汉坤法律评述
2025 年 2 月 21 日

HANKUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

北京 | 上海 | 深圳 | 香港 | 海口 | 武汉 | 新加坡 | 纽约

智驾资本论：自动驾驶企业投融资法律要点概览（下）

作者：吴晓雪 | 万可 | 李熹曦[1]

在此前的《*自动驾驶企业投融资法律要点概览（上）*》中，我们已经梳理与分析了自动驾驶企业从股权架构的搭建到各类业务资质的获取与安排的要点。本文将继续聚焦知识产权保护与数据安全的要点与审查，全面呈现自动驾驶企业在这两个关键领域的核心关注点和应对策略。

一、知识产权保护

自动驾驶技术融合了软硬件与智能化的多元特性，这类技术具有独特的“复合”特质，往往需要企业持续投入大量资源进行开发、优化与积累。在感知层面，激光雷达、毫米波雷达与摄像头图像识别专利，使车辆能敏锐捕捉环境细节，准确辨别物体与路况；在定位导航方面，高精度地图及多传感器融合定位专利，让车辆在任何环境都可精准锁定自身位置与规划路径。因此，在自动驾驶这一高度技术密集且竞争白热化的领域中，知识产权无疑是企业的核心竞争力与发展基石。

（一）无形资产权属审查

1. 从投资者的角度，一般需重点考察自动驾驶公司已申请和获批的知识产权数量，这是衡量公司技术创新成果规模的直观指标。在知识产权类型方面，需全面覆盖自动驾驶的核心技术领域，包括感知层的激光雷达、毫米波雷达及摄像头图像识别技术相关专利，定位导航领域的高精度地图与多传感器融合定位专利，决策算法、控制逻辑等软件著作权，以及公司或公司产品相关的商标、字号等。此外，投资者还需深入审视知识产权的地域覆盖范围，特别是在全球主要汽车与科技市场的布局状况尤为关键，这直接关联到公司在国际竞争格局中构建知识产权壁垒的能力以及应对风险的防御水平。

2. 对于公司委托第三方开发或者与第三方合作开发的知识产权，需仔细审查相关合同条款，明确不同情形下开发成果的权利归属界定是否清晰合法，有无潜在争议风险点，以及是否存在过往或潜在的归属纠纷，确保公司在各类开发合作中对核心技术资产拥有明确且合法的所有权或使用权。

（二）核心技术人员关联审查

核心技术人员的稳定性与是否存在知识产权或劳动纠纷也是需要关注的重点：

[1] 实习生陈镜桐对本文的写作亦有贡献。

1. 公司与核心技术人员签订的劳动合同或合作协议中，是否包含清晰明确的知识产权归属条款、保密协议及竞业禁止协议；

2. 全面梳理历史上离职的研发人员或关键员工是否带走公司核心技术与公司机密；

3. 对于从其他公司跳槽来的核心技术人员，需了解其原单位的研发项目与成果，确认是否存在竞业限制义务以及加入本公司是否合法合规，防范潜在的知识产权侵权风险与纠纷隐患；

4. 核心技术人员若为高校、科研院所的相关人员（兼职或离岗创业），还需进一步关注高校院所内部规章制度或劳动合同的限制、是否履行所在高校的审批流程，核心技术是否使用高校相关人员的职务发明，高校相关人员在公司和高校/科研院所之间的工作任务、精力分配是否存在冲突，公司是否具有独立研发的能力等。

（三）保密政策与商业秘密保护审查

公司的保密政策与商业秘密保护制度是预防公司核心技术流失与重要信息泄露的关键防线。保密制度文件应涵盖技术研发、生产运营、客户信息等关键环节保密规定，且应明确保密范围、期限及违约责任。此外，公司也应重视保密培训开展情况与保密措施执行状况，如对涉密信息存储、传输、使用的管控手段，是否采用加密技术、访问限制等，公司与外部主体合作合同中是否包含保密条款以及商业活动中可能的泄密风险点防范情况，确保公司商业秘密与知识产权在严格保密机制下得到有效保护，避免因泄密导致的竞争劣势与法律风险。

二、数据安全与合规

自动驾驶汽车通过持续采集各类数据来保障行车安全。其中涵盖关乎人身与交通安全的技术数据，也涉及到驾驶员或乘客的个人数据，以及周边无关行人、车辆的影像、视频等。例如，若干智驾公司的招股书中介绍，公司运营涉及收集、存储、传输和处理来自车辆、用户、员工、司机和第三方的数据，其中可能包括个人数据、机密信息或敏感信息。因而公司已实施数据保护政策，如数据分类政策和数据生命周期规范，以确保数据的收集、使用、存储和传输符合各司法管辖区（包括中国和美国）的适用法律。

（一）多维度的数据构成

自动驾驶汽车涉及的数据种类丰富，主要包括：

- 感知数据：摄像头捕获的视觉图像，激光雷达生成的三维点云地图，雷达检测的物体距离与速度信息，超声波传感器的近距离障碍数据，全方位感知车辆周边环境；
- 车辆运行数据：位置、速度、转向角度、制动状态、加速度等数据，反映车辆自身的行驶状态与操作情况，是决策与控制的关键依据；
- 地图与导航数据：高精度地图包含道路几何、车道、交通标志等信息，结合 GPS 数据确定车辆精确位置，用于路径规划与定位导航；
- 通信数据：与外界交互获取实时交通信息以便优化路线，接收软件更新数据来提升系统性能；
- 驾驶员数据：注意力、姿势及生理信号数据，用于监测驾驶员状态，保障驾驶安全或在必要时切换驾驶模式。

