我国汽车行业数据安全现状、问题及对策研究

薛凯　文洋

（中国汽车工程研究院股份有限公司，重庆 404100）

【欢迎引用】薛凯，文洋．我国汽车行业数据安全现状、问题及对策研究[J]．汽车文摘，2025(3)：37-41.

【Cite this paper】XUE K, WEN Y. Research on the Current Situation, Problems, and Countermeasures of Data Security in China's Automotive Industry[J]. Automotive Digest (Chinese), 2025(3): 37-41.

【摘要】为了更好地推进汽车行业数据安全管理，建设行业数据安全管理体系，分析了汽车行业数据安全政策、标准，数据安全现状、企业数据安全合规情况，总结了当前汽车行业数据安全存在数据多重监管、缺乏有效协同、标准规范不统一、供应链防护体系薄弱、缺乏专业人才等问题。针对以上问题，提出以下发展建议：统筹建立汽车行业数据安全监管机制，根据不同处理主体明确责任边界，加快数据分类分级、重要数据管理，提升全产业链数据安全管理和防范意识和能力，以及加强行业数据安全综合人才培养。

关键词：汽车行业；数据安全；政策法规；监管机制

中图分类号：U461.99　　**文献标志码：**A　　**DOI:** 10.19822/j.cnki.1671-6329.20240032

Research on the Current Situation, Problems and Countermeasures of Data Security in Chinese Automotive Industry

Xue Kai, Wen Yang

（China Automotive Engineering Research Institute Co. Ltd., Chongqing 404100）

【Abstract】To enhance data security management in the automotive industry and establish a robust industry-wide data security management system, this paper analyzes policies, standards, current state of data security and the compliance of enterprise data security. The following issues are identified: multiple layers of data regulation lacking effective coordination, inconsistent standards and specifications, a weak supply chain protection system, and a shortage of specialized talent. In response to these challenges, the following development suggestions are proposed: Establish a comprehensive regulatory mechanism for data security in the automotive industry. Clearly define the boundaries of responsibility for different processing entities. Accelerate the classification and grading of data, as well as the management of critical data. Enhance data security management and risk prevention awareness and capabilities throughout the entire industry chain. Strengthen the training and development of professionals specializing in comprehensive industry data security.

Key words: Automotive industry, Data security, Development status, Policy and regulation, Regulatory mechanism

0　引言

在智能化、网联化背景下，汽车行业数据规模也随之呈现出爆发式增长。随着数字经济近两年被国家和社会广泛关注，数据安全问题也成为数字经济在各行业应用管理过程中最重要、最复杂且最具挑战性的工作。当前，在汽车领域中，数据安全研究主要聚焦在智能网联汽车领域，在汽车研发、生产、销售到使用、维护、报废等各个环节的数据安全问题未得到充分关注。本文从汽车行业全链条角度分析行业数据安全发展现状，总结当前存在的问题，提出对策建议，为汽车行业在数据安全领域的研究提供参考。

1　汽车行业数据安全现状

1.1　政策法规

自2016年以来，我国发布了若干网络和数据安全相关政策及法规，为数据安全领域的技术发展和深化应用提供了指导和参考。《网络安全法》《数据安全法》《个人信息保护法》等数据安全相关上位法相继颁布，为我国数据安全监管提供了制度支撑和法律依据。

在国家政策法规的指导下，汽车行业也相继发布了《车联网（智能网联汽车）产业发展行动计划》《智能汽车创新发展战略》《新能源汽车产业发展规划（2021–2035年）》等产业发展战略规划，加强汽车数据安全管理体系建设。在一系列汽车产业发展战略规划的指导下，汽车行业数据安全管理政策法规陆续出台，全面推动汽车行业数据安全管理体系建设[1]。

