The Regulatory Review for Intelligent Connected Vehicles and Automated Driving (September 2025)

Author: FU, Peng Zhao, Qingmeng Bao Jiewei

1、行业网络宣传乱象整治：工信部等六部门联合部署专项行动

2025年9月10日，工业和信息化部等六部门联合印发《关于开展汽车行业网络乱象专项整治行动的通知》（“**《通知》**”），旨在全国范围内开展为期3个月的汽车行业网络乱象专项整治行动I。

A. 行动具体要求

整治问题	具体行为	法律依据
	通过制作**虚假**图片、视频，捏造故事，炒作和散布涉车企负面话题，恶意解读汽车企业销量波动，攻击汽车企业经营发展战略等，赚取网络流量，获取商业利益。	
	利用自身话语权和影响力，以“新闻监督”“舆论监督”“科普”等名义，通过以商养测、以测养商、开展商测结合的**虚假或不规范测评**等方式，获取商业利益，甚至要挟汽车企业提供“保护费”。通过在汽车产品上市发布和汽车企业融资等重要节点，发布涉企虚假不实信息或负面信息，或在评论区带节奏等，胁迫企业开展商务合作。	《网络安全法》第12条：任何个人和组织不得利用网络编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。 《网络信息内容生态治理规定》第7条：网络信息内容生产者应当采取措施，防范和抵制制作、复制、发布含有下列内容的不良信息：（一）使用夸张标题，内容与标题严重不符的；（二）炒作绯闻、丑闻、劣迹等的。
非法牟利问题		第22条、第24条：网络信息内容服务使用者和网络信息内容生产者、网络信息内容服务平台不得通过发布、删除信息以及其他干预信息呈现的手段侵害他人合法权益或者谋取非法利益；不得通过人工方式或者技术手段实施流量造假、流量劫持以及虚假注册账号、非法交易账号、操纵用户账号等行为，

		破坏网络生态秩序。
	利用主板机、生成式人工智能等技术，制造新型“网络水军”，产出**虚假**内容，制造虚假热度和趋势，规避平台监测，谋取非法利益。	《刑法（2023修正）》第274条：敲诈勒索公私财物，数额较大或者多次敲诈勒索的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，并处罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑，并处罚金。
	对汽车、动力电池的性能、功能、质量、销售状况等作**虚假或者引人误解的宣传**，欺骗误导消费者。 汽车企业**操纵机构或评测类账号等搞虚假或不规范测评**。引用、捏造虚假数据，选择性披露销售数据，巧立名目发布销量排行等各种榜单。	除前述《网络信息内容生态治理规定》外，《消费者权益保护法（2013修正）》第20条：经营者向消费者提供有关商品或者服务的质量、性能、用途、有效期限等信息，应当真实、全面，不得作虚假或者引人误解的宣传。 《广告法（2021修正）》第28条：广告以虚假或者引人误解的内容欺骗、误导消费者的，构成虚假广告。 广告有下列情形之一的，为虚假广告： .....（二）商品的性能、功能、产地、用途、质量、规格、成分、价格、生产者、有效期限、销售状况、曾获荣誉等信息，或者服务的内容、提供者、形式、质量、价格、销售状况、曾获荣誉等信息，以及与商品或者服务有关的允诺等信息与实际情况不符，对购买行为有实质性影响的；（三）使用虚构、伪造或者无法验证的科研成果、统计资料、调查结果、文摘、引用语等信息作证明材料的；（四）虚构使用商品或者接受服务的效果的.....。
夸大和虚假宣传问题	借助**展会、论坛**等行业活动及网络营销宣传活动，**制造、炒作话题**，造成行业及社会不良影响。	《反不正当竞争法（2025修订）》第9条：经营者不得对其商品的性能、功能、质量、销售状况、用户评价、曾获荣誉等作虚假或者引人误解的商业宣传，欺骗、误导消费者和其他经营者。 经营者不得通过组织虚假交易、虚假评价等方式，帮助其他经营者进行虚假或者引人误解的商业宣传。

