



观韬中茂律师事务所
Guantao Law Firm

车联网 数据安全监管制度 研究报告 2022



毕马威中国
kpmg.com/cn


观韬中茂律师事务所
guantao.com

2022年03月

本报告来自互联网公开渠道，版权归属原作者所有。

如有疑问，请联系data@01caijing.com



 微信扫一扫，使用小程序

更多报告,请扫描二维码

进入找报告小程序



添加微信lycj002邀请您进入更多行业分类群

群内每日分享更多深度报告！

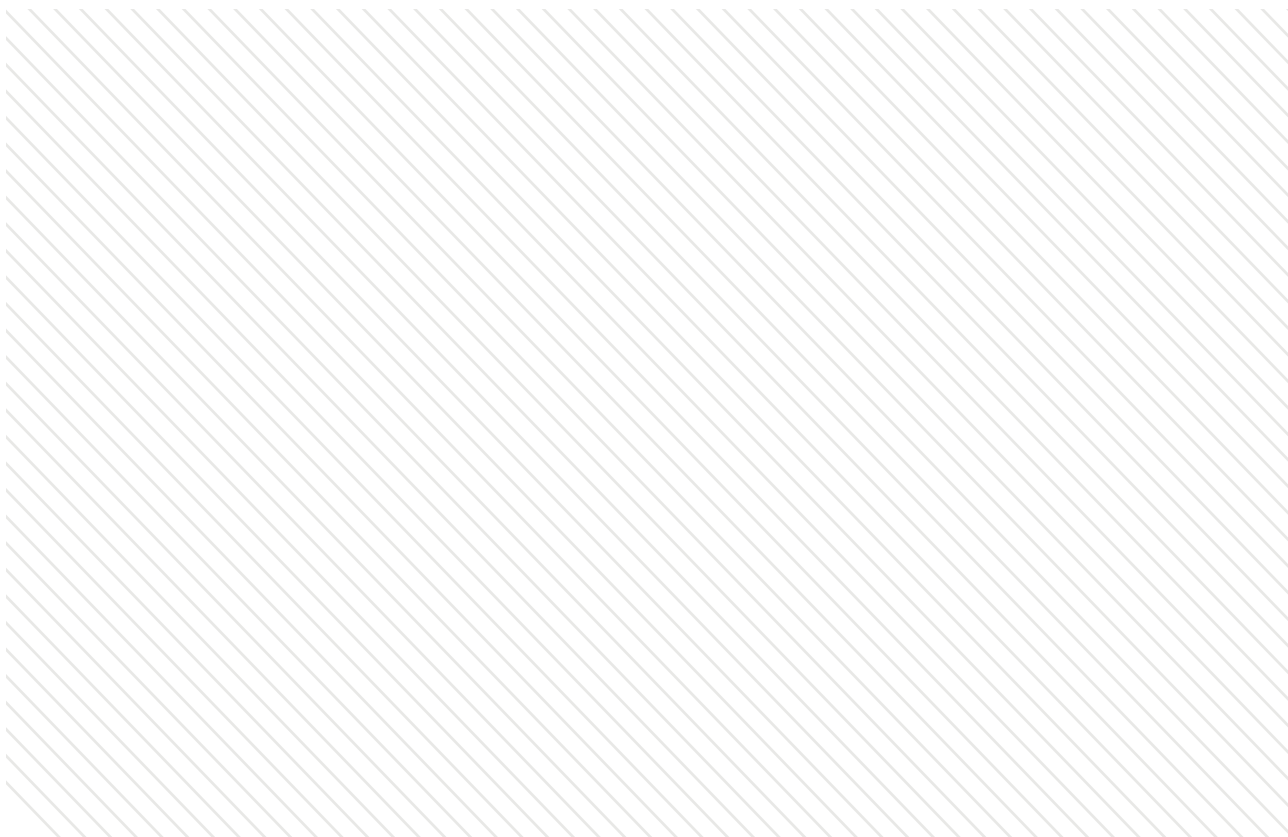
前言 PREFACE

随着现代信息技术的不断发展，汽车行业已经进入新能源数字化时代，汽车逐步向智能化、网联化深入发展。车联网是“互联网+”时代网络空间的延伸，是车辆之间以及与基础设施、行人和网络组成的车际网。车联网的发展将实现人、车、路、云之间数据互通，并服务于智能交互、自动驾驶、智慧交通等各种场景。

然而，智能汽车在车联网中扮演的角色将不仅仅是一般意义上的交通工具，为实现更多的功能与场景，智能汽车正在成为深度收集、处理、传输和使用大量包含个人信息、汽车运行数据和环境数据的可移动、可交互的汽车数据枢纽。汽车数据是车联网运行的关键，其中包含的大量重要数据将涉及到个人、车辆、企业以及国家的安全。如何保障汽车数据安全，并在合规前提下，促进汽车数据的充分合理利用，逐渐成为关系到整个车联网产业健康良性发展的重要课题。

目前，我国已经制定并开始实施《网络安全法》《数据安全法》《个人信息保护法》等数据保护领域的重要法律。在车联网领域，相关部门也在不断加强监管和保护，并陆续出台了《汽车数据安全管理办法（试行）》《关于加强智能网联汽车生产企业及产品准入管理的意见》等重要行业规定和意见，对车联网产业提出了全方位的数据保护要求。

基于此，毕马威中国与观韬中茂律师事务所联合发布《车联网数据安全监管制度研究报告》。本报告对当前车联网领域涉及的汽车数据类型、数据安全的监管现状、行业监管重点等问题进行梳理和分析，并提出监管建议，希望能为社会各界提供借鉴和参考。



目录 CONTENT

数据安全：车联网安全的核心	1
▪ 车联网安全与数据安全关系概述	1
▪ 数据与车联网互动下的数据特征	2
车联网数据安全的制度保障	3
▪ 车联网数据安全国内制度概览	3
▪ 车联网数据安全域外立法借鉴	6
车联网数据安全的监管重点问题	8
▪ 重点数据类型：车联网数据安全的关键	8
▪ 重点业务环节：数据安全监管的风险与隐患	10
车联网数据安全的监管制度挑战	12
▪ 数据分类分级问题	12
▪ 主体之间责任分配问题	13
车联网数据安全监管制度建议	14
▪ 细化行业要求，出台车联网数据安全规范指南	14
▪ 加强政府监管，建立车联网数据安全防护体系	14
▪ 加速试点落地，提供车联网数据安全防护指引	15
结语	16

（一）车联网安全与数据安全关系概述

车联网是新一代网络通信技术与汽车、电子、道路交通运输等领域深度融合的新兴产业形态，是人、车、路、云平台之间全方位连接和信息交互。狭义的车联网应用通常指车载信息服务类应用，即通过车辆把车主与各种服务资源整合在一起；广义的车联网应用还包括面向交通安全的效率类应用以及自动驾驶为基础的协同服务类应用。

