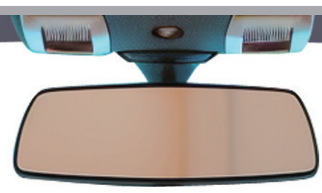

智能驾驶只是它的“幌子”！

国安通报非法测绘背后：智能驾驶涉及哪些敏感数据？企业如何确保合规安全？

事　件

国安部：境外企业以汽车智驾为由非法测绘

智能汽车数据采集和出境问题再度引发社会关注。

10月16日，国家安全部微信公众号发文称，近年来，随着国家安全机关加大对非法测绘活动的打击力度，部分境外组织逐步转向与国内企业开展所谓项目合作逃避监管，非法采集我国原始测绘数据，威胁我国家安全。国家安全机关工作发现，某境外企业A公司通过与我国具有测绘资质的B公司合作，以开展汽车智能驾驶研究为掩护，在我国内非法开展地理信息测绘活动。

公告一出，引发不少网友将事件关联相关新能源车企、智驾企业以及图商。随后，极氪（吉利旗下的新能源车品牌）、特斯拉两家车企，智驾企业Mobileye（以色列高级驾驶辅助系统（ADAS）和自动驾驶解决方案的提供商），以及图商北京四维图新科技股份有限公司紧急发布声明进行辟谣。

理想L6 Pro、阿维塔12、问界M7（从上至下）。

来源互联网 新能源观截图

回　应

●**吉利**　10月16日晚间，吉利控股集团高级副总裁杨学良在微博回应，称此事“跟极氪无关，也不是极氪合作伙伴所为，谣言止于智者”。

●**特斯拉**　10月16日晚间，特斯拉对外事务副总裁陶琳发布微博表示，合规是企业经营的底线，“特斯拉始终相信：合规的智能化才是可持续发展的智能化。”

●**四维图新**　10月16日晚间，@四维图新发文称，四维图新始终秉承合法、合规办企原则，坚决反对一切抹黑、中伤公司名誉的网络谣言，并将采取必要的法律手段进行捍卫。

●**滴滴**　17日，滴滴方面回应称此事“与滴滴无关”。

●**Mobileye**　17日，Mobileye在微博声明称，在包括中国的相关国家和地区，公司在具备相关资质的合作方监督下全面依法经营。Mobileye严格遵守所有相关法律法规。

目前，汽车已由传统出行工具逐渐转变为移动智能终端。搭载大量传感器技术、5G通信技术、V2X以及人工智能技术，智能汽车正成为移动的数据采集器和数据库。

近日，中国汽车工业协会常务副会长兼秘书长付炳锋在第六届数字中国建设峰会数字安全分论坛上表示，L4级自动驾驶汽车每日产生的数据是传统汽车的5—10倍，而且根据相关机构预测，在2030年前后自动驾驶和辅助驾驶乘用车渗透率有望达到90%以上。他强调，汽车数据安全重要性愈发凸显。

汽车行业大数据和人工智能应用企业高科数聚的数据生态与品牌战略副总裁许璐在接受记者采访时表示，地图测绘作为国家战略性资源，其重要性不仅体现在国家安全层面，还与经济发展和社会治理密切相关。在大数据时代背景下，数据安全已成为一个涵盖个人隐私、商业秘密及国家安全等多方面因素的综合性问题。

01 地图测绘资质管理严格 车辆“测绘”或有涉军等风险隐患

近年来，智能驾驶已成为高精地图的重要应用场景。

高精度地图与车联网技术紧密相连，通过激光雷达、摄像头等传感器收集的定位数据，结合车联网的数据处理能力，不仅能够构建和更新地图，还能通过实时数据丰富地图内容，提升地图的准确性和实时性。

业内人士向记者透露，高精度地图绝对精度常在1米以内，横向相对精度在理想状况下可达厘米级，对于自动驾驶的精确定位至关重要。

我国对高精度地图的采集有十分严格的资质管理，相关规定显示，只有拥有甲级电子导航地图测绘资质的企业才能进行数据采集和生产。

自然资源部网站显示，自然资源部于2022年2月、3月、8月先后分三批公布了最新的导航电子地图制作甲级测绘资质复审换证的结果，共有19个单位通过资质复审。而复审前则共有31家单位，这一数字的缩小也直观地表明当前政策缩紧的趋势。

为何地图测绘对于国家安全如此重要？根据我国法律规定，测绘地理信息的原始数据由于可能涉及军事重地、要害部门等高精度测量信息，存在被境外用于标记我关键核心部位的风险隐患。为确保测绘过程中原始数据安全可控，《中华人民共和国测绘法》《中华人民共和国测绘成果管理条例》中有专门细化规定，要求测绘主体除必须拥有测绘资质外，还应严格落实数据保密管理的责任。

