社会科学进展
2025 年 11 月第 7 卷第 11 期

智能网联汽车数据安全法律规制研究

——基于数据权益配置与分类分级的双重路径

李子涵　韩姿洁

上海政法学院，上海

摘　要 | 近年来，国内外相关立法及典型数据泄露事件揭示了智能网联汽车数据在种类复杂性、系统易受攻击性、全流程泄露风险及网络入侵威胁等方面的特征。我国当前法律规制体系存在重要数据权责归属模糊、分类分级管理制度不健全等问题，导致企业监管低效、数据利用与安全平衡困难。基于此，本文提出两项建议：一是确立智能网联汽车重要数据的权利归属，明确汽车企业享有受益权并承担核心保护义务；二是构建可操作的智能网联汽车数据分类分级规则体系，根据不同级别数据实施差异化保护策略，并严格限制敏感数据跨境传输。完善数据权益配置与落实分类分级是保障智能网联汽车重要数据安全、平衡发展与安全的关键法律措施，对于推动智能网联汽车数据安全发展具有重要意义。

关键词 | 智能网联汽车；数据安全；权责划分；分类分级保护

1　智能网联汽车数据安全立法现状及潜在风险

1.1　智能网联汽车数据安全立法现状

智能网联汽车的数据安全主要指数据采集、传输、开发利用、存储、删除、备份与恢复等数据处理过程安全，同时也包括涉及用户身份与行为、车辆运行状态、周围环境等数据信息安全。[1] 2016至2020年间，针对智能汽车的信息安全事件报告数量呈现急剧攀升趋势，增幅高达605%。其中，专门针对智能网联车辆信息系统的恶意攻击事件累计发生155起。[2] 丰田公司于近年确认其网络系统遭到黑客攻击，约240GB的敏感数据被泄露到黑客论坛。该事件由Zero Seven Group黑客组织发起，其声称成功入侵了丰田美国的一个分支机构，窃取了大量涉及员工、客户、财务及网络基础设施的信息。[3] 近年来，包括宝马、大众、通用、蔚来等在内的知名车企，因遭遇内部人员泄密、勒索软件入侵、邮件钓鱼、漏洞利用等攻击，均发生过影响广泛的数据泄露事件。

在智能网联汽车领域，全球范围内对数据安全的立法与监管均表现出高度关注。早在2016年，美国便率先颁布《联邦自动驾驶政策》，该文件确立了包含数据记录要求、共享机制以及车辆安全保障在内的15项关

通讯作者：李子涵，上海政法学院法律学院研究生，研究方向：民商法学。
文章引用：李子涵，韩姿洁．智能网联汽车数据安全法律规制研究——基于数据权益配置与分类分级的双重路径［J］．社会科学进展，2025，7（11）：888-892.
https://doi.org/10.35534/pss.0711151

键评估标准。我国则在《网络安全法》《数据安全法》及《个人信息保护法》构成的基础法律框架下，系统性地制定了多项涉及智能网联汽车数据安全的规范文件，如《汽车数据安全管理若干规定（试行）》（以下简称《规定》）以及旨在确立准入机制与规范道路测试的试点工作通知。[4] 此外，相关行业标准也陆续出台。这些法律、法规、部门规章及规范性文件共同构建起规制体系，明确要求相关义务主体切实承担数据安全保护责任，并倡导在数据处理活动中遵循必要性原则，避免过度收集和不当使用汽车数据。

《规定》中关于“汽车数据”的定义，也引发了关于数据、重要数据与个人信息三者关系的讨论。首先可以明确的是，《数据安全法》等上位法相关规定没有将个人信息排除出数据或者重要数据的范畴；而《规定》则通过“汽车数据”的概念定义进一步确认了个人信息应归属于特殊类型的数据。值得关注的是，《规定》第三条第六款还确立了转化规则，即当所涉个人信息的体量超过法定阈值（如涉及10万以上个人信息主体）时，该类信息将构成法定意义上的重要数据。

基于上述认识，相关主管部门通过《规定》进一步澄清了由来已久的“重要数据不包含个人信息”的争议或误解。2019年公布的《数据安全管理办法（征求意见稿）》第三十八条第五项中对“重要数据”进行了定义，其中规定“重要数据一般不包括企业生产经营和内部管理信息、个人信息等。”但联系该条规定的具体语义环境，对照此次《规定》中对于“个人信息数据”的提法不难发现，所谓“不包括个人信息”应解释为不包含企业生产经营和内部的个人信息。换言之，如果汽车企业在开展生产和经营活动过程中处理达到一定量级的客户或者消费者的个人信息，不排除被认定为重要数据的处理行为。对这一关键概念与法律关系的厘清，也体现了此次《规定》出台的重要价值和意义。

