

智能网联与自动驾驶法律评述（2025年6月）

作者：傅鹏 赵卿梦 包杰薇

1、汽车数据出境：场景化监管的良好示范

2025年6月13日，工业和信息化部等八部门公开征求对《汽车数据出境安全指引（2025版）》（以下简称“**《指引》**”）^[1] 的意见，**《指引》**基于《中华人民共和国网络安全法》《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》《网络数据安全管理条例》等法律法规，进一步细化和规范了汽车数据处理者开展数据出境活动的合规要求。

具体而言，**《指引》**梳理了汽车数据处理者常见的数据出境行为，规定了各类出境行为所适用的出境路径，以场景化分类的方式列举了出境活动中汽车业务场景的重要数据识别和判定规则，并且全面规范了数据出境的实施流程和数据安全保护要求。

海问评述：

A. 监管范围边界相对明晰，辐射汽车行业全链条全场景

《指引》规定的汽车数据处理者范围相较于《汽车数据安全管理办法（试行）》第3条规定的范围（即汽车制造商、零部件和软件供应商、经销商、维修机构以及出行服务企业等）有所拓展：新增列举了电信运营企业、自动驾驶服务商、平台运营企业，更全面地涵盖了涉及汽车数据出境活动的行业链条和场景，有利于行业内企业更清晰地理解自身是否适用该监管规则。

《指引》将行业实践中常见的涉及数据出境活动的两个业态纳入适用范围：自动驾驶服务商和平台运营企业。**《指引》**对该类企业提供了数据出境活动的具体实施规范，体现出**《指引》**对行业现实情况的关注和回应。

例如，较多自动驾驶服务商在境外开设分支机构或研发中心，服务于自动驾驶技术研发测试，涉及跨境科技研发协作和数据交流。把自动驾驶服务商明确纳入**《指引》**的适用

范围，有助于稳定企业的监管预期，也有助于更好地指导行业企业判断可以直接出境的数据类型，以及需要事先申报数据出境安全评估的数据类型。

B. 出境路径豁免：打通多项监管规则，洞悉业务刚需

《指引》第一部分“（三）数据出境路径”的第3条规定了免于申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的情形，整合了此前各项法律法规中涉及的数据出境豁免申报的相关规则，有利于企业整体把握和设计数据出境策略。

具体而言，《指引》列举的前5种豁免情形的核心精神来源于《促进和规范数据跨境流动规定》，包括：

- （1）在境外收集和产生的汽车数据传输至境内处理后向境外提供，处理过程中没有引入境内个人信息或者重要数据的；
- （2）为订立、履行个人作为一方当事人的合同，如跨境购车、跨境寄递、跨境支付、跨境注册账户等，确需向境外提供个人信息（不含重要数据）的；
- （3）按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息（不含重要数据）的；
- （4）紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息（不含重要数据）的；
- （5）关键信息基础设施运营者以外的汽车数据处理者自当年1月1日起累计向境外提供不满10万人个人信息（不含敏感个人信息和重要数据）的。

第6种豁免情形“**自由贸易试验区内登记注册的汽车数据处理者符合自由贸易试验区有关要求，向境外提供负面清单外的数据的**”则与《促进和规范数据跨境流动规定》第6条以及各自贸试验区的数据出境负面清单有关规定相呼应，为自贸区内的汽车数据处理者提供了更大的灵活性。对于汽车行业企业，如符合在特定自由贸易试验区登记注册并开展数据跨境流动相关活动等条件，当出境数据在负面清单外时可被豁免相关跨境数据流动备案程序：

适用的地域范围	汽车行业重要数据出境负面清单
中国（北京）自由贸易试验区 涵盖科技创新片区、国际商务服务片区、高端产业片区。[II]	1. 涉及军事管理区、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；在向政府机关、军工企业及其他敏感重要机构提供车联网信息服务过程中产生的不宜公开信息。 2. 车辆流量、物流等反映经济运行情况的数据。 3. 能够反映一定区域内汽车充电网运行情况的数据。 4. 包含人脸信息、车牌信息、路牌信息等的车外视频、图像数据。 5. 包含车辆远程操控、车辆工况等的关键车联网信息服务数据。 6. 包含车辆控制等在线升级数据；包含电控单元等售后数据。 7. 可能被利用实施对车联网关键设备、系统组件供应链的破坏，以发起高持续威胁等网络攻击相关的数据；可一定程度反映交通、运输等行业性关键信息基础设施网络安全保护情况，可被利用从而对车联网关键信息基础设施实施网络攻击的数据；涉及车联网信息服务的关键信息基础设施相关数据。[III]
中国（天津）自由贸易试验区 涵盖天津港片区、天津机场片区、滨海新区中心商务片区。[IV]	反映重要敏感区域的地理位置、作业状况，以及10万以上智能汽车消费者相关敏感个人信息的数据。如智能汽车运行过程中获取的军事管理区、国防军工单位、县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量数据以及OTA数据等。[V]