数据是车联网的核心要素，车辆与车联网服务平台之间的“车 - 云通信”，车辆之间的“车 - 车通信”，车辆与路基设施之间的“车 - 路通信”，车辆与移动智能终端之间的“车 - 人通信”，以及汽车内部设施与应用之间的车内通信都离不开数据的传输与使用。车联网数据安全关系到行车安全、生命财产安全甚至国家安全。

随着车联网技术发展兴盛的同时，汽车数据安全体系建设也在稳步发展。立法对车辆使用者、公众的个人信息与隐私的保护、汽车数据的分类分级保护、安全风险评估检测以及安全应急处置等有关车辆数据安全的规定相对滞后，相关企业的数据安全防护意识也有待提高。随着车联网技术运用的不断扩张与深入，如何将车联网纳入规范化、制度化的轨道，在产品端纳入数据安全考量的维度，形成数据合理运用、技术良性发展态势是当前亟待探究的命题。本报告试分析车联网应用下数据安全领域的重点问题与难点问题，以期引起业界对此问题的关注并共同寻求解决方案。



（二）数据与车联网互动下的数据特征

车联网技术发展背景下，行业数据有着以下特点：

1. 数据的多样性

数据类别不仅包括了汽车基础数据（车牌号、车辆品牌和型号、车辆识别码、车辆颜色、车身长度和宽度外观等相关数据），也包括基础设施、交通数据、地图数据（红绿灯信息、道路基础设施相关、道路行人的具体位置、行驶和运动的方向、车外街景、交通标志、建筑外观等真实交通数据），以及车主的大量用户身份类数据（姓名、手机号码、驾照、证件号码、支付信息、家庭住址、用户的指纹、面部等生物特征识别信息等）、用户状态数据（语音、手势、眼球位置变化等）、行为类数据（登录、浏览、搜索、交易等操作信息等）等。

2. 数据的规模性

车联网数据融合了来自汽车、道路、天气、用户、智能计算系统等多方面的海量数据，涉及数据类型多，规模大，涉及众多数据处理主体，如智能网联汽车生产企业、车联网服务平台运营企业等，并且随着用户的增加，数据呈指数级增长态势，需要统计分析应用的数据总量大。

3. 数据的非结构性

车联网技术下大量的数据通过车辆内置和外挂的设备不断生成，由于各车厂、零部件商在这部分数据规范定义上存在差异，且没有统一的标准，车联网平台之间的数据无法有效同步，数据的非结构性和非标准性对数据聚合或拆分技术以及权限管理和安全存储都带来了巨大的挑战。

4. 数据的流动性

大量相关主体如智能网联汽车生产企业、车联网服务平台运营企业会参与车联网数据的处理，导致海量数据在用户端、车端、云端等多场景的交互使得数据的流动性增大。如何确保交互流动的数据的安全性，是车联网数据安全体系建设中的一个重要课题。

5. 数据的涉密性

数据的涉密性：网联汽车在公开道路驾驶过程中，会采集大量的地图数据，采集地图数据形成的测绘成果依据《测绘法》涉及国家秘密的，需要按照《保密法》中的相关规定要求进行分级管理。此外，车联网中的一部分数据可能会落入《数据安全法》体系下的重要数据甚至是核心数据的范畴，一旦未经授权披露、丢失、滥用、篡改或销毁，或汇聚、整合、分析后，可能造成影响国家安全、公共安全等严重后果。

（一）车联网数据安全国内制度概览

国内近几年开始重视车联网的数据安全问题，在以政府引导、产业联盟推动、标准委员会执行的模式下积极开展汽车信息安全、数据安全系列的标准制定工作。

在政策法规方面，我国《数据安全法》《网络安全法》《个人信息保护法》对数据安全、网络安全、个人信息保护等问题作出了规定。

行业数据安全相关法规和指导文件也在逐步落地，具体包括《汽车数据安全若干规定（试行）》《关于加强智能网联汽车生产企业及产品准入管理的意见》《关于加强车联网网络安全和数据安全工作的通知》等。

在规范标准方面，国内也在积极跟踪和布局，在智能网联汽车数据应用与保护方面，目前已发布了《车联网信息服务 用户个人信息保护要求》《汽车采集数据处理安全指南》《国家车联网产业标准体系建设指南（智能网联汽车）》《国家车联网产业标准体系建设指南（总体要求）》等。

其他与数据相关的分类分级要求、安全防护技术细则、安全责任划分、授权与使用等一系列标准规范仍待研究制定。

1. 行业数据安全相关法规

《汽车数据安全若干规定（试行）》

2021年10月1日实施的《汽车数据安全若干规定（试行）》（下称“《规定》”）对智能汽车搜集数据的范围和边界做出了规定，明确了“汽车数据”“汽车数据处理者”“个人信息”“敏感个人信息”“重要数据”和涉及汽车数据安全相关行为的范围定义。其中，“汽车数据”包括汽车设计、生产、销售、使用、运维等过程中的涉及个人信息数据和重要数据。“汽车数据处理者”包括汽车制造商、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开展汽车数据处理活动的组织。“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”。《规定》重申的重要数据的概念，即“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”。

车联网数据安全制度框架

法律

- 《个人信息保护法》
- 《数据安全法》
- 《网络安全法》
- 其他一般性法律（如《民法典》《测绘法》《保密法》）

法规 规章 指导性 文件

- 《汽车数据安全若干规定（试行）》
- 《关于加强智能网联汽车生产企业及产品准入管理的意见》
- 《关于加强车联网网络安全和数据安全工作的通知》
- 其他一般性法规、规章、文件，如：
《网络安全审查办法》
《网络数据安全条例（征求意见稿）》

国家 规范 标准

- 《国家车联网产业标准体系建设指南（智能网联汽车）》
- 《国家车联网产业标准体系建设指南（总体要求）》
- 《汽车采集数据处理安全指南》等

行业 标准

- 《智能网联汽车数据安全共享模型与规范（征求意见稿）》
- 《车联网信息服务 用户个人信息保护要求》
- 《机动车保险车联网数据采集规范》等

图1 车联网数据安全制度框架图解

重要数据包括：

- ① 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；
- ② 车辆流量、物流等反映经济运行情况的数据；
- ③ 汽车充电网的运行数据；
- ④ 包含人脸信息、车牌信息等的车外视频、图像数据；
- ⑤ 涉及个人信息主体超过 10 万人的个人信息；
- ⑥ 国家网信部门和国务院发展改革、工业和信息化、公安、交通运输等有关部门确定的其他可能危害国家安全、公共利益或者个人、组织合法权益的数据。



《规定》还提出汽车数据处理者处理个人信息和重要数据的四大原则，并强调汽车数据处理者处理个人信息和处理敏感个人信息时的义务以及个人查询、删除个人信息权利。此外，在数据出境方面，还明确规定了个人信息或者重要数据不出境的原则，以及出境时需要通过网信部门组织的安全评估。