恶意诋毁攻击问题	以遏制、打压竞争对手为目的，**诋毁**攻击汽车企业或者汽车产品，**抹黑**企业声誉或者商品声誉，对企业进行**恶意投诉**。 组织、操纵网络水军、“黑公关”“黑嘴”及“饭圈”粉丝，联动发布涉汽车企业及企业家的**虚假、负面信息，煽动网民情绪**，打“口水战”，恶意抹黑竞争对手。 汽车企业**高管**利用自身影响力在网上**“拉踩”引战**。	除前述《网络信息内容生态治理规定》外，《反不正当竞争法（2025修订）》第12条：经营者不得编造、传播或者指使他人编造、传播虚假信息或者误导性信息，损害其他经营者的商业信誉、商品声誉。 《刑法（2023修正）》第246条：以暴力或者其他方法公然侮辱他人或者捏造事实诽谤他人，情节严重的，处三年以下有期徒刑、拘役、管制或者剥夺政治权利。

B. 网络平台关注事项

《通知》强调：

网络平台企业要深入开展自查自纠，加强对采用生成式人工智能技术等的网络水军、“黑嘴”的甄别管控，健全平台涉企侵权信息投诉举报、争议标签、一键关联辟谣内容等产品功能，防止虚假信息误导公众。

行业协会要引导行业加强自律建设。

汽车企业要深入开展自查，自觉抵制网络水军、“黑公关”“黑嘴”及“饭圈”粉丝等网络乱象。要形成合力，持续净化汽车行业网络舆论环境。

海问评述：

《通知》提及的行业乱象，在相当一部分内容场景，与少部分自媒体的不当活动直接相关。

网信办曾多次对自媒体内容监管采取专项行动。例如，今年7月，网信办发布《关于开展“清朗·整治‘自媒体’发布不实信息”专项行动的通知》，要求重点整治四类突出问题：恶意蹭炒误导公众问题，多种手段歪曲事实问题，不做标注以假乱真问题，专业领域信息不实问题II。其中相当一部分问题，在本次《通知》所指场景中也较为突出。

因此，对于汽车企业而言，需要根据《通知》要求，针对典型的网络场景进行自查自改，包括注意：

进行商品和服务宣传时，形式上无论是通过企业主导的展会或论坛，或是企业日常运营发布的商业广告，或是企业高管、人员自身的社交平台，都应注意**宣传的真实性**，特别是对汽车、动力电池的性能、功能、质量、销售状况等进行真实描述，**避免夸大宣传或使用虚假数据进行宣传**。

在与外部广告机构、测评/榜单机构、网红大V等合作宣传时，应避免夸大宣传或使用虚假数据进行宣传，同时避免对竞争对手进行抹黑、诋毁等行为，建议在与外部广告机构、测评/榜单机构、网红大V签订合作合同时，**明确宣传行为、手段、内容的合法合规性要求**，明晰双方责任边界。

2、网络安全体系的“神经末梢”重塑：网络安全事件报告管理

《网络安全法》第25条明确，网络运营者应当在发生危害网络安全的事件时，按照规定向有关部门报告。

此前，多个地方以及多个推荐性标准规定了网络安全事件的报告要求。总体规则较为零散，其中相当一部分也不具有强制约束力。

另外，网络安全事件发生后，报告本身至关重要，但由于体系性、强制性的报告规则一直缺位，所以企业在发生网络安全事件后，对于报不报、什么时候报、怎么报，往往感到困惑、摇摆不定，无形中增加了决策时间和成本，也间接影响了网络安全事件的及时报告和有效解决。

2025年9月11日，网信办发布《国家网络安全事件报告管理办法》（“**《办法》**”），自2025年11月1日起施行III。

《办法》要求，网络运营者（网络的所有者、管理者和网络服务提供者）在发现或获知涉及本单位的网络安全事件（由于人为原因、网络遭受攻击、网络存在漏洞隐患、软硬件缺陷或故障、不可抗力等因素，对网络和信息系统或其中的数据和业务应用造成危害，对国家、社会、经济造成负面影响的事件）时，应当按照《办法》附件《网络安全事件分级指南》进行研判，属于特别重大网络安全事件、重大网络安全事件、较大网络安全事件的，按照《办法》进行报告。流程如下：

