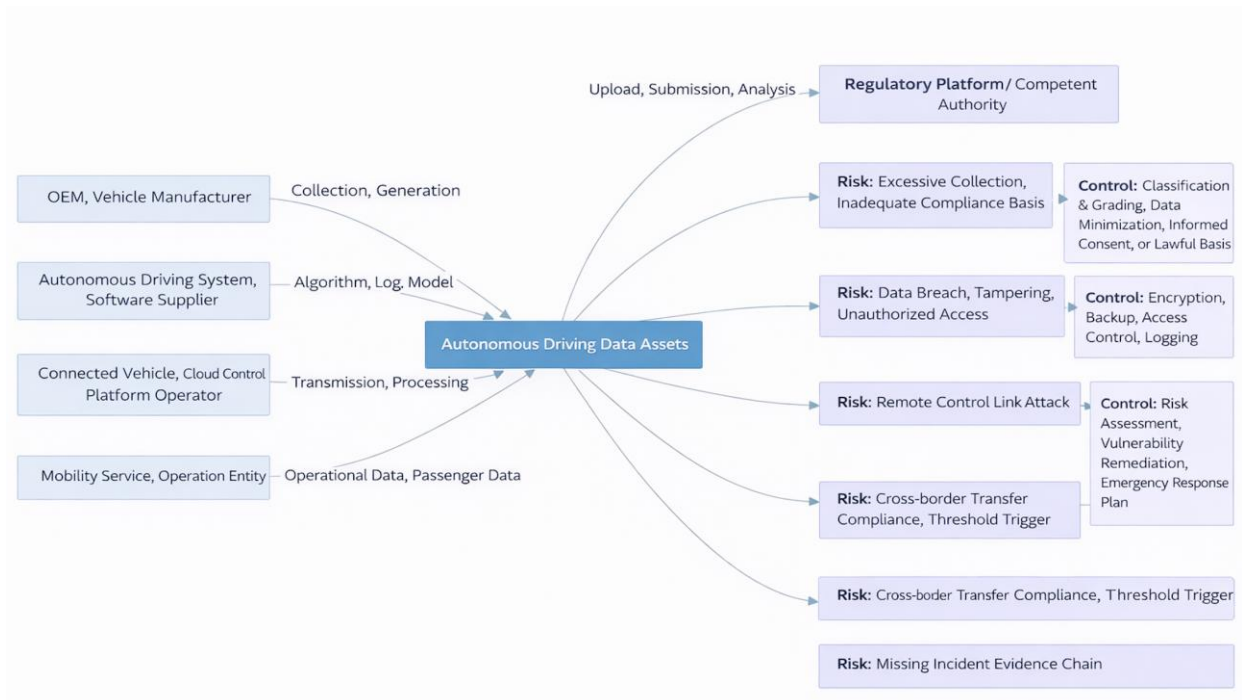


Figure 1. AV-Related Data Subjects and Risks.

At present, China's legal system for AVs adopts decentralised governance based on different branch laws and industrial standards (see Figure 2). In the field of data security, laws including 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 regulate data security and the rights and obligations of manufacturers in different scopes. Meanwhile, administrative regulations further clarify relevant requirements, including the Regulations on Security Protection of Critical Information Infrastructure, the Measures for Security Assessment of Cross-border Data Transfers, and the Regulations on Cybersecurity of Internet Data (see Table 1). In the autonomous driving sector, multiple legal documents provide important legal and policy support for the standardised development of AVs and related enterprises. They consist of the Interim Provisions on Automobile Data Security Management, the Technical Requirements for Whole Vehicle Information Security of Motor Vehicles, the Regulations on Administration of Defective Automobile Product Recall, the Opinions on Strengthening Administration of Access to Intelligent Connected Vehicle Manufacturers and Products, and the Interim Specifications for Road Testing and Demonstration Application of Intelligent Connected Vehicles (see Table 2).

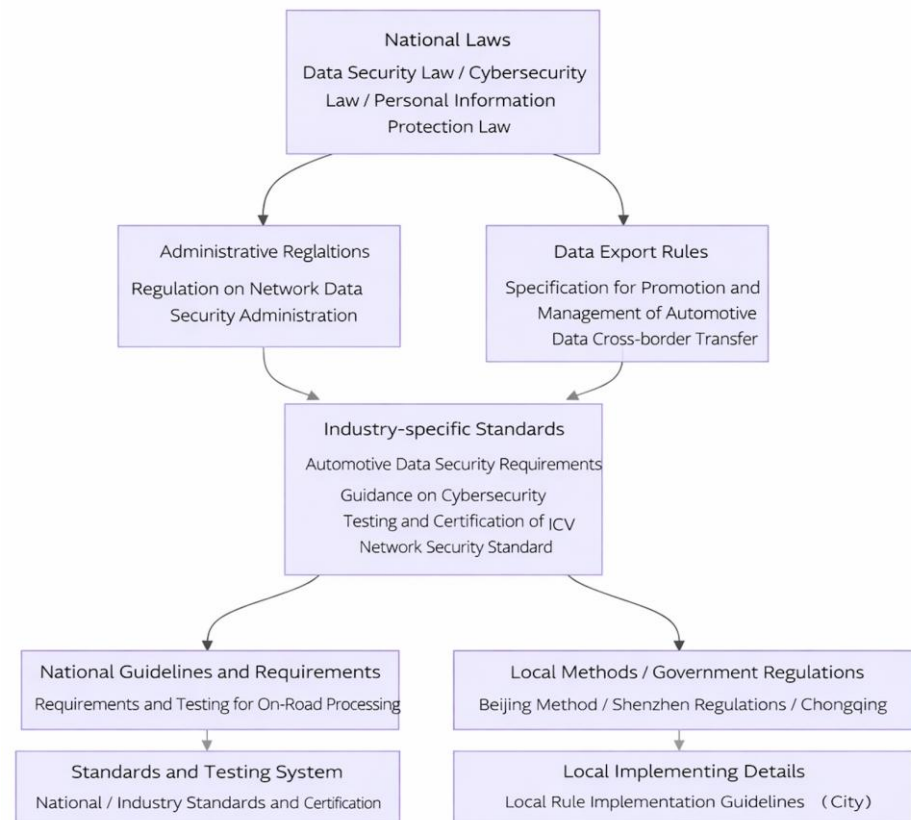


Figure 2. China’s Legal Framework for AV Data Security.

At the national legal and administrative regulation level, China has established various safeguard measures for data security, including data processing, supervision and assessment. Meanwhile, specific legal rules have set technical requirements. More specifically, the Data Security Law forms risk-prevention obligations through institutional arrangements such as classified management, continuous monitoring, regular assessment, remedy and reporting [24]. The Cybersecurity Law ensures relevant assessment and management through a statutory list of minimum security obligations [25]. And the Personal Information Protection Law establishes sustainable and verifiable obligations for rights risk control based on the evaluation of legitimacy and necessity [26].

When applied to autonomous driving data security, China has introduced targeted regulations through special administrative documents. For example, the Interim Provisions on Automobile Data Security Management define high-risk data categories and applicable subjects by law, and they require enterprises to identify risky data in advance and adopt higher-level protection measures. Such requirements reflect risk identification and prior prevention [27]. Documents including the Notice on Strengthening Cybersecurity and Data Security of Connected Vehicles and the Notice on Piloting Access and Road Operation of Intelligent Connected Vehicles require enterprises to build sustainable risk governance and prudent management capabilities. They institutionalise continuous security capacity, assessment materials and supervision inspections. Enterprises are required to verify the controllability of data security, network security and operational security under stricter standards [28,29]. The Notice on Further Strengthening Administration of Product Access, Recall and Over-the-Air Software Update of Intelligent Connected Vehicles integrates continuous effective security management, sufficient testing and verification, incident reporting and supervision. It forms a systematic standard across the entire life cycle [30].

Table 1. Provisions Related to Autonomous Driving Data Security in National Laws and Administrative Regulations.

Instrument	Key Regulatory Provisions
Data Security Law of the People’s Republic of China	Requires eligible outbound transfers to undergo a pre-transfer security assessment.
Cybersecurity Law of the People’s Republic of China (as amended in 2025)	Requires network operators to set up cybersecurity systems, appoint personnel, and enforce graded protection, monitoring and logging.
Personal Information Protection Law of the People’s Republic of China	Requires lawful basis for personal information processing, mandating sensitive data protection, risk assessment, security and incident response.
Regulations on the Administration of Network Data Security	Requires data processors to set up graded-protection-based internal systems and implement security response and reporting.
Provisions on Promoting and Regulating Cross-Border Data Flows	Requires data processors to continuously identify the scale of outbound transfers of important data and personal information, and to select appropriate compliance pathways accordingly.
Regulations on the Security Protection of Critical Information Infrastructure	Requires data processors to measure the scale of outbound transfers of important data and personal information and adopt corresponding compliance pathways.
Measures for Security Assessment of Cross-Border Data Transfers	Requires eligible outbound transfers to undergo a pre-transfer security assessment.

Table 2. Industry-Specific Policy Norms for Autonomous Driving.

Instrument	Specific Regulatory Requirements
Several Provisions on the Security Management of Automotive Data (for Trial Implementation) (Order No. 7)	Clarifies automotive data processors’ scope and relevant data categories with sectoral protection requirements.
Opinions on Strengthening the Administration of Intelligent Connected Vehicle Manufacturers and Product Access	Requires enterprises to set up data security systems, asset inventories, classification-grading, risk assessment, incident reporting, domestic storage and cross-border assessment mechanisms.
Notice on Strengthening Cybersecurity and Data Security in the Internet of Vehicles	Requires IoV stakeholders to strengthen institutions, risk monitoring, and prevention and response capacities.
Administrative Provisions on Road Testing and Demonstration Application of Intelligent Connected Vehicles (for Trial Implementation)	Requires testing and demonstration entities to secure adequate safety capacity, submit self-assessments, and build remote monitoring and regulatory mechanisms.
Notice on Carrying out Pilot Programmes for Market Access and Road Use of Intelligent Connected Vehicles and its supporting Implementation Guidelines	Requires applicants to build full-process assurance and evidentiary mechanisms.
Notice on Further Strengthening the Administration of Product Access, Recall, and Over-the-Air (OTA) Software Upgrades for Intelligent Connected Vehicles	Requires enterprises to enforce full-lifecycle security management, including testing, incident reporting and compliance commitments.
Technical Guidelines for Product Access, Recall, and Over-the-Air (OTA) Software Upgrade Management of Intelligent Connected Vehicles	Requires enterprises to upgrade cybersecurity, data security, privacy protection, OTA management and incident response capabilities.
Several Provisions on the Security Management of Automotive Data (for Trial Implementation) (Order No. 7)	Clarifies automotive data processors’ scope and key data categories with sectoral protection requirements.

