

智能网联与自动驾驶法律评述（2025年5月）

作者：傅鹏 赵卿梦 \*实习生包杰薇对本文亦有贡献

1、智能网联汽车自动驾驶/辅助驾驶宣传用语口径收紧

2025年3月，部分汽车厂商车辆出现与自动驾驶（辅助驾驶）有关的严重事故，引发广泛关注和讨论。

此前，2025年2月25日工业和信息化部（以下简称“**工信部**”）、市场监管总局发布的《关于进一步加强智能网联汽车产品准入、召回及软件在线升级管理的通知》（工信部联通装〔2025〕45号，以下简称“**《通知》**”）提出，汽车生产企业应当主动履行产品质量安全主体责任，要根据《智能网联汽车产品准入、召回及软件在线升级管理与技术指南》，加强与研发生产智能网联汽车产品及开展OTA升级活动相适应的能力建设。企业要对智能网联汽车产品及OTA升级活动开展充分的测试验证，明确系统边界和安全响应措施，确保控制策略合理，严格履行告知义务，确保在开发、生产、运行等阶段进行有效的安全管理，不断提升产品功能、性能和质量安全水平。

2025年4月16日，工信部装备工业一司组织召开智能网联汽车产品准入及软件在线升级管理工作推进会，会议强调汽车生产企业要充分开展组合驾驶辅助测试验证，明确系统功能边界和安全响应措施，不得进行夸大和虚假宣传，严格履行告知义务，切实担负起生产一致性和质量安全主体责任，切实提升智能网联汽车产品安全水平。[1]根据公开报道，本次会议内容主要包括“**收紧智驾能力的宣传**”“**规范智驾能力的使用**”“**严管智驾功能的部署和风险**”。

当前，多家新能源车企都对宣传用语作出不同程度的变更，举例而言：

| 车企        | 宣传用语变更情况                                                                                                                                                     |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 一家美资新能源车企 | 2025年3月，该企业将原“Autopilot自动辅助驾驶”的名称调整为“辅助驾驶”，将原“基础版辅助驾驶”（BAP）的名称调整为“基础辅助驾驶”，将原“增强版自动辅助驾驶”（EAP）的名称调整为“增强辅助驾驶”，将原“完全自动驾驶能力”（FSD）（后改为“FSD智能辅助驾驶”）的名称调整为“智能辅助驾驶”等。 |
| 一家中资新能源车企 | 该企业在2025年4月29日的官方微博动态中，宣传用语由“智能驾驶”改为“智能辅助驾驶”。                                                                                                                |
| 一家中资新能源车企 | 2025年5月1日，该企业微博发布一组宣传物料，其海报中宣传用语由“某某智驾”更换为“某某辅助驾驶”。                                                                                                          |
| 一家中资新能源车企 | 2025年5月1日，该企业产品线负责人微博内容中，宣传用语采用了“辅助驾驶焕新”。                                                                                                                    |

## A. 本次宣传用语规范行动，目前在实践中主要面向量产乘用车

本次规范行动相关的引发事件之一是乘用车使用高阶辅助驾驶导致的严重事故。本次行动主要针对量产乘用车，目前暂时没有新闻信息表明延及自动驾驶物流车辆、自动驾驶清洁车辆、封闭道路特种自动驾驶车辆等各类其他车辆，主要原因在于：

- 量产乘用车涉及大量驾驶人员和乘客的人身安全。自动驾驶物流车辆、自动驾驶清洁车辆、封闭道路特种自动驾驶车辆等各类其他车辆基本不涉及驾驶人员或乘客，运行宽容度相对高。
- 量产乘用车行驶于公开道路，路线不固定，路侧涉及的其他人员多，次生风险大。自动驾驶物流车辆、自动驾驶清洁车辆、封闭道路特种自动驾驶车辆等各类其他车辆一般在固定路线运行，或者仅仅限于封闭区域（例如自动驾驶矿区车辆），在相当一部分场景下路侧涉及的其他人员少，次生风险相对较小。
- 量产乘用车一般不对高阶辅助驾驶速度进行特别严格的限定，或者即使限速，速度也较快。自动驾驶物流车辆、自动驾驶清洁车辆、封闭道路特种自动驾驶车辆等一般进行严格限速，且限速较低。例如，自动驾驶物流车辆速度一般不会高于50km/h。自动驾驶清洁车辆速度更低。

