“标准助推‘新质生产力’发展”征文活动优秀奖

以数据安全标准体系助推智能网联汽车产业发展新质生产力

丁钰 陈桂华 王辰

〔国汽（北京）智能网联汽车研究院有限公司〕

摘 要：数据是推动智能网联汽车产业发展的重要动力，作为新型生产要素，数据既是劳动对象也是劳动资料，也是推动新质生产力发展的关键因素。然而，随着智能网联汽车渗透率的持续提升，数据安全问题也日益突出。当前，智能网联汽车数据安全管理需解决现有规范与市场需求不对应的困境，强化规范与产业发展的黏性。为此，可通过建立健全数据安全标准体系，保障数据的有效保护与合法利用，推动智能网联汽车产业实现安全、高效、合规发展，助推新质生产力的提升。

关键词：智能网联汽车，数据安全，标准体系，新质生产力

DOI编码：10.3969/j.issn.1674-5698.2024.12.001

Boosting the Development of New Quality Productive Forces in the Intelligent Connected Vehicle Industry through a Data Security Standards System

DING Yu CHEN Gui-hua WANG Chen

（National Innovation Center of Intelligent and Connected Vehicles）

Abstract: Data is a crucial driving force for the development of the intelligent connected vehicle (ICV) industry. As a new type of production factor, data serves both as a labor object and a means of production, which is also a key element to drive the growth of new quality productive forces. However, as the penetration rate of ICVs continues to increase, data security issues are becoming increasingly prominent. Currently, the management of ICV data security faces challenges due to the misalignment between existing regulations and market demands, highlighting the need to strengthen the coherence between regulatory standards and industry development. To address this issue, establishing a comprehensive data security standards system can ensure the effective protection and legitimate use of data, fostering the safe, efficient, and compliant development of the ICV industry, thereby promoting the advancement of new quality productive forces.

Keywords: intelligent connected vehicles, data security, standards system, new quality productive forces

基金项目：本文受重庆市教委科学技术研究项目“科技伦理合规体系构建研究”（项目编号：KJZD-K202400305）资助；重庆市教委人文社科研究项目“成渝地区双城经济圈司法数据共享机制研究”（项目编号：22SKJD029）资助。

作者简介：丁钰，工程师，硕士研究生，从事智能网联汽车标准法规研究。

陈桂华，高级工程师，硕士研究生，从事智能网联汽车标准研究。

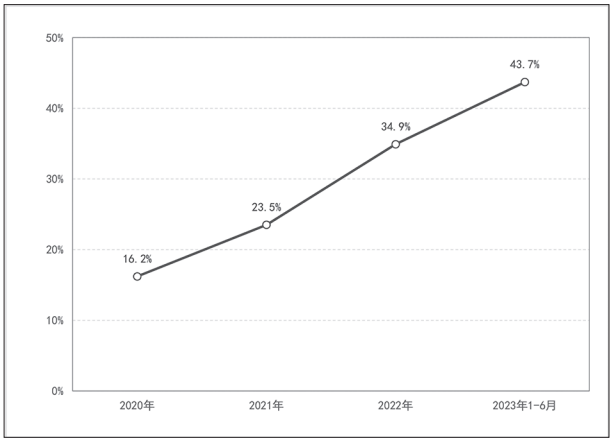
王辰，高级工程师，硕士研究生，从事智能网联汽车标准研究。

0 引言

发展新质生产力的关键之一在于实现科技创新，数据作为新型生产要素，既是劳动对象也是劳动资料，是信息和数字经济的主要承载体，成为承载信息化、数字化、智能化领域的不同创新要素的关键“物的”支撑，与新质生产力密切相关[1]。在世界各国探索自动驾驶汽车发展模式的过程中，我国提出了“车路云”一体化的智能网联汽车“中国方案”[2]，通过利用算法和传感器等软硬件架构持续采集驾驶状态相关数据，通过车端、路侧和云端的互联互通，提升智能网联汽车的驾驶安全性与智能性。但这种技术路线使得数据采集的种类与数量同时增加，带来了更大的数据安全风险，加剧了智能网联汽车数据安全的保障难度。智能网联汽车产业作为数字经济与实体经济融合的代表，数据的收集与分析能够成为新质生产力的重要动力源泉，能够推动数据要素市场发展。建立智能网联汽车数据安全标准体系，能够推动智能网联汽车产业打造安全高效、合规繁荣的数据生态，推动发展新质生产力。本文将探讨智能网联汽车数据安全管理的现实困境，对现有智能网联汽车数据安全保障制度进行审慎反思，以构建数据安全标准体系为改进抓手，实现助推产业新质生产力发展。