报告主体	报告时限	上报部门	报告内容
涉及关键信息基础设施的网络运营者 属于中央和国家机关各部门及其直属单位的网络运营者	第一时间，最迟不得超过1小时及时，最迟不得超过2小时	保护工作部门、公安机关 本部门网信工作机构	（一）涉事单位名称及涉事系统或设施基本情况； （二）网络安全事件发现或发生的时间、地点、类型、级别，以及已造成的影响和危害，已采取的措施及效果；对勒索软件攻击事件，还应当包括要求支付赎金的金额、方式、日期等； （三）事态发展趋势及可能造成的进一步影响和危害； （四）网络安全事件原因初步分析意见； （五）溯源调查工作线索，包括但不限于可能的攻击者信息、攻击路径、存在的漏洞等； （六）拟进一步采取的应对措施以及请求支援事项； （七）网络安全事件现场保护情况； （八）其他应当报告的情况。
其他网络运营者	及时，最迟不得超过4小时	属地省级网信部门	对于规定时间内不能判定事发原因、影响或发展趋势等网络安全事件情况的，可先报告第一项、第二项内容，其他情况及时补报。 网络安全事件报告后出现新的重要情况或调查工作取得阶段性进展的，涉事单位应当及时报告。 网络安全事件处置工作结束后，网络运营者应当于30日内对相关事件发生原因、应急处置措施、造成的危害、责任追究、完善整改情况、教训等进行全面分析总结，形成事件处置总结报告按照原渠道上报。

违法后果：网络运营者未按规定报告网络安全事件的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。因网络运营者迟报、漏

报、谎报或者瞒报网络安全事件，造成重大危害后果的，对网络运营者及有关责任人依法从重处罚。

海问评述：

根据《网络安全法》的要求，网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。《办法》细化了向主管部门进行报告的具体时限要求。汽车企业应当关注并将《办法》提出的报告时限落实进本企业已有的网络安全事件应急预案制度文件中。

