浅析车联网与网络数据安全合规

作者：潘永建 | 朱晓阳 | 沙莎

车联网作为提供车辆互联互通的网络服务，网络安全与数据安全始终是其生命线，我国也一直在推进车联网网络数据安全的立法和执法工作。2022 年 2 月 25 日，工信部正式发布《车联网网络安全和数据安全标准体系建设指南》(“《指南》”)，《指南》延续了 2021 年 6 月发布的《车联网(智能网联汽车)网络安全标准体系建设指南(征求意见稿)》(“征求意见稿”)的体系架构，将车联网网络安全建设分为“总体与基础共性、终端与设施网络安全、网联通信安全、数据安全、应用服务安全、安全保障与支撑”六部分，同时强调网络安全与数据安全并重，将车联网网络数据安全作为建设我国网络安全与数据安全体系的关键内容。以《指南》为契机，笔者特此对车联网网络数据安全建设中的重点问题进行分析，并结合当前车联网行业监管趋势，对企业建设车联网网络安全体系提出合规建议。

一. 车联网数据安全要点

1. 数据分类分级

同征求意见稿相比，《指南》除将《网络安全法》作为上位法依据外，还强调《数据安全法》在车联网网络数据安全体系建设中的重要作用。数据安全具体包括通用要求、分类分级、出境安全、个人信息保护以及应用数据安全等五类标准，对解决车联网数据安全建设中的突出问题予以指导，而数据分类分级则是其中的重中之重。

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

车联网数据分类分级是划分数据安全保护要求、整合车联网企业数据安全管理资源的重要依据。工信部于 2020 年发布的通信行业标准《车联网信息服务 数据安全技术要求》(YD/T 3751-2020)是《指南》要求的车辆网数据分类分级标准之一, YD/T 3751-2020 对车联网信息服务相关数据实施六类三级管理，即将数据分为基础属性数据、车辆工况数据、环境感知数据、车控类数据、应用服务类数据与用户个人信息六类； 并将各类数据按照数据敏感性进一步分为一般数据、重要数据和敏感数据:

数据敏感性	敏感性定义	数据类型示例
一般数据	车联网信息服务运行过程中，车联网各主体间进行信息交互时的一般性、能公开获取或能在一定范围内公开的数据，数据泄露对相关主体的影响范围与程度有限，不会对财产和人身安全造成危害	车牌号；道路状况；车辆一定时间内的平均行驶速度；倒车提示声音数据
重要数据	通过数据能在一定程度标识或识别到特定的车联网信息服务的主体、对象或其重要特征，数据一旦泄露，会对相关主体造成较大影响，在一定范围内影响经济效益或造成财产损失，对人身和财产造成较大影响	车架号；发动机转速；车辆碰撞预警数据
敏感数据	通过数据能够唯一标识或识别到特定的车联网信息服务主体、对象或其敏感特征，且与相关主体的企业利益密切相关，或直接关系到用户的个人隐私，一旦泄露、丢失、滥用、篡改等将造成严重后果	车辆设计核心数据；智能泊车系统的自动泊车确认指令；车辆远程监控数据

YD/T 3751-2020 规范除个人信息外的所有车联网信息服务过程中的数据，车联网服务过程中的个人信息保护要求则由《车联网信息服务 用户个人信息保护要求》(YD/T3746-2020)规制，该标准与 YD/T 3751-2020 同时颁布，也是《指南》要求的个人信息保护标准之一。YD/T3746-2020 将个人信息分为个人一般信息、个人重要信息和个人敏感信息，其中个人重要信息类型的占比最大。YD/T3746-2020 对不同类别个人信息保护标准提出要求，包括访问控制权限、安全管理措施等，同时保证了个人信息的可用性和安全性。个人信息分类示例如下所示:

个人信息敏感性	敏感性定义	个人信息类型示例
个人一般信息	车联网信息服务过程中相关的用户个人信息，在被泄露、非法提供或被滥用后会给用户带来一定影响，但影响范围和程度有限，不会对财产和人身安全构成危害	业务订购、订阅关系
个人重要信息	个人信息在被泄露、非法提供或被滥用后会给用户带来较大危害，甚至在一定程度上影响个人名誉和身心健康	用户基本资料、联系人信息、涉车服务信息、日志、服务记录、交易服务信息、车辆基本资料
个人敏感信息	个人信息一旦被泄露、非法提供或被滥用后会给用户带来严重危害，极易导致个人名誉和身心健康受到损害或歧视性待遇	用户身份证明、生理标识、车联网交易类信息服务身份标识和鉴权信息

有效的数据分类分级也是实现汽车数据跨境流通安全的基础，在日常管理过程中，数据跨境传输是车联网企业，特别是跨国车联网企业无法回避的问题，尤其是重要数据和敏感数据还面临更加严格的监管要求。2021 年底，我国北京、上海、天津、河北、广东等多地车企已经按照《汽车数据安全管理若干规定(试行)》的要求向网信部门提交重要数据处理年度报告，对处理重要数据的基本情况进行说明，其中向境外传输重要数据的企业，还需要进一步报告数据的种类、数量、保存情况、客诉处理、境外接收方信息等。为落实数据出境合规要求，企业必须进行车联网数据分类分级，并以此为基础开展高效的数据治理活动。