At the same time, local legislation establishes more detailed criteria for the on-site testing and practical application of AVs (see Table 3). Nevertheless, regulatory frameworks for autonomous driving data security differ greatly among Chinese provinces and cities. Based on their regulatory requirements and practical implementation effects, these local rules can be divided into three categories: explicit clauses, indirect clauses and principle-only clauses. Local regulations in Beijing, Shanghai, Shenzhen and Suzhou fall into the category of explicit clauses. These regions have built comprehensive data security systems that cover data security, network security and personal information protection. They achieve full-range protection for AV data security. Moreover, their regulatory documents have unified requirements, involving risk prevention, risk threshold control, monitoring in process and reporting after events. By comparison, regulations in Tianjin, Changsha and other cities are classified as indirect clauses. These rules merely focus on incident disposal and unified data takeover platforms. They fail to regulate the whole lifecycle of AV data throughout testing and application stages. As a result, only partial requirements are fulfilled in these regions. In contrast, provincial regulations in Guangdong Province and similar regions only provide general principled guidance. They contain no specific provisions concerning production procedures, testing operations, or data security and risk management after unexpected incidents. Overall, regarding the comprehensiveness of regulatory content, China's local autonomous driving data security rules have formed a multi-level regulatory pattern with coexisting explicit, indirect and principle-only provisions.

2.2. Defects of the Existing AV Data Security Protection

China has established a diversified and integrated legal system for AV data security, covering national laws, administrative regulations and local legislation. This system involves national security, economic operation, social order, public interests and personal rights [31]. However, these requirements are scattered across different regimes governing data security, cybersecurity, personal information protection and intelligent connected vehicle access regulation, and a unified data governance standard has not yet been established. Meanwhile, in local practices, there are substantial discrepancies in data identification and data protection standards across regions, which further give rise to practical risks and dilemmas in AV data security governance.

2.2.1. Ambiguous Criteria for Sensitive Data Determination

The criteria for data judgement in existing departmental laws, administrative rules and technical norms are not unified. There is a large ambiguity in the identification of sensitive data. Specifically, different laws and rules adopt inconsistent definitions and identification standards for data. At the same time, industry-specific rules lack concrete and implementable criteria for sensitive data identification [32].

Different norms hold fundamentally different definitions and identification rules for important data. No unified applicable system has been formed. The Data Security Law establishes a top-down catalogue system. It requires the state, regions, departments and industries to formulate catalogues of important data. In contrast, the Regulations on the Security Management of Internet Data use a broader definition and a bottom-up reporting model. It requires data processors to conduct independent identification and proactive reporting before regulatory announcements. The two differ in responsible subjects, starting logic and definition methods. They conflict with each other. Meanwhile, detailed judgement provisions are missing in many specific fields. Take cross-border data transfer as an example. The Cybersecurity Law and the Data Security Law only set principled provisions on data export. The Several Provisions on the Management of Automobile Data Security (for Trial Implementation) should provide detailed rules. However, it only stip-

ulates that AV data export shall be subject to unified assessment by the Cyberspace Administration of China and other competent authorities. In general, current judgements of important data mostly rely on basic legal principles. There is a lack of detailed and operable standards for industry identification. Insufficiently detailed rules increase ambiguity in identification [33].

Meanwhile, the scope listed in industry-specific rules is limited. These rules also have poor connections and conflicts with superior laws and other departmental regulations. In automotive data regulation, the Several Provisions on the Management of Automobile Data Security (for Trial Implementation) adopt a list model. It clarifies geographic information of sensitive areas, traffic flow data, charging network operation data and external vehicle videos containing facial and licence plate information as important data. However, this provision conflicts with norms such as the Personal Information Protection Law. External perception videos and vehicle trajectory data that can locate individuals must meet anonymisation and de-identification requirements. To comply with automotive data regulation, enterprises often need to retain data for a longer period and in a wider scope. Current rules do not provide unified guidance. This causes practical difficulties in application [33]. In addition, the list is limited. It does not cover potentially important data such as raw AV perception data, connected vehicle control data and supply chain security data. It does not align well with the overall definition of important data in superior laws. On 11 December 2022, NIO, a Chinese manufacturer of AVs, was exposed for leaking approximately 399,000 sets of vehicle owner identity data, including identity card numbers, bank card details and residential addresses. Most of the compromised data were collected by the automaker prior to August 2021 [34]. During daily operations, both vehicle-side systems and the enterprise's internal IT infrastructure lacked adequate cybersecurity defence mechanisms. Meanwhile, the enterprise collected personal information far beyond the necessary scope for business needs, with no clear restrictions on data retention periods. The judgement criteria for defining the permissible scope of data storage remained highly ambiguous.

Furthermore, the Provisions on Promoting and Regulating Cross-Border Data Flows and the Regulations on the Security Management of Internet Data set different exemption rules for cross-border transfer. They clarify that enterprises which complete independent reporting but are not officially recognised as holders of important data can be exempted from cross-border security assessment. This further fragments the criteria for identifying important data. In 2022, DiDi (Beijing, China), a Chinese automotive service provider, was placed under official investigation for cross-border transmission of vehicle positioning data, travel trajectories and other vehicle-related data over multiple years. Regulators later confirmed that the firm had never passed the mandatory security assessment for cross-border data transfer. By the time of the investigation, DiDi had transmitted hundreds of millions of data records overseas, with the illegal conduct spanning seven consecutive years [35]. This incident reveals that China's current regulatory system relies heavily on ex-post security reviews. There is a lack of a coordinated, unified mechanism covering prevention, real-time monitoring and incident reporting across separate sectoral laws. Insufficient ex-ante screening and in-operation supervision substantially lower the illegal costs borne by relevant enterprises.

2.2.2. Inconsistent Data Protection Standards in Local Regulations

In local practice, local regulations have set detailed rules for data security protection. However, their provisions on responsible subjects and liability measures remain inconsistent. This leads to obvious differences among regional AV data security protection (see Table 3).

Table 3. Local Regulations, Government Rules, and Implementing Measures.

Category	Document Name	Specific Provisions
Explicit Clauses	Regulations of Beijing Municipality on Autonomous Driving Vehicles	Require enterprises to upload operational vehicle data to municipal autonomous driving platforms per rules and secure network security, data security, testing and real-time monitoring capabilities.
	Measures for the Administration of Testing and Application of Intelligent Connected Vehicles in Shanghai	Require network security regimes and graded protection; mandate timely submission and 1-year retention of accident records and analyses.
	Regulations of Shenzhen Special Economic Zone on Intelligent Connected Vehicles	Require ICVs to access regulatory platforms, upload safety operation data, and fully retain complete accident records.
	Regulations of Suzhou Municipality on the Promotion and Development of Intelligent Connected Vehicles	Establish integrated security systems for network, data, privacy and vehicle safety, with graded protection, local storage and outbound assessment.
	Regulations of Guangzhou Municipality on the Innovation and Development of Intelligent Connected Vehicles	Formulate network and data security emergency plans; mandate enterprise security systems, graded protection, privacy protection, local important data storage and lawful outbound assessment.
	Detailed Implementation Rules for the Administration of Road Testing and Demonstration Application of Intelligent Connected Vehicles in Wuxi Municipality	Mandate real-time vehicle data transmission, automatic accident recording, platform access and 1-year retention; require submission of security risk assessments and countermeasure certifications.
	Measures for the Administration of Road Testing and Application of Intelligent Connected Vehicles in Chongqing Municipality (for Trial Implementation)	Establish integrated security regimes, clarify responsibilities, enforce graded protection and lawful outbound security assessment.
Implicit Clauses	Detailed Implementation Rules for the Application of Regulations on Promoting Innovation of Unmanned Vehicles in Pudong New Area, Shanghai	Mandate district-level platform access, post-crash upload of 90 s pre-incident vehicle and video data, and retention of accident records and analyses.
Principle- Only Clauses	Regulations of Tianjin Municipality on Promoting the Development of Intelligent Connected Vehicles	Develop municipal ICV data platforms, full-process data governance mechanisms, and graded standards for uploaded data.
	Regulations of Changsha Municipality on the Development of Autonomous Driving	Mandate enterprise protection of autonomous driving data and real-time status recording, storage and monitoring for in-service vehicles.
	Measures for the Administration of Road Testing and Demonstration Application of Intelligent Connected Vehicles in Guangdong Province (for Trial Implementation)	Encourage local governments to build data regulatory platforms and formulate management measures.

First, requirements for data review and protection vary significantly across regions. For example, Shenzhen mandates that data recorded 90 s before accidents or malfunctions be retained for no less than 30 days. In contrast, Pudong, Shanghai requires real-time data transmission to official platforms. It also requires 90 s of pre-incident data to be stored for one year. Meanwhile, Tianjin and Changsha have no requirements for such storage periods. And secondly, provinces and cities adopt different standards for subject identification and liability allocation in autonomous driving [36]. They lack requirements for links such as data collection and data transmission. Specifically, they focus on vehicle manufacturers and test vehicle providers, but exclude key stakeholders like software developers and data service providers. Thus, it is difficult to clearly define responsible parties for disputes over data security and ownership. In addition, risk prevention and monitoring mechanisms differ across regions. For instance, Wuxi, Suzhou and Shenzhen require annual submission of data monitoring documents. By contrast, Tianjin and Wuhu have no regular rules for monitoring, filing or approval. They only clarify post-incident liability allocation. It can be seen that some local regulations prioritise post-incident remedies over prior risk prevention and monitoring.

Therefore, in order to resolve inconsistencies between laws and policies, clarify the boundaries and subjects of various rights and obligations, and achieve the balance and coordination of legal interests on the premise of minimising risks, it is necessary to learn from the different regulatory schemes for autonomous driving data security in various countries and regions, and explore specific improvement paths based on China's current practices.

3. EU Rules on Autonomous Driving Data Security Protection

As AV data security risks have become a key global issue, many countries and regions have introduced unified regulatory systems for AV data security [37]. As a leading advanced economy, the EU has established a world-class legal framework governing autonomous driving and data protection. Since 2018, it has continuously updated relevant rules and adjusted the scope of protection and regulatory systems in light of technological progress and vehicle conditions. The EU AI Act issued in 2024 is widely regarded as a prominent risk-based governance framework for high-risk AI systems [38]. By contrast, other economies, including the US, Japan, and South Korea, have rolled out relevant laws in recent years, yet their rules remain fragmented and limited. They also lack dedicated and unified legislation targeting data risks arising from algorithms. Thanks to steady legislative updates, the EU has formed a more comprehensive and referable framework for data governance, ongoing technical supervision and systematic liability confirmation. This chapter analyses the EU's rules for AV data security before operation, during operation and after operation (see Figure 3), and explores the core reasons behind its institutional strengths.