当前，除了上位法和宏观政策，汽车行业数据安全政策法规的重点主要侧重于总体安全管理要求、数据分级分类、测绘和地图管理等方面。

在数据安全管理要求方面，近两年工信部和网信办等部委相继发布《关于加强智能网联汽车生产企业及产品准入管理的意见》《汽车数据安全管理若干规定（试行）》《关于加强车联网网络安全和数据安全工作的通知》等文件对汽车及智能网联汽车的数据安全管理进行了规范。尤其在《关于加强智能网联汽车生产企业及产品准入管理的意见》中明确提出强化数据安全管理能力，主要内容包括：企业应当建立健全汽车数据安全管理制度，依法履行数据安全保护义务；建立数据资产管理台账，实施数据分类分级管理，加强个人信息与重要数据保护；建设数据安全保护技术措施，落实数据安全风险评估、数据安全事件报告等要求；需要向境外提供的数据，应当通过数据出境安全评估。

在数据分类分级管理方面，《数据安全法》《关于促进数据安全产业发展的指导意见》《网络数据安全管理条例（征求意见稿）》《智能汽车创新发展战略》《新能源汽车产业发展规划（2021—2035年）》《关于加强智能网联汽车生产企业及产品准入管理的意见》《关于加强车联网网络安全和数据安全工作的通知》《工业和信息化领域数据安全管理办法（试行）》等文件均明确了实施数据分类分级管理，需要制定行业重要数据和核心数据具体目录，并开展重要数据备案管理工作，加强个人信息与重要数据保护。

在测绘和地图管理方面，2017年4月，《中华人民共和国测绘法》完成第二次修订，明确要求从事测绘活动的单位应当依法取得相应等级的测绘资质证书；互联网地图服务提供者应当建立地图数据安全管理制度，采取安全保障措施；不得擅自发布中华人民共和国领域和中华人民共和国管辖的其他海域的重要地理信息数据。2022年8月，自然资源部发布了《关于促进智能网联汽车发展维护测绘地理信息安全的通知》，明确了测绘活动和测绘活动的行为主体，强调从事相关数据收集、存储、传输和处理的车企、服务商及智能驾驶软件提供商等应依法取得相应测绘资质或委托具有相应测绘资质的单位开展相应测绘活动，要求存在向境外传输测绘地理信息数据行为或计划的应依法履行对外提供审批或地图审核程序等。

1.2 标准现状

2022年3月，工信部办公厅发布了《车联网网络安全和数据安全标准体系建设指南》，为车联网产业的安全发展提供了支撑。2023年7月，工信部和国家标准委员会联合发布了《国家车联网产业标准体系建设指南（智能网联汽车）（2023版）》。智能网联汽车标准体系横向以智能感知与信息通信层、决策控制与执行层、资源管理与应用层为基础，纵向以功能安全和预期功能安全、网络安全和数据安全通用规范技术为支撑，形成“三横两纵”的核心技术架构。汽车数据安全标准用于确保智能网联汽车数据处于有效保护和合法利用的状态并具备保障持续安全状态的能力，对数据提出明确的安全保护要求，对重要数据和个人信息提出重点安全保护要求。

目前来看，汽车行业智能网联汽车网络安全和数据安全标准体系框架已形成，但90%的标准尚未发布，尤其是分类分级、应用数据安全、安全能力评估等亟需的标准还在制定中。同时，汽车行业整个产业链的数据安全标准及体系仍然缺失。在生产端，工控安全的标准要求能部分适用于汽车生产过程，而其他环节上的数据安全相关标准目前仍处于空白阶段[2]。

1.3 行业数据安全现状

汽车行业数据存在于汽车研发设计、生产制造、经营管理、运行维护、平台管理等各个环节[3]。随着汽车行业数字化变革的不断深入，汽车行业数据量与日俱增。研发设计环节，智能网联汽车迅速发展，平台开发、模块开发、软硬件开发的代码数据在车企和系统集成供应商内部大量增加，智能网联汽车代码数量已是传统汽车的4~5倍，且还在不断增长。在生产环节，数字化技术的应用大幅提升了数据的采集量，一套AI计算机视觉系统对每辆车的喷漆表面进行拍照和分析，仅100 s就可拍摄10万张照片。在车辆使用过程中，尤其是智能网联汽车通过车内外传感器采集大量行驶数据、环境数据和行为数据，还采集海量操作系统的用户行为数据，一辆L4级自动驾驶汽车每日会产生约10 TB数据，约为传统汽车的10倍，已逐渐成为产生与连接海量数据的中枢。此外，在企业日常经营过程中，用户个人信息、车辆信息、充电信息等数据均以TB级甚至PB级的规模。