第7至9种豁免情形，可以认为是针对**汽车行业漏洞修补、技术升级**等“跨境刚需”场景量身定制的情形。

第7种和第8种情况中，特别对于外资车企而言，安全漏洞数据和安全事件数据往往需要向境外关联方传输，用于制作补丁、进行安全升级，并总体纳入集团产品安全策略进行考虑，在后续开发中进一步使用，提升汽车安全水平。

此类数据如果进行数据出境安全评估等程序，花费相对长的时间，也可能影响了安全漏洞的修补、安全策略的升级，提高“社会成本”。直接规定前述情形不需要进行申报，是基于务实的考虑。

第9种情形是关于因产品缺陷、实施召回需要而进行OTA升级的软件包源代码数据的出境豁免。

在此前智能网联汽车占比较低的时代，应用OTA升级不是产品缺陷、实施召回中常用的方式。近年来，随着智能网联汽车的快速普及，特别是许多辅助驾驶功能、驾驶控制功能的升级或者漏洞修补，主要通过OTA升级完成，所以OTA升级成为了智能网联汽车缺陷修补、产品召回的最为重要的方式。

因此，为传输给境外关联方进行总体研发、协调、测评和使用，软件包源代码数据出境趋于频繁。此类情形如果需要进行数据出境安全评估等手续，耗时较长，影响批量汽车的召回或者缺陷修复，也具有较高的“社会成本”，因此，《指引》将这一场景专门列入了豁免情形。

C. 数据出境规则语境下的重要数据识别：场景化规定与类型化的定性定量

场景化规定

《指引》以场景化的方式对重要数据进行了列举说明，分为研发设计场景（包括产品研发、产品测试）、生产制造场景、驾驶自动化场景、软件升级服务场景、联网运行场景（包括车辆数据、车路感知、车路分析、车联网平台运营）、其他符合判定规则的出境业务场景，涉及49个数据项。

场景化的方式有利于避免重复和遗漏，更便于企业理解监管实质，关注监管重点。对此，企业在重要数据识别和分类的过程中，需要重点考虑根据《指引》在场景中进行分类、评估和管理。

类型化的定性和定量

《指引》在场景化的基础上，进一步划分了具体的数据类别和数据项，在具体数据项中增加定性或者定量的“判定规则”，有利于指导企业相对明确地判断某些数据是否属于重要数据。

这一方式与此前地方工信部门采取的网联汽车和自动驾驶企业重要数据识别试点工作的方法一致，逻辑在于部分数据项的名称可能相近甚至相同，在场景中才能知悉数据项的具体指向。

例如，对于车辆识别码（VIN）数据项，限定为原始VIN、去标识化后且可还原的VIN，且自当年1月1日起向境外提供与其他出境信息结合可识别累计100万人以上个人身份的才构成重要数据。由此能从一个数据项中，真正筛选出重要的部分，真正体现出监管“重要数据”的目的和原因。

其他场景和边缘场景

需要注意的是，《指引》的最后一个场景规定“汽车数据处理者按照国家有关规定和行业标准规范识别、申报重要数据，工业和信息化部、国家网信办等相关部门公开或告知

企业属于重要数据的”，汽车数据处理者也需申报数据出境安全评估。

对于该兜底条款，企业需要结合地方主管机关（例如工信部门）开展的网联汽车和自动驾驶企业的重要数据识别和认定试点来一同准备。根据笔者的经验，部分地方主管机关也使用清单式的重要数据识别指导文件，且地方的清单和《指引》清单的具体要求和范围可能存在不一致，企业依旧需要根据地方主管机关具体使用的清单，开展重要数据识别。

2、车端应用：个人信息保护的持续关注

根据国家计算机病毒应急处理中心于2025年6月19日发布的《国家计算机病毒应急处理中心检测发现64款违法违规收集使用个人信息的移动应用》，检测发现64款移动应用存在违法违规收集使用个人信息情况，[VI] 其中，涉及多款车端应用的合规问题：