《关于加强智能网联汽车生产企业及产品准入管理的意见》

2021年8月12日，工业和信息化部发布了《关于加强智能网联汽车生产企业及产品准入管理的意见》（以下称“《企业管理意见》”）。《企业管理意见》旨在加强汽车数据安全、网络安全、软件升级、功能安全和预期功能安全管理，保证产品质量和生产一致性，推动智能网联汽车产业高质量发展。汽车生产企业应当建立健全汽车数据安全管理，实施数据分类分级管理，需要向境外提供数据的，应当通过数据出境安全评估，强化数据安全管理能力和网络安全保障能力，加强自动驾驶功能产品安全管理。

《关于加强车联网网络安全和数据安全工作的通知》

2021年9月16日，工业和信息化部发布了《关于加强车联网网络安全和数据安全工作的通知》（下称“《安全工作通知》”）。《安全工作通知》要求汽车企业建立网络安全和数据安全管理制度，明确负责人和管理机构，落实网络安全和数据安全保护责任；要求汽车企业加强整车网络安全架构设计，落实安全漏洞管理责任，加强车联网服务平台安全防护，加强数据安全保护，健全安全标准体系。

2. 国家规范标准

《国家车联网产业标准体系建设指南》

2017 年 12 月 27 日，工业和信息化部和国家标准化委员会联合发布《国家车联网产业标准体系建设指南（智能网联汽车）》（下称“《建设指南（智能网联汽车）》”）。根据《建设指南（智能网联汽车）》提出的标准体系建设目标，2025 年将系统形成能够支撑高级别自动驾驶的智能网联汽车标准体系；制定 100 项以上智能网联汽车标准，涵盖智能化自动控制、网联化协同决策技术以及典型场景下自动驾驶功能与性能相关的技术要求和评价方法，促进智能网联汽车“智能化 + 网联化”融合发展，以及技术和产品的全面推广普及。2018 年工信部和国家标准化委员会发布了《国家车联网产业标准体系建设指南（总体要求）》（下称“《建设指南（总体要求）》”）。《建设指南（总体要求）》充分发挥标准在车联网产业生态环境建构中的顶层设计和基础引领作用，按照不同行业属性划分为智能网联汽车、信息通信、电子产品与服务、车辆智能管理等若干部分。通过《建设指南（总体要求）》可以快速了解车联网行业的顶层设计体系架构和行业动态。

《汽车采集数据处理安全指南》

2021 年 10 月 8 日，全国信息安全标准化技术委员会发布了《汽车采集数据处理安全指南》（下称“《指南》”），规定了对汽车采集数据进行传输、存储和出境等处理活动的安全要求。在数据内容方面，《指南》将汽车采集数据分为车外数据、座舱数据、运行数据和位置轨迹数据。其中，车外数据可能包含个人信息、敏感个人信息和重要数据；座舱数据可能包含敏感个人信息；在数据传输方面，除符合例外情形或经个人信息主体单独同意，不得通过网络向外传输包含未匿名化处理个人信息的车外数据、座舱数据；在数据存储方面，除非符合例外情形，否则车外数据、位置轨迹数据在车外位置保存时间不应超过 14 天；在数据出境方面，车外数据、座舱数据、位置轨迹数据不应出境，运行数据出境前应通过数据出境安全评估。

3. 其他行业标准

2021 年 1 月 20 日，由中国智能网联汽车产业创新联盟提出的《智能网联汽车数据安全共享模型与规范（征求意见稿）》CSAE 标准对汽车基本配置信息、行程信息、行驶位置信息、行驶状态信息、车内部情况、驾驶员驾驶行为、道路信息、天气环境、行人检测、环保检测等信息作出安全等级划分。根据不同类别数据遭篡改、破坏、泄露或非法利用后，可能对个人、车厂、行业、社会秩序造成的潜在影响对数据进行分级，提出了五级分类方法。

2020 年 10 月 1 日实施的工信部发布的通信行业《车联网信息服务 用户个人信息保护要求》（YD/T 3746-2020）将车联网信息服务中的用户个人信息分类进一步细化，规定了车联网信息服务中用户个人信息内容分类、敏感性分级和分级保护要求，进一步明确了分级保护要求，为汽车厂商、零部件和元器件供应商、软件提供商、数据内容提供商和服务提供商等运营者在提供服务过程中的个人信息保护提供了具体的指导。

《机动车保险车联网数据采集规范》是中国保险行业协会于 2019 年 3 月 28 日发布的一项车险相关标准。该标准针对保险公司的机动车保险经营管理工作、企业生产企业、车联网科技企业的数据采集共享工作，规定了基于机动车保险经营管理应用的车联网数据采集工作中所涉及的基础数据的范围、类型、精度等方面的内容，同时规定了数据有效性、合理性、真实性的验证机制。

（二）车联网数据安全域外立法借鉴

1. 道路车辆的网络安全（UNECE R155）和软件更新（UNECE R156）

联合国欧洲经济委员会（UNECE）在 2020 年 6 月通过了道路车辆的网络安全（UNECE R155）和软件更新（UNECE R156）两部新的规定，并将于 2021 年 1 月起生效。根据这两个规定，汽车制造商（OEM）需要符合软件更新管理系统（SUMS）和网络安全管理认证（CSMS）的要求以完成车辆型式认证。这两部规定适用于《关于统一条件批准机动车辆装备和部件并相互承认此批准的协定书》（简称《1958 年协定书》）的成员国。为能够投入欧盟市场和 1958 协议成员国市场，新车型的汽车制造商都需要使用符合 UNECE R155 法规要求的网络安全管理系统，并证明车辆类型的技术设计和架构符合要求。

2021 年 3 月 10 日，联合国世界车辆法规协调论坛（WP.29）第 183 次全体会议审议通过了由 WP.29 自动驾驶与网联车辆工作组起草的 UNECE R155 和 UNECE R156 解读文件。该文件属于指南性质，旨在帮助企业 and 审核机构理解法规要求，保障不同审核机构评审活动的一致。解读文件对法规中的“型式批准”“信息安全管理（CSMS）”等条款进一步说明，并且以示例的方式将 UNECE R155 中的部分条款与《道路车辆 - 网络安全工程标准》（ISO/SAE DIS 21434）的相关条款进行映射解读。

2. EDPB《车联网个人数据保护指南》

早在 2016 年，欧盟委员会便发布了欧盟网联汽车战略，表明了个人数据和隐私保护对于自动驾驶汽车能否成功落地起着决定性作用。欧盟认为必须使用户对他人的个人数据未被当作商品感到放心，且让消费者如何及何种目的使用他们的数据保有有效的控制权力。2017 年，欧盟网络和信息安全机构（ENISA）发布了《智能汽车网络安全与适应力》的研究报告，提出了应对网络威胁，保障智能汽车安全的最佳实践和建议。