汽车行业数据量的激增使数据安全问题越发凸显。数据安全不仅影响企业品牌和声誉，核心技术资料、客户数据、财务数据等敏感信息泄露还将为企业和个人带来更大的资金风险和安全隐患。近年来，黑客入侵、数据窃取、暗网贩卖数据、通过网络控制企业生产设施逼迫企业停工停产的事件时有发生，包括奔驰、奥迪、宝马、丰田、大众、蔚来等知名车企都受到数据安全问题侵袭[4]。统计显示，2020年12月至2022年底，共有980起车企数据泄露事件在暗网平台发布，其数据获取的渠道除了来自车企外，也有可能来自车管所、经销商以及第三方平台等。可见，汽车行业数据安全风险问题日趋严重。

1.4 企业数据安全合规情况

在企业数据安全管理体系建设方面，为降低数据安全风险，车企积极建立数据安全防护管理体系[5]。在流程制度上，构建全面的安全体系管理策略；在体系章程、事件管理、组织人员等数据安全制度上，沿用信息安全管理制度，进行企业内部数据分类分级、数据安全评估、数据共享使用等方面的工作；在安全防护技术手段，从数据全生命周期进行技术能力建设。同时，跨国车企也已在中国建立数据中心，以实现数据存储的本地化要求[6]。

在企业数据分类分级方面，目前大部分企业已经建立覆盖企业全部管理范围和企业行业数据的分类分级相关制度文件，制定依据如表1所示。由表1可以看出，企业的分类分级工作依据来源多样化。企业综合考虑上位法律及工业和信息化部、国家互联网信息办公室等主管部门的规章，参考车联网、信息安全、金融等方面的分类分级和分级管理标准及其他地方性、海外相关政策法规等，制定符合企业自身的汽车行业数据分类分级制度。

2 我国汽车行业数据安全存在的问题

2.1 多重监管，缺乏协同

数据安全管理存在于汽车产业全生命周期的各个环节，包括车辆研发、生产、产品准入及测试、使用等，所有环节产生的各种类型数据又同时涉及数据全生命周期安全管理。因此，汽车行业数据现已跨越汽车管理的边界，在产业链各主体之间流转，车辆全生命周期与数据全生命周期交织叠加，极大地增加了数据安全管理难度。国家网信办、工信部、自然资源部等多部门均具有汽车行业数据安全监管职责，各部门亟需理清管理边界和职责范围。此外，随着数据合规监管不断加强，企业需在数据全生命周期做到合规管理，但由于各部门对汽车数据管理职责不明确、缺乏有效协同，出现重复审查等多重监管问题，增加了企业数据安全合规成本和管理难度。

表1 企业制定数据分类分级的依据

文件类型	文件名称
法律	《中华人民共和国网络安全法》 《中华人民共和国数据安全法》 《中华人民共和国个人信息保护法》
规章	《工业和信息化领域数据安全管理办法（试行）》 《汽车数据安全管理若干规定（试行）》
标准	GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》[7] GB/T 22240—2020《信息安全技术 网络安全等级保护定级指南》[8] GB/T 35273—2020《信息安全技术 个人信息安全规范》[9] GB/T 41871—2022《信息安全技术 汽车数据处理安全要求》[10] R/T 0197—2020《金融数据安全 数据安全分级指南》[11] YD/T 3751—2020《车联网信息服务 数据安全技术要求》[12] YD/T3746—2020《车联网信息服务 用户个人信息保护要求》[13]
其他国内文件	《智能网联汽车数据分类分级实践指南》 《北京市高级别自动驾驶测试示范区数据分类分级白皮书》
国外相关文件	ISO/IEC 27001:2013《信息技术 安全技术 信息安全管理体系要求》[14] ISO/IEC 27002:2013《信息技术 安全技术 信息安全管理实用规则》[15]

