我国智能网联汽车数据安全风险与控制

张金浩
长城汽车股份有限公司

[摘 要]随着人们物质生活水平的提高，私家车数量与日俱增，大大推动了汽车行业的发展与转型。2015年，我国首次提出“互联网+”的概念，推动各个产业进入网联时代，云计算、大数据、5G技术等科技快速发展促进了汽车智能化发展，成为未来我国汽车产业的主要发展方向与目标。汽车产业转型升级成为时代选择，网络化智能汽车成为中国制造业发展的重要方向。因此，探索车联网技术的发展方向，将继续刺激中国汽车产业的增长，规避不可预知的风险。提高我国智能电网的技术水平，可以有效提升车辆的自动驾驶功能。

[关键词]智能网联汽车；数据安全风险；控制
【DOI】10.12252/j.issn.2096-6288.2020.03.1064

引言

近年来,随着汽车产业的转型升级,智能网联汽车进入快速发展机遇期。自动驾驶、智能座舱、互联科技等数字化功能正加速“登录”汽车产品,虽然这些功能强化了驾乘便利性,丰富了座舱娱乐性,但其背后的安全问题却成为产业上下游的共同关切。全程联网的车机应用,以及“数以T记”的行车数据,给汽车行业带来了网络安全与数据安全的新挑战。加强汽车网络安全与数据安全的保障能力,未来将成为车企的主要竞争力,更将为智能网联汽车产业发展保驾护航。

一、我国智能网联汽车研究背景

目前，我国智能网联汽车正处于技术快速演进、产业加速布局的关键阶段，基本与全球先进水平处于“并跑”阶段。近年来，为实现弯道超车，确保汽车科技研发与实际运用同步发展，我国在已有汽车制造技术的基础上，积极推行智能化、网联化等新技术，同时积极落实行业规范、生产标准，国家及地方政策、标准体系、功能量产、技术方案、示范运行等都在加速落地、布局、完善、迭代，进而满足智能网联汽车发展的需要，推动汽车产业的健康可持续发展。2009年，中国超越美国，成为全球最大的汽车制造国和最大的汽车市场，当年产销均超过1350万辆。2017年，汽车保有量突破2亿，根据市场调研报告显示，购买意愿超过5亿，在受到资源约束的情况下，购买意愿在2017年控制在4亿之内。2013年，在国家政策的大力支持下，多家主机厂商、科研机构、运营商以及高等院校等组织达成智能网联与未来汽车发展趋势的研究共识，共同成立“中国车联网产业技术创新战略联盟”，2015年更名为“智能网联汽车产业技术创新战略联盟”。联盟成立之后，集众家之所长，借助协同创新，借助先进技术促进技术共享，优化资源配置，并且将智能网联技术作为汽车发展的主要技术。通过完善制度标准的体系、搭建数据技术共享平台来促进案例试点工程推进，促进汽车生产建设的发展，对汽车的可持续发展有良好的作用，更有利于推动智能网联汽车产业模式的正向发展，为我国汽车产业的总体发展奠定了良好基础条件。随着智能化、网联化乃至于数字化等新技术的不断注入，越来越多的企业加入到智能网联汽车赛道，汽车产业链、供应链以及生态链都进入重塑重构状态，智能网联汽车的市场规模日益扩大。2015年以来，乐视、蔚来、理想、小鹏、威马等造车新势力层出不穷，围绕汽车技术生产与研发端，倡导将传统汽车生产技术优势与现阶段互联网技术发展特点相结合，进一步推动了智能网联汽车的快速发展。

二、我国智能网联汽车数据安全风险

（一）数据采集

根据研究估算，一辆智能汽车每天大概会产生大约10TB的数据。智能网联汽车厂商采集信息，不仅是用于汽车自动驾驶分析决策，还是为了获得进行商业创新和拓展市场的数据资源。