1 困境：产品将入市而规范待明确

2023年11月工业和信息化部等四部门印发《关于开展智能网联汽车准入和上路通行试点工作的通知》（后称《准入通知》）后，于2024年6月公布了首批9个进入试点的联合体名单，将进一步遴选具备量产条件的智能网联汽车产品，推进准入试点工作。随着驾驶辅助技术逐步成熟、成本持续降低，以及消费者接受度不断提升，车企正在加快L2级组合驾驶辅助功能的前装导入，中国市场乘用车新车L2级功能渗透率逐步提升。2023年1–6月，中国L2级乘用车渗透率已达到43.7%，如图1所示。



（来源：中国智能网联汽车产业创新联盟）

图1 中国乘用车市场新车L2级渗透率变化趋势

在《准入通知》中，要求试点汽车生产企业或使用主体履行数据安全保护义务，落实数据安全主体责任，通过健全数据安全管理制度、建立数据资产管理台账、采取技术措施等，确保车辆运行安全①。围绕智能网联汽车数据安全，2021年9月，国家互联网信息办公室、发改委、国家发展和改革委员会、公安部、交通运输部联合发布了《汽车数据安全管理若干规定（试行）》（后称《汽车数据规定》），明确了“汽车数据”“汽车数据处理”“敏感个人信息”“重要数据”等概念的范围与定义，制定了汽车数据处理的基本要求和安全原则，并进一步规范了个人信息、敏感个人信息和重要数据的处理方法②。同月，工业和信息化部发布《关于加强车联网网络安全和数据安全工作的通知》，强调汽车数据有效保护和合法利用，实施数据分类分级管理，提升数据安全技术保障能力，规范数据开发利用和共享使用。2022年2月工业和信息化部发布《车联网网络安全和数据安全标准体系建设

注：① 工业和信息化部、公安部、住房和城乡建设部、交通运输部《关于开展智能网联汽车准入和上路通行试点工作的通知》（工信部联通装〔2023〕217号），附件1中《智能网联汽车准入和上路通行试点实施指南（试行）》有关内容。

② 参见《汽车数据安全管理若干规定（试行）》第三条相关定义，汽车数据处理的基本要求和安全原则参见第四条至第六条，个人信息处理方法参见第七条、第八条，敏感信息个人处理方法参见第九条，重要数据处理方法参见第十条至第十四条。

指南》，在数据安全部分，提出研制通用要求、分类分级、出境安全、个人信息保护、应用数据安全5类标准，规范智能网联汽车、车联网平台、车载应用服务等数据安全和个人信息保护要求。2023年7月，工业和信息化部、国家标准化管理委员会印发《国家车联网产业标准体系建设指南（智能网联汽车）（2023版）》（后称《标准体系建设指南》），将智能网联汽车标准体系划分为“三横两纵”核心技术架构，如图2所示③。《标准体系建设指南》中将智能网联汽车数据安全划到两纵结构中，意味着数据安全不仅要承载与三横结构的交互，还要实现对基础设施、移动终端、智慧城市、出行服务的建设支撑。《标准体系建设指南》强调数据的“保护—利用—安全”，即智能网联汽车数据安全标准要确保智能网联汽车数据处于有效保护和合法利用的状态中，并具备保障持续安全状态的能力。

智能网联汽车存在多层次、多类型的数据安全风险，具体而言可分为对国家安全的影响、对驾驶安全的影响以及用户的隐私安全[3]。智能网联汽车面临的数据安全风险不同于手机、电脑等传统智能设备范围局限于使用者个人和周边有限空间，而是对社会生活各个层面存在普遍渗透，导致数据安全风险突破了对个人的影响并延伸到公共安全甚至国家安全范围中[4]。由此可见，智能网联汽车产品在进入市场的过程中，即使政策规范持续出台，但对比产业的大规模商业化进程，有关智能网联汽车数据安全仍缺少明确、可量化参照的规范体系。