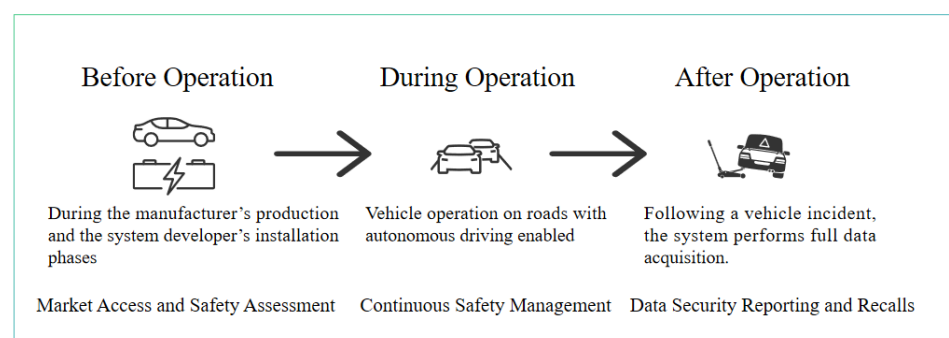


Figure 3. Three-stage Protection Framework for EU AV Data Security.

3.1. Importance of EU Rules

At present, many jurisdictions attach importance to the protection of data security rules for autonomous driving. The United States, Japan, South Korea and the European Union have all responded to data security risks of AVs to different degrees [12,37–39]. However, their institutional functions and degree of reference value are clearly different. Based on risk governance theory and combining full lifecycle management requirements for autonomous driving data security and artificial intelligence regulation, this paper aims to address technical risks with complex, uncertain and systemic characteristics through a continuous governance process. This process includes risk identification, risk assessment, risk management, risk communication and corrective feedback. On this basis, a more stable, continuous and unified regulatory model is selected as the main comparative object. From this perspective, the European Union has gradually shifted its autonomous driving data security rules from fragmented and single-point regulation to a staged, classified and enforceable full lifecycle governance structure. This development provides a more advanced regulatory model, which may help improve China's governance system for autonomous driving data security.

From the perspective of existing regulatory approaches in different jurisdictions, the United States has long relied on enterprise self-certification, federal safety guidance and state-level testing and deployment rules [39]. Its main advantage lies in leaving broad space for technological testing and innovation. The National Highway Traffic Safety Administration (NHTSA) requires manufacturers to demonstrate that vehicles are safe through their own assessments [39]. Overall, the US model mainly depends on corporate compliance statements, accident reporting and ex post enforcement. Data security in autonomous driving has not yet been integrated into a unified mandatory full lifecycle regulatory framework. For China, the US model provides useful reference in terms of regulatory flexibility and enterprise responsibility. However, it is less suitable for addressing China's fragmented rules, uneven local implementation and unclear boundaries for sensitive data.

In contrast, Japan introduced regulatory responses to autonomous driving earlier through the Road Traffic Act and the Road Transport Vehicle Act [12]. According to the National Police Agency of Japan, the 2022 revision of the Road Traffic Act established a permit system for "specified automated operation", covering Level 4 autonomous driving. This model focuses on integrating autonomous driving into road traffic management and operational permission systems. It is suitable for limited-area, fixed-route and public transport scenarios. However, Japan's regulatory focus is mainly on road use, operational permission and commercial deployment conditions. Its system is less developed in areas such as data risk governance, real-time monitoring during operation, post-incident data review and systematic AI risk management. Therefore, while Japan's experience is useful for pilot zones and operational management in China, it is not sufficient as a complete full-lifecycle governance model for autonomous driving data security.

South Korea mainly promotes autonomous driving through industrial support policies, pilot zones and vehicle safety standards. The Autonomous Vehicle Commercialisation Promotion Act emphasises industrial development and commercialisation support and establishes a foundation for safe deployment [39]. This approach provides a useful reference for understanding pilot zone governance and industrial policy tools in China. However, its focus remains on industrial promotion and demonstration projects, and the integration of data security, AI risk governance, product safety and post-incident correction is still limited.

The European Union is distinctive in that it addresses autonomous driving data security through a set of interconnected legal instruments. These rules cover vehicle product safety, market access, cybersecurity management, software update control, personal data

protection, data sharing, AI risk governance and market supervision. This institutional combination allows the EU to translate data security risks into specific regulatory tasks across different stages, including assessment before operation, monitoring during operation and correction after operation. Compared with the fragmented US model, the permission-based Japanese model and the industry-driven Korean model, the EU approach provides a more suitable reference for analysing how China can integrate scattered rules, clarify data boundaries and build a continuous compliance system.

Accordingly, this paper mainly adopts normative and comparative methods. The normative analysis is applied to examine the internal structure and institutional logic of the EU's data security rules for AVs. Specifically, taking regulatory norms covering vehicle market access, safety management, monitoring, artificial intelligence risk governance, and recall and rectification as research objects, this paper investigates their corresponding regulatory procedures and legal effects. Through this method, this paper reveals how the EU embeds abstract data security obligations into the continuous lifecycle of AVs, including market entry, road operation, and accident rectification, and translates diverse data security risks into targeted regulatory tasks for each stage. The comparative analysis aims to justify the rationality of taking the EU regime as the core reference and clarify its institutional boundaries. Focusing on China's practical demands of integrating scattered existing rules, clarifying the judgement criteria for sensitive data, unifying local implementation standards, and establishing a continuous compliance mechanism, this paper explores whether the EU's AV data security protection rules can address the structural problems existing in China's current autonomous driving data security governance system.

3.2. Analysis of the EU Phased Data Security Protection Rules for AVs

In recent years, the European Union has developed a relatively clear lifecycle governance structure for autonomous driving through rules on type approval and market access, in-operation monitoring and continuous reporting, and serious incident reporting and recall correction. Based on differences in data risk across operational stages of AVs, this paper divides the EU data security protection rules into three stages, including before operation, during operation and after operation (see Figure 3). Before operation, data security protection mainly takes place before manufacturing, system installation and market entry or road use. Through market access, type approval, technical document review, cybersecurity management and safety assessment, the EU ensures that AVs meet basic data security and operational safety requirements. During operation, AVs are already in use on roads. The regulatory focus shifts from static approval to continuous safety management, including ongoing monitoring and reporting requirements. After operation, regulation focuses on data retention, accident review, vulnerability repair, incident reporting and product recall after accidents, system failures or data security events, in order to ensure risk correction and system improvement.

3.2.1. Before Operation: Market Access and Safety Assessment

Since 2018, the EU has established a general framework for vehicle type approval and market supervision via Regulation (EU) 2018/858 [40]. Subsequently, Regulation (EU) 2019/2144 laid down unified data foundations and specific standards for autonomous driving, shifting from general provisions to technology-focused rules [41]. Commission Implementing Regulation (EU) 2022/1426 mandates inspections on the security and validity of AV data documents [42]. In terms of detailed rules, UN Regulation No. 155, No. 156 and No. 157, which took effect in 2021, set out specific requirements for cybersecurity management, OTA update security and software identification [43–45]. The upcoming EU AI Act further integrates driving safety and data risks of AVs into unified governance and mandates third-party safety assessments for high-risk AI systems.

Collectively, multiple EU laws and regulations align on unified market access and safety assessment criteria for AV data security. Since 2018, manufacturers have been required to submit documentation, EU type-approval certificates or UN type-approval certificates when applying for type approval. Competent authorities and technical service bodies may access vehicle systems and algorithms within the scope of their duties, with software and algorithm security listed as core criteria for driving safety. The EU also defines advanced emergency braking systems, intelligent speed assistance, emergency lane-keeping systems and harmonised technical rules as preconditions for AVs to operate on roads. It empowers the European Commission to formulate technical standards for fully automated vehicles and automated driving systems (ADS). Relevant rules require ongoing safety management and scenario verification for AVs, and oblige authorities to conduct ADS risk assessments to eliminate unreasonable risks. Additional rules impose strict requirements on manufacturers and system developers [40–42]. UN Regulation No. 155 requires manufacturers to put in place a Cybersecurity Management System (CSMS) to defend against cyber threats. They must also conduct threat analysis and risk assessment, establish risk mitigation mechanisms, and manage cybersecurity risks throughout the vehicle lifecycle. UN Regulation No. 156 mandates a Software Update Management System to guarantee that software updates do not compromise vehicle safety, environmental performance or regulatory compliance. UN Regulation No. 157 requires ALKS-equipped vehicles to be fitted with a Data Storage System for Automated Driving (DSSAD) [43–45]. The upcoming EU AI Act creates a new pre-assessment mechanism centred on third-party evaluation, expanding the scope of traditional reviews conducted by manufacturers and regulators. All relevant products must pass a conformity assessment carried out by independent notified bodies.

To sum up, the EU places data security protection at the pre-event stage prior to vehicle operation. Uniform data review standards and multi-party safety assessments ensure vehicles are equipped with reliable data security capabilities and free from unreasonable risks. While these legislations do not classify every potential risk source one by one, the adopted anti-risk evaluation and risk management mechanisms can effectively address existing and emerging safety risks accompanying technological advances in autonomous driving.

3.2.2. During Operation: Continuous Safety Management

In the full lifecycle protection system for autonomous driving data security, the ongoing supervision system established by the EU serves as the core link. Different from the basic norms for before market access, the dynamic supervision mechanism features dynamic monitoring, continuous compliance and full traceability formulated by a series of EU regulations. Therefore, it is necessary to require that the legislative plan can fully cover all scenario-based data security risks of AVs after they are put on the road, realising the integrated management of continuous compliance, operational monitoring and safety supervision of vehicles.

In terms of compliance management, the EU implements continuous supervision over vehicle operational changes on the basis of previously established compliance standards. Competent authorities are empowered to take necessary measures to ensure production consistency and even withdraw type approval if manufacturers fail to produce vehicles in accordance with approved models and regulatory requirements [40]. Meanwhile, manufacturers are obliged to promptly notify competent authorities of any changes to vehicles, systems or technical materials during operation. In terms of operational monitoring, early regulatory provisions stipulate that autonomous driving systems must maintain safe operation throughout the vehicle lifecycle and clarify the review and reporting obligations of manufacturers and system operators during vehicle operation [41]. Sub-

sequent regulatory provisions further refine the in-operation safety inspection requirements and clarify the specific safety responsibilities of manufacturers during vehicle operation. Annexe III Part 2 requires manufacturers to ensure the controllability and safety of autonomous driving systems throughout the whole lifecycle, manage the overall safety and continuous compliance of autonomous driving systems, and establish and improve the safety management system. In addition, manufacturers are required to formulate standardised procedures to collect vehicle data and multi-source data, so as to monitor and analyse safety-related accidents caused by autonomous driving systems [42]. Regulatory authorities are entitled to verify the continuous compliance of relevant certification requirements at any time. The detailed rules for in-operation driving data security are further supplemented and clarified in unified automotive regulatory provisions. Manufacturers are mandated to continuously monitor and respond to vehicle cybersecurity threats, track driving environments, driver statuses and system operating conditions in real time and build a complete cybersecurity incident response mechanism. They also need to maintain the stable operation of the software update management system and record the whole process of software updates. The latest legislative requirements represented by the EU AI Act further extend the data protection obligations of AVs to full-lifecycle log recording, requiring system providers to build standardised and stable dynamic monitoring systems that can actively and systematically collect, record and analyse relevant data, which significantly enhances the standardisation of in-operation data security governance.

