头豹 LeadLeo
www.leadleo.com

市场简报：数据安全新规发布，智能汽车将何去何从？

Briefing Report: What will happen to smart cars with the release of new data security regulations?

市場速報：データセキュリティの新規制発表、スマートカーはどうなる?

报告标签：智能汽车、数据安全、自动驾驶

主笔人：罗浩峰

Q1：360全景影像、全程监控等功能对智能汽车有何重要性？

图表1：特斯拉360全景影像

■ **360°全景影像等功能的引入大大提高了驾驶员的驾驶体验，成为消费者选择新能源汽车的关键因素之一**

智能网联化功能成为新能源汽车主要卖点。在汽车智能化趋势下，360°全景影像、远程监控等智能网联化功能已经成为越来越多汽车，尤其是新能源汽车的标配功能和宣传卖点。凭借强大的功能，智能网联化功能吸引了大批消费者。

360°全景影像等功能赋能驾驶体验。360°全景影像是大众最为熟悉也是最常使用的智能功能之一。在驾驶员在倒车入库时，自动触发倒车影像和报警设备，可以帮助驾驶员看清四周障碍物避免碰撞。同时，智能倒车轨迹可以精确显示车轮即将经过的轨迹实现辅助倒车。在行车过程中，四周摄像头会实时监控并记录四周情况，杜绝行车盲区，也为碰瓷留下证据。除此之外，很多新能源汽车还配置了远程监控功能。车主可以通过手机APP远程调用车上的摄像头，以便车主可以观察车辆周围的一些异常情况。

图表2：热门车型硬件对比

单位：【个】	特斯拉 Model Y	理想L9	蔚来ET7	小鹏P7
摄像头数量	8	11	11	13
超声波雷达数量	12	12	12	12
毫米波雷达数量	1	1	5	5
激光雷达数量	0	1	1	0

■ **车载摄像头是新能源汽车智能化的重要手段**

车载摄像头堪称“智能汽车之眼”。车载摄像头被广泛运用于智能驾驶环境感知、环境探测视觉呈现、驾驶舱监控三大方面。事实上，拍照相关的功能只是车载摄像头的作用之一，大部分人工智能技术在很大程度上也都需要依赖于它。摄像头作为自动驾驶汽车采集信息、分析图像的重要途径，在L2级以上自动驾驶中起着主导作用。根据数据显示，现阶段智能汽车发展处于L2 ++阶段，大概需要3-12个摄像头。随着自动驾驶等级不断提高，越来越多的摄像头将会被安装在新能源汽车上。对比四款在售的热门车型，摄像头的数量基本都是8个以上，小鹏的P7更是安装了13个摄像头。由此，不难看出摄像头在汽车智能化、网联化扮演了重要角色。

来源：有驾、智驾最前沿、太平洋汽车网、头豹研究院

Q2：针对智能汽车数据安全颁布了哪些重要法规？

图表3：相关政策梳理

■ 智能汽车数据安全相关法规逐渐完善

顶层设计构建中国数据安全基本框架。从2017年到2021年，全国人民代表大会常务委员会陆续通过三部大法，表明了中国政府对于全行业信息安全的重视程度，构建了中国信息安全的法律基本框架。

2021年开启中国智能汽车数据安全元年。2021年开始，从中央到地方政府都陆续出台了一系列智能汽车信息安全、数据安全、网络安全等相关政策文件，为智能网联汽车信息安全进一步健全起到促进和指引作用。

■ 《汽车数据安全管理若干规定（试行）》出台意义非凡。

中国首部针对汽车数据安全的正式法规。2021年8月，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、交通运输部五部门联合发布了《汽车数据安全管理若干规定（试行）》（以下简称《规定》）。《规定》自2021年10月1日起正式施行。

《规定》主要从车内座舱数据、车外人脸或车牌等敏感数据、个人隐私告知三方面，对汽车内外的数据采集、传输、使用进行了规范界定，对汽车数据处理者进行了责权划分。倡导汽车数据处理者在开展汽车数据处理活动中坚持以下原则：

