Open Journal of Legal Science 法学, 2026, 14(3), 50-55
Published Online March 2026 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2026.143066

Hans汉斯

智能网联汽车数据处理法律规制研究

常怀宇

长春理工大学法学院，吉林 长春

收稿日期：2026年1月29日；录用日期：2026年2月10日；发布日期：2026年3月9日

摘　要

智能网联汽车在运行过程中产生海量数据，涉及驾驶行为、用户隐私、交通环境等多个维度。随着《数据安全法》《个人信息保护法》等法律的实施，我国逐步构建起以安全为核心的数据治理法律框架。然而在实际应用场景中，智能网联汽车领域仍存在诸多亟待解决的问题，例如个人数据边界界定不清晰、知情同意原则难以有效运用、缺乏科学合理的数据共享机制等。为有效解决这些问题，应当合理运用技术手段，进一步健全智能网联汽车领域的法律法规体系，强化企业间的协作，携手探索智能网联汽车数据安全风险防控与数据治理的有效路径。

关键词

智能网联汽车，数据安全，法律规制

Research on the Legal Regulation of Intelligent and Connected Vehicles Data Processing

Huaiyu Chang

School of Law, Changchun University of Science and Technology, Changchun Jilin

Received: January 29, 2026; accepted: February 10, 2026; published: March 9, 2026

Abstract

Intelligent and Connected Vehicles (ICVs) generate massive volumes of data covering driving behavior, user privacy and traffic-environment information. With the entry into force of the Data Security Law and the Personal Information Protection Law, China has begun to build a security-centred legal framework for data governance. In practice, however, three problems remain acute: the boundaries of personal data in ICVs are ill-defined; the notice-and-consent regime is hard to implement; and

文章引用: 常怀宇. 智能网联汽车数据处理法律规制研究[J]. 法学, 2026, 14(3): 50-55. DOI: 10.12677/ojls.2026.143066

there is no sound mechanism for data sharing. To address these issues, technical measures should be used judiciously, the relevant legal rules for the ICV sector should be refined, the notice-and-consent and data-sharing regimes should be tailored to industry characteristics, and closer cooperation among enterprises should be encouraged to jointly develop models for preventing data-security risks and governing data.

Keywords

Intelligent and Connected Vehicles, Data Security, Legal Regulation

1. 智能网联汽车数据处理概述

(一) 智能网联汽车的数据链

在对智能网联汽车的数据处理行为进行法律规制之前，有必要先厘清其在运行过程中的数据处理流程与基本逻辑。智能网联汽车的技术体系主要围绕“感知”与“控制”两个核心环节展开，二者之间通过“智能算法”实现连接。整个驾驶流程大体可划分为三个阶段：起初，车辆借助雷达、传感器以及车载通信系统等装置，对外部的周边环境展开感知，收集原始数据信息；其次，系统对多源感知信息进行融合处理，利用智能算法预测其他交通参与者的行为，规划出合理的行驶路径，实现类似人类驾驶员的决策行为；最后，车辆根据规划结果，实时控制油门、刹车和转向等执行机构，调整车速、方向和位置，确保行驶过程的安全与稳定。

在这一过程中，数据不断生成并流转。感知数据由车载传感器采集，经融合处理后形成用于决策与控制的数据，并在车内系统、车与车、车与云、车与路之间传输，构成一条完整的数据链条。围绕驾驶行为产生、处理和应用的数据，可统称为“驾驶数据”。此外，随着智能网联汽车服务功能的拓展，车辆在使用过程中还可能产生与驾驶无直接关联的数据，例如车载应用收集的用户个人信息等，这类数据可归类为“非驾驶数据”。[1]

(二) 智能网联汽车数据特点

一是数据的复杂性。智能网联汽车所涉及的数据种类极为繁杂。一方面，包含车辆基础数据，像车牌号、车辆型号、车辆尺寸这类基础信息，它们是车辆身份与基本属性的直观体现。另一方面，在车辆的测试阶段和实际驾驶阶段，还会采集并处理大量其他数据。具体而言，有通过摄像头、雷达等各类传感器获取的车外数据，这些数据涵盖了建筑、地形、道路状况以及天气情况等车外环境信息，为车辆了解外部世界提供了丰富的素材；还有借助传感器从汽车座舱内采集的座舱数据，例如驾驶员的人脸特征、声纹信息以及指纹数据等，这些数据有助于对驾驶员身份进行识别以及对其状态进行监测；汽车内置传感器从车辆电子电气系统获取的运行数据也至关重要，它能反映车辆各个系统的运行状态和性能指标；此外，与汽车定位和行驶路径相关的位置轨迹数据也不可或缺，它记录了车辆的行驶轨迹和位置信息。相关研究揭示，各类数据的敏感程度有着显著区别，正因如此，有必要依据不同数据类型实施差异化的安全防护与管控举措，进而在确保数据安全 0 的基础上，达成数据利用效益的最大化。