2 成因：规范与产业发展黏性不强

在数字经济社会中，想要对技术进行规制，如果只从政策视角进行讨论，哪怕制定了相关法律，

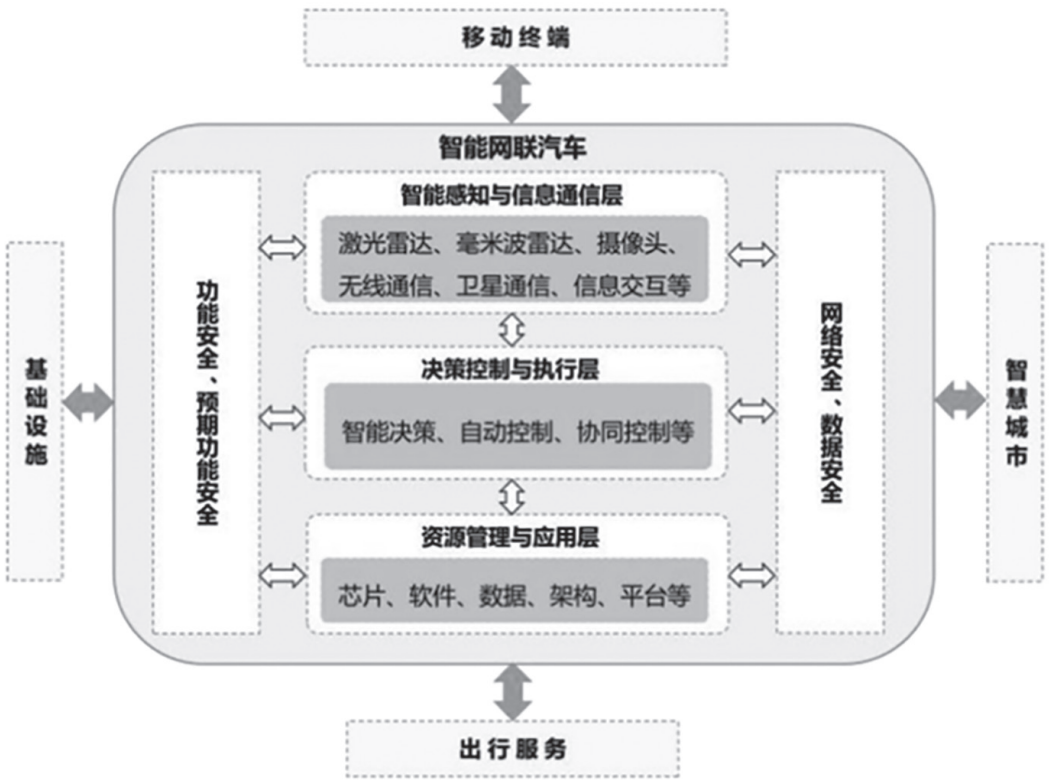


图2 智能网联汽车标准体系技术逻辑框架

注：③ 图源工业和信息化部、国家标准化管理委员会《关于印发〈国家车联网产业标准体系建设指南（智能网联汽车）（2023版）〉的通知》（工信部联科〔2023〕109号），第3页。

可能也没有办法达到实际规制效果；只站在技术视角讨论，随技术发展不断制定更新法律，那法律本身的权威性将荡然无存。技术与制度是新兴产业发展的两个重要驱动力，但主流经济理论尚未完全兼容对二者的分析。协同演化理论不同于主流经济理论和传统创新理论，它将技术和制度视为内生变量，二者互为选择、相互影响，共同推动产业发展[5]。智能网联汽车是科技产物，带有全球化属性，但不同国家和地区有不同的管理政策及侧重，因此形成的法规和标准存在显著的差异[6]。这种差异导致汽车制造商和相关企业需要在全球范围内遵守不同的法规和标准，增加了智能网联汽车数据合规的复杂性和成本。同时，区域化的法规和标准对于数据处理、保护和安全要求不尽相同，需要企业在不同地区采取不同的安全措施，增加了技术实施的难度，限制了智能网联汽车数据的流通，影响了智能网联汽车数据的共享和利用。

2.1 数据权益未明确

数据催生新的产品和服务，对传统产业实现数据赋能，推动社会的进一步发展[7]。当下对于数据权利的讨论仍未停止，一方面，数据要素已经成为国民经济重要组成部分，随着技术加速迭代，本就复杂多元的社会问题越来越多地出现不稳定性、不确定性、高度复杂性和模糊性，使社会在形态转型和发展过程中需面临一系列潜在安全风险[8]。另一方面，由于数据要素不断渗透了公共治理、经济运行、公共服务和社会治理多个领域，这使数据要素风险呈现出复杂性、系统性、隐蔽性和不确定性的显著特点[9]。由于数据的流动性、可分割性以及独立确权性，数据立法具有独立性，这些特征为现有法律规则在技术问题上的应用带来了新的挑战。在学界讨论之中，数据本身的经济属性在很大程度上得到了多方认可，但脱离“数据+载体”谈数据安全建设，不仅会导致监管针对性减弱，还会导致实践中落地应用难度加大。