该指南指出车联网汽车个人数据保护应该通过默认设计（by Design and by Default）遵循相关性和数据最小化原则，并对数据主体权利以及车载 WIFI 技术在非个人信息处理方面等提出了建议。针对在联网车辆中处理的生物特征和位置数据的问题，指南建议用户能够控制其数据在车辆中的收集和处理方式，并且规定这些数据不应传输给任何第三方，数据主体应能够在出售车辆之前永久删除任何个人数据。

3. 德国《使用联网和非联网车辆时的数据保护》

2016 年德国联邦和州政府的独立数据保护机构和德国汽车工业协会发布《使用联网和非联网车辆时的数据保护》联合声明，将车联网数据处理纳入《德国联邦数据保护法》《德国电信法》《德国社会保险法》等上位法的范畴，强调了车主的数据主权，明确了制造商“设计隐私”的法律责任，将数据控制者区分为“离线控制者”和“在线控制者”，对制造商和第三方服务提供商的控制状态做出合理区分。

4. 美国《自动驾驶法案》

2017 年美国众议院通过了《自动驾驶法案》（Self Drive Act）。该法案第五章要求自动驾驶车辆厂商必须制作出网络安全计划，包括如何应对网络攻击、未授权入侵以及虚假或者恶意控制指令等安全策略，用以保护关键的控制、系统和程序，并根据环境的变化对此类系统进行更新，制定内部人员的安全培训和管理制度。

第十二章为自动驾驶汽车隐私保护计划，要求厂商必须制定隐私保护计划，包括对车主以及乘客信息的搜集、保存、使用等方面的保护措施。同时，联邦交易委员会展开研究，以确认获得车主或者乘客的隐私信息的参与方、信息公开的范畴、隐私信息处理的界限等等。

5. 英国《智能网联汽车网络安全关键原则》

该规定于 2017 年由交通部和国家基础设施保护中心联合制定，提出了企业评估和管理供应链中各环节的安全风险的要求，以及企业供应商、分包商和潜在的第三方机构应进行独立认证以提高整体安全性、所有软件的安全管理应贯穿生命周期，保障数据存储和传输安全可控等在内的八大原则、二十九项细则，将网络数据安全责任拓展到车联网产业链的每个主体，并强调应在汽车生命全周期内纳入网络数据安全问题。



（一）重点数据类型：车联网数据安全的关键

鉴于车联网行业数据的多样性和规模性，可对汽车产生的数据进行类型化管理。随着智能化和网联化程度的提升，智能网联汽车通过配备的摄像头、麦克风、传感器、信息娱乐系统等无时无刻不在收集用户的行为习惯和个人隐私，这些驾驶和使用过程中产生着的大量数据，包含外部环境、车辆位置、车外音视频信息、人流车流数据、高精地图测绘等敏感信息。车联网数据根据数据类型分类大致如右图所示。

车联网数据分类



图3 车联网数据分类图解

1. 环境数据，自动驾驶的基础

环境数据的采集与处理是网联汽车实现自动驾驶的基础，包括实时交通数据、地图数据、周边环境感知数据和高级驾驶辅助系统（ADAS）状态数据。环境数据中涉及数据安全的是地图数据。高精定位技术下，采集自然地理信息的行为很大程度上会落入《测绘法》第2条所规定的测绘范围。

鉴于高精地图涉及国家安全，由此可能引发以下问题：**1）**数据出境方面，这类数据可能涉及《网络安全法》《数据安全法》《汽车数据安全管理办法》中重要数据的规定，在数据出境方面受到严格限制，包括通过国家网信部门组织的安全评估；**2）**数据采集方面，测绘行为在我国实行的是资质准入，测绘活动的开展应以拥有测绘资质证为前提；**3）**数据管理上，根据《测绘地理信息管理工作国家秘密范围的规定》《导航电子地图安全处理技术基本要求》《测绘资质管理规定》《测绘资质分级标准》等相关规定，测绘地理信息可能会涉及不同层级的国家秘密。**4）**根据《外商投资准入特别管理措施（负面清单）（2020年版）》，测绘地理信息属于外资禁入的负面清单。**5）**根据《测绘法》等规定，我国实行测绘成果汇交制度，测绘项目完成后，向主管部门汇交测绘成果资料。属于基础测绘项目的，应当汇交测绘成果副本；属于非基础项目的，应当汇交测绘成果目录。因此地图数据在采集、管理上都应当是车联网企业所应重点关注的数据类型。

此外，智能网联汽车还需收集道路周边情况协助驾驶，在此过程中可能会拍摄到周围行人。此时对行人进行告知并获取同意的方案并不可行。因此，当不可避免收集到行人相关个人信息时，车联网应用软件提供者需在达到收集目的后及时删除或进行匿名化处理。比如拍摄周围行人是为了降低行人碰撞风险，当汽车行驶过该路段后，该行人个人信息即不再必要，需及时删除或进行匿名化处理。

2. 汽车自身数据，驾驶功能的必备

汽车自身数据包括座舱数据、运行数据和位置轨迹数据。智能汽车电子构架变革路径是从 ECU 到域控制器，再到超级计算机。因此，智能汽车电子架构一般划分为五个域：驾驶辅助 / 自动驾驶域、智能座舱控制域、车身控制域、底盘控制域、动力总成域。其中驾驶辅助 / 自动驾驶域、智能座舱控制域与汽车数据安全直接相关。根据《车联网信息服务 用户个人信息保护要求》车辆基本资料和设备、系统或平台信息属于个人重要信息。而在《智能网联汽车数据安全共享模型与规范（征求意见稿）》中将大量的车辆数据分级为第I级，即完全公开数据，遭到篡改、破坏或泄露后，不存在潜在的负面影响，可以面向大众公开；也有大量的数据被定义为第IV级，即遭到篡改、破坏或泄露后，潜在的影响较大，对个人与车厂利益产生特别严重的损害，宜在车厂和相关主体的严密监控下使用。总结来看，可以从两个维度进行判断，一是与个人的关联度，与个人关联度越高，这类数据安全等级应当越高；二是静态数据与动态数据的区分，动态数据的安全等级应当高于静态数据。但一般认为，这些数据收集是围绕车辆的基本驾驶功能开展，是实现车辆驾驶的必备数据，此外互联网时代的车辆监测、快速维修的需要也使得这类数据的收集具有必要性。因此，这类数据的收集使用可以达到必要性的要求。

3. 用户数据，车人交互的桥梁

用户数据包括个人车内活动数据，如车主和乘客信息（如姓名、身份证、电话）、消费与生活习惯信息、用户部分生理数据（体温、心跳频率等）、车主、乘客图像及语音数据，以及驾驶活动数据，如驾驶员习惯、车辆静态信息（如车牌号、车辆识别码）、车辆动态信息（如位置信息、行驶轨迹）等。