二是数据的流动性。智能网联汽车凭借自身特性，从纵向与横向两个维度对产业生态进行了拓展，显著提升了数据的流动性。在纵向层面，智能联网汽车的数据流通并非局限于车内。它需要构建起一个

多维度的数据交互网络，实现车与人、车与车、车与路以及车与云等不同主体之间的数据传递。这种交互打破了传统车内数据的封闭状态，极大地拓宽了数据交互的范畴。而且，由于车辆处于持续移动状态，数据必须保持动态特性。这就要求数据在用户端、车端、云端和路端之间进行实时传输与处理，以确保信息的及时性和准确性。随着数据交互频率的不断提高，整体数据的流动性得到了大幅增强。从横向角度分析，在整个智能汽车产业链中，上下游行业之间的数据流动十分活跃。以汽车生产、汽车保险和汽车维修等行业为例，这些行业在运营过程中相互关联、相互影响。为了实现更高效的协同运作、提供更优质的服务，它们之间不可避免地需要进行数据的共享与交换。这种跨行业的数据流动，进一步丰富了智能网联汽车的数据生态，促进了产业生态的多元化发展。[2]

三是数据的精确性。智能网联汽车在行驶期间，各类判断和决策的制定均高度依赖从多元信息渠道获取的数据。倘若决策出现偏差，不仅可能造成用户财产受损、人身受到伤害，还可能对道路交通安全产生负面影响，进而给他人的生命财产安全以及公共利益构成潜在威胁。所以，在智能网联汽车的应用场景中，对数据的完整性和精确性提出了极为严苛的要求。数据的完整性意味着在智能驾驶的整个过程中，所采集以及产生的各类数据应当维持其原始面貌，不能出现任何未经许可的改动或者损毁情况，从而确保数据从生成、存储到传输的每一个环节都能准确无误。只有数据完整无缺，智能网联汽车才能依据可靠的信息做出正确决策。数据精确性意味着在智能驾驶场景下，所采集到的数据所承载的信息，必须和现实世界的实际情况高度一致。这种一致性主要体现在两个方面：其一，在数据收集的全面性上，要尽可能减少信息遗漏，全面反映真实世界的情况。这意味着不仅要收集道路及其周边的静态信息，如建筑物的位置、道路的宽度等，还需获取道路上的动态数据，如车辆的行驶速度、交通流量等，以及其他根据实际需求特定的数据。其二，在数据传递的准确性上，要最大程度降低误差，确保所传递的数据和信息精准可靠。

2. 智能网联汽车数据处理存在的问题

(一) 个人数据边界模糊

智能驾驶所涉数据类型繁杂、来源多样，不同性质的数据必须匹配差异化的安全与治理策略。其中，个人数据因直接关涉自然人权益，在中、欧、美、加等法域均受专门立法严格约束。然而，将抽象条文落到智能驾驶这一具体场景，首要难题是厘清哪些数据算个人数据。现行定义普遍采用“与已识别或可识别自然人相关联”的标准，并呈现两条识别路径：一是“数据 → 人”，即单凭该数据或结合其他信息可指向特定个体；二是“人 → 数据”，只要特定个体已能被识别，其相关数据即落入个人数据范畴。以人为中心直接采集的姓名、住址、证件号、人脸、声纹、浏览习惯等，显然属于个人数据。而以车为中心产生的行驶轨迹、维保记录等，虽最初仅关联到车辆，却可以间接锁定驾驶者或车主，故在特定组合下也可能被认定为个人数据。若一概将车辆相关数据均视为个人数据，又难免过度扩张概念，抑制数据流通与价值释放。[3]

除了因数据本身的复杂性使得个人数据的边界难以清晰界定外，还存在一个更为普遍的因素，即数据的匿名化处理。依据《中华人民共和国个人信息保护法》第四条的相关规定，经过匿名化处理的数据不再被视为个人数据。然而，法律并未具体阐明数据需达到何种脱敏程度方可被认定为匿名数据。当前的数据脱敏技术在实践中难以实现完全的匿名化，而且即便某些数据在当下满足了匿名化的标准，随着未来新数据的不断涌现以及识别技术的持续进步，这些数据仍有可能被重新识别出来。这种潜在的重新识别风险，进一步加剧了个人数据边界的模糊性。