## B. 企业应注意严格规范宣传用语，杜绝误导性表述

- 企业应注意采用《汽车驾驶自动化分级》（GB/T 40429-2021）标准定义的官方术语：L2级系统称为“组合驾驶辅助”，L3级及以上可使用“有条件自动驾驶”等表述。避免在未达到L3级别的情况下，使用“自动驾驶”“高阶智驾”等模糊概念，导致消费者混淆责任主体。
- 广告视频中若出现驾驶员脱手画面，需叠加“请勿模仿，需全程监控”警示标识。
- 官网技术参数页需标注驾驶功能等级，例如“当前功能等级：L2级组合驾驶辅助”。
- 在用户协议、车书等文件中明确系统局限性（如可能无法识别静止障碍物），并声明：“系统为辅助工具，驾驶员需全程监控路况并承担最终责任”。

## C. 企业应注意强化OTA升级全流程合规管理

- 一般升级：不涉及技术参数变更的OTA，备案后可直接实施。
- 重大变更升级：涉及产品主要技术参数变更的，企业应当在取得产品变更许可并完成备案后，方可实施升级。涉及汽车自动驾驶功能的OTA升级活动，应当按照准入管理有关规定，取得相应许可。
- 缺陷修复升级：企业实施OTA升级活动消除汽车产品缺陷、实施召回的，应当按照《缺陷汽车产品召回管理条例实施办法》组织实施，并立即停止生产、销售缺陷汽车产品。若消除缺陷的措施涉及产品主要技术参数变更，企业应当在取得产品变更许可后，方可恢复相应汽车产品的生产。
- 升级前向用户清晰推送风险告知信息，例如说明“升级后制动响应阈值调整”等具体变化，并完整保存软件版本的溯源数据。
- 避免利用OTA升级手段隐瞒产品缺陷或规避法定的召回责任。

## D. 企业应建立报告机制

- 企业在获知其生产销售的智能网联汽车产品发生组合驾驶辅助系统失效导致功能退出等事件或搭载组合驾驶辅助系统车辆发生碰撞等事故的，根据要求向工信部、市场监管总局报告。
- 事故报告：“事故”指组合驾驶辅助系统使用期间发生碰撞等事故，包括但不限于安全气囊展开、不可逆乘员约束装置或者弱势道路使用者辅助安全系统展开、人员受伤、人员死亡等情形。企业应当在事故发生后48小时内（如造成人员伤亡或重大社会影响的，应在事故发生后24小时内）提交事故信息。

- 事件报告：“事件”指在组合驾驶辅助系统使用期间，智能网联汽车产品所发生的与安全相关的驾驶行为、情况等描述。企业应当在自然月的4月、7月、10月的前15个工作日内提交上一个季度的事件报告，1月的前15个工作日内提交上一个年度的事件报告。

## 2、车载端应用个人信息处理活动违规检测：系统性纳入监管关注视野

根据2025年5月国家网络安全通报中心发布的通报，经国家计算机病毒应急处理中心检测，某主机厂预装的第三方应用存在违法违规收集个人信息情况，类型涵盖视频应用、某生活服务应用、教育应用、天气应用、新闻应用、音乐应用。[11]

### 海问评述：

#### A. 监管视野：从“手持端”延展到“车端”

此前，监管部门对移动APP个人信息保护的关注，主要集中在手机、平板等典型的移动终端上的移动应用（APP）、小程序及软件开发工具包（SDK），很少直接关注车载端应用，实际通报的案例也很少。本次通报反映出监管已经关注到车载端应用的个人信息保护情况。

#### B. 企业：针对车端应用和场景进行个人信息保护合规检视

- 考虑到车载端应用的特殊性，企业有必要为应用的个人信息合规情况评估和相应调整预留充足时间。

以安卓系统为例，较多车载端应用需针对车载操作系统进行专门适配和独立开发，在设计和实现用户授权、权限请求、弹窗提醒等用户交互环节的技术实现和配置更为复杂，权限变更及弹窗设置等合规要求的调整难度高于移动端应用。

- 基于车载端应用在个人信息保护和数据安全方面的合规要求与移动端应用在原则上是一致的，车载端应用的开发企业可以借鉴手机应用的合规要求，提前进行个人信息合规评估和保护措施核查，将涉及权限调整、弹窗提示和选项勾选等功能的配置纳入项目规划，预留充足的开发和合规审查时间，确保车载应用上线前能够满足监管要求。

## 3、个人信息保护合规审计落地：汽车行业企业的“日常体检”

2025年2月，《个人信息保护合规审计管理办法》（国家互联网信息办公室令第18号，以下简称“《**合规审计管理办法**》”）发布，并于2025年5月1日正式施行。