In terms of overall supervision, the EU has built a complete in-operation data security protection system for autonomous driving through continuous compliance inspection of data security standards, real-time data collection and risk reporting mechanisms during vehicle operation, and unified full-lifecycle log monitoring systems. This system effectively clarifies the responsibilities of multiple stakeholders and forms a collaborative supervision pattern with clear rights and obligations. Relevant regulations connect manufacturers, system providers and regulatory authorities, defining manufacturers as the core responsible subjects for the full-lifecycle data security of autonomous driving systems. Manufacturers are required to formulate standardised processes for special data collection, accident analysis and risk reporting, and bear primary responsibilities for driving data security management, safety accident traceability and risk rectification. System providers need to build regular and standardised dynamic monitoring systems, and fulfil the obligations of full-lifecycle log recording, data archiving and software update traceability to ensure the full traceability of data circulation. Meanwhile, regulatory authorities are granted substantial supervision powers, including verifying the compliance qualifications of enterprises and the operational status of safety management systems, and adopting rectification notices, type approval revocation and other restrictive measures against non-compliant production and substandard data management behaviours. Relying on this systematic monitoring mechanism, the EU realises standardised, normalised and traceable management of autonomous driving data security.

3.2.3. After Operation: Data Security Reporting and Recalls

Data security reporting, rectification and vulnerability handling in the aftermath of operations serve as the most vital part for steadily improving autonomous driving data security. The EU has built a sustainable protection system via data recording, submission, compliance review and system upgrades after events.

Accurate retention of accident data lays the foundation for supervision and governance after operation. Multiple EU regulations set clear rules on data recording after accidents. One regulation requires EDR to capture driving safety data before and after accidents in conventional vehicle scenarios [41]. Another rule mandates DSSAD to record the

activation of ALKS, driver takeover and changes in system status to facilitate technical analysis after incidents [45]. Such data collection and analysis establish a complete workflow for data security supervision, rectification, system upgrade and product recall. On this basis, the EU has put in place a rigorous reporting mechanism for data security incidents. Manufacturers are obligated to report all data security incidents [42]. The EU AI Act further expands and strengthens reporting requirements. It stipulates that system providers must report all serious incidents and launch immediate investigations, including risk assessment and corrective actions [43]. After reports are submitted, EU market surveillance authorities will conduct reinspections against vehicle data security standards. Where vehicles, systems, components or separate technical units pose serious risks, market surveillance authorities shall order operators to take appropriate corrective measures immediately, including restricting market placement, withdrawal from the market or product recall [30]. Vehicles are prohibited from being put on the market or used again until their cybersecurity meets licensing requirements [41]. Relevant rules refine the above requirements into detailed provisions and allow authorities to revoke or cancel the SMS compliance certificates of non-compliant parties, so as to fully implement rectification liabilities after operation [42]. The EU has also formed a standardised management system for security vulnerability remediation and long-term system optimisation. A host of EU laws and directives govern vulnerability treatment and system updates. Manufacturers must adopt mitigation measures once cybersecurity loopholes or attacks are detected and maintain records of all security incidents [43]. Software updates shall not compromise vehicle compliance and operational safety. Manufacturers need to keep complete update records, identify update anomalies accurately and prevent new data security risks caused by software iteration [44].

Different from prevention before the operation and control during the operation, the after-operation response system focuses on governance and iterative improvement. It follows a complete governance logic from problem identification and rectification to recurrence prevention through standardised data retention, mandatory incident reporting, strict rectification and penalties, as well as regulated vulnerability repair and system updates. The incident reporting and licensing rules can promptly address ongoing data security incidents and defuse relevant risks. Meanwhile, the review and analysis of accident data push manufacturers and system providers to optimise data security management. This helps continuously enhance the data protection, cybersecurity and risk prevention capabilities of autonomous driving systems, remedy deficiencies in technology and management, and provide a solid guarantee for the safe, compliant and long-term development of the autonomous driving industry.

3.3. Limitations of the EU Rules

Although the European Union has established a relatively complete framework for autonomous driving data security protection covering market access, in-operation monitoring and post-accident correction, the system still has several unresolved institutional limitations.

First, EU data security governance for autonomous driving relies heavily on type approval, technical service assessment bodies, continuous compliance supervision and post-incident reporting mechanisms. While this arrangement can raise the safety threshold before and after vehicles enter the market, it also means that compliance costs are shared by both regulators and market actors. On the one hand, regulators must review technical documents, safety management systems and operational data submitted by manufacturers, and also supervise the qualification and independence of technical service bodies to avoid formalistic certification. On the other hand, manufacturers are required to maintain cybersecurity systems, software update systems, safety management systems, logging

mechanisms and in-operation reporting throughout the full lifecycle of vehicles, while also complying with multiple frameworks such as type approval rules, GDPR, the Data Act and the AI Act. As third-party testing and certification costs are generally borne by applicants, this model increases the overall regulatory burden, raising the entry threshold for advanced autonomous driving systems, especially for start-ups, small software providers and component suppliers. In addition, differences among Member States in regulatory capacity and administrative resources further increase implementation costs within the EU.

Second, there are still gaps in technical and data standard alignment across different regulatory stages, which may lead to a disconnect between before-operation compliance and during-operation safety. In the before-operation stage, safety is mainly assessed through type approval, operational design domain (ODD) descriptions, scenario testing and simulation. However, there is still no fully unified standard for scenario datasets, test coverage metrics or simulation data formats. The link between these tests and real-world performance still depends largely on manufacturer statements and technical service assessments. In the during-operation stage, regulation focuses on safety-critical events, out-of-ODD operation, system failures and abnormal user interaction, mainly through continuous monitoring and periodic reporting. However, these reports are usually short-term or aggregated annually, and are not fully aligned with before-operation testing indicators. In other words, before-operation regulation focuses on whether the vehicle passes predefined scenarios, while during-operation regulation focuses on whether abnormal events occur in real driving, and there is still no unified classification of events, data fields, interfaces or risk thresholds. The implementation of the AI Act further highlights this gap, as many supporting standards and guidance documents are still under development. For AVs, this means that requirements on risk management, data governance, technical documentation, logging, accuracy, robustness and cybersecurity have not yet been fully translated into unified technical indicators across approval, monitoring and after-incident review.

Finally, although EU rules strengthen data recording, during operation reporting and system traceability, they do not fully resolve the issue of liability determination in autonomous driving accidents. Such accidents often involve multiple actors. Even with DSSAD, EDR and system logs, it is not always possible to clearly determine legal responsibility. When the human driver is no longer the direct controller of the vehicle, the boundary of responsibility between driver, system and manufacturer remains unclear. Therefore, EU data security rules can provide an evidentiary basis for accident investigation, but they cannot replace liability rules. Further development of product liability, tort liability and specific autonomous driving legislation is still required.

4. China's AV Data Security Protection Drawing on the EU Rules

With the further deepening of China's autonomous driving industry layout, China's new energy vehicle sales reached 16.49 million units in 2025, accounting for 47.9% of total new vehicle sales. The export volume of new energy vehicles hit 2.615 million units, doubling year on year [46]. Meanwhile, data security issues concerning AVs exert remarkable impacts on consumers' purchasing willingness [47]. More seriously, such risks may hinder the sustainable development of the whole industry. China has, at an earlier stage, proposed a layered theory of data governance. However, the linkage between current data-related legislation and transport-related legislation in China remains weak. There is still a lack of targeted traffic data legislation that balances innovation needs and the protection of rights, especially legislation that promotes the open sharing of vehicle, road and transport operation data [12]. Therefore, how to implement the EU phased data security protection approach in China's legal practice, and how to build a framework that is both

unified and adaptable to China's national conditions, is of great importance. Based on a full understanding of the EU phased governance approach, this chapter further examines its applicability and limitations in China, and proposes optimisation paths tailored to China's legal and practical context.

4.1. Feasibility of the EU Phased Data Security Protection Rules for AVs in China

Compared with some jurisdictions that mainly regulate autonomous driving data security at isolated stages and have not yet formed an integrated framework covering both cross-regional coordination and full lifecycle regulation of system construction and operation, the EU phased protection model, centred on pre-operation review, in-operation monitoring and post-operation correction, provides an important reference for China in integrating fragmented data security rules, unifying compliance assessment paths and responding to the continuous evolution of autonomous driving technology. The main reason for unclear data boundaries and inconsistent local practices in China lies in the fragmentation of relevant rules. Although sectoral laws, vehicle industry-specific regulations and local rules are all closely related to vehicle data security, the lack of a unified application logic makes it difficult to form a stable and consistent compliance assessment path in practice [48].

On the one hand, the EU phased data security protection rules help establish a clear regulatory process. Through three stages, they define specific tasks at each stage, including risk identification and risk assessment before operation, continuous monitoring and record-keeping during operation, and information disclosure and remedial measures after operation. This regulatory framework helps unify the application order of conflicting laws and policies and align implementation standards across regions [49]. It also clarifies the boundaries of rights and obligations for different actors. Public authorities are responsible for setting and supervising market access standards, reviewing and filing manufacturer and system functions, and handling emergency response and liability allocation after data security incidents. In contrast, manufacturers and system developers are required to carry out comprehensive risk monitoring, take effective remedial measures and maintain complete post-incident data records. The adoption of the EU approach would further promote China to translate abstract identity-based liability allocation into risk-based and proportional due diligence standards within the vehicle-road-cloud multi-actor structure [49]. Existing fragmented assessment and reporting mechanisms can thus be understood as the implementation of a unified risk governance process across different legal domains and scenarios. In fact, this type of standard has already been widely used in China's traffic accident law within a risk governance framework and is gradually being incorporated into autonomous driving regulation. The EU phased model would further support its systematisation and consolidation [50].