(二) 知情同意原则落实难

同意原则源于契约自治理念，历来被视作处理个人信息最核心的正当性基础理论。其逻辑是：控制

方必须先就采集、使用目的、数据类型、处理方式及可能风险等事项向信息主体履行全面告知，信息主体在真正理解后作出清晰、主动地同意表示。当下最常见的应用模式是“隐私政策”和“用户协议”，用户滑到页面底端点击“同意”即被视为授权。[4]

然而，在智能网联汽车场景里，这一套“知情–同意”模式遭遇三重冲击：其一，数据主体碎片化且链条长，车主、驾驶员、乘客乃至路边行人都可能被卷入，让行人提前阅读并点击同意几乎不现实；其二，即便协议文本再详尽，也因篇幅冗长、术语密集，不同教育背景的用户往往直接拉到底部秒点同意，知情环节流于形式，沦为用了就算答应的默示规则；其三，自动驾驶需实时、连续采集多源数据，若用户中途拒绝某类数据，车辆功能可能立即受限；更棘手的是突发状况下的临时数据调用，若先停下征求同意再处理，极易贻误安全时机。

(三) 如何设置数据共享机制

在智能驾驶的大环境下，数据具备鲜明的公共属性。在智能驾驶的实际运行过程中，信息在车、路、云、人之间持续不断地进行传输交互。整个交通系统所做出的指示与决策，并非凭空产生，而是基于对来自多方信息的汇聚、整合与深度处理。智能网联汽车作为交通系统中的关键一环，其自身所产生和承载的数据也是整个系统数据体系的重要组成部分。这些数据的共享程度，直接关系到整个交通系统能否正常、高效地运转。倘若数据无法顺畅共享，交通系统就可能因信息缺失或不准确而出现决策失误，进而影响交通秩序和安全。

不过，智能驾驶数据的公共属性并非绝对，还会受到多种因素的制约。例如，数据的获取往往需要相关企业在财力、技术等方面投入大量资源，这些数据在一定程度上承载着企业的核心竞争力和商业利益，企业会将其作为商业机密进行严格保护和使用。同时，数据中还可能包含大量个人数据，如果直接进行使用和共享，可能会给个人带来不必要的困扰，甚至侵犯个人隐私。因此，在制定相关制度时，必须全面、综合地考量各方利益，在保障公共利益的同时，充分尊重企业的商业权益和个人的隐私权利，实现多方利益的平衡与协调。

3. 完善智能网联汽车数据处理法律规制的建议

(一) 个人数据的边界判定

个人数据边界的模糊状态并非毫无边界，在智能驾驶这一特定场景下，清晰界定数据属性对提高数据利用效能、推动行业进步具有重要意义。正因如此，诸多与行业相关的规范文件都致力于明确个人数据的内涵与外延。判断个人数据边界，可依据数据与个体之间的关联紧密程度。在智能驾驶情境中，存在“车”与“人”两个核心数据源，以此为基准可将数据划分为三类。第一类数据完全源自车辆本身及其所处的外部环境，像道路状况数据、天气信息数据以及车辆的基础信息数据等，这类数据与个人毫无关联，不属于个人数据范畴。第二类数据完全来自于个人或者个人的行为活动。像车主在购车时登记的诸如姓名、联系方式、身份证号等个人基础信息，乘客使用车内娱乐系统时留下的浏览记录、操作偏好等数据，还有驾驶人的面部轮廓、音色音调等生物特征数据均属于个人数据。第三类数据是车辆运行与个人操作共同作用而生成的，具体包含车辆的行驶轨迹、累计行驶里程以及车辆各部件的损耗情况等数据。对于这类数据，很难直接判断其是否属于个人数据，需要借助一个关键要素来确定，这个要素就是特定的智能汽车。倘若这些数据能够精确对应到某一辆具体的车辆，那么就可以把它们划归为个人数据，因为在现有的制度体系里，特定车辆和特定主体之间有着比较清晰且紧密的关联；反之，如果这些数据无法识别出具体车辆，那就不属于个人数据，能够进行相对灵活的使用。[5]

然而，随着数据量的持续积累以及识别技术的不断进步，能够识别到个人的数据数量日益增多，个人数据的边界也随之不断拓展。因此，为更有效地促进数据利用，在明确个人数据边界的基础上，更为

关键的是对个人数据进行分级分类管理，进一步细化相应的保护和利用规则。

(二) 知情同意原则的制度重构

在智能驾驶情境中，数据主体呈多元且随机流动，数据形态繁杂且需毫秒级更新，若沿用传统“一事一授权”的知情同意范式，几乎难以落地。但这并不等同于该原则可被架空；相反，知情同意仍是个人信息保护的基石，其底层逻辑在于承认个人对数据享有初始权利，体现意思自治，并为权利的部分让渡提供正当依据。一旦彻底摒弃该原则，即等于否定个体自由意志与权利本身的正当性。所以，我们能够针对知情同意原则的具体制度规划作出相应调整：