2.2 标准规范不统一

数据标准化是数据环境建设中的重要环节，通过数据标准可以保障基础数据的一致性和严密性。目前，我国数据安全已形成初步标准框架，在数据分类分级、出境安全等方面均有覆盖，然而现有标准仍然处于探索阶段，已规划标准仍有部分处于未发布状态，同时在管理体系建设、安全审查、相关标准制定等方面存在缺失。此外，汽标委和通标委都在汽车行业数据安全方面制定了一些标准，但由于起草单位视角不同，要求实现方式也不相同，存在现阶段各类标准规范思路和框架不统一的现象。部分标准要求内容交叉，落实指导意见存在差异，暂未形成统一协调的汽车数据安全监管体系，对重要数据识别存在认知不一致，因此难以实现统一监管和企业数据安全合规落地。

2.3 供应链防护体系薄弱

企业掌握的数据类型和数据规模不断增加，需要针对数据的特性进行更加精细化的安全策略保护。但对于大多数企业来说，近年来伴随着汽车行业的数据安全管理要求逐步完善，数据安全保护意识和数据

安全保护能力建设刚起步，无论从人员配置、资金投入、培训力度等都有待提高。

同时，虽然车企积极建立数据安全防护体系，但是供应链其他企业由于成本高、建设难度大、数据安全意识不足等原因，自建数据安全防护体系的积极性不足，仅少数头部公司有数据安全防护体系。此外，整车企业对供应链数据安全管理没有改进落实，车企对供应商的选择评估要求，目前依然沿用传统的质量、价格、响应、交货、管理、技术能力和设施等方面的选择评估要求，并没有涉及对供应商的数据安全管理防护的相关要求，数据安全隐患较大[16-17]。

2.4 缺乏专业人才

随着政府与企业对数据安全的要求逐步提升，对相关人才的需求也不断增多。我国每年自高校输送的数据安全毕业生数量十分有限，汽车行业数据安全的人才缺口大。此外，除了人才短缺，行业还存在人才“不好用”的问题，汽车数据安全领域有很多应聘者都是“半路出家”，往往是从相关领域“转行”到数据安全工作，对汽车行业本身了解并不深刻，不足以应对汽车行业的数据安全问题。

3 对策及建议

3.1 统筹建立汽车行业数据安全监管机制

我国数据安全法律框架已基本形成，为国家各行业数据安全监管提供制度参考和法律依据。在国家政策法规的指导下，聚焦汽车领域，数据安全被纳入汽车产业发展战略规划，明确要从政策法规体系、安全管理体系和支撑保障体系三方面发力，加强汽车数据安全管理体系建设，全面推动汽车安全防护进入数据安全监管时代。然而为更好实现产业链各企业数据安全合规落地，政府及行业研究机构应当兼顾车辆全生命周期和数据全生命周期的汽车行业数据，全面梳理汽车行业数据资产，并依据汽车管理流程及各部门职责范围，统筹建立汽车行业数据安全监管机制，提升监管能力，落实规章制度，对企业开展数据安全合规给予明确指导。

3.2 根据不同处理主体明确责任边界

现行法律法规对数据处理者提出了明确要求，然而随着汽车数据流转的复杂性，多方主体在保护汽车行业数据安全方面的权责义务不够清晰，彼此间的责任难以界定。应当根据汽车制造商、零部件和软件供应商、出行服务企业等不同责任主体，划分数据安全合规责任边界，明确责任主体在处理数据过程中所涉及的数据范围、处理环节和安全防范措施，明确彼此间的工作边界以及协作机制。此外，在明确整车企业和零部件供应商责任的基础上，应进行明显标识以作为处理事故追责的凭证，开展实行数据安全责任制，实现全产业链数据安全防护。

3.3 加快数据分类分级、重要数据管理

充分发挥标准对汽车行业数据安全的支撑作用，加快推动汽车数据安全重点标准研究和制定。着眼标准统一性、协调性、落地性，促进行业数据安全技术、产品、服务和应用标准化，提升数据保护和使用能力，鼓励科研院所、企事业单位、普通高等院校及职业院校等各类主体积极参与汽车行业数据安全标准制定。同时，政府应牵头制定汽车行业数据分类分级指南，明确数据分类分级原则和方法，提升企业数据分类分级的可实施性和可操作性，指导企业进行重要数据识别和目录备案。基于分类分级结果，企业应制定具有针对性的安全策略和措施，积极开展数据安全管控措施落地实践，为车辆数据安全管理提供支撑。