On the other hand, the phased data security protection rules are also well suited to the continuous evolution of autonomous driving technology. As risk sources and levels continue to change [51], single inspection mechanisms, static compliance standards and post-operation liability determinations are no longer sufficient to keep pace with technological iteration. In terms of regulatory structure, the EU model adjusts institutional requirements at each stage to respond to emerging risks. Through adjustments in market access thresholds, operational monitoring and incident reporting feedback, relevant actors are required to update risk assessments and adjust preventive measures in light of new risk information, research findings and technological progress [52]. This structural advantage aligns with the regulatory needs of China's autonomous driving sector and provides clear top-level guidance for a continuous and dynamic regulatory framework. Accordingly, the regulatory logic shifts from one-off static compliance review to continu-

ous risk identification, risk control and transparent risk disclosure, promoting the governance of AV data security from static compliance to dynamic management.

However, the Chinese government should also note that due to differences in market structure, administrative systems, data sovereignty priorities and enforcement capacity, the EU phased data security protection model cannot be directly transplanted into China's regulatory system for autonomous driving data security. In the process of application, differences in institutional, cultural and legal systems between the two sides must be fully taken into account (see Table 4).

A comparison of institutional arrangements across three phases between the two jurisdictions reveals prominent divergences in their respective governance paths. Against this backdrop, localised and targeted adjustments aligned with China's existing protection framework are essential when drawing on the EU regulatory model. This paper conducts a layered comparison of the EU's phased data protection rules and China's current AV data security governance system based on before operation, during operation and after operation. When learning from the EU experience, it is necessary to fully acknowledge the institutional gaps between China's legal framework and the EU regime so as to formulate indigenous regulatory solutions suited to national conditions.

Firstly, in the before-operation phase, the EU builds a mature third-party technical evaluation system based on vehicle type approval, supported by comprehensive norms governing market entry testing assessment and supervision. However, China has not yet established a unified dedicated third-party evaluation system for AV data security. A direct copy of the EU third-party evaluation model will fail to gain recognition from regulatory authorities. It will also add extra procedures for qualification review standard formulation and mutual recognition of evaluation outcomes, driving up administrative law enforcement costs. Then, secondly, in the during-operation phase, the EU's unified continuous dynamic compliance monitoring mechanism cannot be transplanted as-is. Domestic AV supervision relies on local pilot programmes and territorial platforms to collect and manage operational environmental and human takeover data within respective jurisdictions. A nationwide centralised data monitoring system would conflict with established local data infrastructures. Inconsistent data standards across regions hinder cross-regional data circulation and create tensions regarding localised data storage requirements. Moreover, the EU implements centralised supervision by national authorities. Blind replication of this structure in China would create dual monitoring at national and local levels, triggering redundant data submission, excessive data collection and inefficient supervision. Finally, in the after-operation phase, China already boasts a complete post-incident review system, which eliminates the need to fully replicate the EU's entire ex-post supervision framework. Regulators only need to refine the coverage, triggering conditions, reporting entities and handling procedures for AV data incident reports. Clear logical connections between new and existing regulatory norms must be defined to eliminate duplicated reporting and multiple filing reviews for a single incident. Cumbersome reporting regimes would discourage corporate technological innovation, including algorithm iteration and software updates. Enterprises may deliberately slow technical optimisation to evade regulatory accountability.

Table 4. Comparison of EU and China Autonomous Driving Data Security Protection Institutions and Functions across Different Stages.

Stage	EU Main Institutions and Functions	China Main Institutions and Functions	Core Differences
Before Operation	● Vehicle type approval authorities in Member States are responsible for type approval;	◆ The Ministry of Industry and Information Technology is responsible for type approval; technical service bodies undertake testing, inspection and technical assessment;	● EU: regulatory focus is on whether vehicle data protection capability meets safety requirements across the system.
	● Technical service bodies undertake testing, inspection and technical assessment.	◆ Local governments formulate autonomous driving data security standards and management platforms based on local conditions.	◆ China: regulatory focus is on driving safety. Data security standards are fragmented and lack unified rules across regions.
During Operation	● Type approval authorities and market surveillance authorities supervise continuous compliance of vehicle data security;	◆ Public security and transport authorities focus on road traffic safety;	
	● Technical service bodies participate in ongoing verification;		● EU: emphasises the lifecycle responsibility of manufacturers and system actors, forming a continuous compliance chain.
	● Data protection authorities supervise personal data processing;	◆ Local governments undertake operational management, testing supervision and platform-based data reporting;	◆ China: focuses more on road traffic safety, with relatively weaker attention to data protection; local governments bear most operational supervision responsibilities.
	● AI supervisory authorities monitor high-risk AI systems;		
	● Manufacturers are responsible for cybersecurity management, software updates, logging and incident monitoring.	◆ Cyberspace authorities supervise data processing and cross-border data flows.	
After Operation	● Market surveillance authorities are responsible for handling product risks, and for reporting systems involving high-risk artificial intelligence systems;	◆ Market supervision authorities are responsible for handling product risks, defective vehicle product recalls and supervision of recall effectiveness;	
	● Type approval authorities are responsible for the withdrawal or restriction of type approval;	◆ The Ministry of Industry and Information Technology is involved in follow-up measures related to product access, software updates and automotive data security requirements;	● EU: post-operation governance focuses on product risk, data protection and serious AI incident reporting, and emphasises tracing accident data back to corrective measures and market withdrawal.
	● Data protection authorities are responsible for handling data breaches and related issues;	◆ Cyberspace administration and relevant authorities handle data security incidents, personal information breaches and important data risks;	◆ China: implementing authorities show no significant difference, but a dedicated risk reporting system for data security has not yet been fully established.
	● Manufacturers and legal entities bear obligations for accident data preservation, defect repair, software updates and product recall.	◆ Manufacturers and legal entities bear obligations for accident data preservation, defect repair, software updates and product recall.	

4.2. The Practical Path for AV Data Security Protection Rules in China

After comparing autonomous driving data security protection in the European Union, it can be found that the EU formed a full-chain data security governance approach centred on risk prevention, risk monitoring and risk reporting. This section analyses how the Chinese government can improve the coordination of existing legal rules, and puts forward suggestions on standardising identifiable, enforceable and traceable data security governance mechanisms for autonomous driving enterprises, operating entities and regulatory authorities at all stages, including system design, road operation and incident handling. It aims to gradually transform China's autonomous driving data regulation from a fragmented and post-event-oriented rule system to an institutionalised governance model focusing on whole-lifecycle risk control.

4.2.1. Prevention Before Operation

In the prevention stage, the AV data security protection is mainly reflected in risk assessment and prior authorisation systems [52]. Any authorisation decision should be based on the risk assessment required under China's existing data laws. Before conducting data processing activities with potential data security risks, regulatory authorities shall require AV manufacturers, system developers, data processors and other entities to obtain sufficient information through assessment procedures so as to make prudent authorisation decisions. The scope of such assessment shall cover scenarios closely related to the information security of vehicles being on public roads. These include product access and road testing applications, collection of important data and personal information, planning for cross-border data transfers, as well as the design and verification of over-the-air (OTA) upgrades. Existing risk identification mechanisms strive to translate the abstract concept of "harm risk" into operable evaluation criteria. However, detailed guidance for precise risk identification of important data remains insufficient, alongside ambiguous delineation of rights and obligations between regulatory authorities and enterprises. Accordingly, institutional construction at the prevention-before-events stage can be optimised from two aspects. In terms of assessment content, current data assessment mechanisms can establish multi-dimensional evaluation criteria according to the scope and objects of data infringement. According to the functional allocation of Chinese government authorities, the data security access assessment standards for autonomous driving vehicles should be coordinated by the State Council, led by the Ministry of Industry and Information Technology, and jointly developed with the Cyberspace Administration of China and the State Administration for Market Regulation, together with technical practice from domestic vehicle manufacturers. These authorities should jointly study and issue a core assessment indicator system. In practice, the Ministry of Industry and Information Technology should be responsible for the unified implementation of market access review for autonomous driving vehicles, and for ensuring the baseline of factory release and technical compliance. Public security traffic management authorities may rely on the results of market access compliance. For autonomous driving vehicles that fail to meet data security standards or have systemic data security risks, they should not issue road operation permits, or should revoke such permits in accordance with laws and regulations. This would prevent non-compliant vehicles from entering road operation at the source. Specifically, when AV data processing involves national security, economic operation, social order, public interests, organisational rights and personal rights, probability assessment and harm consequence identification shall be conducted respectively for potential adverse impacts. Based on the importance of the affected interests and the degree of harm, different risk objects and their consequences can be classified into different risk levels [53] (see Table 5). Moreover, when enterprises apply for data collection, transmission and utilisation

tion, they shall submit risk analysis reports on potential harms in addition to complying with data scope standards. Assessment elements of such reports include potential trans-boundary harms to individuals, properties and environment, possibility and severity of potential harms, and feasible risk mitigation measures [52]. In terms of access indicators, the capacity to prevent data security risks can be integrated into enterprise qualification evaluation in AV product access review. Applicant enterprises shall be required to prove technical and managerial capabilities in identifying, assessing and responding to data security risks [29]. Such capacity requirements can be specified as the establishment of data security incident monitoring mechanisms and emergency response plans.

Meanwhile, it is necessary to integrate the assessment functions of existing laws, regulations and administrative rules concerning AV data security. Following the principle of new norms prevailing over old ones for redundant assessment and verification procedures, authorities shall clarify responsible review institutions, evaluation entities and the credibility of review outcomes. As the competent authority for autonomous driving vehicles, the Ministry of Industry and Information Technology should clearly define the review institutions, assessment entities and the credibility of review outcomes [54]. At the same time, the State Council may, through the formulation of special legislation on autonomous driving or revising the Interim Provisions on Automobile Data Security Management, ensure that precise pre-event assessment can be realised based on data processing subjects, specific data processing scopes and data processing assessment results [8]. And priority among different subjects can also be defined. Each subject shall complete assessment within its corresponding risk scope, while avoiding redundant assessment overlapping with other subjects. For key data within the above scope, additional specialised and legitimate assessment procedures shall be established. On the premise of retaining original assessment systems, targeted evaluation shall be conducted for specific matters. For instance, when assessing state-related data, on the basis of permitting domestic circulation and utilisation of data in China, precise targeted assessment shall be carried out for foreign-related sensitive data. Such arrangements ensure the accuracy and effectiveness of overall data assessment.

