汉坤法律评述

2021 年 5 月 27 日

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

北京 | 上海 | 深圳 | 香港

简评《信息安全技术 网联汽车 采集数据的安全要求（草案）》与《汽车数据安全管理若干规定（征求意见稿）》

作者：段志超 | 王雨婷 | 蔡克蒙[1]

近期，汽车行业数据合规相关的国家标准与部门规章相继出台草案与征求意见稿，勾勒出针对汽车行业个人信息与重要数据收集、使用、存储、共享、跨境传输的监管框架。下文中我们将梳理《汽车数据安全管理若干规定（征求意见稿）》、《信息安全技术 网联汽车 采集数据的安全要求（草案）》的核心内容，并简要评述存在争议或有待进一步明确的地方，以供讨论。

一、简评《汽车数据安全管理若干规定（征求意见稿）》

5 月 12 日，国家网信办公布了《汽车数据安全管理若干规定（征求意见稿）》（**“《汽车数据安全规定》”**），向社会公开征求意见。《汽车数据安全规定》是首部专门规范汽车行业数据处理的部门规章。与近期颁布的针对智能网联汽车的国家标准[2]不同，《汽车数据安全规定》的适用范围可扩展至所有类型的车辆。《汽车数据安全规定》的核心内容如下：

- 明确汽车行业内重要数据的范围。处理重要数据应遵守一系列合规要求，例如满足最小必要原则、车内处理原则、数据本地化存储、数据出境安全评估、数据处理报告、年度汇报等。
- 强调个人信息主体针对个人信息收集和删除的控制权。
- 加强针对数据处理活动的行政监管。
- 若《汽车数据安全规定》以目前版本正式生效，其规定的最小必要原则、车内处理原则、数据主体控制权、数据本地化要求，将极大改变当前车机端数据处理活动的设计和实践。

我们将在下文梳理和总结《汽车数据安全规定》中关于个人信息和重要数据处理的关键要求，并同时提出我们的解读。

（一）适用范围

根据《汽车数据安全规定》第 2 条和第 3 条，《汽车数据安全规定》适用于运营者在中国境内设计、生产、销售、运维、管理汽车过程中，对**个人信息**或**重要数据**的处理活动。《汽车数据安全规定》

[1] 实习生蔡诗萌对本文的写作亦有贡献。

[2] 如信安标委于 4 月 28 日颁布的《信息安全技术 网联汽车 采集数据的安全要求（草案）》。

规定运营者指汽车制造商、部件和软件提供者、经销商、维修机构、网约车企业、保险公司等**其他汽车设计、制造、服务企业或者机构**。换言之，《汽车数据安全规定》的适用主体范围基本涵盖汽车行业全产业链的参与者。若经营者的数据处理活动涉及车主、驾驶人、乘车人、行人等的个人信息或重要数据，则需遵守《汽车数据安全规定》的有关规定。

然而，《汽车数据安全规定》尚未明确，运营者开展的、与汽车经营活动无关的数据活动是否同样落入适用范围，例如经营者基于内部管理需要针对员工个人信息开展的数据处理活动。此外，针对已售、再售、在产车辆，是否以及如何适用《汽车数据安全规定》，这一点也待后续进一步明确。

（二）重要数据的范围

《汽车数据安全规定》第 3 条明确了汽车行业重要数据的范围，具体包括：

- 军事管理区、国防科工等涉及国家秘密的单位、县级以上党政机关等重要敏感区域的人流车流数据；
- 高于国家公开发布地图精度的测绘数据；
- 汽车充电网的运行数据；
- 道路上车辆类型、车辆流量等数据；
- 包含人脸、声音、车牌等的车外音视频数据；
- 国家网信部门和国务院有关部门明确的其他可能影响国家安全、公共利益的数据。

实践中判断重要数据范围的具体方法仍有待明确，例如如何计算人流车流数据、如何识别重要敏感区域等。但可以肯定的是，国家高度关注和重视车载摄像头、雷达、激光雷达和其他传感器收集的车外数据。因此，若经营活动涉及前述重要数据，经营者应额外谨慎对待。

（三）数据处理目的和原则

根据《汽车数据安全规定》第 4 条，处理个人信息或重要数据的目的应当合法、具体、明确，与汽车的设计、制造、服务直接相关。《汽车数据安全规定》第 6 条结合汽车行业特点，进一步细化了《网络安全法》与《个人信息保护法（二审稿）》确立的数据最小化原则，倡导运营者处理个人信息和重要数据过程中坚持：（1）车内处理原则，（2）匿名化处理原则，（3）最小保存期限原则，（4）精度范围适用原则，（5）默认不收集原则。