1.2 智能网联汽车数据安全存在的挑战

（1）数据种类的繁多

智能网联汽车涉及的数据，遍布于从设计生产到使用过程的各个环节，既包括车辆本身配置和产生的数据，也包括用户端即个人的人脸、声音、图像视频等隐私信息，还包括车企的设计制造、销售、服务相关数据。数据的类型复杂多样，对数据资产梳理、分类分级管理、数据流通过程跟踪管控都是不小的挑战。

（2）系统成为易受攻击的潜在目标

智能网联汽车的软件系统比传统车辆复杂得多，涉及感知、决策、控制等多个模块，每个模块都依赖复杂的算法和大量的数据处理。近年，多个汽车品牌的自动驾驶系统和联网功能被曝出存在不同程度的安全漏洞，导致系统本身成为易受攻击的潜在目标。[5] 如DDoS攻击通过大量虚假请求使车辆的计算系统超载，从而造成系统崩溃，通过Wi-Fi、蓝牙等无线通信系统对车辆进行远程入侵可获取系统控制权，通过篡改传感器数据或导航信息能够误导自动驾驶系统做出错误的驾驶决策。

（3）各个环节中存在泄露风险

在智能网联汽车持续运行状态下，其传感器系统会对周边道路环境、地理坐标等要素进行持续性采集与存储。若其中包含的高精度地理空间数据、实时驾驶行为记录等核心信息被非法获取，经由技术手段整合分析后可能引发系统性风险。尤其当涉及军事管制区域、关键电力设施、战略港口等敏感位置的测绘信息时，此类数据的非法利用极可能突破国家秘密保护边界，最终对国家经济命脉与核心安全利益构成实质性威胁。[6] 除了道路安全基础设施及关键地理坐标信息面临泄露隐患外，汽车数据在其生成、收集、流转与存储的全生命周期中牵涉产业链多环节参与主体。上下游企业均需依赖此类数据资源实现技术迭代升级与产品性能优化，而第三方环节的数据交互行为正构成信息安全威胁的关键风险源。同时，交易端为用户提供个性化配置和服务的营销、运营、用户隐私数据被大量交换共享，相关员工因安全意识薄弱造成的权限滥用和操作失误，也是导致数据泄露的重要原因。

（4）重要数据面临网络入侵威胁

在总体国家安全框架涵盖的多维度安全体系中，网络、数据及信息资源已深度融入政治安全、国土安全、军事安全等核心领域，并强化了各领域间的渗透性关联。随着技术迭代加速，数据安全保障已上升为网络空间治理的关键组成部分，特别是重要数据中蕴含的国家政治决策、经济运行态势、军事部署等敏感信息，可能被外部势力系统化解码。[7] 当前我国在重要数据防护领域仍存在能力短板，针对网络非法侵入、恶意代码攻击等新型安全威胁，尚未建立完备的法律保障体系。[8] 以2015年披露的宝马Connected Drive服务安全缺陷为例，攻击者通过逆向工程车辆控制指令协议，成功获取了远程操控车载系统的权限。此类技术漏洞若被非授权个体恶意利用，可能引发大规模交通系统瘫痪等公共安全危机，直接威胁国家安全体系。

2 我国智能网联汽车数据安全保护存在的问题

2.1 重要数据的权责规定不明确

当前，数据权属确认问题在学界存在显著争议，其中智能网联汽车企业重要数据所有权的界定尤为复杂。在汽车数据治理领域，明确数据权属具有基础性意义，它是实施数据分类分级的先决条件，更是构建涵盖信息采集规范、数据开放共享、促进交易流通、强化安全保护等全环节治理体系不可或缺的前提。[9] 当前在实务中，汽车制造企业依托其专属服务器平台对智能网联车辆数据实施排他性管控，实质削弱了终端用户与第三方

https://doi.org/10.35534/pss.0711151

服务机构等主体的合法数据权益，妨碍了智能网联汽车数据的高效公平流转与利用。这种现象本质上指向汽车数据财产性权利的归属争议。相关数据权益的配置框架不仅决定着数据安全治理与利用目标的实现，更涉及私人利益与公共利益的合理平衡。