In terms of access review, the examination system shall comprehensively cover four dimensions: cybersecurity protection, data security management, software update governance and autonomous driving safety guarantee. Moreover, differentiated access thresholds shall be set according to distinct data processing subjects and corresponding risk levels. For example, access criteria for road testing entities focus on dual evaluation of operational capacity and cybersecurity protection capacity. Operators of critical information infrastructure shall establish dedicated safety management departments and complete personnel background reviews. Entities engaged in AV transportation shall formulate transportation safety protection plans and assign dedicated safety officers [55–57]. Such classified and hierarchical governance reflects differentiated regulatory strategies for testing scenarios and mass-production application scenarios [58,59]. To bridge the gap between administrative access review and engineering implementation, pre-operation compliance must mandate specific cybersecurity baselines. Market access applications for AVs should require the mandatory integration of Hardware Security Modules (HSM) within in-vehicle Electronic Control Units (ECUs) and the adoption of zero-trust architecture concepts for strict internal network access control [60]. Furthermore, for V2X data transmission, the regulatory framework must enforce advanced cryptographic primitives to ensure the end-to-end confidentiality and integrity of vehicular communications, thereby mitigating unauthorised network access at the protocol level [61].

Table 5. Criteria for Assessing the Severity of Risks in Autonomous Driving Data.

Affected Subject	Risk Level	Assessment Criteria
National Security	High	Directly endangers key areas or sectors of national security, such as politics, territorial integrity, and military affairs
	Relatively High	Poses a serious threat to key areas of national security
	Medium	Poses a general threat to key areas of national security
Economic Operation	High	Directly affects critical aspects of the national economy, causing particularly severe impacts on economic operation
	Relatively High	Directly affects macroeconomic performance and development trends, causing serious impacts on economic operation
	Medium	Causes general impacts on the development of a specific industry or the order of economic operation
Social Order	High	Directly leads to particularly serious emergencies, severely disrupting normal social functioning
	Relatively High	Directly leads to major emergencies, seriously disrupting daily social order
	Medium	Directly affects daily life and the order of activities in public places
Public Interest	High	Involves major public interests, such as causing particularly serious cybersecurity and data security incidents
	Relatively High	Endangers public health and safety, such as triggering major public health emergencies
	Medium	Causes general harm to public interests within a limited scope
Organisational Interests	Medium	Organisation is subject to severe penalties, resulting in significant technical, economic, or reputational losses
	Relatively Low	Organisation is subject to regulatory penalties, resulting in considerable technical, economic, or reputational losses
	Low	Leads to isolated disputes or incidents, causing minor economic or reputational losses
Individual Interests	Medium	Causes significant harm to individuals, such as infringement of dignity or threats to personal and property safety
	Relatively Low	Causes noticeable impact on individuals, but can be mitigated at a relatively high cost
	Low	Individuals may experience inconvenience or disturbance, but the impact is manageable

4.2.2. Monitoring During Operation

Meanwhile, the risk assessment is not a one-time procedure. Its regulatory requirements extend throughout the entire duration of relevant activities. This has formed broad international consensus across various fields [62]. In other words, data security monitoring constitutes an inherent part of its normative connotation [52]. Accordingly, an effective, stable and long-term data monitoring and management system shall also be established in China's autonomous driving data security governance. Thus, the monitoring entities shall include vehicle manufacturers, cloud platform operators, mobility service providers and operational entities, as well as local regulatory authorities. Such monitoring shall specifically target real-time vehicle operation and data interaction, data transmission, storage and access control, identification of abnormal data behaviours and risk early warning, as well as data log retention and desensitisation management. At present, China has adopted threat analysis and risk assessment methods to identify and monitor potential cybersecurity risks of AVs. The whole procedure includes six steps: asset identification, threat scenario identification, impact level assessment, attack feasibility assessment, risk value determination and risk response decision-making [63]. Nevertheless, China's current risk monitoring system still suffers from inconsistent regional standards and ambiguous provisions on data processing.

Accordingly, institutional construction in the monitoring stage shall achieve comprehensive monitoring and refined management. In terms of monitoring scope, regional data monitoring standards shall be unified and strengthened to ensure full supervision over data activities. On the one hand, monitoring intensity shall be adjusted according to potential data risks. Detailed risk analysis shall be conducted across the whole data lifecycle, including data collection, utilisation, sharing, transmission and storage. Furthermore, different risk factors shall be evaluated. Monitoring measures and intensity shall be differentiated based on occurrence probability and potential harm consequences of respective risks. The classification method in this paper is based on the study by Wirtz, Weyerer and Kehl [64]. This study systematically develops a risk-oriented classification framework for artificial intelligence governance, and makes an important methodological contribution to research on AI risk governance [64] (see Table 6). For low-level risks such as data loss and reduced data validity, flexible remedial measures can be adopted after verifying overall system security. Available solutions include data backup recovery, cache replenishment and operational record correction. For high-level risks including data leakage, data tampering, illegal cross-border transfer and unlawful data disclosure, relevant processing activities shall be suspended immediately. Authorities shall seal involved data and systems, conduct special self-inspection and submit incident reports. Legal liabilities shall be imposed on responsible parties for resulting damages. On the other hand, highly divergent regional data monitoring and management standards shall be unified to guarantee consistent implementation of data security risk management nationwide. A unified national standard for autonomous driving data regional monitoring may be drafted by an autonomous driving industry association based on industrial practice. After review, approval and standardisation by the Ministry of Industry and Information Technology, it can be issued as a national industry standard or departmental regulation and implemented by local competent authorities. Where existing local regulatory rules and data platforms conflict with the unified national standard, they should complete systematic rectification, adaptation and harmonisation within one year after policy implementation. The implementation of rectification should be included in key governmental performance assessments and reported to higher-level competent authorities. In addition, ambiguous regulatory expressions shall be clarified. For instance, Shenzhen's autonomous driving regulations require safety data from onboard equipment to access government supervision platforms, yet the specific scope of such data and corresponding regulatory basis remain unclear. Therefore, supporting legislation and detailed management rules can be improved to

specify upload requirements for different types of data, such as data collected by vehicle sensors and braking system operation data [27].

Relevant norms shall be formulated for different types of data and corresponding processing principles. It is necessary to coordinate and balance monitoring intensity among various data categories to avoid conflicts between regulatory objectives. Besides the onboard operational safety data mentioned above, facial recognition data is another major factor leading to ambiguous data boundaries and excessive data collection by enterprises. Reference can be made to the privacy policy of Twitter, which stipulates that data shall be deleted immediately after identity verification to adhere to the principle of minimal data collection. Corresponding privacy control mechanisms shall also be strengthened simultaneously [65]. On the one hand, enterprises shall submit annual reports on data collection, deletion, transmission, backup and utilisation to ensure the implementation of monitoring standards. On the other hand, public interest litigation mechanisms shall be promoted by courts or procuratorates in various regions. Collective litigation procedures can safeguard consumer rights sufficiently when autonomous driving enterprises infringe upon user privacy. In addition, detailed data processing rules shall be further refined. Clear classification criteria, including mandatory reporting, optional reporting and internal retention, can provide practical guidance for enterprises to conduct data processing and fulfil monitoring obligations [66].

4.2.3. Remediation After Operation

The normative function of monitoring in process lies in risk tracking and timely early warnings. Nevertheless, the requirements do not terminate once potential risks evolve into actual harms. When determining preventive and mitigative measures, relevant data processors shall consider multi-party interests in good faith and pursue equitable solutions [52]. Under this regulatory framework, vehicle manufacturers and operational entities shall actively take damage mitigation measures and submit voluntary incident reports. Competent industry authorities, together with judicial and law-enforcement agencies, shall balance the interests of multiple stakeholders in the subsequent handling of data security incidents. At present, China has established preliminary risk reporting mechanisms. These include an information collection network for autonomous driving safety incidents, a data security incident reporting system, and an annual risk assessment reporting system [24,56]. However, these provisions obviously lack specific requirements. They fail to specify the specific form, procedures for investigation reports and subsequent corrective measures after accidents occur but before liability determination. This will grant excessive discretionary power to enforcement authorities in practice, easily leading to inconsistent investigation and reporting standards and unclear liability determination.

Therefore, China should further improve the reporting obligations and liability remedy obligations after accidents occur, particularly in incidents such as data leakage, data breach, or cybersecurity incidents, traffic accidents caused by automated driving, vehicle defect investigation and product recall, as well as illegal cross-border data transfer or other non-compliance events. In terms of post-event data security reporting, it is necessary to further refine the relevant reporting and preliminary investigation mechanisms in the subsequent revision of the current Interim Measures for the Administration of Road Testing and Demonstration Application of Intelligent Connected Vehicles. First, the competent authority for receiving data security reports shall be clarified. A dual-entity coordinated reporting mechanism may be established. Routine data security compliance reports and fault traceability reports from automobile manufacturers should be submitted to the Ministry of Industry and Information Technology. Special data security reports involving road traffic accidents and driving safety risks should be simultaneously submitted to public security traffic management authorities. The two authorities should establish a regular information sharing and joint handling mechanism. This can help avoid duplicate reporting and excessive data collection. This will implement

specific jurisdiction responsibilities and avoid delays in information transmission, shirking of responsibilities or poor connection in investigations due to unclear boundaries of duties after accidents occur [29]. Second, the time limit for data security reporting shall be strictly regulated, and a hierarchical reporting mechanism shall be established according to the severity of accident consequences. For example, for accidents causing heavy casualties, major property losses or triggering significant data security risks, immediate reporting or initial reporting within an extremely short time limit shall be required. For general accidents, a relatively reasonable but clear reporting time limit can be set. The State Council may, with reference to the regulatory standards for major public security incidents and work safety incidents, establish classification standards and differentiated reporting time limits for autonomous driving data security incidents. Local governments should, based on existing data platforms, ensure strict implementation of the system. Third, the Cyberspace Administration of China, in coordination with the Ministry of Industry and Information Technology, should further standardise the content of data security reports and establish unified, clear and operational definitions for reporting items. The report content shall not be limited to general factual information such as the time, location and damage results of the accident. It shall also include key contents such as preliminary analysis of the cause of the accident, a complete description of the accident process, vehicle operation status, algorithm traceability data of the decision-making logic of the autonomous driving system, records of sensors and control modules, records of manual takeover or intervention, remote control status, and data storage and retrieval status [59]. From a forensic engineering standpoint, post-operation accountability relies heavily on reliable data provenance. This necessitates upgrading the technical specifications of current Event Data Recorders (EDR). Specifically, AVs must employ cryptographic immutable storage technologies—such as lightweight blockchain frameworks or tamper-proof log systems—to securely archive autonomous decision-making algorithm traceability data and OTA update logs [5]. Such technical enforcement ensures that post-accident investigations can definitively distinguish among hardware sensor failures, external cyberattacks, and internal algorithmic decision flaws [67].