问题一	在APP首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；个人信息处理者在处理个人信息前，未以显著方式、清晰易懂的语言真实、准确、完整地向个人告知个人信息处理者的名称或者姓名、联系方式、个人信息的保存期限等。
提示关注	车端APP应当在首次运行时以合规方式提示用户阅读隐私政策等个人信息处理规则，并且确保隐私政策中说明了个人信息处理者的情况，并告知用户其个人信息保存期限等内容。
问题二	隐私政策未逐一列出APP（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式、范围等。
提示关注	车端APP如嵌入第三方的代码或插件（包括SDK、API等），收集、共享用户的个人信息，需要在个人信息处理规则中全面说明处理个人信息的目的、方式和范围。
问题三	通过自动化决策方式向个人进行信息推送、商业营销，未同时提供不针对其个人特征的选项，或者未向个人提供便捷的拒绝方式。
提示关注	车端APP如应用自动化决策进行信息推送或营销，应当提供非针对个人特征的功能选项，或提供便捷的关闭个性化选项的渠道。
问题四	未采取相应的加密、去标识化等安全技术措施。
提示关注	车端APP收集的个人信息应当采取数据安全保护措施，例如加密或去标识化，并且该等保护措施情况可以在隐私政策等个人信息处理规则中向用户告知。
问题五	无隐私政策。
提示关注	前装/后装的车载APP应有隐私政策等个人信息处理规则文本。

3、中国汽车软件解决方案：美国管制再升级

2025年1月，美国商务部工业与安全局（“**BIS**”）通过最终规则（Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles，**“BIS最终规则”**）认定，由中国控制的实体提供的网联车辆技术对国家安全构成“不可接受的风险”，并禁止相关交易。

美国联邦通信委员会（“**FCC**”）据此启动更新程序，2025年5月，FCC的公共安全和国土安全局（“**PSHSB**”）与工程与技术办公室（“**OET**”）依据2019年安全可信通信网络法案（The Secure and Trusted Communications Networks Act of 2019）和第13873号行政命令（Executive Order No. 13873），发布了有关网联车辆技术的征求意见，内容是计划更新受

限通信设备与服务清单（“受限清单”）。[VII]

本次更新在受限清单中加入了下述与中国相关的设备和服务，具体包括：

由中国拥有、控制或受其管辖或指示的主体设计、开发、制造或供应的自动驾驶系统（Automated Driving Systems，“ADS”）及完整网联车辆（“受限清单更新类项一”）。

由中国拥有、控制或受其管辖或指示的主体设计、开发、制造或供应的拟被集成于美国境内的完整网联车辆的车辆连接系统（Vehicle Connectivity Systems，“VCS”）硬件；或集成了由中华人民共和国拥有、控制或受其管辖或指示的主体设计、开发、制造或供应的受限制软件（该软件能够直接实现车辆层级的ADS或VCS功能）的VCS硬件（“受限清单更新类项二”）。

海问评述：

A. 管制方式的更新

不同于此前受限清单主要以纳入具体企业及其提供的设备或服务的方式对通信设备和服务进行限制，本次FCC以纳入特定类别或功能的设备和服务方式，对受限清单进行更新，通过对设备、功能和供应链关系进行管制，覆盖的范围更广。

此外，FCC澄清了根据委员会规则第2.903(b)条，每个“被列入受限制清单并生产受限制设备”的实体必须向委员会提供其子公司和附属公司信息，但由于本次更新针对的不是特定实体生产或提供的设备，不会涉及要求相关实体提供前述信息。

B. 受限清单的补充意见与豁免情况

FCC提出，根据FCC现行规则第2.903(a)条，被列入受限清单的设备不能获得设备授权。对于受限清单更新类项一涉及的ADS及完整网联车辆，由于组成ADS的软硬件系统集合与完整网联车辆本身不是需要FCC授权的射频设备，因此不存在授权问题。

对于受限清单更新类项二，如果VCS硬件并非拟用于美国境内完整网联车辆，则理论上

不构成受限制设备，仍可获得授权。

对此，FCC希望征求更多意见，因为FCC认为如何判断VCS硬件是否“拟用于完整网联车辆”在实践中可能面临挑战，并提出满足以下条件之一的可以认定为属于“拟用于美国境内完整网联车辆的VCS硬件设备”：第一，是远程信息处理控制单元；第二，包含集成受限制软件；第三，使用5.895-5.925 GHz 频段的频谱。