根据目前《汽车数据安全规定》的规定，上述原则为倡导性规定，尚未上升至经营者的强制性义务。然而，未来主管部门或将基于上述原则制定《汽车数据安全规定》的落地细则。同时，运营者应尤其注意在汽车设计、研发阶段，尽早贯彻车内处理原则[3]与默认不收集原则[4]，以避免后续基于合规要求变更设计而产生高昂成本。

[3] 《汽车数据安全规定》第 6 条第（1）项规定，车内处理原则，除非确有必要不向车外提供。

[4] 《汽车数据安全规定》第 6 条第（2）项规定，默认不收集原则，除非确有必要，每次驾驶时默认为不收集状态，驾驶人的同意授权只对本次驾驶有效。

（四）个人信息处理规则

根据《汽车数据安全规定》第 9 条，运营者收集个人信息应当取得被收集人同意，法律法规规定不需取得个人同意的除外。当运营者处理个人信息时，运营者应按照第 7 条[5]规定，向数据主体提供数据处理相关的必要信息，包括负责处理用户权益责任人的有效联系方式、收集每种类型数据的触发条件以及停止收集的方法、删除个人信息的方法步骤等。如果实践上难以取得被收集人同意（如收集车外个人信息），经营者可针对采集的个人信息进行匿名化或脱敏处理，例如删除含有能够识别自然人的画面，或对这些画面中的人脸等进行局部轮廓化处理。

前述规定回应了长期困扰汽车行业经营者的难题，即如何合规处理车外行人的个人信息。考虑到实践中几乎不可能逐一获得车外行人的授权同意，经营者可根据第 9 条规定，通过数据匿名化和脱敏处理合规收集车外行人个人信息，而无需征得其授权同意。但目前仍有两个问题有待后续进一步明确：（1）“脱敏处理”是否与“匿名化”[6]同义，或是指代“去标识化处理”[7]；（2）是否只有车内完成数据匿名化和脱敏方可免除经营者获得取得同意的要求，抑或是在服务器端完成数据匿名化和脱敏也可免除授权同意的合规要求。如果匿名化和脱敏处理必须在车机端完成，那么运营者必须确保车辆具备强大的数据处理能力。否则，运营者需按照届时生效的《个人信息保护法》，基于授权同意之外的合法基础开展个人信息处理活动。

（五）敏感个人信息的增强保护

《汽车数据安全规定》第 8 条对敏感个人信息处理活动提出了更高的合规要求。《汽车数据安全规定》尚未定义汽车行业的敏感个人信息，仅列举三类典型数据，即车辆位置、驾驶人或乘车人音视频等、以及可以用于判断违法违规驾驶的数据。在处理敏感个人信息时，经营者不仅需要符合前述提及的个人信息处理规则，还需额外注意以下要求：

- **目的限制**：以直接服务于**驾驶人或者乘车人**为目的，包括增强行车安全、辅助驾驶、导航、娱乐等。
- **告知同意**：默认为不收集，**每次**都应当征得**驾驶人**同意授权，驾驶结束（驾驶人离开驾驶席）后**本次授权自动失效**。通过车内显示面板或语音等方式告知驾驶人和乘车人正在收集敏感个人信息。
- **个人控制**：**驾驶人**能够随时、方便地终止收集。允许**车主**方便查看、结构化查询被收集的敏感个人信息。**驾驶人**要求运营者删除时，运营者应当在 2 周内删除。

相比之下，《汽车数据安全规定》规定的敏感个人信息处理要求比现行法规更为严格、详细，例如数据删除期限更短。每次驾驶都应征得驾驶人的同意授权等合规要求，可能会极大改变现有车辆技术设置以及人们的驾驶习惯。此外，第 8 条可能会被解释为，授权同意是处理敏感个人信息的唯一合法性基础。换言之，运营者或许无法基于其他合法基础处理敏感个人信息，例如为履行法定义务或在紧急情况

[5] 《汽车数据安全规定》第 7 条规定，运营者处理个人信息应当通过用户手册、车载显示面板或其他适当方式，告知负责处理用户权益责任人的有效联系方式，以及收集数据的类型，包括车辆位置、生物特征、驾驶习惯、音视频等，并提供以下信息：（一）收集每种类型数据的触发条件以及停止收集的方法；（二）收集各类型数据的目的、用途；（三）数据保存地点、期限，或者确定保存地点、期限的规则；（四）删除车内、请求删除已经提供给车外的个人信息的方法步骤。