根据《车联网信息服务 用户个人信息保护要求》车辆基本资料和设备、系统或平台信息属于个人重要信息。此处的重要信息不同于重要数据，在个人信息安全保护要求中，重要信息属于第二档，即一般信息—重要信息—敏感信息。对于个人重要信息应实施必要的技术和管理措施，保护用户的知情权和选择权，保护用户个人信息的机密性和完整性，确保用户个人信息访问控制安全，建立用户个人信息安全管理规范，一般只需符合个人信息保护的基本要求。身份证、电话等传统敏感信息在个人信息保护领域已经有了相对完善的规定，车联网场景中遵守个人信息保护中关于敏感信息规定即可。车联网领域中特殊的用户数据包括地理信息和生物识别信息。

为了保证车辆安全，高精地图需要反映参与交通主体的地理信息，包括位置、速度、行驶方向、路线等，以实现“车—人”实时交互。地理位置数据能够揭露数据主体的生活状态和生活习惯，包括家庭住址、工作地址以及活动范围等信息，涉及到隐私侵犯。另一类敏感信息是生物识别信息，在使用生物识别信息时，应当保证数据主体对其涉及的数据具有完全的控制权限。一方面，不能将生物识别作为认证的唯一方案，应当提供非生物识别的替代方案，且不会向个人数据主体施加额外的约束条件。另一方面，对生物识别信息采用本地、加密方式存储，不使用外部终端处理。而对构成生物识别模板和用于用户验证的原始数据进行实时处理时，坚决不存储原始生物识别数据。遵循生物识别数据相关的其他要求，例如避免存储原始数据，对构成生物识别模板和用户验证的原始数据进行实时处理。因此，信息处理者在处理地理信息和生物识别信息时，应当严格遵守个人信息保护领域相关原则，最重要的是最小必要原则和知情同意原则。

（二）重点业务环节：数据安全监管的风险与隐患

1. 数据采集：大数据背景下数据过度采集和滥用隐患

车联网信息服务所采集的如车主身份信息（如姓名、身份证、电话）、车辆静态信息（如车牌号、车辆识别码）、车辆动态信息（如位置信息、行驶轨迹）以及用户的驾驶习惯等，都属于用户个人信息，而在必要情形下采集的指纹、声纹、人脸、心律等生物识别特征信息则属于敏感个人信息。目前由整车厂商、车联网服务平台商采集和利用。根据我国个人信息保护原则，个人信息的搜集需遵循“知情同意”“最小必要”“目的限定”三大原则。而处理敏感个人信息需要在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，且取得个人的单独同意。由于车联网属于新兴行业，管理还在完善中，对于哪些数据可被采集、数据如何利用、是否可以分享给第三方等关键问题，还需要细化管理要求，因此目前数据采集还存在过度采集和滥用的风险。

2. 数据传输：产业链条过长加大数据泄露风险

车联网服务具有场景复杂化和功能多元化的特点。车联网生态整合了出行、娱乐、交通管理、导航、车辆远程检测与控制及其他服务等。目前，车联网相关数据主要存储在智能网联汽车和车联网服务平台上，存储和传输方案主要由整车厂商、车联网服务商设计实现。由于数据的采集、传输、存储等环节没有统一的安全要求，即数据具有非结构性特征，可能因访问控制不严、数据存储不当等原因导致数据被窃。

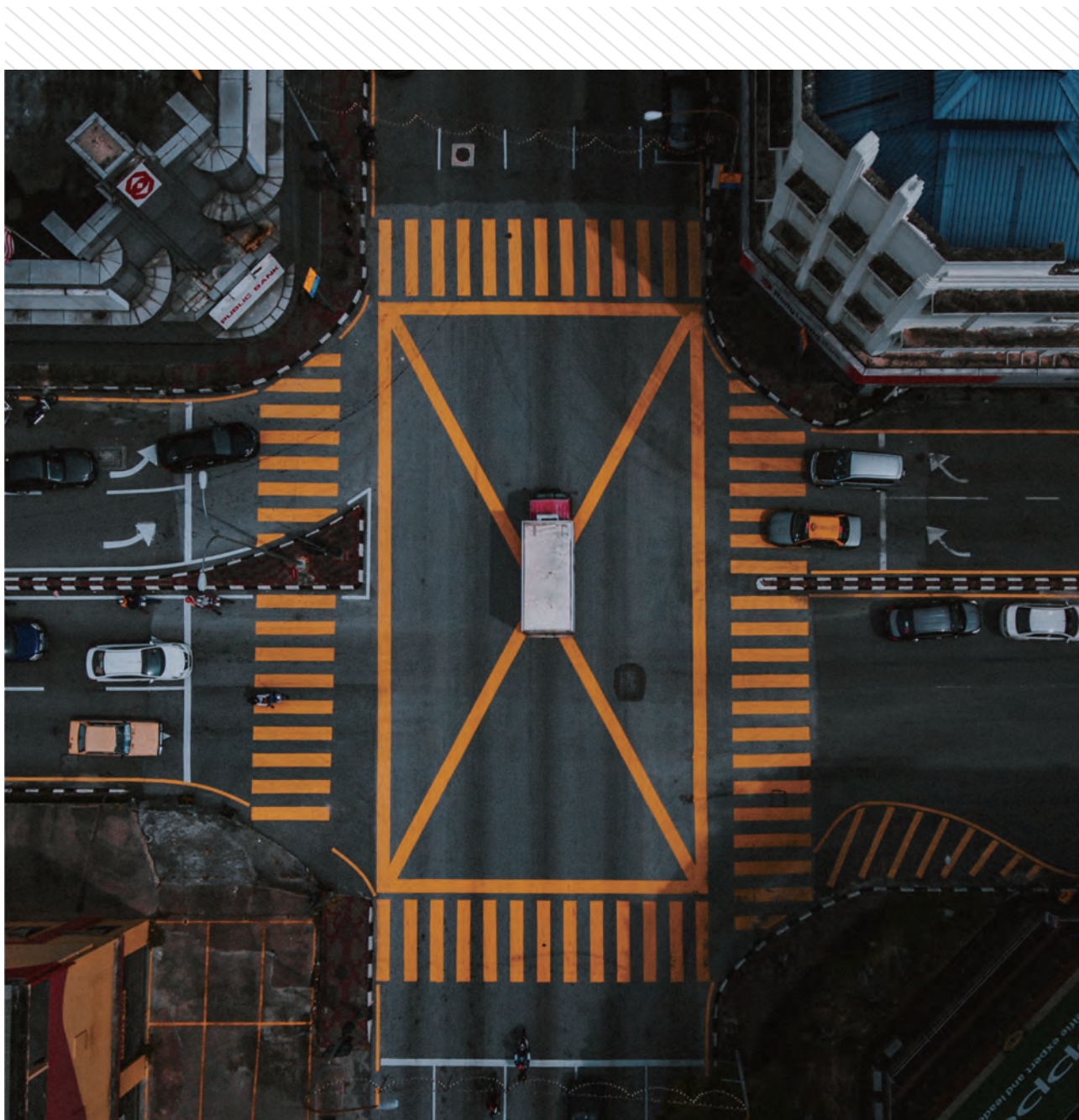
目前主要存在两类风险：一是数据内部传输风险，主要包括 CAN 报文被篡改和伪造的安全风险，连接接口、通信总线被阻塞从而导致数据不可用或无法及时反馈的风险以及 CAN 总线与 ECU 之间缺少相应的认证保护技术引起的风险；二是数据外部传输风险，主要包括车外通信网络传输数据时，在通信链路上会面临被窃听或遭受中间人攻击的风险；以及在特定模式下智能网联汽车会通过 V2V 广播本车的坐标和轨迹信息，从而带来的地理位置信息数据泄露的风险。另外，车联网所构建的网络架构中数据呈双向甚至是多向的流动状态。例如，数据可能从车辆端流向某服务供应商，服务供应商向车辆端反馈特定的信息内容，上下游服务供应商之间、相关人员的移动智能终端与服务供应商之间也会发生点对点或链条式的数据流动，多向流动状态与非结构性特征导致数据传输风险加剧。