In terms of liability remedy, the AV data security protection does not end with data security reporting after accidents. It also guides the state to establish clear, effective and enforceable mechanisms for liability bearing and damage remedy. At present, China's liability allocation for autonomous driving traffic accidents still mainly relies on the traditional tort liability framework for motor vehicles. This framework is built on the premise that human drivers directly control vehicles. When facing scenarios where autonomous driving systems participate in decision-making or even dominate vehicle operation, the framework gradually exposes prominent problems. These include difficulty in identifying liable subjects, ambiguous liability boundaries and insufficient efficiency in victim relief [68]. Accordingly, China shall formulate differentiated liability allocation rules corresponding to different levels of autonomous driving as soon as possible [69]. For low-level AVs, the driver-centred liability model can be maintained. Meanwhile, corresponding liabilities of vehicle manufacturers, software providers and operating entities shall be confirmed in cases of system defects, insufficient risk warnings and monitoring failures. For high-level AVs, clear liability division criteria shall be established among multiple subjects including producers, system developers, operators, owners and users. Such arrangements prevent dilemmas such as ambiguous liability attribution or excessive liability concentration on a single subject after accidents [70]. In addition, supporting insurance and social relief systems shall be improved simultaneously. For instance, compulsory insurance, commercial insurance schemes and necessary social compensation mechanisms adaptive to risk characteristics of autonomous driving shall be promoted. These systems enable victims to obtain timely and basic damage compensation before complete liability determination. Afterwards, insurers and relevant liable parties may conduct recourse and liability sharing in accordance with final liability determination results [71].

Table 6. Specific Risks and Monitoring Measures.

Risk Category	Severity Level	Monitoring Measures	Technical Countermeasures
Unlawful or Non-compliant Data Processing	High	Conduct regular audits of data sources, purposes of use, and data sharing practices	Zero-Trust concepts & Access Control Protocols
Excessive Collection of Sensitive Personal Data	Medium	Periodically verify whether the scope of data collection exceeds the necessity principle	Edge-computing based data minimisation
Data Loss and Damage Risk	Medium	Continuously inspect the status of data backup, storage, and recovery mechanisms	Redundant encrypted cloud backup via HSM
Data Tampering and Fabrication Risk	High	Monitor abnormal modifications, substitutions, and operation logs	Cryptographic immutability (e.g., blockchain)
Data Abuse Risk	Medium	Monitor authorisation usage and abnormal access patterns	Strict role-based access control (RBAC)
Data Leakage Risk	High	Monitor abnormal access, downloading, and data transmission activities	Anomaly-based Intrusion Detection Systems (IDPS)
Cross-border Data Transfer Risk	High	Monitor the scope and flow of cross-border data transmission	Automated IP-geofencing and Gateway control
Data Inference Risk	Medium	Regularly assess risks related to data linkage and re-identification	Real-time differential privacy & spatial-blurring
Data Transmission Failure Risk	Low	Monitor transmission latency, packet loss, and link stability	V2X QoS monitoring & fail-safe mechanisms

5. Conclusions

The rapid development of AVs has fundamentally reshaped the structure of data generation, circulation and governance. As vehicles evolve into highly integrated digital systems, traditional regulatory approaches that rely on scattered legal provisions and static compliance standards are increasingly inadequate to address the dynamic nature and rising risk intensity of autonomous driving. Based on a comparative analysis of the EU AV data regulatory system, this study takes different application stages of autonomous driving technology as its entry point. The phased protection rules for autonomous driving data security discussed in this paper help clarify the regulatory priorities of data protection at each stage and are of great significance for coordinating legislation and policies across different fields. By summarising and organising risk sources at different stages, protection priorities can be adjusted, and the order of applicable norms can be clarified. Therefore, this paper advocates the establishment of a unified phased protection framework that integrates risk prevention, risk monitoring and risk identification to overcome the structural limitations of current supervision. This framework shifts regulatory logic from fragmented rule classification to standardised risk-oriented assessment. Meanwhile, such a unified system effectively reduces regulatory uncertainty and improves the operability of compliance mechanisms. This study not only proposes a feasible and reasonable approach for China to optimise its AV data supervision system, but also provides an expandable governance model for international reference. Through cross-regional comparative analysis, it facilitates institutional improvement and standardised industrial development, enabling legal supervision to keep pace with the evolving characteristics of technological risks in autonomous driving.

Author Contributions: Conceptualization, Y.W. and H.T.; methodology, Y.W.; software, Y.W.; validation, Y.W., H.T. and C.L.; formal analysis, H.T.; investigation, Y.W.; resources, C.L.; data curation, Y.W.; writing—original draft preparation, Y.W. and H.T.; writing—review and editing, Y.W. and C.L.; visualisation, Y.W.; supervision, H.T.; project administration, Y.W.; funding acquisition, C.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Social Science Fund of China (NSSFC) Key Project entitled “Research on Building a Global Community of Health for All and International Responsibilities for Pandemic Prevention and Control” (grant number: 22AFX026) and the China Scholarship Council (grant number: 202206270151).

Data Availability Statement: No new data were created or analysed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Zhang, X.; Qiu, B. Data Security Risks and Governance in Autonomous Vehicles. *J. Anhui Norm. Univ. Soc. Sci.* **2025**, *53*, 125–135.
2. OLIGO. Airborne: Wormable Zero-Click Remote Code Execution (RCE) in AirPlay Protocol Puts Apple & IoT Devices at Risk. Available online: <https://www.oligo.security/blog/airborne> (accessed on 15 April 2026).
3. CNEVPOST. Nio Suffers User Data Breach, Hacker Demands \$2.25 Million Worth of Bitcoin. Available online: <https://cnevpost.com/2022/12/20/nio-suffers-data-breach-company-respond/> (accessed on 15 April 2026).
4. Hu, Y.; Kuang, W.; Qin, Z.; Li, K.; Zhang, J.; Gao, Y.; Li, W.; Li, K. Artificial Intelligence Security: Threats and Countermeasures. *ACM Comput. Surv.* **2021**, *55*, 20.
5. Chen, R.; Li, M. Regulatory Logic and Construction of Product Access Standards for Autonomous Vehicles. *J. Chongqing Univ. Posts Telecommun. Soc. Sci.* **2025**, *in press*.

6. Zhang, Y. Hacker Attacks on Autonomous Vehicles: Criminal Risks and Regulation. *Intell. Connect. Veh.* **2021**, *2*, 54–60.
7. Wang, X. Research on Algorithmic Safety Regulation of Autonomous Vehicles. *Hebei Enterp.* **2025**, *10*, 157–160.
8. Jia, B.; Chen, Z.; Li, J.; Li, G.; Yang, Q. Regulations and Evaluation Methods for Autonomous Vehicles: Research Progress and Prospects. *Automot. Dig.* **2025**, *10*, 19–23.
9. Zheng, Z. Autonomous Vehicle Legislation: Global Practice and Local Landscape. *Shanghai Law Res.* **2024**, *11*, 115–142.
10. Zhao, J.; Zheng, Z.; Zheng, F.; Chen, J.; Zhang, J. China's Approach to Autonomous Driving Governance: Background and Innovations of the Beijing Autonomous Vehicle Regulations. *Digit. Rule Law* **2025**, *1*, 120–132.
11. Chen, B. Coordinating security and connectivity to promote autonomous driving data governance. *People's Trib.* **2023**, *18*, 73–77.
12. Zheng, G. Data rule of law and future transportation: A discussion on autonomous vehicle data governance. *China Law Rev.* **2022**, *1*, 202–214.
13. Zheng, L.; Li, M. On the Dual Legal Barriers to Market Access for Autonomous Vehicles and Their Resolution. *J. Ocean Univ. China Soc. Sci.* **2023**, *4*, 61–70.
14. Bai, J. Whether the Factor Has Fulfilled the Duty of Prudence Is Irrelevant to Factoring Liability. *People's Judic.* **2019**, *17*, 66–70.
15. Li, R. Legal regulation of cybersecurity in autonomous vehicles. *Adm. Reform* **2019**, *10*, 43–49.
16. Zhang, T.; Jiang, Y. Personal data protection in intelligent vehicles: Explorations and implications from the European Union and Germany. *Ger. Stud.* **2019**, *34*, 92–113.
17. China Association of Automobile Manufacturers. 2024 Automotive Industry Economic Performance. Available online: https://pdf.dfcfw.com/pdf/H3_AP202501171641965011_1.pdf (accessed on 15 April 2026).
18. Qiu, B.; Li, G. Research on Data Security Management of Intelligent Connected Vehicles. *Automot. Eng. J.* **2022**, *12*, 307–313.
19. KPMG. Cybersecure Vehicles. Available online: <https://assets.kpmg.com/content/dam/kpmgsites/xx/pdf/2024/04/cybersecure-vehicles.pdf.coredownload.inline.pdf> (accessed on 15 April 2026).
20. Li, Z.; Li, S.; Zhang, H.; Zhou, Y.; Xie, S.; Zhang, Y. Overview of sensing attacks on autonomous vehicle technologies and impact on traffic flow. *arXiv* **2024**, arXiv:2401.15193.
21. Gupta, S.; Maple, C.; Passerone, R. An Investigation of Cyber-Attacks and Security Mechanisms for Connected and Autonomous Vehicles. *IEEE Access* **2023**, *11*, 90641–90669.
22. Sun, Y.; Wu, L.; Wu, S.; Li, S.; Zhang, T.; Zhang, L.; Xu, J. A survey of security mechanisms for edge computing-based connected autonomous vehicles. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 2682–2720.
23. UNECE. Regulation No. 155: Uniform Provisions Concerning the Approval of Vehicles with Regard to Cyber Security and Cyber Security Management System (Annex 5). Available online: <https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security> (accessed on 15 April 2026).
24. The National People's Congress of the People's Republic of China. Data Security Law of the People's Republic of China. Available online: http://www.npc.gov.cn/npc/c2/c30834/202106/t20210610_311888.html (accessed on 16 April 2026).
25. The National People's Congress of the People's Republic of China. Cybersecurity Law of the People's Republic of China (2026 Current Version). Available online: <https://www.ssf.gov.cn/portal/rootfiles/2026/02/27/1773947155578281-1773947155587379.pdf> (accessed on 16 April 2026).
26. The National People's Congress of the People's Republic of China. Personal Information Protection Law of the People's Republic of China. Available online: https://www.cac.gov.cn/2021-08/20/c_1631050028355286.htm (accessed on 16 April 2026).
27. Cyberspace Administration of China. Provisions on the Management of Automotive Data Security (Trial). Available online: https://www.cac.gov.cn/2021-08/20/c_1631049984897667.htm (accessed on 16 April 2026).
28. NCSTI. Notice on Strengthening Cybersecurity and Data Security in the Internet of Vehicles. Available online: https://www.ncsti.gov.cn/zcfg/zcwj/202109/t20210916_41642.html (accessed on 16 April 2026).
29. Ministry of Public Security of the People's Republic of China. Notice on Launching Pilot Programs for Market Access and Road Testing of Intelligent Connected Vehicles. Available online: <https://www.mps.gov.cn:9080/n6557558/c9297309/content.html> (accessed on 16 April 2026).
30. NCSTI. Notice on Further Strengthening the Administration of Market Access, Recall and Over-the-Air (OTA) Software Updates of Intelligent Connected Vehicle Products. Available online: https://www.ncsti.gov.cn/zcfg/zcwj/202503/t20250303_197224.html (accessed on 16 April 2026).
31. Lu, Y.; Guo, X.Y.; Liu, J.; Li, H.; Tu, H.Z. Data Security Risk Assessment Method for Autonomous Driving Road Test Data. *Shanghai Highw.* **2024**, *4*, 119–131.