2025年5月19日，全国网络安全标准化技术委员会秘书处还发布了《网络安全标准实践指南——个人信息保护合规审计要求》（网安秘字〔2025〕62号，以下简称“《**合规审计要求**》”），该文件虽不具有法律强制力，但对《合规审计管理办法》的附件《个人信息保护合规审计指引》进行了细化，为企业和审计机构开展个人信息保护合规审计（以下简称“**合规审计**”）明确了具体操作流程。

### 海问评述：

#### A. 什么样的企业要开展合规审计

- **处理超过1000万人个人信息的企业：**依据《合规审计管理办法》第4条，处理超过1000万人个人信息的企业，应当每两年至少开展一次个人信息保护合规审计。

- **没有处理超过1000万人个人信息的企业：**可以根据自身业务情况和个人信息处理情况，合理决定审计的开展时间。

具体而言，企业可以参考《合规审计要求》第4.2.4条的要求：

处理超过100万、不超过1000万人个人信息的个人信息处理者每三年或四年至少开展一次个人信息保护合规审计。

处理不超过100万人个人信息的个人信息处理者应根据个人信息合规风险、处理个人信息数量、业务规模等合理确定合规审计频率，宜每五年至少开展一次个人信息保护合规审计。

- **监管部门主动要求进行审计：**依据《合规审计管理办法》第5条，在特殊情形下，例如企业的个人信息处理活动可能侵害个人权益或发生个人信息安全事件等，个人信息保护部门（例如网信部门），可以要求企业委托专业机构进行合规审计。

## B. 汽车行业企业需要予以特别关注的原因

- 汽车行业企业向用户提供的智能网联服务普遍支持用户通过车机端、移动端和网页端等多种终端的接入与操作，应用功能涵盖影音娱乐、导航定位、辅助驾驶等丰富场景，涉及大量个人信息（包括用户的行踪轨迹、出行习惯等敏感个人信息）的处理活动。

- 由于多数功能的实现依赖外部供应商的技术服务支持，涉及个人信息的共享，若与境外智能网联和自动驾驶解决方案服务商合作，还涉及个人信息跨境传输。

- 除了复杂的数据流转，直接面向车主的车企及自动驾驶企业处理的个人信息量级往往庞大，一些企业可能容易超过《合规审计管理办法》的“1000万人”量级门槛。因此，企业需尽早梳理数据资产，若处理的个人信息量级超过1000万，则有必要尽快为每两年至少一次的自我合规审计的开展做准备。

- 汽车行业企业即使处理的个人信息量级没有超过1000万，也往往数量很大，很可能多位于数十万人到数百万人之间。这一处理个人信息的数据量级本身具有一定程度敏感性，一旦出现个人信息保护方面的事件，产生的后果可能严重。因此，此类企业也宜尽快根据《合规审计管理办法》的要求，组织开展个人信息保护合规审计。

- 另外，依据《合规审计管理办法》第12条的规定，处理100万人以上个人信息的个人信息处理者应当指定个人信息保护负责人，负责个人信息处理者的个人信息保护合规审计工作。达到该门槛的车企需要完善内部个人信息保护管理制度，将合规审计相关事项纳入个人信息保护负责人的职责清单。

## 4、数据出境申报背景下的数据识别：汽车行业企业的关注

根据国家互联网信息办公室2025年5月30日发布的《数据出境安全管理政策问答（2025年5月）》（以下简称“**问答**”），如果数据处理者被告知掌握重要数据或者掌握的数据被公开发布为重要数据，应当按照相关法律法规的要求，履行重要数据安全保障责任。**没有发布行业、领域的数据分类分级标准规范和重要数据识别申报规则，数据处理者也没有被有关部门告知应当进行重要数据识别申报的，未识别申报重要数据，未对相关数据进行重点保护，不会被认定为违反重要数据保护相关规定，不会因此受到行政处罚。** [11]

### 海问评述：

#### A. 本次问答澄清了监管要求，有利于稳定企业预期

对于尚未发布明确重要数据识别申报规则，且未被有关部门告知应当进行重要数据识别申报的行业企业，本次问答在重要数据的认定、保护以及数据出境领域，澄清了企业的法律义务边界，减轻了企业对可能构成重要数据出境、从而需要完成数据出境安全评估程序的担忧。