第一，行车安全风险。由于智能网联汽车搭载了车载传感器，若车载传感器会被攻击，可能会采集到一些虚假数据，影响到行车安全。

第二，个人隐私风险。目前智能网联汽车法律规制和行业规范尚未完善，厂商可能会以欺诈、诱骗、误导等方式收集个人数据，并隐瞒数据的使用目的、方式和范围；在车辆相关不同功能或者产品收集多种用户个人数据时，会强制用户一次性全部授权同意等；在采集数据的过程中，存在未经授权的非法采集隐患，即汽车上装载的传感器会对车上用户甚至车外的行人持续获取信息，存在侵犯个人隐私的风险。

第三，国家安全风险。在智能网联汽车厂商采集数据过程中，特别是涉及到实时环境信息、敏感的地理位置信息等，一旦被滥用或恶意泄露，会对国家安全带来巨大的风险。

（二）数据使用

第一，敏感数据易被获取。由于智能网联汽车在存储阶段对数据分级分类不清，对重要和敏感的数据未进行加密保护，从而导致敏感数据在未经过授权的情况下极易被非法获取，也一定程度上存在个人隐私泄露的风险。

第二，数据滥用。当前，智能网联汽车的数据是掌握在车企手中的，数据也成为其产品开发和市场扩展的重要资源，但我国《民法典》明确规定公民是数据的所有者，个人数据能否成为车企开发产品的资源是值得商榷的，而且由于智能网联汽车数据的权责不明确，也存在数据滥用的风险。

第三，数据公开难且真实性存疑。在智能网联汽车中，虽然个人是数据的所有者，但是数据掌握在车企手中。一方面，车企一方在最初以各种理由推诿且不愿意公开有关数据，在数据使用的过程中存在数据公开难的问题，公开与不公开都是车企一方自主决定。另一方面，数据真实性存疑，某种意义上而

言，数据层面的“第一现场”已经失去，更改黑匣子数据的可能性是存在的。某些车企将自己管理的数据在未经第三方监管的情况下拿出来，数据公信力不足。

三、我国智能网联汽车数据安全风险控制措施

（一）完善相关标准法规

目前各大国际标准化组织围绕信息安全开展了跨领域的研究，很多标准项目由多个标准化组织共同研究。近些年我国逐渐加入了国际标准的研究与制定过程中。早在2014年，联合国WP.29就成立了智能交通/自动驾驶（ITS/AD）非正式工作组，统筹协调智能交通系统和自动驾驶技术的共性问题和法规，并修订相关法规条款。在汽车信息安全方面，已经发布了UNR155《信息安全与信息安全管理系统》和UNR156《软件升级与软件升级管理系统》2项法规，对新认证车型从2022年7月起实施，新生产车2024年7月起实施，如不满足则不能销售。国际标准化组织ISO下设ISO/TC22和ISO/TC204两个智能网联汽车相关的技术委员会，其中ISO/TC22涉及汽车信息安全业务。在汽车信息安全方面，ISO与SAE（前美国汽车工程师学会）成立了联合工作组，共同制定了ISO/SAE21434：该标准全面规定了车辆及其部件和网络接口的网络安全风险管理，包括风险评估方法、资产识别、威胁分析、影响评估、漏洞分析、攻击分析及风险处理等内容。ISO/SAE21434与UNR155共同为网络安全监管和相关认证提供重要文件参考。我国智能网联汽车标准体系的建设充分借鉴了国际标准的路线。2003年，全国智能运输系统标准化技术委员会（SAC/TC268）正式成立，目前已完成智能网联驾驶标准体系的初步构建，包括信息服务及信息安全在内的5个重点领域。2017年，全国汽车标准化技术委员会智能网联分技术委员会（SAC/TC114/SC34）正式成立，之后陆续成立包括“信息安全标准工作组”在内的多个工作组。截至目前，信息安全标准工作组依据体系规划已分4批次开展了15项标准制定及研究项目，涵盖整车、系统部件技术与过程管理类标准。