3.4 提升全产业链数据安全管理和防范意识和能力

在数据安全管理意识方面，政府及行业机构应通过多种渠道宣传数据安全对汽车行业的重要性，做好政策宣贯落实，开展企业数据安全培训，定期组织召开汽车行业数据安全管理经验交流会议，加强企业数据安全防护的责任和义务，提高产业链各环节主体的数据安全意识。同时，企业应定期开展数据安全培训，培养数据安全管理能力，并设立专门的安全合规工作组开展定期检查、抽查等，全面负责产业链甚至跨领域的企业相关数据安全管理及合规工作。同时，企业应梳理数据资产，开展数据分类分级管理、重要数据识别和备案，提升数据安全防护技术，强化数据安全监测预警和应急处置能力，建立完善的数据安全管理体系。

3.5 加强行业数据安全综合人才培养

首先，提升企业现有人才综合能力：建立健全数据安全人才选拔、培养和激励机制，立足企业实际数据安全建设需求，明确数据安全岗位能力要求，针对性加快紧缺岗位人才培养。其次，借助高校、企业事业单位和行业机构的力量，通过汽车行业数据安全能力提升培训平台等方式，加快单一专业人才向复合型人才的转变。通过推进职业资格评价、职业技能等级认定、专项职业能力考核等，通过产学研用闭环人才培养机制。最后，推动普通高等院校加强数据安全学科教育。强化课程体系、师资队伍和实习实训等，加大精通汽车行业数据安全治理复合型人才的补充。将汽车数据安全测试实际经验和教学相结合，提高在

校学生对汽车行业数据安全治理的专业能力培养。

4 结束语

汽车行业数据安全已经逐渐成为汽车产业高质量发展重要保障，各主体单位都应深刻认识到加快汽车行业数据安全建设的重要性和必然性。对政府而言，加快政策出台和落实，加强数据安全监管力度，才能更好的保障汽车行业的数字化发展和应用。对整个汽车产业链、供应链而言，提升各环节主体单位的数据安全保障能力，加强数据安全意识培养，才有可能进一步提升数字化应用对企业及行业的赋能，实现汽车行业数字经济的高质量、高效率、高水平发展。

参 考 文 献

[1] 毕马威中国，观韬中茂律师事务所．车网联数据安全监管制度研究报告[R/OL].2022(2022.03). https://assets.kpmg.com/content/dam/kpmg/cn/pdf/zh/2022/03/data-security-regulations-internet-vehicles-2022.pdf.

[2] 北京车网科技发展有限公司，国汽(北京)智能网联汽车研究院有限公司．北京市高级别自动驾驶测试示范区数据分类分级白皮书 2.0[R/OL]. 2023(2023-09). https://www.doc88.com/p-74487942050726.html.

[3] 数据安全推进计划．智能网联汽车数据分类分级实践指南[R/OL]. 2022(2023-01). https://mp.weixin.qq.com/s/mpwqXzl0n2qsIoYM-sUeDQ.

[4] 全国信息安全标准化技术委员会．信息安全技术 网络安全等级保护基本要求：GB/T 22239—2019[S/OL].（2019-05-10）[2019-05-10]. https://www.bzwy.cn/details/30c6ea1c87ff4c4c8f4e94ccad60c90b?bzbh=GB%2FT%2022239-2019&bzid=30c6ea1c87ff4c4c8f4e94ccad60c90b&uuid=76E52BE1F9196E7F8476692CC8A369B8.

[5] 全国信息安全标准化技术委员会．信息安全技术 网络安全等级保护定级指南：GB/T 22240—2020[S/OL].（2020-04-28）[2020-04-28]. https://www.bzwy.cn/details/nocgb-gb_bzgg-7597?bzbh=GB%2FT%2022240-2020&bzid=nocgb-gb_bzgg-7597&uuid=6E0C1110ACF7192B8A742F3AEB3CE131.