因此，《汽车数据安全管理办法（试行）》第六条提出了车内处理原则，即除非确有必要不向车外提供数据。第六条还规定了脱敏处理原则，即要求汽车数据处理者对汽车数据尽可能进行匿名化、去标识化等处理。脱敏处理原则可认为是对车内处理原则的补充。EDPB 的指南实际上也提出了类似的“车内处理”原则，其建议车辆和设备制造商、服务提供商和其他数据控制者处理的数据时应尽可能不涉及个人数据或不将个人数据传输到车辆外部（即数据在车内处理），以保证用户对个人数据的完全控制。

3. 数据出境：全球产业链融合引发数据跨境流动安全隐患

汽车行业的最大特点是全球产业链的高度融合，因此平台数据跨境流动管理问题成为车联网数据安全的重要隐患。数据出境涉及个人信息出境问题和重要数据出境问题。根据《汽车数据安全管理办法（试行）》规定，重要数据包括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，网络运营者应报请主管部门组织安全评估。

从形式上看，数据跨境问题主要体现在两个方面：一是存在境外车联网服务商跨境服务隐患。我国大部分汽车是合资品牌汽车，还有部分汽车属于境外进口汽车，其车联网服务可能由境外企业及其子公司提供，需将车主身份信息、使用习惯、车辆状态及行驶路径等用户信息传往境外。此外，通信数据及车联网数据传往境外，可能泄露国家地理位置信息，危害国家安全。二是存在境内外云平台数据共享隐患，合资企业车联网服务以境内云平台为主，但其外资公司通常负责全球车联网运营，境内平台与境外平台是否互联，是否存在数据传输共享，是国家数据管理需要关注的重点内容。车联网企业应当构建自身的数据评估体系，对于无法出境，或无法判定是否能够出境的数据，应存储在境内的服务器，境内数据中心的设立和管理是数据跨境战略的重要安排。



（一）数据分类分级问题

在车联网数据分类分级指南制定之前，相关企业只能自行对数据进行分类分级。根据目前法律规定，要求企业识别出个人信息、敏感个人信息和重要数据。

车联网数据中存在着大量关于车辆行驶过程中、驾驶者与乘客使用某些车联网应用时系统自动产生的数据，即“Machine generated data”。此类“Machine generated data”是否属于个人信息，从而需要遵守个人信息保护的相关法律规定？这是不少企业在分级过程中面临的困境。

关于个人信息，我国采用的是识别说，根据《个人信息保护法》规定，个人信息指的是“以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息”。因此，个人信息包括两大类，一类是信息本身能够识别出特定自然人，另一类个人信息是由特定自然人在其活动中所产生的信息，与其他信息结合能够识别出特定自然人。很显然，如果一条信息识别到特定自然人所需要结合的其他信息越多，那么其本身构成个人信息的可能性就越低，从而得到的法律保护也应该越弱。因此可以从信息的结合程度进行判断。在实践中，判断信息是否属于个人信息可以结合以下三个方面进行综合判断：

从信息内容上看，判断信息是否出现身份信息、通信通讯联系方式等能直接识别特定自然人的信息，是否能识别出自然人的行踪轨迹。

从信息特征上看，判断其内容是否涉及具体个人，信息是否有助于评价个人的行为或状态，是否能够关联到车辆所有人等特定自然人。

从信息重新结合识别特定自然人的成本上看，判断将已知信息与其他信息结合识别所需的技术门槛、经济成本、耗费事件等。

欧盟 GDPR 规定需要结合客观因素进行考量，例如结合其他信息识别个人所需的时间及处理数据时的可用技术等，但我国法律到目前为止尚未有类似的规定。因此，“Machine generated data”在某些情况下的确有可能构成个人信息，网络运营者应对该类数据按照个人信息的保护要求进行收集、处理、存储及保护。在目前的规范体系下，建议运营者按照已发布指南的示例先行判定，在是否属于个人信息问题上，将个人信息作宽泛理解，从严规范数据处理体系。

隐私认定方面，可以根据隐私的定义从主观方面和客观方面进行综合判断。根据《民法典》第一千零三十二条第二款规定，空间、活动与信息能否界定为隐私，关键在于是否满足以下条件：一是主观上不愿为他人知晓；二是客观上具有私密性。主观层面的“不愿为他人知晓”是指当事人有内容不为他人所知的主观意愿，对内容受保护已经形成了预期，并且这种主观心态或期待应当是合理的，符合社会一般观念，能得到社会普遍接受或认可。客观层面的私密性在于存在空间、活动与信息处于隐秘状态的客观事实，此种隐秘状态与他人利益和社会公共利益无关，不会给他人或社会公共利益带来不可容忍的减损。

（二）主体之间责任分配问题

车联网产业链覆盖“两端一云”，服务产业链条长，参与主体众多，其中包括：汽车制造商、设备制造商、汽车零部件供应商、汽车维修商、汽车经销商、汽车租赁 / 共享公司、车队管理商、保险公司、互联网平台、电信运营商、道路基础设施管理方和公共部门以及驾驶员、所有人、承租人和乘客等。多个汽车网络安全相关标准都明确指出网络安全需要汽车供应链上下游通力合作，推动建立健全安全责任体系要求明确汽车厂商、元器件和软件提供商、设备提供商、通信运营服务商、云服务平台提供商、数据和内容供应商等相关主体的安全责任。

在实践中，数据安全责任按照谁所有谁负责、谁持有谁负责、谁管理谁负责、谁使用谁负责、谁采集谁负责的原则确定。但是在车联网产业中由于供应商众多，采集、持有、管理、使用的流程会出现主体分离的情形，监管机构也很难一次次对数据进行溯源监管。因此，为了保障车辆安全，应当加重整车企业（平台）的义务。