特别就汽车企业掌控的重要数据而言，其收集存储依托于车辆自身，后续控制与分析行为则由企业主导。审视现行法律框架，企业在重要数据全生命周期治理中的具体义务与安全责任边界尚存模糊地带，特别是权责配置存在系统性缺失，此种制度缺失为汽车数据安全治理带来了严峻挑战。法律界定不明直接导致企业在合规监管领域的动力不足，相关安全保障技术升级受限，对国家层面的数据安全构成现实威胁，亦为重要数据的安全治理增添了实际障碍。

2.2 数据分类分级管理制度不健全

数据安全治理的初始环节在于建立基于数据类型与风险等级的分级管理体系，以此界定数据流通边界并配置差异化的监管强度。《数据安全法》第二十一条明确要求构建数据分类分级保护制度，确立层级化防护的法定框架。2024年实施的GB/T 43697–2024《数据安全技术 数据分类级规则》[10]系统性规定了数据分类分级的基本原则、实施框架、操作方法及实施流程，其规范性附录G《重要数据识别指南》为核心数据识别提供了标准化依据。尽管该标准为数据分类分级管理提供了基本的操作指南，但在智能网联汽车领域，现行部门规章尚未对以下关键问题作出回应：分类分级具体规则缺位，缺乏针对车路云一体化数据特征的专项分级标准（如军事管理区地理信息的4级防护要求）；企业权责配置真空，未明确车企在数据资产盘点、分级标识、访问控制等环节的作用和角色；制度落地机制模糊，如何将《规定》第八条的“精度范围适用原则”转化为车企可执行的分级操作流程仍存实践障碍。[11]

2025年1月6日，安华金和与Smart携手发布《智能网联汽车数据分类分级白皮书》（以下简称“《白皮书》”），结合了数据的特性和用途，从企业管理的视角对数据进行分类，分为对内经营管理数据和对外业务数据。经营管理数据细分为战略策划数据、人力资源数据、财务管理数据、法律合规数据[12]、数字化运行数据、行政管理数据等六个大类；业务数据依据“研、产、销”一体化结构分为：研发数据、生产数据、营销管理数据、客户个人信息、车联网客户数据、车联网数据、维保售后数据、客户维保数据，以及其他业务数据等。《白皮书》进一步根据数据在经济社会发展中的重要程度，从影响程度和影响对象两个方面，考虑采用定性指标识别并判定数据的等级，先整体将数据分为核心数据、重要数据、一般数据[13]，从而形成分级规则矩阵。

虽然《白皮书》强调数据在数字经济中的重要性，探讨了数据分类分级在保障数据安全方面的作用，从而为智能网联汽车数据的分类分级提供了综合分析和实践指导，但是《白皮书》属行业指导性文件，不属于立法机关或行政机关制定的规范性文件，故不具备法律强制力。《白皮书》中明确写道，“本文档仅供信息参考，不构成任何形式的法律、财务、技术或专业建议”。其内容主要体现为行业共识与技术建议，企业可自愿采纳，但违反《白皮书》建议不直接导致行政处罚。

3 完善智能网联汽车企业数据安全的法律完善措施

3.1 确定企业重要数据权利归属

与实物生产要素不同，数据资源通常呈现多方协同生成的特征，自初始阶段即面临复合权益诉求的交织。这种特性决定了数据产权制度建构的核心任务并非确定单一所有权主体，而需系统识别不同参与方对同一数据资产所享有的分层法定权益。[14]在智能网联汽车领域，数据权益配置涉及三重结构性约束：一是在先权益限制，含个人信息的智能网联数据处理必须遵循《个人信息保护法》第四十五条确立的知情同意原则，用户可依托数据可携权机制实现跨平台流通利用；二是强制开放义务，对于非个人信息类数据，汽车企业应依法保障终端用户、第三方服务商及公共管理部门的合理访问权限，该义务源于《反垄断法》第二十二条必需设施原则；三是收益权边界限定，重要数据控制者虽享有法定收益权，但其行使需符合《数据安全法》第二十一条设定的国家安全审查要求，且不得排除合理使用情形。[15]

由于此问题高度依赖场景，数据权益界定应遵循场景化响应机制：依据具体应用场景中的数据类型属性、风险等级及主体合理预期，动态配置各方权责结构。这种基于场景适配的赋权模式本质上是对传统财产权静态归属规则的范式革新。因此，立法机关在制度设计中应当确立智能网联车辆运行产生的重要数据初始配置给车企的权属规则。该制度安排既契合数据获取过程的技术独占性特征，亦能强化企业对核心数据的直接管控能力。