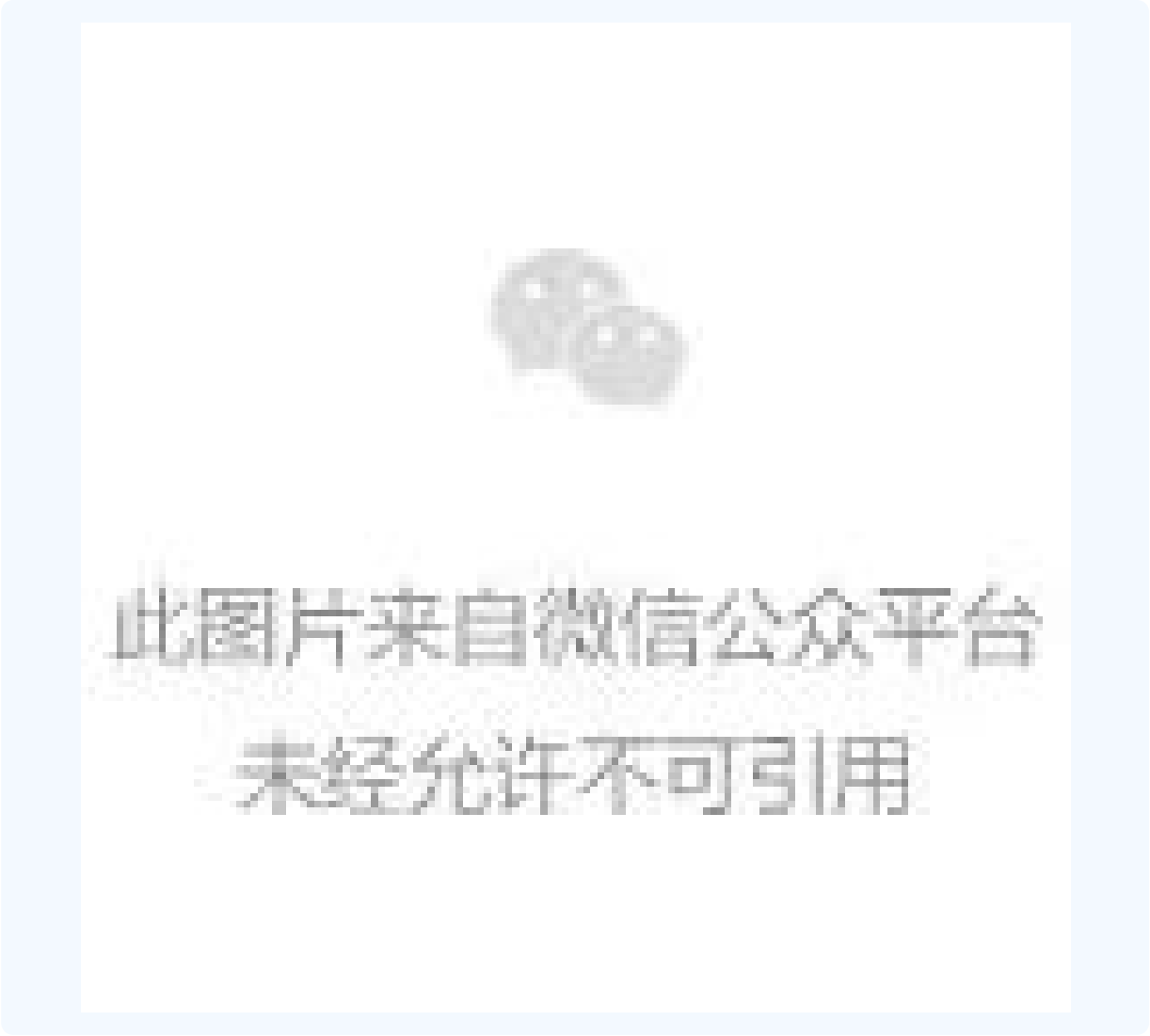
同时，汽车企业还应当关注本行业特殊的应急要求，例如根据《工业和信息化领域数据安全事件应急预案（试行）》的规定，工业和信息化领域数据处理者认为可能发生较大及以上数据安全事件的，应当立即按的要求向地方行业监管部门报告。涉嫌违法犯罪的，还应当及时向公安机关报案。

3、APP个人信息保护的持续关注：泛汽车出行领域多家经营者APP被通报

国家计算机病毒应急处理中心于2025年9月10日发布《国家计算机病毒应急处理中心检测发现69款违法违规收集使用个人信息的移动应用》，检测发现69款APP存在违法违规收集使用个人信息情况IV。

本次通报中**出行服务类小程序的违规问题尤为突出**。此类小程序收集用户的姓名、联系方式、出行路线等个人信息，涉及信息量大且敏感度高。在过往实践中，部分企业可能注意到APP个人信息保护合规的重要性，但是没有意识到小程序在此领域的监管要求与APP相同，或者没有给予足够的重视程度，导致小程序中的个人信息保护问题反而容易成为盲区。

海问评述：



4、网联汽车测绘地理信息安全新探索：《上海市智能网联汽车测绘地理信息安全管理导则（试行）》

2025年8月23日，上海市规划和自然资源局发布《上海市智能网联汽车测绘地理信息安全管理导则（试行）》（“**《导则》**”），提出地方层面测绘地理信息安全合规具体路径V。