在车联网中，整车企业相当于如今的互联网平台，将一系列服务连接到一起。网联汽车的发展将加速一级供应商开发新产品，届时也会有更多新供应商加入主机厂采购体系。整车厂作为关键节点，应当以网络安全标准为基础，设计健全的供应商准入体系。例如德国汽车 OEMs 对其供应商的信息安全内部审计机制 TISAX，将网络和信息安全能力评估或审计作为与 OEMs 签约和德系汽车行业的市场准入条件。整车企业还应设立与供应商的定期信息交流与信息共享渠道，做好数据安全责任界定和文档记录工作。良好的供应链体系使得数据安全问题有源可溯、有据可查，在数据漏洞问题上也有利于快速定位和及时修复，打通整个供应链链条，才能将汽车网络做成一个安全闭环。

目前，平台监管正在转型升级，算法问责机制等新的监管形式也正在探索，车联网监管可以借鉴平台监管思路，建构数据监管新体系。



当前我国智能网联汽车产业发展进入快车道，数据在智能网联汽车发展中的重要性不言自明。加快推进智能网联汽车数据安全防护能力建设，是贯彻落实《网络安全法》《数据安全法》《个人信息保护法》《汽车数据安全管理办法（试行）》《关于加强智能网联汽车生产企业及产品准入管理的意见》《关于加强车联网网络安全和数据安全工作的通知》《车联网产业发展行动计划》的有力抓手。立足我国智能网联汽车数据安全发展现状，可以从行业调研、落实监管、试点落地等方面加强工作。

（一）细化行业要求，出台车联网数据安全规范指南

结合《网络安全法》《数据安全法》《个人信息保护法》等数据安全法律法规和政策文件，指导智能网联汽车数据安全管理工作。落实《关于加强车联网网络安全和数据安全工作的通知》，按照《车联网（智能网联汽车）网络安全标准体系建设指南》稳步推行按照《国家车联网产业标准体系建设指南》稳步推行指南的制定，加强车联网安全标准的统筹部署。指南中应包含智能网联汽车数据涵盖的范围、数据的分类标准，不同场景下数据安全管理办法，以及对产业链上中下游企业的安全管理要求，以及满足要求的保护措施等。相关部门应当积极主导或参与车联网安全国际标准化活动及工作规则制定，推动具有自主知识产权标准成为国际标准，逐步提升我国在车联网安全国际标准化组织中的影响力。

（二）加强政府监管，建立车联网数据安全防护体系

监管主体方面，保障车联网安全，需强化行业主管部门、市场安全监管部门、交通运输部门以及网络信息主管机构等多部门多机构的协同联动。明确政府各部门在车联网行业领域的职责划分，按照国家政策规定监督指导相关单位落实车联网安全保护责任。加强各部门在车联网安全保护工作上的协调配合，建立完善部门间不定期交流机制，促进监管经验与相关成果共享。

监管对象方面，不同的汽车制造厂商，由于基因不同，对数据安全的认识或者保护能力也大有差异。在监管上应当根据不同类型的企业特征，实施针对性的监管策略，为车联网健康发展保驾护航。目前最主要的智能网联汽车制造商来源于三类企业：

第一类是传统车企，其发展模式是渐进式的，包括目前国产自主品牌的汽车，还有合资品牌的汽车，这类传统车企在推进相关的新技术开发和应用，以及数字化转型工作，其数据安全的认识和理解还在发展当中。传统车企有必要进一步加强数据安全保护工作，以满足监管要求。

第二类是信息技术企业，像百度、阿里、腾讯、华为、滴滴、小米等信息技术企业，这类企业基于在信息技术领域强大的能力和生态，大力推广相应的技术系统、自动驾驶系统等，通过跨越式的方式进军智能网联汽车行业。2020年，阿里联合上汽、上海浦东新区政府，共同打造智能纯电汽车品牌“智己汽车”。华为与长安汽车、宁德时代联合打造智能汽车新品牌等消息层出不穷。2021年9月28日，由小米、OPPO、vivo牵头发起，长安汽车、吉利控股、上汽集团、远峰科技、中科创达、中汽院智能网联等机构共同筹备的「智

慧车联开放联盟 ICCOA」正式成立，参与者包括来自移动智能终端、汽车主机厂、方案和技术提供商、互联网公司、三方检测认证机构及权威科研院所。这些信息技术企业在互联网领域扎根多年，经历了数据宽松到数据严格的过程，与监管“交锋”多年，经验丰富，理应成为监管重点。

第三类是造车新势力。理想、蔚来、小鹏等在发展过程当中是激进式发展过程，他们对于数据安全的考虑和布局可能尚不完善，这类企业对车和软件产品都有一定的研发能力，由于这类企业几乎参与供应链全过程，对其的监管应当覆盖完整的供应链。

（三）加速试点落地，提供车联网数据安全防护指引

车联网数据安全合规存在的一个典型问题是实际落地案例较少，缺少指导性强的操作指南，边界不明确，企业探索成本高。智能网联汽车本身是一个新生事物，又涉及到很复杂的系统，需要政府通过开展试点示范的工作，总结一些优秀的做法，进行后续的推广。目前，正在加快上海临港新片区跨境数据的试点，路测、风险评估以及风险管控相关试点的工作也都在推进过程当中。2021年7月16日，上海经信委发布“关于《上海市智能网联汽车测试与示范实施办法（征求意见稿）》公开征询意见的公告”。2021年6月8日，工业和信息化部办公厅为贯彻落实《新能源汽车产业发展规划（2021-2035年）》《智能汽车创新发展战略》和车联网产业发展专委会第四次全体会议工作任务要求，加快推进车联网网络安全保障能力建设，构建车联网身份认证和安全信任体系，推动商用密码应用，保障蜂窝车联网（C-V2X）通信安全，工信部开展了车联网身份认证和安全信任试点工作；为落实《关于加强智能网联汽车生产企业及产品准入管理的意见》（工信部通装〔2021〕103号，下称《意见》）有关要求，受工业和信息化部装备工业一司委托，我中心组织开展汽车数据安全、网络安全、软件在线升级（又称OTA升级）和驾驶辅助功能情况自查工作。7月27日，《智能网联汽车道路测试与示范应用管理规范（试行）》的通知发布

从政府推进产业发展和保障数据安全的角度也面临不少挑战。一是整个法规体系、标准体系还是相对滞后于产业的发展速度。二是存在多头监管的问题，还需尽快细化一些行业性的管理要求。从数据安全监管的角度，国家网信部门作为牵头部门，近期已经出台了一系列政策文件，还需要一些重要的行业协会去推动相关工作。三是实操性的举措还不够，数据安全监管和治理的一项基础性工作就是要做到数据分类分级，对于数据既要管，又不能管得太死，哪些要管，哪些需要高强手段的监管，哪些需要在市场上流动，这些问题的回答高度依赖数据分类分级体系。