其一，对兼具个人属性与公共属性的数据可豁免同意。典型如直接服务于交通效率与公共安全的数据。前者旨在优化整体通行，后者意在避免瞬间风险，其合法性基础在于“保护数据主体重大利益”与“实现公共利益”，而非用户授权。豁免范围须以原始目的为限，且应依最小化标准精准圈定使用边界。

其二，对普通个人数据，按主体差异配置分层同意。

1) 长期使用者(车主、常规驾驶人)可在取得车辆使用权前，通过一次性协议对未来一段时间内的数据收集与处理作出概括授权。

2) 随机乘客通过 APP 完成统一告知，乘客网络操作叫车或落座即视为对当次行程数据处理的默示同意；系统须同步为其数据打上“乘客”标签，并提供一键删除入口。若涉及人脸、支付账户等敏感信息，须于采集瞬间以语音方式二次提示，确保告知充分。

3) 行人数据仅用于瞬时避障与路况协同，无需识别身份，可借助实时脱敏和去标识技术即时处理，事后立即销毁，无需征得同意。

(三) 构建三层数据共享机制

从维护公共利益的角度出发，构建一种数据共享机制显得尤为必要。通过这一机制，各企业能够有机会获取并利用其他企业所掌握的智能汽车数据，进行模型的训练与优化，从而不断完善车辆的运行系统。此举措不仅能有效降低同类事故出现的概率，助力整个行业稳健前行，还可大幅提升交通运行效率，筑牢交通安全防线，进而达成智能汽车数据应用社会效益的最优解。因此，有必要通过科学合理的制度构建，在保障数据持有企业合法权益的同时，兼顾行业内其他企业的利益诉求，以及社会整体的公共利益，实现多方利益的均衡与协调。[6]

考虑到获取事故数据所付出的成本相较于险情数据更高，那么事故数据所蕴含的价值自然也更为突出。基于这样的现状，我们可以搭建一个包含“事故数据–险情数据–一般驾驶数据”三层级的数据共享体系架构。在事故数据的共享环节中，政府公共机构应当发挥主导作用。按照相关法律规定，一旦发生事故，相关经营主体有责任上报事故数据，此时公共机构便可承接这些数据的共享工作。同时，在开展共享操作之前，需对数据进行匿名化处理，如此一来，便能防止企业的声誉遭受负面影响。而对于险情数据，企业并不存在向第三方机构进行报告的法定责任与义务。不过，政府可以通过出台相关政策加以引导，激励企业把经过匿名化处理的险情数据通过官方指定的渠道进行共享。例如，行业中的其他经营方可借助支付特定费用获取这些数据，从而为共享数据的企业给予经济层面的激励。与此同时，政府需要对费用进行监管并合理定价，防止企业自行定价过高，从而牟取不正当利益。除了上述举措，政府不妨在责任界定、税收减免等层面，为共享数据的企业提供相应的政策扶持。对于普通驾驶数据而言，因其普遍性较强，数据共享的相关事宜可由企业间自主商议，借助市场机制加以调节。但需要注意的是，在共享期间，企业务必严格遵循针对特定类别数据(如个人隐私信息、关键数据等)的处理规范。

4. 总结

智能驾驶领域如今正处于迅猛发展的上升阶段，伴随产业规模持续拓展，数据规模也将迎来爆发式

增长。在此背景下，如何处理相关数据及对其进行有效规制，已然成为智能驾驶行业前行过程中亟待解决的关键议题。当下，国家针对智能驾驶领域数据所制定的规范尚有不足。因此，有必要紧密结合当前行业实际状况，充分发挥技术手段、法律制度以及行业组织这三方面的协同作用，共同构建一套全方位、多层次的数据治理规范体系，积极探索并完善数据风险防范机制与数据治理模式。

参考文献

[1] 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(1): 133-140.

[2] 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(1): 147-163.

[3] 梅傲, 尹诗楠. 法国网联汽车的数据合规方案及中国启示[J]. 中国科技论坛, 2023(6): 180-188.

[4] 邓文娟, 高圣平. 论智能网联汽车监管的沙盒模式——兼评中国相关地方立法[J]. 江汉论坛, 2023(4): 125-128.

[5] 徐子淼. 智能网联汽车数据处理的法律规制: 现实、挑战及进路[J]. 兰州大学学报(社会科学版), 2022, 50(2): 100-111.

[6] 王甲铄. 人工智能时代的智能网联汽车法律规制——评《智能网联汽车协同决策与规划技术》[J]. 中国科技论文, 2021, 16(8): 927.