《导则》适用于上海市智能网联汽车高精度地图应用试点及“车路云一体化”应用试点中涉及的测绘地理信息安全工作，上海市其他智能网联汽车相关工作可以参照适用。

A.《导则》规定了具体的主体责任

主体	责任

依法取得导航电子地图制作测绘资质的单位（“**图商**”）	作为测绘活动的实施主体，是测绘地理信息安全的责任主体。具体业务中，出资方应获得导航电子地图制作资质或委托图商主导，协议形成“车、路、云、网、图”测绘地理信息多方合作架构，开展安全合规的智能网联汽车测绘活动和地理信息应用。 图商应结合自身在智能网联汽车领域的业态特点，扎实开展安全合规能力建设，主动承担多方合作架构的测绘地理信息安全协调工作，对可能存在的安全风险保持关注，确保风险防控手段持续改进。 图商作为测绘地理信息多方合作架构的主体，应与主管部门保持必要的沟通，主动及时告知智能网联汽车所涉及的测绘活动。
开展智能网联汽车测绘活动或利用地理信息数据成果的**车企、服务商及智能驾驶软件提供商**	应建立健全地理信息数据全流程安全管理制度，在车端、云端、网端、应用等方面积极配合图商，在确保测绘地理信息安全的基础上促进自动驾驶产业持续健康发展。

对于保障体系的建设，在实施主体能力建设方面，《导则》明确，多方合作架构中，各企业应贴合自身业务场景，在组织建设能力、制度建设能力、技术应用能力和人员业务能力四个方面提升测绘地理信息安全保障能力。**图商应牵头提供解决方案**，协助多方合作架构中其他相关企业建立完善的测绘地理信息安全保障措施。

在监督主体机制建设方面，为配合主管部门对智能网联汽车测绘地理信息的全链条监管，在上海市开展智能网联汽车测绘活动前，**图商应将业务形态、技术条件、采集目标、数据规模、触发策略、路线规划、数据应用等情况告知市规划资源部门。**在进行事中风险防控时，图商应在车端、云端建立企业级测绘地理信息安全风险防控体系，以地理围栏、数据审计、态势感知等方式开展风险预警监测和数据全周期跟踪,为主管部门留有数据审查和报告报表接口。

在安全防控技术应用方面，为实现智能网联汽车数据全流程闭环，总体策略上，多方合作架构中各企业应做到数据即时安全处理、数据采集最小必要、地理信息脱密脱敏、数据分类分级管理、数据安全可控保障、事故即时应急响应。

B.《导则》针对数据全生命周期安全提出了具体要求

环节	要求
采集	智能网联汽车地理信息数据回传采集应遵循触发式原则，在地理围栏的范围内，仅在发生交通安全事件、自动驾驶接管事件、地图要素变化等特定策略下执行，确保**数据采集的必要性和最小化**。数据成果来自多项传感器的，应确保可解耦和可视化，必要时可被审查。 车端地理信息数据的存储、传输、处理应按相关技术标准设置参数并执行。**地理信息数据出车前，应按照国家认定的地理信息保密处理技术进行安全处理后，并使用商用密码加密向车外传输。**
传输	智能网联汽车地理信息数据应基于**国密算法建立安全传输链路**，直接传输至图商管理的数据中心或云服务器。传输链路应可以被验证。应设置位置判断服务，数据覆盖空间范围在非涉密涉敏区域的数据方可进行回传。 向路侧设备进行传输时，应按数据集最小、空间范围最小、时长最短进行必要传输。

数据中心或云服务器必须至少满足**网络安全等级保护第三级**的要求，并取得相应的认证。用于存储、处理地理信息数据的业务系统，需通过商用密码应用安全性评估测评，确保数据的安全处理。在进行跨云互通、多云互通时，防火墙的配置应遵循最小必要原则，仅开通必要的IP/域名和端口，以减少潜在的安全风险。

数据中心或云服务器分为**图商管理使用的安全专有云区域和车企等应用方使用的合规云区域**。

存储

- **安全专有云是由图商进行完全管控的数据中心或云服务器**，是智能网联汽车测绘活动数据成果回传的第一落点。图商应对安全专有云负有完全的管理和运营责任，全程控制建设过程、云资源配置、各类网关情况，有完全、独立的控制权,确保抵御恶意攻击和对数据事故的预警处理能力。图商在该区域对数据进行审查、验证、清洗、过滤，确保数据合规安全后方可向合规云区域单向传输。安全专有云一般不进行数据的大量存储、汇聚和应用。
- **合规云是数据成果应用的合规空间**，由图商进行监管。图商应搭建全面的监控审计系统，掌握该区域中的数据进出流向、算力资源配置、数据访问权限、数据应用业务、其他数据注入等情况，关注各类应用中的测绘地理信息安全风险，杜绝境外访问和传输。在合规云中，可存储、汇聚、应用经安全处理后的地理信息数据，原则上不向外传输。确需数据出云的，应以确保数据始终安全为原则，在有图商提供的安全管理环境之下进行交接、存储、应用。