此外，根据BIS最终规则，VCS硬件进口商在满足以下条件时，可从事原本被禁止的交易，免于提交符合性声明：

- （1）对于无车型年份标识的VCS硬件，其进口日期早于2029年1月1日；或
- （2）该VCS硬件与2030年前的车型年份相关联，或者VCS硬件作为2030年前车型年份的网联车辆的一部分进口，或者VCS硬件是为维修或保修2030年前车型年份的网联车辆而进口的。

网联汽车制造商在满足以下条件时，可从事原本被禁止的交易，免于提交符合性声明：

- （1）集成了受限制软件的完整网联车辆是在2027年前的车型年份制造的。
- （2）对于由中国管辖、控制或指示的网联汽车制造商，集成了VCS硬件和/或受限制软件的完整网联车辆是在2027年前的车型年份制造的。[VIII]

4、L2辅助驾驶标准在路上：辅助驾驶/自动驾驶逐步拥抱强制标准

根据全国标准信息公共服务平台公开信息显示 [IX]，工业和信息化部提出了制定《智能网联汽车 组合驾驶辅助系统安全要求》的国家标准立项计划，并委托全国汽车标准化技术委员会智能网联汽车分会执行。

该标准适用于装配了组合驾驶辅助（2级驾驶自动化）[X] 系统的M和N类汽车，将对组合驾驶辅助系统的通用技术要求作出规范，主要包括运动控制能力、驾驶员状态监测、驾驶员干预、系统边界及响应、系统探测能力、系统安全性要求、功能安全等方面，并将规定相应的审核要求，明确典型工况的试验方法。

海问评述：

该标准为强制性国家标准，其制定与出台将为L2辅助驾驶产品的安全性能和行业管理提供更坚实的监管依据和支撑，提升L2辅助驾驶产品的安全性能，减少由于产品性能缺陷导致的安全事故，有助于提升我国道路交通整体安全水平。

我国汽车、智能网联、自动驾驶/辅助驾驶领域的国家标准、行业标准、团体标准很多。其中，在国家标准领域，强制性标准大多集中在汽车产业链的传统领域和话题，例如整车安全、零部件要求等。目前，针对自动驾驶/辅助驾驶以及智能网联领域的强制性国家标准不多，仍旧以推荐性国家标准为主。

这两类标准在适用过程中的差别较大。企业和服务提供者可以参考适用推荐性标准，但是必须适用强制性标准。所以，在智能网联、自动驾驶/辅助驾驶领域颁布更多强制性标准，有助于实质性地提升行业发展质量，这对以“安全”为最重要原则之一的自动驾驶/辅助驾驶领域，具有格外重要的意义。

[I]参见工信部官网，https://www.miit.gov.cn/jgsj/waj/wjfb/art/2025/art_181a52f57d14451ba4c85

[II]参见《中国（北京）自由贸易试验区总体方案》（国发〔2020〕10号）。

[III]参见《中国（北京）自由贸易试验区数据出境管理清单（负面清单）（2024版）》。

[IV]参见《中国（天津）自由贸易试验区总体方案》（国发〔2015〕19号）。

[V]参见《中国（天津）自由贸易试验区数据出境管理清单（负面清单）（2024版）》。

[VI]参见国家计算机病毒应急处理中心官网，<https://www.cverc.org.cn/zxdt/report20250619.htm>。

[VII]参见美国联邦通信委员会官网，<https://www.fcc.gov/document/fcc-seeks-public-input-commerce-department-determination>。

[VIII]参见美国商务部工业与安全局官网，<https://www.bis.gov/press-release/commerce-finalizes-rule-secure-connected-vehicle-supply-chains-foreign-adversary-threats>。亦可参见美国联邦通信委员会规则§ 791.308 Exemptions，<https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-E/part-791/subpart-D/section-791.308>。

[IX]参见全国标准信息公共服务平台官网，<https://std.samr.gov.cn/gb/search/gbDetailed?id=14366B6505BA7711E06397BE0A0A151B>。

[X]根据《汽车驾驶自动化分级（GB/T 40429-2021）》，组合驾驶辅助（2级驾驶自动化）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的能力的系统。

2025-07-17