数据出境安全评估流程由于其材料要求相对严格、审核周期相对长、材料补充和修改的沟通往来相对复杂等因素，是企业评估申报策略的重点领域。此前，特别是在数据出境安全评估流程启动之初，缺乏对重要数据识别认定和申报的具体指导，所以部分企业在梳理数据资产过程中，存在依据不清、边界不明等顾虑。特别是对于部分拟出境数据是否属于重要数据，是否应当在没有明确清单、目录的情况下，专门就出境事项进行主动和宽泛的重要数据识别，缺乏必要指导。本次问答的出台，有利于稳定企业预期。

**B. 汽车行业的特殊情况和特别关注**

对于汽车行业，情况会较为复杂，企业需要结合法规要求以及与主管部门的沟通，对是否构成重要数据进行综合判断。

在法规层面，本次问答提及的部分行业、领域已经公开发布的数据分类分级标准规范和重要数据识别申报规则之一《工业领域重要数据识别指南》（YD/T 4981-2024），适用于汽车行业部分场景，并为汽车装备过程以及汽车联网产品服务过程中的重要数据识别提供了一定指引。

《汽车数据安全若干规定（试行）》（国家互联网信息办公室令第7号）虽然未在问答中被明确列举，且其细节上不够完善，未形成具有操作性的重要数据清单或者目录，但对重要数据的识别具有一定参考价值。企业在结合前述法规进行初步数据识别后，必要情况下应与主管部门沟通，进一步研判认定结果。

根据笔者多个项目经验，实践操作中，相当一部分主机厂、智能网联解决方案服务商、自动驾驶企业已经在地方政府、行业主管部门的指导下，针对性进行了专项重要数据识别和申报备案。这些企业需要根据个案中收到的目录、清单，认真识别自身重要数据，并且结合实际是否存在数据出境的情形，履行相应的合规义务。

**5、人脸识别技术应用备案开启：汽车行业备案合规新关注点**

根据《人脸识别技术应用安全管理办法》（国家互联网信息办公室公安部令第19号，2025年6月1日实施）和国家互联网信息办公室2025年5月28日发布的《关于开展人脸识别技术应用备案工作的公告》，企业应用人脸识别技术处理的人脸信息存储数量达到10万人之日起30个工作日内，应当向所在地省级以上网信部门履行备案手续（实践中，通过网信办线上系统启动）。

**海问评述：**

- 对于汽车行业，建议首先针对车联网实名认证、汽车金融贷款、疲劳驾驶检测等所有采用人脸识别技术的业务场景，系统梳理并分类登记人脸识别的具体功能用途、数据流向、存储方式和操作流程。明确每一场景下数据收集的必要性和合法性，判定是否“为实现特定目的确需收集人脸信息”，避免功能冗余或过度采集。
- 建立有效的统计机制，实时监测人脸信息存储数量，对于接近10万门槛的，应提前预警，确保及时备案。处理涉及人脸信息存储数量达到10万人时，应在30个工作日内，向所在地省级以上网信部门完成备案。
- 对于某些强身份认证场景（如金融贷款、实名登录等），人脸识别确实无法被其他方式替代的情况下，可综合采用双因子认证、多模态生物识别等提升安全性和体验。对于疲劳驾驶监测等场景下，若人脸识别数据的出车、存储与上传云端不具有必要性，应采取技术措施，实现即用即删，不留存数据也不向车外传输原始人脸图像，降低数据泄露风险。

海问长期深耕汽车、智能网联、自动驾驶以及泛出行行业垂直领域，服务主机厂、智能网联与自动驾驶解决方案服务商、图商、出行企业、新能源充换电企业、动力电池企业等行业上下游主体。该领域法律监管发展迅速，实践操作高度依赖经验与个案判断。海问持续跟踪该领域法律监管动态，结合丰富的项目经验，提供针对复杂问题的分析和务实的解决方案。

[I] 参见工信部网站，[https://wap.miit.gov.cn/jgsj/zbys/qcgy/art/2025/art\\_e244b52a7cd44175904cd5fa82a29df6.html](https://wap.miit.gov.cn/jgsj/zbys/qcgy/art/2025/art_e244b52a7cd44175904cd5fa82a29df6.html)。

[II] 参见央广网：《国家计算机病毒应急处理中心检测发现65款违法违规收集使用个人信息的移动应用》，<https://news.cctv.cn/2025/05/12/ARTIvtHeJEJGtDXyGtGN3ptk250512.shtml>。

[III] 参见国家互联网信息办公室网站，[https://www.cac.gov.cn/2025-05/30/c\\_1750315283722063.htm](https://www.cac.gov.cn/2025-05/30/c_1750315283722063.htm)。

2025-06-12