智能网联汽车测绘活动的数据成果一般包括位置类、点云类、影像类、惯导类、构图类等。形式上和其它数据融合的，应按“就高就严”原则进行安全处理。

处理

图商在安全专有云内对数据集（数据流）开展安全处理，技术上包括但不限于关键内容模糊、数据切片、数据抽取等。图商应在确保安全处理质量的基础上，提升处理效率，缩短数据在安全专有云中的存储周期。

应用

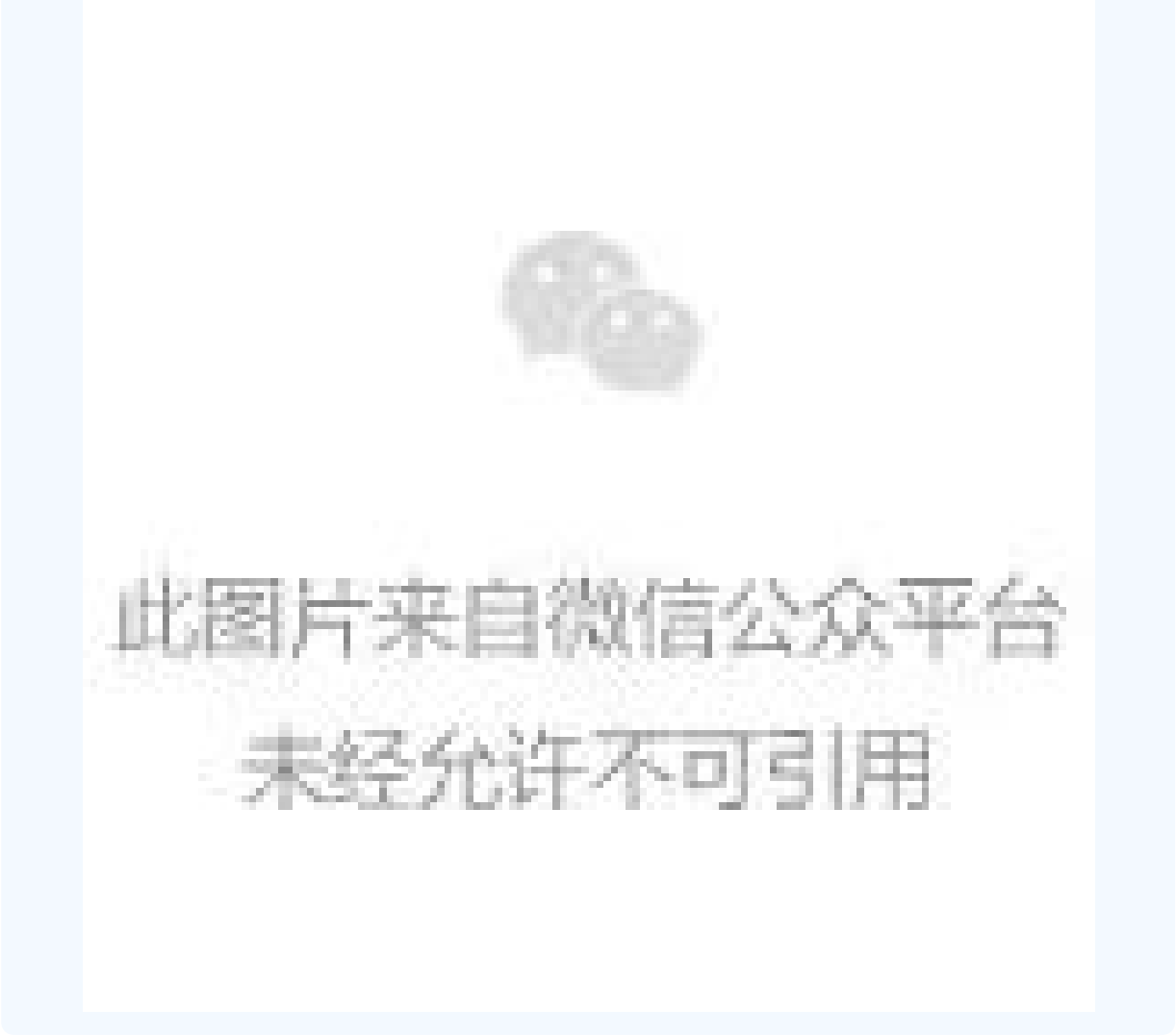
与图商和车企等其他数据应用方在合规云区域开展各类应用。数据成果的应用主要包括导航电子地图、数据标注、人工智能算法训练、孪生模拟、仿真测试等。导航电子地图制图和更新时，应基于安全处理后的数据进行构图，确保表达符合规范要求的地理信息。数据标注应用时，应将影像、点云等数据进行切片、抽取及在线发布，标注团队不直接接触全量数据集。自动驾驶模型训练时，不应针对涉密敏感目标识别进行算法训练。数字孪生测试应用时，应基于安全处理后的数据建立场景库。