- **车内处理原则**，除非确有必要不向车外提供；
- **默认不收集原则**，除非驾驶人自主设定，每次驾驶时默认设定为不收集状态；
- **精度范围适用原则**，根据所提供功能服务对数据精度的要求确定摄像头、雷达等的覆盖范围、分辨率；
- **脱敏处理原则**，尽可能进行匿名化、去标识化等处理。

《规定》指出，因保证行车安全需要，无法征得个人同意采集到车外个人信息且向车外提供的，应当进行匿名化处理，包括删除含有能够识别自然人的画面，或者对画面中的人脸信息等进行局部轮廓化处理等。这一规定，**对现有的360°全景影像等功能的作用产生了极大的限制作用。**

来源：中国工信产业网、智驾最前沿、头豹研究院

Q3：360全息影像等功能如此便捷，为何要出台相关政策予以限制？

■ **人工智能技术加速渗透汽车产业，汽车数据安全等隐患日益加剧。**

随着人工智能技术与汽车产业加速融合，智能汽车产业快速发展。汽车数据采集和处理能力不断提高的同时，也暴露出的汽车数据安全问题和风险隐患日益突出。工信部指出，近年来，整车企业以及车联网信息服务商等相关企业和平台遭遇的恶意攻击高达280余万次，85%的关键部件存在着安全漏洞。中国车联网的信息安全问题十分严峻，危害巨大。

图表4：特斯拉数据泄露

TESLA

NON-DISCLOSURE AGREEMENT

THIS NON-DISCLOSURE AGREEMENT (this "NDA") is entered into as of the date indicated above (the "Effective Date") between Tesla Motors, Inc., a Delaware corporation ("Tesla"), and the company or individual identified below ("Company"). Tesla may disclose Confidential Information to Company for purposes of considering a potential business relationship with Company or fulfilling the objectives of such business relationship (collectively, the "Purpose"). Tesla and Company are each referred to herein as a "Party" or collectively as the "Parties". The Parties hereby agree as follows:

1. "Confidential Information" means information disclosed by Tesla to Company including, but not limited to, trade secrets, physical samples, financial, business, sales or technical information, terms of agreements, negotiations or proposals, all data, and such other information disclosed (a) in written or other tangible form and marked "Confidential" or with words of similar import, (b) orally or visually and identified as confidential or proprietary information at the time of disclosure, or (c) under circumstances by which Company should reasonably understand such information is to be treated as confidential, whether or not marked "Confidential" or otherwise. All Confidential Information and derivations thereof shall remain Tesla's sole and exclusive property and no license or other right to such Confidential Information or

4. No Publicity. Company agrees that it shall not make any public disclosures relating to the existence of this NDA or the Purpose without the prior written consent of Tesla.

5. Exceptions. The obligations of Section 2 of this NDA shall not apply to information that: (a) is already known to Company at the time of disclosure without obligation of confidentiality to Tesla, (b) is or becomes publicly known through no wrongful act or omission of Company, (c) is rightfully received by Company from a third party without obligation of confidentiality, (d) is approved for release by Tesla's written authorization, or (e) was developed by Company independently and without the use or benefit of any of the Confidential Information. A disclosure of Confidential

数据上云引发的数据泄密和网络安全问题日益突出。智能化时代，大量重要的数据被上传到云端，并运用人工智能技术进行分析处理。由于缺乏网络安全防控措施，云上服务器正在沦落为网络攻击的最新目标。2018年，网络安全公司UpGuard的研究员Chris Vickery发现包括特斯拉、丰田、大众在内的上百家车企机密文件可以被轻松访问。机密文件涉及从车厂发展蓝图规划到各种保密文件，共计157千兆字节，包含近47,000个文件。2021年特斯拉又爆发"隐私门"事件，外国一名黑客发现特斯拉车内摄像头能够清晰地记录驾乘人员的各种举止甚至面部微表情。车主隐私无法得到保障，采集到的相关数据也存在泄密的可能。此外，2022年3月，丰田旗下一家汽车零部件供应商小岛冲压工业遭到网络攻击，发生系统故障，导致丰田的零部件管理系统中断运行。丰田不得不暂时停止日本全境14家工厂、28条生产线的汽车生产工作，汽车减产数量约为1.3万辆。