目前，市场上的主要参与者包括百度、四维图新和高德，这几家企业占据了市场的大部分份额。

需要注意的是，有图商负责人向记者指出，因节约地图授权使用成本等因素，目前不少车企宣称采用不依靠高精地图的无图智驾方案。但车载摄像头和激光雷达等传感器对周围道路环境建模也是“现场画图”，严格来看，同样属于“测绘”行为，相关数据安全问题值得关注。

02 本地化储存 车企跨境数据安全解决之道

除了非法获取测绘数据，该起违法事件还涉及一个重要方面，就是跨境数据传输。

公告提及，为尽可能直接获取原始测绘数据，A公司越过项目转包的层层节点，重点把控测绘数据的存储、处理和流转等环节。最后在A公司的操控指使下，B公司将测绘所得数据转移出境。

许璐表示，就跨境数据流动监管来说，特别是对于涉及公民个人信息的内容，除非出于特定目的并得到当事人认可，否则原则上禁止将其转移至境外；此外，像地质构造图、交通网络布局图这类看似无关紧要但实际上可能影响国家战略利益的信息同样需要受到严密管控。

近年来，为保障数据跨境安全、合规流动，国家网信办等相关部门频繁出台与数据跨境流动相关的政策法规。

2021年，中国接连颁布了《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》两部法律；《数据出境安全评估办法》正式实施；2024年3月22日，网信办发布《促进和规范数据跨境流动规定》，对现有数据跨境制度的实施和衔接作出了进一步明确。

数据的本地化储存是目前车企普遍使用的数据安全保护方式。

作为第一家进入中国的外商独资汽车制造商，特斯拉也曾因跨境数据传输问题引发不小争议。而目前，特斯拉已实现了数据的本地化存储。

特斯拉方面表示，已于2021年成立特斯拉上海数据中心，实现数据本地化存储。此外，特斯拉引入第三方权威机构对公司信息安全管理制度进行审核，并通过安全管理体系认证（ISO27001）。

同样，路特斯科技也建立了中国数据中心。路特斯方面表示，为满足各地区和国家数据跨境及数据本地化存储的合规要求，建立了全球数据中心架构布局，在全球已建立或规划五个数据中心，分别位于中国、德国、美国、新加坡和阿联酋。

03 个人隐私、商业机密……这些数据同样有潜在风险

作为一种可随意移动的终端，智能网联汽车的数据可谓包罗万象，其重要数据主要包括三大类：车辆运行状态数据、道路环境和人员数据、车内人员隐私数据。数据不仅仅作为企业研发而用，驾驶数据还关系到公共安全、国家安全，以及个人隐私保护等问题。

许璐向记者表示，智能汽车数据安全保障的首要任务是保障数据在其整个生命周期内的完整性与机密性，即保证不被窃取。这要求采用先进的加密技术以及严格的访问控制措施，防止任何未经授权的第三方获取敏感信息。

针对消费者个人隐私保护，她表示，商业活动中，对消费者个人信息的收集与处理必须严格遵守相关法律法规，并获得用户的明确同意。未经许可不得随意公开或转售此类信息给第三方机构。

对于车企来说，商业机密防护同样不可忽视。许璐认为，当多个企业通过同一平台共享业务数据时，如何有效隔离彼此之间的核心资产显得尤为重要。以汽车行业为例，各大制造商可能会将自身研发成果、市场表现等相关指标上传至云服务提供商处以便于分析比较。此时，该服务商有责任确保这些珍贵资源不会泄露给竞争对手或其他非授权用户。

监管方面，当下，智能网联汽车数据安全问题已经受到有关部门的高度重视。

近期，工信部组织制定的《汽车整车信息安全技术要求》《汽车软件升级通用技术要求》和《智能网联汽车自动驾驶数据记录系统》三项强制性国家标准发布，涉及外部连接安全、通信安全、软件升级安全、数据安全等方面的技术要求和试验方法，将于2026年1月1日起实施。

从技术角度来看，有业内技术人士向记者介绍，数据脱敏目前已成为实现智能网联汽车数据安全的关键手段。

数据脱敏指的是通过采取有策略地修改或替换原始数据的方式，进而生成一个看似真实却不含有敏感信息的数据副本，以便在非生产环境（像开发、测试以及分析等场景）中使用，例如对行人脸部、机动车号牌进行遮挡处理等。其核心要点在于，在降低数据敏感程度的同时，还能够维持数据的业务价值与可用性。

该业内人士表示，通过对敏感数据进行处理，可以降低数据在各个环节被攻击和窃取的风险。在智能汽车领域，车辆数据经过脱敏后，即使被非法获取，也难以从中提取出有价值的敏感信息，进而可以保护用户隐私和车辆安全。

据澎湃新闻、中国青年报等