鉴于重要数据的高价值性，在赋予企业数据收益权的同时，必须课以其对应的风险控制义务。[16]当企业有效履行法定安全防护责任时，即可在合规框架内行使对控制数据的剩余控制权，该权利边界以法律明文禁止为限。具体制度建构需分两层推进：在规范层面，通过部门规章要求企业构建重要数据全生命周期管理机制，设立专职管理机构并实行法定代表人负责制；在技术标准层面，依托《规定》第八条确立的行业规范，形成“车—云—管—端”一体化保护系统。[17]

3.2 实现智能网联汽车数据的分类分级保护

智能网联汽车企业在数据采集阶段完成后，所获数

据资源呈现无序状态。此时汽车企业需履行《规定》第七条要求的法定义务，建立安全高效的存储管理机制。在操作层面，可先行通过分类分级双重识别机制对原始数据进行系统性梳理与类型识别，继而针对识别出的重要数据实施差异化防护体系，重点强化其存储安全等级与访问控制强度。依据《信息安全技术大数据安管理指南》（GB/T 37973–2019）的规范框架，智能网联汽车企业实施数据安全治理需遵循递进式程序结构：首先界定数据全生命周期的安全保护目标，其次通过分类分级双重识别机制对数据资源进行系统性梳理，即先行依据数据属性划分类型，再根据敏感程度与影响范围实施定级，继而明确大数据采集、存储、处理等环节的合规义务要求，最终基于量化评估结果建立与数据等级相匹配的分级保护体系。

对于数据分类，考虑到数据采集场景、重要程度和保护要求的不同，比起《白皮书》主张的“结合数据的特性和用途，从企业管理的视角对数据进行分类”，笔者更倾向于根据数据的来源与功能进行分类的方法，将数据分为车辆数据、用户数据、应用服务数据以及外部环境数据[18]。

对于数据分级，可依据《数据安全法》第二十一条确立的框架，构建智能网联汽车企业数据分级体系。在具体操作上，需综合考虑数据安全事件可能波及的国家安全、公共利益、组织利益以及个人权益四类对象，并评估其对保密性（C）、完整性（I）、可用性（A）这三个核心安全属性的冲击程度，依据损害后果的严重性（分为严重损害、一般损害、轻微损害三个层级）设定判定方法。通过对不同维度对象所受损害层级的系统分析，将已分类的智能网联汽车数据映射至相应安全级别，最终形成结构清晰的数据分级目录。值得注意的是，重要数据的安全属性具有动态特征，其等级并非固定不变。因此，当数据安全级别发生变化时，监管主体或企业有责任及时启动复评程序，重新核定其等级归属。[19]

鉴于智能网联车辆运行产生的数据规模庞大且价值各异，强化重要数据保护的核心策略在于对其收集与利用的数据实施精准的重要性评估与分级管理。据此，应当针对不同安全级别的数据特性，量身定制差异化的监管策略与具体措施。特别是对于收集过程中涉及的高敏感数据类型（如关乎个人隐私、国家秘密、车内外音视频信息等），必须实施与之匹配的强化保护手段。在处理含个人身份或特征的数据时，其收集、存储及利用等各环节行为，均须严格遵守法律法规设定的边界，不得突破法律的禁止性规定。为有效降低数据泄露风险，重要信息传输过程需应用可靠的匿名化技术，并对数据的本地化存储期限实施严格把控。[20]当确因智能网联汽车业务发展需求需进行数据的跨境传输、存储或利用时，必须对数据传输方案的安全性进行全面且独立的事前评估。经评估符合法定安全要求的数据方可在管控下出境；而对于涉及个人信息、高精度道路交通信息、重要地理信息等核心类别的重要数据，法律上则设置了明确的出境限制。

需要强调的是，数据分类分级工作的核心价值不在于过程本身，而在于其最终目标——为不同类型及安全级别的数据精准匹配相适应的差异化保护规则。在完成科学有效的分类分级工作后，即可将企业采集的重要数据识别为安全防护的核心目标，将其与其他非重要数据分开存储与管理，并针对其特殊性配置更高级别的安全保障措施与监管要求。

4　结语与展望

本研究表明，智能网联汽车重要数据安全面临种类繁杂、系统脆弱、泄露点多与网络威胁等严峻风险。当前法律规制体系的缺陷在于重要数据权责归属模糊与分类分级制度缺失，导致企业保护动力不足、治理效能低下。本文创新点在于提出“场景化确权”，明确企业作为重要数据核心受益者与保护者的双重身份；并构建了融合安全属性（CIA）、影响对象维度的智能网联汽车数据分类分级操作框架，为差异化保护提供理论基础。在实践层面，有助于推动行业建立清晰的数据治理结构，平衡数据利用与安全，促进产业合规发展。研究局限在于主要依赖法规文献与公开案例，缺乏企业实践层面的深度访谈数据。未来研究需深入探索具体场景下权责边界的操作性规则，评估分类分级制度在企业的落地成效，并关注跨境数据流动规制与国际规则的协调问题。