[6] 全国信息安全标准化技术委员会．信息安全技术 个人信息安全规范：GB/T 35273—2020 [S/OL].（2020-03-06）[2020-03-06]. https://www.bzwy.cn/details/c9f0e6db51104afc862809786c6dcf1e?bzbh=GB%2FT%2035273-2020&bzid=c9f0e6db51104afc862809786c6dcf1e&uuid=F2801DAFD85770B1D64B4975291463B3.

[7] 全国信息安全标准化技术委员会．信息安全技术 汽车数据处理安全要求：GB/T 41871—2022 [S/OL].（2022-10-12）[2022-10-12]. https://www.bzwy.cn/details/eaf076ae6778438c89d73406ec955376?bzbh=GB%2FT%2041871-2022&bzid=eaf076ae6778438c89d73406ec955376&uuid=AF41FA2C27A7651CEB4A2140FC4627B7.

[8] 全国金融标准化技术委员会．金融数据安全 数据安全分级指南：JR/T 0197—2020 [S/OL].（2020-09-23）[2020-09-23]. https://www.bzwy.cn/details/131647cd1f284dfda8cac4b4ed848b81?bzbh=JR%2FT%200197-2020&bzid=131647cd1f284dfda8cac4b4ed848b81&uuid=0A9C94D637A815B061F83CE5950BC706.

[9] 中国通信标准化协会．车联网信息服务 数据安全技术要求：YD/T 3751—2020 [S/OL].（2020-08-31）[2020-08-31]. https://www.bzwy.cn/details/3c8c602a32094baf9da92b538529a99d?bzbh=YD%2FT%203751-2020&bzid=3c8c602a32094baf9da92b538529a99d&uuid=2F89826F725F98EE879D37DB2367E9BB.

[10] 中国通信标准化协会．车联网信息服务 用户个人信息保护要求：YD/T3746—2020[S/OL].（2020-08-31）[2020-08-31]. https://www.bzwy.cn/details/13576aac35344c97bff006875a4ef5b4?bzbh=YD%2FT%203746-2020&bzid=13576aac35344c97bff006875a4ef5b4&uuid=C9C6D5026ABB35F42F0595A8A7DD6E9E.

[11] 西班牙标准化和认证协会．信息技术 安全技术 信息安全管理体系要求：ISO/IEC 27001:2017 [S/OL].（2017-05-24）[2017-05-24]. https://www.bzwy.cn/details/87cd482f-be80-11ee-a25f-b8599f4d3b32?bzbh=UNE-EN%20ISO%2FIEC%2027001%3A2017&bzid=87cd482f-be80-11ee-a25f-b8599f4d3b32&uuid=44BEC0C1D4D891754B538D41E006EE29.

[12] 西班牙标准化和认证协会．信息技术 安全技术 信息安全管理实用规则：ISO/IEC 27002: 2017[S/OL].（2017-05-24）[2017-05-24]. https://www.bzwy.cn/details/87cd4be9-be80-11ee-a25f-b8599f4d3b32?bzbh=UNE-EN%20ISO%2FIEC%2027002%3A2017&bzid=87cd4be9-be80-11ee-a25f-b8599f4d3b32&uuid=C618808557CB9F64AB9BB35344A3D15F.

[13]《中国工业和信息化》编辑部．吉利汽车 数据安全治理硬实力[J]. 中国工业和信息化, 2023(11): 21.

[14] 赵丽梅．共谋数据安全与治理的高质量发展之道[N]. 中国青年报, 2023-05-30 (005).

[15] 卢梦琪．加快制定汽车全生命周期数据安全标准[N]. 中国电子报, 2023-03-10 (003).

[16] 赵子垚．车企数据安全风险加剧 [J]. 汽车纵横, 2023(2): 18-21.

[17] 杨梓．新能源车企须系好“数据安全带”[N]. 中国能源报, 2023-01-02 (012).

（责任编辑 **明慧**）