对智能网联汽车企业而言，为了确保汽车的安全运行和维护，相关企业都在积极生成并收集相关数据，对智能网联汽车数据的生成、收集和利用是维护企业商业模式和发展的核心[10]。但目前智能网联汽车数据安全相关要求持续提高的同时，叠加数据确权难以确定的影响，使得智能网联汽车数据安全成本增大却缺少可预期的收益，直接影响了智能网联汽车数据安全建设动力。

2.2 针对性规范缺少

通过对国家标准的梳理，主要发现有两个问题。一是汽车、交通、地理信息、产品缺陷与安全管理标委会现行的智能网联汽车数据安全相关标准均在2023年前发布，见表1，而全国网络安全标准化技术委员会（TC 260）制定的数据安全相关标准，下达立项时间多在2023年后。2024年获准发布的两项智能网联汽车相关强制性标准于2026年1月1日起实施，另有3项相关国家推荐性标准发布，一方面企业需要与标准磨合的时间，另一方面仍需对标在研标准，可能出现较长时间现行标准衔接不足的情况。

二是数据安全标准有待体系化，比起智能网联汽车数据安全相关标准的针对性而言，TC260涉及的数据安全标准在宏观层面更为完善，见表2。智能网联汽车数据安全标准，在关注领域特性的同时，一方面需要强相关、可执行的相关法规标准，另一方面也需要产业内可供宏观指引的标准。④数据安全标准的不完善，制约了智能网联汽车产业的健康发展，也为未来的市场扩展带来了潜在的风险。

即使如：《准入通知》和《汽车数据规定》等文件对智能网联汽车数据安全提出了基本要求和安全原则，并对汽车数据的分类、分级、处理方式等做出了初步界定，但与智能网联汽车产业的大规模商业化进程相比，现有的规范体系仍显不足。智能网联汽车数据涉及驾驶环境、驾驶功能和用户隐

注：④ 参见20240401-T-469《〈数据安全技术 数据安全和个人信息保护社会责任指南〉（征求意见稿）》编制说明中，标准编制原则和确定主要内容的论据及解决的主要问题。

表1 智能网联汽车数据安全相关国家标准

序号	标准名称	标准号/计划号	下达/发布时间	标准状态	标委会
1	智能网联汽车 自动驾驶数据记录系统	GB 44497–2024	2024–08–23	发布	TC114
2	汽车整车信息安全技术要求	GB 44495–2024	2024–08–23	发布	
3	汽车诊断接口信息安全技术要求及试验方法	GB/T 44778–2024	2024–10–26	发布	
4	汽车信息安全应急响应管理规范	GB/T 44774–2024	2024–10–26	发布	
5	汽车数据通用要求 （标准曾用名：智能网联汽车 数据通用要求）	GB/T 44464–2024	2024–08–23	发布	
6	道路车辆 自动驾驶传感器与数据融合单元间数据通信 逻辑接口	20231590–T–339	2023–12–01	征求意见	
7	智能网联汽车数字身份及认证通用规范	20221429–T–312	2022–12–13	报批	TC576
8	道路交通管理车路协同系统信息交互接口规范	20221430–T–312	2022–12–13	报批	
9	智能网联汽车时空数据传感系统安全检测基本要求	20230947–Q–334	2023–08–22	征求意见	TC230
10	智能网联汽车时空数据安全处理基本要求	20230949–Q–334	2023–08–22	征求意见	
11	汽车产品召回 信息缺陷评估指南	20213424–T–469	2021–08–24	征求意见	TC463

（来源：全国标准信息公共服务平台）

表2 数据安全相关国家标准（TC 260）

序号	标准名称	标准号/计划号	发布/下达时间
1	数据安全技术 数据分类分级规则	GB/T 43697–2024	2024–03–15
2	数据安全技术 个人信息转移技术要求	20242027–T–469	2024–06–28
3	数据安全技术 个人信息保护合规审计要求	20240896–T–469	2024–04–25
4	数据安全技术 数据接口安全风险监测方法	20240331–T–469	2024–03–25
5	数据安全技术 数据安全和个人信息保护社会责任指南	20240401–T–469	2024–03–25
6	数据安全技术 数据安全保护要求	20240405–T–469	2024–03–25
7	数据安全技术 大型互联网企业内设个人信息保护监督机构要求	20230793–T–469	2023–08–06
8	数据安全技术 个人信息跨境处理活动安全认证要求	20230255–T–469	2023–03–21
9	数据安全技术 政务数据处理安全要求	20230247–T–469	2023–03–21
10	数据安全技术 数据安全风险评估方法	20230257–T–469	2023–03–21
11	数据安全技术 敏感个人信息处理安全要求	20230254–T–469	2023–03–21
12	数据安全技术 数据安全评估机构能力要求	20230256–T–469	2023–03–21