发布

现阶段，地理信息数据应以导航电子地图的形式向车端发布。图商应建立健全企业内部的地图安全审校制度，利用技术工具生成审校报表。发布前应提交地图审核，取得审图号后方能发布使用。

海问评述：

《导则》为企业开展测绘地理信息数据处理和应用等活动提供了明确的操作指南和安全底线。对于智能网联汽车行业的参与主体企业（包括但不限于图商、车企、服务商及智能驾驶软件提供商）而言，在合作模式、服务器部署和数据处理活动等环节均应落实合规要求，主要包括：



5、智能网联汽车领域强制性标准进一步推进

2025年9月17日，工业和信息化部公开征求《智能网联汽车　组合驾驶辅助系统安全要求》强制性国家标准（“**标准**”）的意见VI。

其中，组合驾驶辅助系统（“**系统**”）是指在其设计运行条件下持续地执行动态驾驶任务中的车辆横向和纵向运动控制，且具备与所执行的车辆横向和纵向运动控制相适应的部分目标和事件探测与响应能力的硬件和软件所共同组成的系统。

随着组合驾驶辅助系统的广泛应用，其安全能力愈发受到社会各界的广泛关注。在此背景下，标准为强化组合驾驶辅助系统行业管理提供关键技术支撑。

标准适用于安装有基础单车道组合驾驶辅助系统、基础多车道组合驾驶辅助系统、领航组合驾驶辅助系统的M类、N类汽车（即至少有四个车轮并且用于载客/载货的机动车辆。具体参见GB/T　15089-2001《机动车辆及挂车分类》），并在多个方面提出了具体要求。

1.明确功能性能	
主要方面	**具体要求**
严格限定设计运行条件激活范围	系统仅能在设计运行条件内激活： • 基础单车道组合驾驶辅助系统、基础多车道组合驾驶辅助系统仅可在A类道路环境（高速公路及快速路）激活。 • 领航组合驾驶辅助系统可在A类道路环境和/或B类道路环境（A类道路环境以外的道路环境）激活，但需针对不同道路环境补充对应的探测与响应能力（如B类道路环境需额外探测交通信号灯、非机动车等元素）。
分层设定系统功能合规要求	基础单车道组合驾驶辅助系统、基础多车道组合驾驶辅助系统需符合GB/T 44461.1—2024《智能网联汽车 组合驾驶辅助系统技术要求及试验方法 第1部分：单车道行驶控制》、GB/T 44461.2—2024《智能网联汽车 组合驾驶辅助系统技术要求及试验方法 第2部分：多车道行驶控制》相关要求，同时需满足驾驶员状态检测、提示信号清晰可辨等人机交互要求等。 领航组合驾驶辅助系统需具备限速控制辅助能力（如持续显示道路限制速度与驾驶员设置车速、车速超限时发出声光提示）等与其他交通参与者的合理交互能力，且需针对我国交通特征构建交叉口通行、施工区域绕行等试验场景，通过场地试验、道路试验与文件检验三重验证，确保系统对复杂交通场景的适配性。