[6] 《GB/T 35272-2020 信息安全技术 个人信息安全规范》3.14 匿名化：通过对个人信息的技术处理，使得个人信息主体无法被识别或者关联，且处理后的信息不能被复原的过程。注：个人信息经匿名化处理后所得的信息不属于个人信息。

[7] 《GB/T 35272-2020 信息安全技术 个人信息安全规范》3.15 去标识化：通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别或者关联个人信息主体的过程。注：去标识化建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段替代对个人信息的标识。

下为保护驾驶人安全而收集处理车辆位置数据。

（六）个人信息与重要数据本地化存储

《汽车数据安全规定》第 12 条规定，运营者应当依法将个人信息或者重要数据在境内存储，确需向境外提供的，应当通过国家网信部门组织的数据出境安全评估。就个人信息是否必须本地存储，该条款存在两种解读方式。一方面，考虑到汽车行业数据的高度敏感性，《汽车数据安全规定》要求所有类型的车辆个人信息都必须在中国境内存储。另一方面，该条款也可以理解为未超出《个人信息保护法（二审稿）》范围而创设更严格的数据本地化义务。换言之，只有被认定为关键信息基础设施运营者的汽车经营者，或处理个人信息达到国家网信部门规定数量的汽车经营者，才有义务将个人信息存储在中国境内。就重要数据而言，考虑到《数据安全法（二审稿）》授权国家网信办协同国务院其他部门制定重要数据的本地化规则，我们倾向于认为，《汽车数据安全规定》旨在要求汽车行业的所有重要数据都应在本地存储。

（七）第三方数据查询利用

《汽车数据安全规定》第 16 条规定，科研和商业合作伙伴需要查询利用境内存储的个人信息和重要数据的，运营者应当（1）采取有效措施保证数据安全，防止流失；（2）严格限制对重要数据以及敏感数据的查询利用。

目前，第 16 条尚未明确该条款是否仅适用于**境外**第三方查询利用境内数据的行为。根据文义解释，《汽车数据安全规定》第 16 条的适用对象包括所有第三方数据查询利用行为，而不仅局限于数据跨境传输。此外，又考虑到目前常见的数据远程访问（代替数据传输）的行业实践、以及隐私计算等新兴技术，我们认为。第 16 条适用范围是否同时覆盖**境内与境外**科研和商业伙伴，值得进一步探讨。

（八）数据处理活动的行政汇报义务

《汽车数据安全规定》在以下几个方面加强了经营者针对数据处理活动的行政汇报义务：

- **处理重要数据的提前报告：**第 11 条要求在处理重要数据之前，运营者应当提前向省级网信部门和有关部门报告数据类型、规模、范围、保存地点与时限、使用方式，以及是否向第三方提供等。与《数据安全管理办法（征求意见稿）》第 15 条[8]规定的备案义务不同，《汽车数据安全规定》要求运营者对重要数据处理活动作出预判、并提前报告。
- **在数据跨境抽查中以明文、可读方式展示数据的类型和范围：**根据《汽车数据安全规定》第 15 条，国家网信部门会同国务院有关部门以抽查方式核验向境外提供个人信息或重要数据的类型、范围等，运营者应当以明文、可读方式予以展示。

[8] 《数据安全管理办法（征求意见稿）》第 15 条：网络运营者以经营为目的收集重要数据或个人敏感信息的，应向所在地网信部门备案。备案内容包括收集使用规则，收集使用的目的、规模、方式、范围、类型、期限等，不包括数据内容本身。

- **数据安全管理的年度报告：**处理个人信息涉及个人信息主体超过 10 万人、或者处理重要数据的运营者，应当在每年 12 月 15 日前将年度数据安全管理情况报省级网信部门和有关部门[9]。如果存在向境外提供数据，运营者应报告跨境数据传输的情况[10]，特别是数据主体的投诉及处理情况等。

二、简评《信息安全技术 网联汽车 采集数据的安全要求（草案）》

4 月 28 日，全国信息安全标准化技术委员会（**“信安标委”**）发布了《信息安全技术 网联汽车 采集数据的安全要求（草案）》（**“《网联汽车数据采集安全要求》”**）。《网联汽车数据采集安全要求》首次针对网联汽车[11]的数据收集与传输、存储、跨境提出推荐性要求。结合上述《汽车数据安全规定》，《网联汽车数据采集安全要求》针对数据脱敏处理、座舱内音视频、图像数据传输限制、网联汽车数据存储期限、数据跨境传输等环节提出了更为严苛的要求。考虑到《网联汽车数据采集安全要求》作为推荐性国家标准，不具有强制约束力，若未来生效版本与《汽车数据安全规定》、《个人信息保护法》、《数据安全法》生效版本不一致，应以上位法规定为准。