政府的角度，推进产业发展和保障数据安全包括四个方面：一是统筹产业创新发展与保障数据安全。二是尽快出台数据分类分级指南和管理细则，在国内一些重要的行业领域，比如金融、工业互联网等领域，已经出台了相应的分类分级指南，智能网联汽车行业可以予以借鉴。三是建立事前风险评估和事后应急响应机制，比如国家级的专业技术机构可以探讨如何更好的提供服务和支撑。四是重点关注跨境数据流动问题，国家网信部门也在密集调研和研究，希望后续在借鉴全球通用做法的同时，细化相应的数据流动规则。

06 结 语

随着《汽车数据安全管理办法（试行）》等汽车行业数据安全的细化规则的实施，数据安全成为车联网安全的核心，完善车联网产业数据安全标准与规范成为当下引导车联网产业数据安全建设的重点措施。在车联网行业中，其数据具有多样性、规模性、非结构性、流动性、保密性等特征，因此在数据管理中，区分重点数据类型与重点业务环节有利于抓住主要矛盾。车联网行业中的数据安全挑战包括数据分类分级问题、重要数据的处理、存储和出境问题和主体责任分配问题，解决这些问题需要行业、企业、政府多方协力，细化行业要求、加强政府监管、加速试点落地。

二〇二二年三月



参考文献 REFERENCES

- [1] 区块链技术与数据安全工信部重点实验室. 自动驾驶数据安全白皮书 (2020)[R].2020.
- [2] 中国信息通信研究院. 车联网网络安全白皮书 (2017)[R].2017.
- [3] 中国信息通信研究院. 车联网白皮书 (2018)[R].2018.
- [4] 360 智能网联汽车安全实验室. 2019 智能网联汽车信息安全年度报告 [R].2019.
- [5] 中国信息通信研究院. 大数据安全白皮书 (2018)[R].2018.
- [6] 中国信息通信研究院. 电信和互联网用户个人信息保护白皮书 (2018)[R].2018.
- [7] 中国汽车工程学会等. 智能网联汽车信息安全白皮书 (2016)[R].2016.
- [8] 网喵:《“车联网”的安全问题关键还是网络信息安全》, 载 <https://cn-mobi.com/?p=3894>。
- [9] 车讯网:《2020 年车联网信息安全十大风险与车联网数据合规建议》, 载 <http://www.chexun.com/2020-09-25/111856155.html>。
- [10] 张迪:《车联网场景下的个人信息保护》, 载 <http://www.fajida.com/h-nd-68.html>。
- [11] 陈际红等:《GDPR 下车联网个人数据风险及应对——解读 EDPB< 车联网个人数据保护指南 >》, 载微信公众号 TMT 法律论坛, https://mp.weixin.qq.com/s/q4iTMkOENgYnmdQpC3_fvg。
- [12] 吴卫明:《车联网的网络及数据合规问题研究》, 载微信公众号锦天城律师事务所, <https://mp.weixin.qq.com/s/zaErdPgHdZosWLXBI4vWHQ>。
- [13] 新基建产业金融:《车联网个人数据合规漫谈》, 载微信公众号数字研究, <https://mp.weixin.qq.com/s/6ZUAEfqE8LIXkYKQNfxsAw>。
- [14] 潘永建, 邓梓珊:《简析车联网应用下个人隐私保护难点与对策》, 载微信公众号通力律师, <https://mp.weixin.qq.com/s/lkojz8BmPPWZJR8KRAhwkw>。
- [15] 尚浩东, 杨千惠:《万物互联——关于车联网的法律监管》, 载微信公众号中伦视界, <https://mp.weixin.qq.com/s/S99EotoX8PXSQX7K8bkcOg>。
- [16] 吴卫明, 赵彬吟:《智能网联汽车数据的归属——个人信息保护的视角》, 载 <https://www.allbright-law.com/CN/10475/50097758efcc19f2.aspx>。
- [17] 陈兵, 胡珍:《筑牢数据安全底线 推进车联网数据安全建设》, 载第一财经, <https://www.yicai.com/news/101036917.html>。
- [18] 肖马克, 赵新华:《自动驾驶汽车: 如何处理隐私问题? 》, 载微信公众号金杜研究院, <https://mp.weixin.qq.com/s/Q-Sn6pZIW8AQn-YR-4H5gw>。
- [19] 陈立彤:《国内外自动驾驶法律环境分析》, 载《自动驾驶蓝皮书》。
- [20] 覃庆玲, 谢俐惊. 车联网数据安全风险分析及相关建议 [J]. 信息通信技术与政策, 2020(8): 37-40.

关于我们 ABOUT US

毕马威中国



毕马威是一个由独立的专业成员所组成的全球性组织。遍布全球 145 个国家和地区，拥有专业人员超过 236,000 名，提供审计、税务和咨询等专业服务。毕马威在中国二十八个城市设有办事机构。毕马威咨询服务向客户提供一系列数字和业务转型解决方案，屡获殊荣。在过去一年，IDC、Forrester 和 HFS 称赞毕马威的数字战略、数据分析和人工智能服务具有“领先地位”。毕马威深耕中国金融业多年，非常幸运地参与中国银行业变革和里程碑事件，与业内同仁在每一次的变革浪潮中共同奋楫前行。毕马威认为，未来银行是银行业把握科技变革对商业社会重塑的奇点性机遇，以此重新认知和构建银行的生态和企业价值链，重塑银行与社会和客户的链接。毕马威面向银行业客户，提供数字化银行、开放银行战略，金融科技生态与智慧风控、智慧财务、智能租赁、智能合规等未来银行的全方位解决方案。将会携手银行共同把握未来银行的机遇，通过客户洞察、产品与服务、渠道交互、运营流程等进行智能化改造，从而实现对未来银行的全方位赋能。

观韬中茂律师事务所



观韬中茂律师事务所成立于 1994 年 2 月，是总部设于中国北京的专业化、综合性大型律师事务所。经过与创设于上世纪五十年代的香港王泽长·周淑嫻·周永健律师行，以及创建于上世纪九十年代的上海市中茂律师事务所、上海市申达律师事务所的合并，观韬中茂现拥有 800 余名律师、200 余位合伙人，在法律服务、专业建设和律师团队等方面已成为中国优秀律师事务所之一。

王渝伟律师数据合规团队是观韬中茂律师事务所专注网络安全、数据隐私合规法律服务的专业团队，在大数据、人工智能、互联网、金融科技、云计算、物联网等领域拥有为头部企业提供涉及复杂技术与商业场景项目提供全面数据合规服务的丰富经验和卓越能力。

联合出品 CO-PRODUCER



观韬中茂律师事务所
Guantao Law Firm

报告出品人

王渝伟 张令琪

报告作者

刘裕 邬敏华 陈刚 朱敏婕

联络邮箱

wangyw@guantao.com

richard.zhang@kpmg.com

fm.wu@kpmg.com