（来源：全国标准信息公共服务平台）

私等多层次、多类型的风险，这些风险超出了传统智能设备的范畴，不仅影响到消费者个人，还可能对公共安全和国家安全造成威胁。然而，现阶段的法规对于如何量化和评估这些风险、如何确保数据处理的安全合规方面，缺乏详细且可操作的规范。结合政策、法律法规、标准现状，虽然道路交通安全、数据安全等与智能网联汽车有关的法规监管正在搭建，但是在高强制性、指引性标准缺少的情况下，传统规制模式仍然难以打破局限性。

2.3 动态防护难形成

智能网联汽车企业多是根据自身业务的不同需求对数据进行分级，制定相应的数据保护要求和策略，导致数据分类分级的差异化，这种差异也意味着现有数据分类分级规则存在适用不匹配[11]。一方面，智能网联汽车产业催生了新技术、新产品、新服务，随之而来的也是越来越大的风险暴露面。作为监管关注的重点领域，智能网联汽车需要处理大量实时性、稳定性、安全性等方面的技术问题，传统的网络安全和个人信息保护法律框架并未充分考虑到这些特性，导致现有法规难以在技术层面提供具体指导，阻碍了智能网联汽车数据安全标准体系的形成，滋生了产业发展隐患[12]。另一方面，智能网联汽车的数据生命周期更为复杂，包括数据采集、传输、存储、处理等多个环节，由于缺乏专门针对智能网联汽车数据安全的标准和规范体系，容易出现数据安全漏洞。单项标准法规的内

容需要更强的针对性，体系的迟缓形成导致问题的片面、单一，始终无法形成动态安全保护体系。

在智能化、网联化的趋势下，汽车、通信、交通等产业正加速融合，在我国车路云一体化产业发展的背景下，智能网联汽车数据也出现爆发式增长。“驾驶”这一行为的动态性决定了智能网联汽车数据安全不是静态恒定的防护，而是要做到全周期的动态防护，使各项数据有对应规范进行保护。这一趋势下，车路云一体化数据安全成为国家战略安全的不可或缺的组成部分，智能网联汽车数据安全问题也映射了我国正面临的数据要素治理挑战。

3 对策：由点及面形成体系化治理

随着与智能网联汽车数据相关政策文件的陆续出台，尤其《准入通知》所提出的更高的数据安全要求更是将数据安全与产品合格评价进行关联，使智能网联汽车数据安全的重要性不断提升。而车路云一体化产业的发展涉及多个环节，集成了大量涉及安全的敏感信息和重要数据，关系到国家安全、经济发展、社会稳定和公众利益，相关数据要素也成为了我国重要的战略资产之一。因此，亟须避免随着智能网联汽车技术的不断发展和市场渗透率的快速提升，现有法规和标准与产业发展管理缺口的持续拉大。为保障数据安全，促进数据的共享和利用，亟须构建“技术—制度”协同的智能网联汽车数据安全保障体系。

3.1 体系构建逻辑：自下而上

面临技术、产业发展的多元现实需求，伴随着数据权利化、制度化发展，顺应智能网联汽车产业发展趋势，解决智能网联汽车数据安全问题迫在眉睫[13]。智能网联汽车领域作为集成科技领域的代表，所涉及的数据处理和传输技术相较传统模式更为复杂，引发的法律困境远大于其他技术领域[14]。智能网联汽车数据要跨领域、跨地域、跨系统等进行流通，基于信息流动性的本质，对相关场景难以进行有效规制[15]。但智能网联汽车企业数据面临的阿罗信息悖论，将直接影响数据的流动性，弱化智能网联汽车数据的价值。