2.强化过程管理要求	
主要方面	**具体要求**
清晰界定系统功能边界与能力阈值	明确系统的功能范围（如基础单车道系统仅辅助单一车道内行驶、基础多车道系统仅辅助相同行驶方向的车道间换道）、能力上限（如横向加速度限值：M1类汽车不大于3m/s²，M2、M3类汽车不大于2.5m/s²）。 同一型式判定时，若涉及系统的相关视同条件变更，需按要求完成补充测试与审批。
建立科学完整的安全保障方法	要求车企建立主动的安全风险管理能力，以评估并缓解组织、人员和技术层面的风险。 在研发阶段，需建立设计与开发流程，包括安全设计、需求管理、需求实施、测试、失效追溯、改进和发布的开发流程；在生产阶段，需具备生产管理流程，记录生产过程和活动，以保障生产阶段的稳健性；在运行阶段，需具备安全监测与管理的能力，并符合智能网联汽车安全事件数据交互与管理系统国家标准的相关要求。

3.规范系统使用方式	
主要方面	**具体要求**

确保驾驶员持续参与动态驾驶任务	领航组合驾驶辅助系统的设计应使驾驶员持续地执行相应的动态驾驶任务，在任意时刻响应驾驶员执行的有效运动控制干预或退出系统的操作，并符合相关要求。
严格系统激活的前置条件	车辆每次上电/点火后（发动机自动启停除外），系统不应处于激活状态。 系统应识别驾驶员完成系统的使用培训（通过生物识别或账号登录验证），且确认驾驶员已阅读并理解系统使用说明（该确认环节需驾驶员在车辆静止时完成至少两个独立动作）后才允许进入激活状态。
强化驾驶员状态检测与违规禁用	系统需具备手部脱离检测与视线脱离检测能力，车速大于10km/h时： • 手部脱离转向盘后最迟5秒发出手握转向盘提示（“**HOR**”），未响应则10秒内升级提示。 • 视线偏离驾驶区域后最迟5秒发出视线回归提示（“**EOR**”），未响应则3秒内升级提示，仍未响应则5秒内发出立即控制警告（“**DCA**”）。 • 领航组合驾驶辅助系统发出升级的HOR或DCA后10秒内触发风险减缓功能（“**RMF**”）。 若因驾驶员脱离导致系统触发1次RMF，或持续发出10秒升级的HOR或EOR（若不具有RMF），或系统发出2次EOR升级后的DCA，或30分钟内出现3次升级的HOR或升级的EOR，系统需在当前上电/点火周期内禁用至少30分钟，且禁用期间需提示驾驶员重新阅读使用说明。

海问评述：

标准为组合驾驶辅助系统的安全划定了红线，不仅关注传统的功能安全（避免系统故障导致危险），更强调了 “预期功能安全” 和 “人机交互安全”。对此，车辆生产企业应当关注将标准要求融入产品规划和研发顶层设计，确立“安全优先”原则；在开发中强化设计运行条件的范围、人机交互流程，确保安全贯穿始终；增加复杂场景测试，并发展虚拟仿真以覆盖“长尾问题”，提前进行符合性验证。

[I]参见https://www.miit.gov.cn/jgsj/zbys/qcgy/art/2025/art_c9a25877b2e04ca5a19ba8e878210ed2.html。

[II]参见https://www.cac.gov.cn/2025-07/29/c_1755503642582366.htm。

[III]参见https://www.cac.gov.cn/2025-09/15/c_1759583017717009.htm。

[IV]参见https://www.cverc.org.cn/zxdt/report20250910.htm。

[V]参见https://ghzyj.sh.gov.cn/zcwj/chgl/20250825/7fb303a0931747f9a4f24b34dc4bfe60.html。

[VI]参见https://wap.miit.gov.cn/jgsj/zbys/qcgy/art/2025/art_b4c467db98344caaaed2ff97b56cc3dd.html。

2025-10-20