（二）多方面的法规体系

多维度的法律法规体系交织构建起数据合规的坚实框架，为自动驾驶汽车的数据处理活动锚定了清晰的规范路径与严格的准则要求。《网络安全法》《数据安全法》与《个人信息保护法》确立了收集、存储、传输与处理数据的基本原则，确保网络运营者开展经营和服务活动履行网络安全保护义务，落实数据安全保护责任，保护重要数据与个人信息。工业和信息化部发布的《关于加强智能网联汽车生产企业及产品准入管理的意见》则从行业准入端要求自动驾驶企业在数据安全管理等方面严控风险，筑牢合规根基。《汽车数据安全管理若干规定（试行）》（"**《若干规定》**"）针对汽车数据特性规范处理者义务，鼓励汽车数据依法合理有效利用，相关合规要求在《信息安全技术 汽车数据处理安全要求》（"**《汽车数据处理安全要求》**"）中得到细化。自然资源部于 2024 年 6 月 25 日发布的《智能网联汽车时空数据安全处理基本要求》《智能网联汽车时空数据传感系统安全基本要求》两项强制性国家标准公开征求意见，更是预示着未来自动驾驶汽车在时空数据处理与传感系统安全方面将有更为细致、严格的规范体系。

（三）信息保护的要点与审查

《若干规定》将收集、存储、使用、加工、传输、提供、公开过程中的汽车数据分为个人信息与重要数据两类。

1. 重要数据

重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益或者个人、组织合法权益的数据，包括但不限于军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等数据；车辆流量、物流等反映经济运行情况的数据；汽车充电网的运行数据；包含人脸信息、车牌信息等的车外视频、图像数据；涉及个人信息主体超过 10 万人的个人信息等。

《若干规定》要求自动驾驶公司等汽车数据处理者应对重要数据处理活动进行风险评估，并向相关政府部门报告。据公开信息显示，为符合《若干规定》的要求，部分自动驾驶公司在部分市场对其功能进行了调整，确保数据仅存储在车主的 U 盘中，不上传至云端，以此避免违反数据出境相关规定。《若干规定》要求，汽车数据处理者基于业务目的需要跨境传输重要数据时，汽车数据处理者需要通过网信办及其他相关政府部门组织的安全评估，不得提供超出安全评估范围的重要数据。因此，自动驾驶公司应确认对重要数据处理活动进行了风险评估并向相关政府部门报告；同时深入了解公司针对风险评估所识别出的各类风险，以及未知制定的应对策略与措施，以保障重要数据处理过程中的安全性与合规性。

2. 个人信息

个人信息的收集、存储、使用、加工、传输、提供、公开应注意以下合规要求：

- 收集个人信息应履行告知义务。自动驾驶汽车应通过用户手册、车载显示面板、语音、汽车使用相关应用程序等显著方式告知正在收集个人信息，且根据《汽车数据处理安全要求》的相关规定，应向个人信息主体告知各类型个人信息的保存期限（例如 30 天或 1 年）、个人信息保存的精确地点等。

- 车外数据匿名化处理。自动驾驶汽车在行进过程中需不断收集车外信息，因道路环境信息（走向、标志标线）与其他交通参与者特征数据（行人、车辆的相关状态），才能精准判断周边状况，做出驾驶操作。由于激光雷达、摄像头等设备所采集的车外数据，很难获得该等行人、车主的全部同意，

因此只能进行匿名化处理，包括删除含有能够识别自然人的画面，或者对画面中的人脸信息等进行局部轮廓化处理等。除个人信息外，车外视频中的人脸与车牌信息如果累计到一定量，还可能构成前文所讲的重要数据，在此情形下公司需要满足报送风险评估报告等要求。

- 默认不收集座舱数据。除非用户自主设定，车主每次驾驶时应默认设定为不收集数据的状态，包括不打开车内的摄像头、传声器、红外传感器和指纹传感器等部件，只有当驾驶人通过实体按键或触摸按键等方式主动选择后才能开始收集。

- 敏感个人信息处理的特殊要求。对于敏感个人信息[2]的收集、存储及使用，首先，必须取得个人单独同意而不得捆绑同意；其次，允许个人自主设定同意期限，而不应设置“始终允许”或类似的限制个人自主选择的选项，以保障个人对其敏感信息在时间维度上的控制权；再者，敏感个人信息的使用目的应直接服务于个人，包括增强行车安全、智能驾驶、导航等等；最后，需以适当方式提示收集状态，针对持续收集的情况要持续提示，对于不同敏感个人信息则应设置不同的提示方式，使个人能清晰知晓其敏感信息的收集进展与相关情况。

三、结语

随着科技发展的日新月异，以及自动驾驶技术在交通出行领域应用场景的不断拓展，其发展前景令人满怀期待，也同样面临着诸多法律合规的挑战与机遇。投资者在涉足自动驾驶企业的股权投资时，需严谨对待并全面掌握各方面法律要点，才能切实保障投资项目在合法合规的轨道上稳健前行，有力规避潜在的法律风险，与企业携手共创自动驾驶行业的辉煌未来。

[2] 根据《若干规定》，敏感个人信息，是指一旦泄露或者非法使用，可能导致车主、驾驶人、乘车人、车外人员等受到歧视或者人身、财产安全受到严重危害的个人信息，包括车辆行踪轨迹、音频、视频、图像和生物识别特征等信息。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

吴晓雪

电话： +86 21 6080 0566
Email： dana.wu@hankunlaw.com