将数据进行封闭，会对数字经济发展造成不良影响。首先，当企业放弃从数据中获取衍生价值，对其作出数据合规与否的评价将不再重要。抑或，当企业放弃数据的可交易性，其数据本身流动风险将极大降低，合规评估带有的“比较”或“激励”目的与企业保守选择的底线安全将断开联系，面对不需要被评价价值的智能网联汽车数据，也将不存在合规评价的价值。其次，智能网联汽车产业发展面临多方面的挑战，与之相关的数据处理和传输是一个复杂的技术体系，现有的法规难以充分满足智能网联汽车系统对实时性、稳定性等方面的特殊需求，需要企业通过技术实现数据合规。依托于企业技术革新，智能网联汽车技术才得以丰富和发展，由于不同企业的技术能力和技术路线不同，企业对智能网联汽车数据的封闭，也不利于形成行业数据合规的共识。最后，智能网联汽车数据一旦封闭，也是企业社会责任消极不承担的体现[16]。一方面，封闭行为将导致用户在数据处理中的权益难以得到妥善保护，如：智能网联汽车企业在利用平台经济进行发展时，通过隐私协议作为权利清单，形式上作出了合规行为，却未能充分保护用户的隐私权益。另一方面，一旦仅保证数据的底线安全、保持数据处于消极不获益状态，企业在数据安全板块的投入的实际情况便难以得知，有出现数据安全保护惰性的风险，降低企业合规动力，无法推动智能网联汽车数据合规路径的形成。

随着《数据安全法》《个人信息保护法》的出台，业已确定数据分类分级保护理念和现状，需进一步对数据类型进行区分化和精细化保护、适配不同数据类型的利益平衡理念和社会积极效应。数据安全工作需要涵盖数据的采集、传输、存储、使用、分享以及销毁等各个阶段，需要根据数据分类分级结果制定相应等级的安全管理要求，并执行相应的安全治理策略，以确保智能网联汽车数据在全生命周期内得到安全合理的应用，对于涉及国家安全、国民经济核心、重要民生和重大公共利益的关键数据，以及包含个人敏感信息的数据，

应当实施更加严格的管理制度。数据分类分级工作为确定相关主体的数据使用权限和安全治理义务提供了依据，通过明确数据安全治理的底线，划定数据流转范围并设定各主体的数据使用权限，支持相关机构对智能网联汽车数据的有效访问和安全使用。至此，自下而上形成的智能网联汽车数据安全标准体系，将切实保障数据安全工作的规范化，最大程度地释放数据资产的价值，从而提高数据业务的运营效率。

3.2 体系构建关键：多维协同

技术中立表现出技术在进入社会时的独立状态，而在当今道德分歧和社会合作压力下，法律应通过融入科技重构模式来回应技术发展，现代社会因科技进步受益良多，但也面临更多由此引发的复杂难题[17]。因技术发展程度与智能网联汽车的行驶安全关系密切，为确保车辆在各种情况下的稳定运行，智能网联汽车领域技术标准需求数量、领域范围庞大，导致了技术标准碎片化。这种碎片化增加了不同智能网联汽车系统之间、同类技术不同企业之间的兼容性难题。由于标准涉及智能网联汽车技术的方方面面，碎片化的标准难以促进技术实现互联互通，导致汽车产品在技术实现上存在显著差异，增加了企业为实现产品全球化的研发生产难度。

就数据相关法规而言，不同国家和地区对于个人信息和数据安全的关注点不同导致规定有所不同，或侧重个人隐私保护，或强调数据安全性，法规制定更偏向考虑本国实际。针对智能网联汽车数据，不同国家和地区在车辆行驶状态、用户行为收集、信息获取授权、数据加密和脱敏、跨境传输和共享等方面，规定的严格程度和限制程度也不同，使得汽车制造商的同一产品在全球范围内要遵守多个不同的法规要求。同时，区域化的法规也会限制智能网联汽车数据的流动，影响整车企业、解决方案公司、零部件企业在全球范围内实现数据的高效共享和利用，对技术创新和行业发展造成阻碍。此外，设立承担特别经济功能的特殊经济区域、实施有别于其他区域的经济体制改革的诸项政策措施，是我国实现先行先试保障社会稳定发展的重要举措[18]。就我国实际而言，由于智能网联汽车目前处于由在各个示范区测试验证转为准入通行试点阶段，遵守的是各地区制定的有关规范，考虑各地实际与行政分工，出现了立法主体多元的情况，更倾向于考虑本地区利益，而非考虑协同其他地区的经济发展，甚至在特殊情况“以邻为壑”，导致规范协同面临困境[19]。

如图3《标准体系建设指南》中智能网联汽车标准体系框架所示，不同技术领域之间需要有效协同才能保障智能网联汽车标准体系的科学性、应用性。对智能网联汽车数据安全而言，同标准板块下网络安全对于数据安全的要求，以及跨一级板块中功能安全、预期功能安全、驾驶交互、座舱交互中对于数据安全的要求，一方面与数据安全标准自身的要求间也可能存在差异，另一方面不同板块标准采取的技术方法也将增加标准协调的难度。这种异构性使得智能网联汽车数据安全贯穿其研发、生产、应用全生命周期面临困境，有必要促进跨领域标准制修订的协调和合作，推动标准制定主体之间的信息交流与互通，以便搭建共同的标准制修订基础并有利于补充和调整，才能降低标准碎片化所带来的技术和管理难题[20]。