2. 识别风险源并正确抵御风险

根据中国信通院 2021 年 12 月发布的《车联网白皮书》，[1]车企视角下的网络安全风险主要来自车机自身网络安全、汽车通信安全、车联网服务平台安全三方面，企业应当正确识别风险源，并结合《指南》要求及时采取有效防御措施。结合《指南》规定的标准体系，我们整理了车企视角下的风险类别、风险描述以及抵御措施:

《指南》标准	风险类别	风险描述	防御措施
终端与设施网络安全	车机自身网络安全	车载联网终端(T-BOX)、车载信息娱乐系统(IVI)、软件在线升级系统(OTA)等设备和系统是网络攻击的重点对象，攻击者利用联网设备的系统漏洞进行跳板式攻击，进而干扰车内部件功能	车内网络安全防护系统
网联通信安全	汽车通信安全	车内通过 CAN 总线、车载以太网等技术实现车内部系统和设备间通信，车外通过车载诊断接口(OBD)、无线通信技术(WiFi、蓝牙、4G/5G、C-V2X 等)与外部实体和平台进行信息交互，攻击者通常利用身份认证或数据加密缺陷发起攻击，产生伪造、篡改、窃取等安全风险	应用身份认证技术，以可信数字身份为基础保障业务安全开展;落实车联网安全防护与检测要求
应用服务安全	车联网服务平台安全	汽车与相关车联网平台连接获取服务，面临传统信息服务平台安全威胁，攻击者可以远程发起拒绝服务、暴力破解、恶意脚本注入等攻击	平台安全防护技术

[1]《车联网白皮书》，参见 https://pdf.dfcfw.com/pdf/H3_AP202112291537269200_1.pdf?1640769117000.pdf

二. 行业监管趋势

1. 加强数据跨境传输监管

汽车行业的数据出境问题一直是监管机关关注的重点。由于车联网企业收集的数据类别复杂、数量庞大，其中还涉及精准位置信息、行踪轨迹、身份信息、生物识别信息等重要数据或敏感个人信息，一旦跨境传输过程中出现数据泄露、篡改，可能对我国国家安全、企业安全以及个人信息主体权益产生重大影响。同时，境外数据监管要求、数据处理者的数据安全保障能力各不相同，企业应当规范与境外接收方的数据处理关系，并对境外接收方处理数据的行为进行监督。对跨国车联网企业而言，数据处理活动除了满足中国法的要求外，可能还需搭建多个法域的数据合规体系。

根据《数据出境安全评估办法(征求意见稿)》，数据处理者向境外提供数据前，应当进行自评估；如果出境数据中包括重要数据，或者出境数据的数量达到一定范围和条件，或者数据出境主体满足特定要求，则需要向网信部门申请安全评估。《指南》规定的数据出境安全标准就包括数据安全评估规范，在汽车数据安全评估方面，企业可能既需要进行自评估，同时还需完成监管部门的外部评估要求，并根据数据安全风险等级及时调整管理和安全措施。

当然，车联网数据跨境传输监管并不意味着禁止数据流通。2020 年 12 月，《中国(上海)自由贸易试验区临港新片区智能网联汽车产业专项规划(2020-2025)》发布，该计划对智能网联汽车技术数据的国际跨境流通进行规定，要求交通场景库信息、自动驾驶算法输出、自动驾驶测试数据、车载软件 OTA 升级信息和远程故障分析等信息可实现在监管条件下的跨境传输。在车联网数据跨境传输方面，不排除未来成立专门的数据跨境监管机构或职能部门，规范车联网数据在符合监管条件的情况下向境外传输。

2. 安全技术措施与漏洞管理监管

如前所述，车联网企业采集数据庞杂，应当在建立数据分类分级的基础上落实合规要求。根据《指南》，车联网服务的参与企业既需要注意终端、基础设施等设备与平台安全，也应保证网联通信等环节与流程安全，因此，车联网服务相关企业应当在数据采集、传输、共享、存储等各个环节落实安全技术要求，特别是对于车联网服务过程中的特殊性问题，如网联通信安全等，应当利用身份认证、安全防护等多种技术手段保证数据安全。

2021 年 9 月，《网络产品安全漏洞管理规定》和《关于加强车联网网络安全和数据安全工作的通知》生效，两部规定对车联网网络安全与数据安全提出要求。特别是在漏洞管理方面，根据两部规定的相关要求，车联网企业应当落实日志留存义务，如留存网络产品安全漏洞信息接收日志不少于 6 个月，同时明确本企业漏洞发现、验证、分析、修补、报告等工作程序，在发现漏洞后采取补救措施并按规定进行上报。

三. 企业合规建议

1. 《指南》发布后，车联网企业应当密切关注相关标准的制定与发布，并按照标准的具体内容在企业内落地合规要求。

2. 车联网服务相关企业应当在企业内部建立数据治理标准与流程，包括数据分类分级制度、数据访问控制制度、漏洞管理制度、安全审计标准以及整改制度。

3. 车联网服务企业涉及汽车生产企业、服务平台运营企业等多种类型主体，除了应当符合安全管理制度、数据采集与传输合规等共性要求外，还应当注重法律法规或标准对企业的特殊要求，如车联网汽车生产企业应当加强整车网络安全架构设计；车联网平台运营企业则需要建立车联网应用程序开发、上线、使用、升级等安全管理制度等。

如您希望就相关问题进一步交流，请联系：

潘永建
+86 21 3135 8701
david.pan@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市朝阳区光华东里 8 号 中海广场中楼 30 层 T: +86 10 5081 3888 F: +86 10 5081 3866	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	**伦敦**	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野