（二）科学应用人工智能技术

1.复杂场景下驾驶应用

在我国，交通运输有着十分复杂的应用场景，比如建筑垃圾清运、山体滑坡抢修、矿山特种设备运载服务。这些复杂的场景，由人来驾驶，对人员的技术要求很高，也会对相关的车辆和工程机械会产生一定的风险。比如在矿山领域出现的各种突发的地质灾害，有可能对驾驶员和车辆造成致命影响。在这种情况下，无人驾驶就有了比较典型的应用，基于人工智能技术开发面向复杂场景的驾驶辅助技术，利用5G、大数据、云计算等技术，实现对车辆的定位以及突发情况的预警，能够实现复杂场景下驾驶应用，极大地提升特种领域的作业水平，减少安全风险。

2.自动避险应用

汽车最大的红线是安全，通过人工智能技术的应用，实现智能网联汽车自动避险，从而保障乘坐人员的人身安全，是人工智能技术的重要目标。目前，已经有多项成熟的人工智能技术服务于自动避险应用。比较典型的如V2X技术，与移动互联网融合，实现与外界信息的即时互动，再通过人机交互传递到人大脑信号，及时提醒驾驶人做出避险动作，比如在前方发生泥石流、滑坡时，车载雷达检测到之后，迅速将相关的信息传递到车载大屏上，能够为用户提供突发状况提醒服务，提醒驾驶人及时避让，绕行通过。

（三）网络数据深度利用

基于车联网技术，智能汽车未来应进一步加强网络和大数据的应用。同时，利用大数据技术引导交通，实现车辆控制、交通塑造标志、交通拥堵等数据的良好匹配率，汽车驾驶可以有效避开道路拥堵，调整红绿灯时间。根据汽车提供的拥堵数据，智能汽车与交通系统的实时融合可以有效缓解交通压力。通过在汽车和网络大数据的监督和引导下智能协调车与车之间的距离和速度，可以有效减少交通事故。

（四）制定智能网联汽车数据安全标准实施细则

针对智能网联汽车数据采集和存储中出现的安全风险，虽然目前在部门规章中多次提出要加强数据分级分类，对敏感数据加强保护等等，但具体的内容和实施细则并未规定。因此，要加快制定智能网联汽车数据安全标准实施细则，与此同时还可以通过促进科研机构和智能网联汽车厂商相互合作的方式，研究制定智能网联汽车数据安全相关的全生命周期管理、技术、测评等标准规范，共同推进智能网联汽车数据安全标准的运用。第一，制定数据分级分类的标准细则。一方面，对数据安全等级划分，对敏感数据和个人信息加强保护和提高访问权限，以防国家秘密被窃取、泄露和个人信息被滥用的风险。另一方面，对数据进行分类存储。对不同行业不同种类的数据进行分类存储而非统一集中化无序存储，将极大便利数据的使用。第二，明确智能网联汽车厂商采集数据的范围。对于涉及个人隐私的数据，应该在数据安全标准实施细则中明确规定是否可以采集、采集后应如何防止个人隐私被泄露和如何加强对采集的个人信息的技术保护。第三，禁止智能网联汽车厂商强制性要求用户一次性授权同意采集所有用户个人数据。在实践中，用户在使用智能网联汽车产品的功能和服务前，常常会出现车企强制性要求用户一次性授权全部个人数据，否则就不能使用该产品。在数据安全实施细则中，应严厉打击此种行为，并在合理的范围内对车企收集用户个人数据的种类和范围进行明确规定。

结语

当前社会迫切需要一种高效、环保、便捷的出行工具，智能网联汽车在满足以上条件的同时，更兼备了低能、安全、舒适等优点，成为当前高效环保汽车产业的主要重要部分。其重要性不仅在于汽车产品和技术的提升，更在于汽车及相关产业的全业态和价值链体系的变革。如果能够充分整合多方技术优势，依托先进的设计，中国网络联盟下的汽车技术和产业发展必将成为汽车产业转型提升的重要推动力。

参考文献

[1]张浩,唐林, and 陈全思.2019智能网联汽车政策法律观察[J].智能网联汽车.(2019):6.