3.3 体系构建效果：动态治理

未来智能网联汽车将成为世界各国集成科技、尖端科技的“演武场”，智能网联汽车产业发展也将成为激发制造业市场主体活力，发展数字经济的动力之源。在数据安全层面，我国先后出台并实施了《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》及相关规范性文件，明确了数据安全保障范围和管理原则，为配套标准规范制定和安全保障工作开展提供了重要指导。2024年1月15日印发的《关于开展智能网联汽车“车路云一体化”应用试点工作的通知》中明确，为探索数据收益新模式新业态，鼓励数据要素流通与数据应用，推进跨地区数据共建共享共用的发展方向，由此，对数据的规制不仅涉及安全和价值的双重属性，还应关注数据安全建设实效。

智能网联汽车数据安全问题，本质也是“技

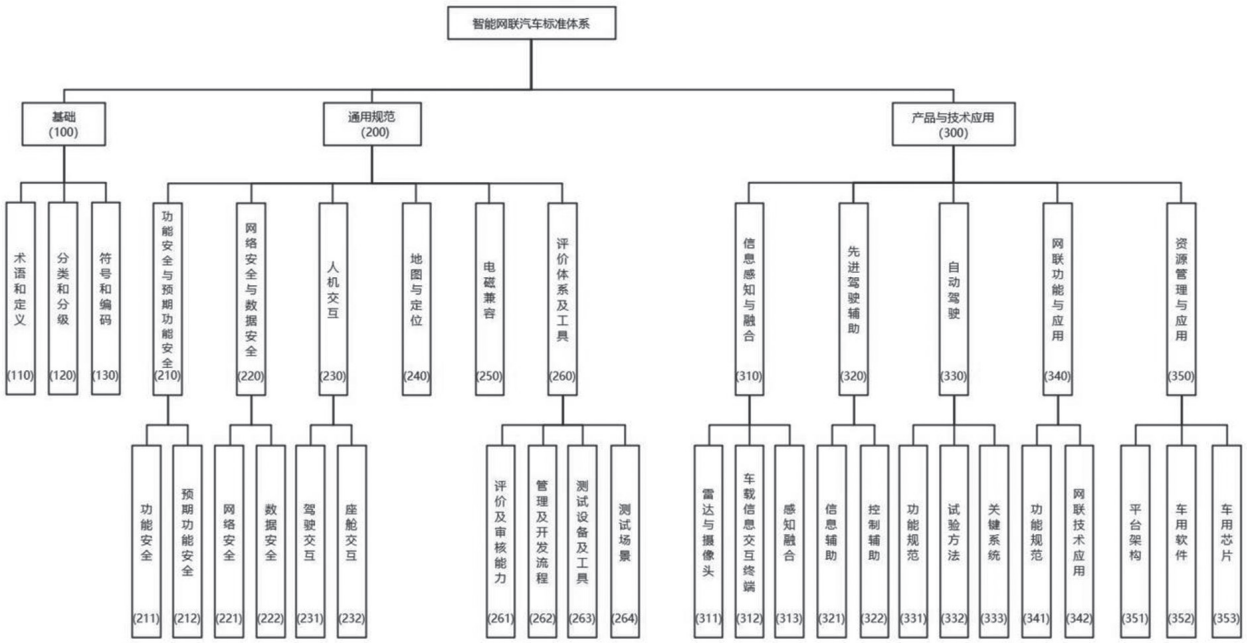


图3 智能网联汽车标准体系框架图

术—制度”协同的问题，转化到实践维度，一方面要思考“规范”如何“落地”，另一方面要强化“法律”与“标准”的关联，才能保证智能网联汽车数据管理的安全性、合规性，从而带来收益。[21]数据是科技产业重要竞争力之一，也是法律保护的重要对象之一，智能网联汽车作为技术集成领域的代表，所涉技术子领域的监管也面临同样的合规困境，其产品本身的特殊性与数据的流动性也对监管提出了更高要求。因此，一方面可以进一步明确各部门对于智能网联汽车数据安全的管理职能，解决智能网联汽车数据管理重叠问题及漏洞。另一方面，由于地域差异，监管机构和执法部门在不同地区可能有不同的合规监管要求和执法力度，为确保符合当地法规要求，企业需要根据具体地区的监管环境进行调整，增加了企业合规监管的复杂性。监管机构在制定法规时可能受限于技术理解和法规更新的速度，导致法规缺乏对智能网联汽车独特挑战的全面考虑，从而阻碍了合规机制的顺利实施。