参考文献

[1] 吴海燕，陈朴. 智能网联汽车数据安全国内外治理机制及政策研究[J]. 电信快报，2022（9）.
[2] 赵建国. 特拉斯“偷脸”？智能汽车如何跨越数据安全鸿沟[J]. 中国信用，2021（4）.
[3] 王玉臻，刘丽荣. 智能网联汽车发展的法律障碍与应对[J]. 时代汽车，2025（3）.
[4] 高完成. 车数据共享的困境与法律应对[J]. 河南财经政法大学学报，2023（6）.
[5] 吴博峰. 为智能汽车数据安全加把数据安全加把“锁”[N]. 中国消费者报，2022–07–29（3）.
[6] 毕颖，杨紫瑶，董昭瑜，等. 我国智能网联汽车企业重要数据安全的法律保护[J]. 工业信息安全，2022（5）.
[7] 杨蓉. 从信息安全、数据安全到算法安全——总体国家安全观视角下的网络法律治理[J]. 法学评论，2021（39）.
[8] 祝高峰. 论数智经济时代重要数据安全的法律保护[J]. 社会科学家，2021（11）.

https://doi.org/10.35534/pss.0711151

［9］刘宇，黎宇科，刘洋洋，等．对自动驾驶汽车数据分类分级的思考［J］．汽车与配件，2021（18）．
［10］佚名．重要数据识别国家标准发布［J］．现代传输，2024（2）．
［11］毕颖，杨紫瑶，董昭瑜，等．我国智能网联汽车企业重要数据安全的法律保护［J］．工业信息安全，2022（5）．
［12］钟璐潞，卢栋．基于数据分类分级的港口企业数据安全管理［J］．中国港口，2021（10）．
［13］全国信息安全标准化技术委员会（SAC/TC 260）．信息安全技术 网络预约汽车服务数据安全要求：GB/T 42017–2022［S］．北京：中国标准出版社，2022.
［14］赵精武．科技伦理嵌入人工智能治理体系的路径展开——以自动驾驶应用场景为例［J］．法治社会，2024（5）．
［15］高郦梅．智能网联汽车数据财产权益配置理路［J］．湖南大学学报（社会科学版），2025（39）．
［16］马宇飞．企业数据权利与用户信息权利的冲突与协调——以数据安全保护为背景［J］．法学杂志，2021（42）．
［17］毕颖，杨紫瑶，董昭瑜，等．我国智能网联汽车企业重要数据安全的法律保护［J］．工业信息安全，2022（5）．
［18］张琼丽，陈翼．数据分类分级方法及实践研究［J］．技术与市场，2022（29）．
［19］钟璐潞，卢栋．基于数据分类分级的港口企业数据安全管理［J］．中国港口，2021（10）．
［20］李晓宇，李研．人工智能生成数据权利配置的路径选择——以智能汽车生成数据为例［J］．法治论坛，2023（2）．

Research on Legal Regulation of Data Security for Intelligent Connected Vehicles
—A Dual Approach based on Data Rights Allocation and Classification/Grading

Li Zihan　Han Zijie

Shanghai University of Political Science and Law, Shanghai

Abstract: In recent years, relevant domestic and international legislation, along with notable data breach incidents, have revealed the risk characteristics of intelligent connected vehicle data. These include the complexity of data types, the vulnerability of systems to attacks, the risk of leakage throughout the entire process, and the threat of cyber intrusions. China's current legal regulatory framework suffers from issues such as ambiguous attribution of rights and responsibilities for critical data and an incomplete classification and grading management system. This leads to inefficient corporate oversight and difficulties in balancing data utilization with security. Based on this, this paper proposes two recommendations: First, establish the ownership of critical data in intelligent connected vehicles, clarifying that automotive enterprises hold beneficial rights while bearing core protection obligations. Second, construct an operational classification and grading system for intelligent connected vehicle data, implementing differentiated protection strategies based on data levels and strictly restricting cross-border transmission of sensitive data. Refining data rights allocation and implementing classification and grading are crucial legal measures to safeguard critical data security in intelligent connected vehicles while balancing development and security. These steps hold significant importance for advancing the secure development of intelligent connected vehicle data.

Key words: Intelligent connected vehicles; Data security; Division of rights and responsibilities; Classification and graded protection