（一）数据传输

《网联汽车数据采集安全要求》禁止网联汽车未经被收集者的**单独同意**，通过网络、物理接口**向车外传输**包含**个人信息**的数据，但清晰度转换为 120 万像素以下且已擦除可识别个人身份的人脸、车牌等信息的视频、图像数据除外。此外，不得向车外传输自汽车座舱内采集的所有**音频、视频、图像**等数据及经其处理得到的数据（**“车内数据”**）。

针对车内数据的禁止性规定适用范围广（包括原始数据以及经其处理后得到的数据），且不存在例外。这似乎与前款征得同意后可向车外传输个人信息的规定相矛盾。我们理解，前述两款规定可以被理解为：

- 不得向车外传输车内数据，且没有任何例外。
- 经被采集者单独同意后，可向车外传输：（1）自座舱内采集的、非音频、视频或图像的车内个人信息，如用户基本信息、车辆软件使用数据；以及（2）自车外采集的个人信息，如驾驶数据、轨迹数据和车外环境数据。
- 车内数据范围之外的非个人信息，可以在未经用户同意的情况下向车外传输。

（二）数据存储

根据《网联汽车数据采集安全要求》，网联汽车采集的车辆位置、轨迹相关数据在车内存储设备、远程信息服务平台[12]中保存时间均不得超过 7 天。考虑到经营者的日常业务需求，7 天的数据存储期限

---

[9] 《汽车数据安全规定》第 17 条：处理个人信息涉及个人信息主体超过 10 万人、或者处理重要数据的运营者，应当在每年十二月十五日前将年度数据安全管理情况报省级网信部门和有关部门，内容包括：（一）数据安全负责人以及负责处理用户权益相关事务责任人的姓名和联系方式；（二）处理数据的类型、规模、目的及必要性；（三）数据的安全防护和管理措施，包括保存地点、期限等；（四）与境内第三方共享数据情况；（五）数据安全事故及处理情况；（六）与个人信息和数据相关的用户投诉及处理情况；（七）国家网信部门明确的其他数据安全情况。

[10] 《汽车数据安全规定》第 18 条：如果存在向境外提供数据的情况，运营者应当在本规定第 17 条基础上，报告以下情况：（一）接收者的名称和联系方式；（二）出境数据的类型、数量及目的；（三）数据在境外的存放地点、使用范围和方式；（四）涉及向境外提供数据的用户投诉及处理情况；（五）国家网信部门明确的向境外提供数据需要报告的其他情况。

[11] 《网联汽车数据采集安全要求》3.2 网联汽车：通过网络与远程信息服务平台连接并进行数据交换的汽车。

[12] 《网联汽车数据采集安全要求》3.1 远程信息服务平台：用于车辆管理或者提供信息服务的远程系统。

似乎过于严苛，另外，经过匿名化或脱敏处理的数据是否不受此期限限制，仍有待进一步明确。

（三）数据跨境

就数据跨境而言，《网联汽车数据采集安全要求》禁止以下数据出境：（1）网联汽车通过摄像头、雷达等传感器从车外环境采集的道路、建筑、地形、交通参与者等数据（例如乘客、行人、司机、骑行者等），（2）以及车辆位置、轨迹相关数据。其他与车辆运行有关的数据，如网联汽车行驶状态参数、异常告警信息等数据如需出境，应当符合国家关于数据出境的相关规定。此外，网联汽车通过加密方式跨境传输数据的，当监管部门开展抽查验证时，应提供传输的数据格式、加密方式等信息，并按要求明文提供相关数据内容。

相比之下，《网联汽车数据采集安全要求》针对网联汽车收集的车外数据以及车辆自身的行驶数均提出了严格的本地化存储要求。鉴于《个人信息保护法（二审稿）》与《数据安全法（二审稿）》仍在审议中，《汽车数据安全规定》亦处于征求意见阶段，目前国家层面的数据出境监管框架、以及针对汽车数据的具体规定均未落地，我们理解，网联汽车数据的本地化要求与跨境传输限制仍有待上位法以及部门规章的确定。

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：

段志超

电话： +86 10 8516 4123
Email： kevin.duan@hankunlaw.com