智能网联汽车数据安全标准体系能够最大化实现动态治理效果，通过充分考虑智能网联汽车数据特性，确保标准体系建设兼顾精准度与覆盖面，以应对智能网联汽车面临的安全挑战。也即，在智能网联汽车数据安全标准体系中不仅针对网联汽车的评估要点，包括但不限于车辆通信安全、远程控制风险、车辆软硬件集成安全等技术重点，还可以设置涵盖数据全生命周期的指引性规范，形成可动态适应需求的评估机制以防范风险。

4 结 语

智能网联汽车产业作为数字经济的重要组成部分，依赖数据驱动其技术进步与市场扩展，数据安全也是保障本产业技术创新和法律规范有机结合的关键挑战。为了有效应对数据安全风险，科学实现智能网联汽车数据安全的动态治理，有必要构建数据安全标准体系，智能网联汽车数据的全方位、多维度管理，实现制度建设和监管手段双优化。通过完善和落实智能网联汽车数据安全标准体系，能够确保技术创新与法律规范在安全的前提下共同推进，促进产业健康高效发展，发展智能网联汽车产业的新质生产力。

参考文献

[1] 杨国强,许明月. 新质生产力生成中数据要素交易监管的完善进路[J]. 湖北大学学报(哲学社会科学版), 2024,51(03):125–136.

[2] 李克强. “中国方案” 智能网联汽车发展思路[J]. 智能网联汽车, 2020(03):44–47.

[3] 李强,王文强. 智能网联汽车及其数据安全问题探析[J]. 中国安防, 2021(12):44–47.

[4] 赵舒捷. 智能网联汽车数据安全的风险、冲突与规制：基于总体国家安全观的规范建构[J]. 数字法治, 2023(04):81–95.

[5] 眭纪刚,陈芳. 新兴产业技术与制度的协同演化[J]. 科学学研究, 2016,34(02):186–193.

[6] 刘云甫,朱最新. 多维视角下区域行政协议法治化研究[J]. 法治社会, 2020(05):36–44.

[7] 张永忠,张宝山. 构建数据要素市场背景下数据确权与制度回应[J]. 上海政法学院学报(法治论丛), 2022,37(04):105–124.

[8] 李梅,汤志伟. 中国智慧社会建设的风险表现、分析及防范研究[J]. 电子政务, 2019(04):27–34.

[9] 姚洪,徐晓林,毛子骏. 从能源要素到数据要素：关键生产要素变革中的安全风险对比及治理对策研究[J/OL]. 海南大学学报(人文社会科学版),1–10. [2024–08–12].https://doi.org/10.15886/j.cnki.hnus.202306.0072.

[10] 付新华. 企业数据财产权保护论批判——从数据财产权到数据使用权[J]. 东方法学, 2022(02):132–143.

[11] 付新华. 论智能网联汽车数据的治理之道[J]. 法制与社会发展, 2024,30(01):147–163.

[12] 李若兰. 数据安全和产业发展双重视角下的自动驾驶数据规制[J]. 行政管理改革, 2021(08):79–85.

[13] 丁钰. 涉智能网联汽车数据的标准与法律规制困境[J]. 标准科学, 2023(09):24–29.

[14] 陈亮,张翔. 人工智能立法背景下人工智能的法律定义[J]. 云南社会科学, 2023(05):162–170.

[15] 赵正,郭明军,马骁,等. 数据流通情景下数据要素治理体系及配套制度研究[J]. 电子政务, 2022(02):40–49.

[16] 李玉华,冯泳琦. 数据合规的基本问题[J]. 青少年犯罪问题, 2021(03):4–16.

[17] 郑玉双. 破解技术中立难题——法律与科技之关系的法理学再思[J]. 华东政法大学学报, 2018,21(01):85–97.

[18] 叶姗. 特定区域的特制税法规范何以续造[J]. 政法论丛, 2022(03):87–97.

[19] 黄兰松. 区域协同立法的实践路径与规范建构[J]. 地方立法研究, 2023,8(02):18–38.

[20] 陈兵,胡珍. 数字经济下统筹数据安全与发展的法治路径[J]. 长白学刊, 2021(05):84–93.

[21] 朱家豪. 智能网联汽车的法律规制结构研究[J]. 北京科技大学学报(社会科学版), 2023,39(05):634–644.