32. Hebei Governance. Guidelines for the Construction of the National Internet of Vehicles Industry Standard System (Intelligent Connected Vehicles) (2023 Edition) (Annex 2). Available online: <https://gxt.hebei.gov.cn/hbgy-hxxht/zcfg30/gnzc/2025042121422493047/2023072710093811318.pdf> (accessed on 16 April 2026).
33. Qian, L. Data Security Risks and Legal Protection for Autonomous Driving. *China Inf.* **2023**, *4*, 65–67.
34. Caijing (Financial News). NIO Vehicle Data Theft Leads to “Sky-High” Ransom Demand: China Association of Automobile Manufacturers: Should Not Compromise with Criminal Behavior. Available online: <https://www.cls.cn/detail/1218021> (accessed on 26 June 2026).
35. Cyberspace Administration of China. Statement by the Responsible Official of the Cyberspace Administration of China on the Administrative Penalty Decision Regarding Cybersecurity Review of DiDi Global Inc. China Cyberspace Administration Network. Available online: https://www.cac.gov.cn/2022-07/21/c_1660021534364976.htm (accessed on 26 June 2026).
36. Ba, Z.; Zhao, Z.; Zhang, B. Liability for Autonomous Vehicle Torts: Who Should Be Held Responsible? *World Electr. Veh. J.* **2025**, *16*, 665.
37. Dede, G.; Hamon, R.; Junklewitz, H.; Naydenov, R.; Malatras, A.; Sanchez, I. *Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving*; Publications Office of the European Union: Luxembourg, 2021. Available online: <https://www.enisa.europa.eu/publications/enisa-jrc-cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving> (accessed on 27 June 2026).
38. World Bank. Digital Progress and Trends Report 2023. World Bank. 2023. Available online: <https://www.worldbank.org/en/publication/digital-progress-and-trends-report> (accessed on 7 June 2026).
39. Seul, M.-s. Current Status and Directional Improvement of Korea’s Regulatory Framework on Development of Automated Vehicles, Benchmarking the U.S.—Focusing on Technological Features, Motor Vehicle Safe, Regulating Agency, Test Drive on Public Roads. *JURIS* **2019**, *1*, 445–498. Available online: https://www.kci.go.kr/kciportal/landing/article.kci?arti_id=ART002472786 (accessed on 3 June 2026).
40. European Parliament and Council. Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the Approval and Market Surveillance of Motor Vehicles and Their Trailers, and of Systems, Components and Separate Technical Units Intended for Such Vehicles. Available online: <https://eur-lex.europa.eu/eli/reg/2018/858/oj> (accessed on 7 June 2026).
41. European Parliament and Council. Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on Type-Approval Requirements for Motor Vehicles and Their Trailers, and of Systems, Components and Separate Technical Units Intended for Such Vehicles, as Regards Their General Safety and the Protection of Vehicle Occupants and Vulnerable Road Users. Available online: <https://eur-lex.europa.eu/eli/reg/2019/2144/oj> (accessed on 7 June 2026).
42. European Commission. Commission Implementing Regulation (EU) 2022/1426 of 5 August 2022 Laying Down Rules for the Application of Regulation (EU) 2019/2144 as Regards Uniform Procedures and Technical Specifications for the Type-Approval of the Automated Driving System (ADS) of Fully Automated Vehicles. Available online: https://eur-lex.europa.eu/eli/reg_impl/2022/1426/oj (accessed on 7 June 2026).
43. United Nations Economic Commission for Europe. *UN Regulation No. 155: Uniform Provisions Concerning the Approval of Vehicles with Regard to Cyber Security and Cyber Security Management Systems*; United Nations: New York, NY, USA, 2021. Available online: <https://unece.org/sites/default/files/2023-02/R155e%20%282%29.pdf> (accessed on 7 June 2026).
44. United Nations Economic Commission for Europe. *UN Regulation No. 156: Uniform Provisions Concerning the Approval of Vehicles with Regard to Software Update and Software Updates Management Systems*. Available online: <https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update> (accessed on 7 June 2026).
45. United Nations Economic Commission for Europe. *UN Regulation No. 157: Uniform Provisions Concerning the Approval of Vehicles with Regard to Automated Lane Keeping Systems*; United Nations: New York, NY, USA, 2021. Available online: <https://unece.org/sites/default/files/2023-12/R157e.pdf> (accessed on 7 June 2026).
46. China Digital Economy Portal. Large-Scale Deployment of AI Models in Vehicles Achieved in China. Available online: https://www.szzg.gov.cn/2025/xwzx/qwfb/202509/t20250924_5082198.htm (accessed on 16 April 2026).
47. KPMG. *24th Annual Global Automotive Executive Survey: Getting Real About the EV Transition*; KPMG: Amstelveen, The Netherlands, 2024. Available online: <https://assets.kpmg.com/content/dam/kpmgsites/ch/pdf/kpmg-global-automotive-executive-survey-2024.pdf.coredownload.inline.pdf> (accessed on 16 April 2026).
48. International Law Commission. *Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law*; United Nations: New York, NY, USA, 2006. Available online: https://legal.un.org/ilc/documentation/english/a_cn4_l702.pdf (accessed on 16 April 2026).

49. OECD. Due Diligence Guidance for Responsible Business Conduct. Available online: https://www.oecd.org/en/publications/2018/02/oecd-due-diligence-guidance-for-responsible-business-conduct_c669bd57.html (accessed on 16 April 2026).
50. Xu, W.; Zhang, L. Artificial intelligence legislation: EU experience and China's pathway. *Ger. Stud.* **2024**, *39*, 76–93.
51. RAND Corporation. Driving to Safety: How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability? Available online: https://www.rand.org/pubs/research_reports/RR1478.html (accessed on 16 April 2026).
52. UN. *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with Commentaries*; United Nations: New York, NY, USA, 2001. Available online: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_7_2001.pdf (accessed on 16 April 2026).
53. Stanford University, University IT. Risk Classifications. Available online: <https://uit.stanford.edu/guide/riskclassifications> (accessed on 26 June 2026).
54. Meng, F. Administrative Regulation of Autonomous Vehicles. Master's Thesis, Tianjin Normal University, Tianjin, China, 2023.
55. Ministry of Ecology and Environment of the People's Republic of China. Regulations on the Security Protection of Critical Information Infrastructure. Available online: https://www.mee.gov.cn/zcwj/gwywj/202108/t20210817_858013.shtml (accessed on 16 April 2026).
56. Cyberspace Administration of China. Regulations on the Security Management of Network Data. Available online: https://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm (accessed on 16 April 2026).
57. Ministry of Transport. Guiding Opinions of the Ministry of Transport on Promoting the Development and Application of Autonomous Driving Technology in Road Transportation. Available online: https://xxgk.mot.gov.cn/2020/jigou/kjs/202111/t20211110_3625462.html (accessed on 16 April 2026).
58. NSCTI. Opinions on Strengthening the Administration of Market Access of Intelligent Connected Vehicle Manufacturers and Products. Available online: https://www.ncsti.gov.cn/zcfg/zcwj/202108/t20210812_38612.html (accessed on 16 April 2026).
59. Ministry of Public Security of the People's Republic of China. Administrative Specification for Road Testing and Demonstration Application of Intelligent Connected Vehicles (Trial). Available online: <https://www.mps.gov.cn/n6557558/c8087335/content.html> (accessed on 16 April 2026).
60. Aliwa, E.; Rana, O.; Perera, C.; Burnap, P. Cyberattacks and countermeasures for in-vehicle networks. *ACM Comput. Surv.* **2021**, *54*, 21.
61. Sun, X.; Yu, F.R.; Zhang, P. A survey on cyber-security of connected and autonomous vehicles (CAVs). *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 6240–6259.
62. ITLOS. Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area. p. 10. Available online: https://www.itlos.org/en/main/cases/list-of-cases/case-no-17/?utm_source=chatgpt.com (accessed on 16 April 2026).
63. GB 44495-2024; Technical Requirements for Vehicle Information Security. National Public Service Platform for Standards Information: Beijing, China, 2024. Available online: <https://std.samr.gov.cn/gb/search/gbDetailed?id=208DEC46F6B347EEEE06397BE0A0AA4A0> (accessed on 16 April 2026).
64. Wirtz, B.W.; Weyerer, J.C.; Kehl, I. Governance of artificial intelligence: A risk and guideline-based integrative framework. *Gov. Inf. Q.* **2022**, *39*, 101685.
65. Office of the Privacy Commissioner of Canada. Study of the Use and Impact of Facial Recognition Technology Issue Sheets. Available online: https://www.priv.gc.ca/en/privacy-and-transparency-at-the-opc/proactive-disclosure/opc-parl-bp/ethi_20220502/is_ethi_20220502/ (accessed on 16 April 2026).
66. Zhang, J. The Shield of Privacy in the Digital Age: The Clash between Facial Recognition Technology and Personal Information Protection—Case Analysis and Strategy Discussion. *Adv. Soc. Behav. Res.* **2024**, *8*, 66–77.
67. Cebe, M.; Erdin, E.; Akkaya, K.; Aksu, H.; Uluagac, S. Block4Forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles. *IEEE Commun. Mag.* **2018**, *56*, 50–57.
68. Gurney, J.K. Sue My Car Not Me: Products Liability and Accidents Involving Autonomous Vehicles. *Univ. Ill. J. Law Technol. Policy* **2013**, *2*, 247–277. Available online: <https://illinoisjltlp.com/file/62/Gurney.pdf> (accessed on 3 June 2026).
69. European Parliament. Civil Law Rules on Robotics (2015/2103(INL)). Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2018_252_R_0026 (accessed on 16 April 2026).

70. Long, B.; Zhao, Z.; Cai, Q. Comparing Tort Liability Frameworks in Autonomous Vehicle Accident Governance. *World Electr. Veh. J.* **2026**, *17*, 32–49.
71. Geistfeld, M. A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation. *Calif. Law Rev.* **2017**, *105*, 1611–1694. Available online: <https://lawcat.berkeley.edu/record/1127996?v=pdf> (accessed on 3 June 2026).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.