终端方面，车辆遭遇远程操纵和功能失效的案例屡见不鲜。2019年，黑客通过入侵共享汽车App、改写程序和数据的方式，盗走德国汽车租赁公司Car2Go多达100辆奔驰豪华轿车。同样在德国，2022年1月，一名少年黑客通过第三方软件可远程操控特斯拉汽车，实现控制车窗、无钥匙启动汽车、关闭安全系统、以及监视驾驶员。

重要敏感区域和个人信息存在侵犯可能，或危害国家安全、公共利益或者个人、组织合法权益。新能源汽车搭载的移动摄像装置会实时记录汽车周边以及车内的各种信息，并且上传到汽车厂商的服务上。尤其是当汽车接近一些敏感的军事区域或者政府部门，记录下的建筑和交通信息或许会创造巨大的安全隐患。2021年，特斯拉汽车被俄罗斯禁止进入军工单位和军事基地，因为担心很多敏感信息将会被收集并直接实时传回美国。无独有偶，2022年6月，柏林警方也因为特斯拉汽车摄像头系统而做出决定，禁止特斯拉汽车进入警局各单位或在警局各单位泊车。并且，警察总部和州刑事警察局等部门，也禁止购买特斯拉制造的汽车作为共用财产。

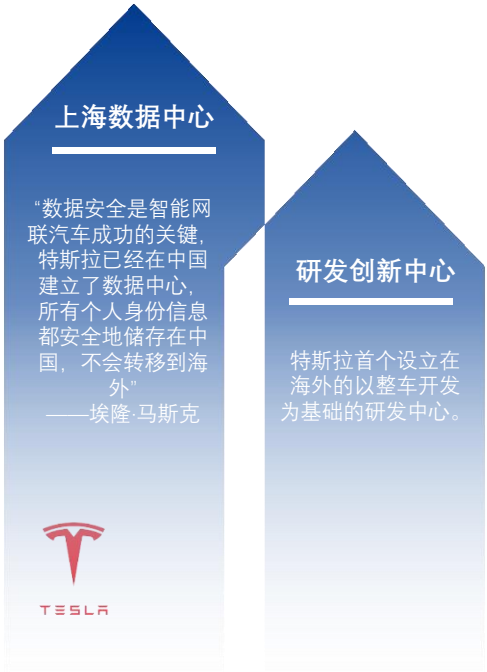
来源：中科信安、有驾、懂车帝、头豹研究院

Q4：相关政策对智能汽车行业有何影响？

■ **短期内，车企为了应对数据安全监管不得不暂停使用多项人工智能技术。**

车企纷纷禁用360°全景、远程监控等功能，遭到车主投诉。2022年6月起亚汽车发布《360°全景功能关闭通知》公告表示，根据国家个人信息保护及汽车数据安全管理相关法律法规的要求，自7月11日起，将关闭360°全景功能。受限功能主要是指通过手机APP实时查看车辆周围环境的功能。实际上，起亚汽车这步举措相比其他车企是晚了一大拍。自从2021年10月《规定》发布以来，以比亚迪和长安汽车为代表的传统汽车厂商，小鹏汽车为代表的造车新势力，以及特斯拉等海外车企，纷纷响应政策，下架了车外摄像头的访问功能。随着车企整改进一步渗透，车主们质疑的声音也随之而来。长安汽车"减配"现象引起了大量车主们的不满，认为自己花钱购买的配置却无法使用，称车企涉嫌虚假宣传，对品牌形象造成严重的负面影响。

图表5：特斯拉在建立数据和创新中心



来源：头豹研究院

■ **长期来看，政策的颁布对智能汽车行业多个方面产生了深远影响。**

车企为满足数据合规必然需要进行软硬件升级，增加额外成本。从技术角度来看，图片的脱敏处理可以通过OTA进行在线升级实现。硬件层面，图像脱敏需要一定的算力支持，很多老款车型由于没有将数据合规的问题考虑进去，座舱芯片并不足以支撑OTA升级。因此，未来车企在开发新车型时，不会只是一味地堆砌最新技术，而是会从成本、功能效果以及收益等多个角度进行衡量。

对外国车企来说，数据离境也是一大难题。根据中国相关政策，网联汽车通过摄像头等传感器从车外环境采集的各类数据不得出境。对于确需向境外提供的数据和信息，需要通过国家网信部门组织的数据出境安全评估。因此，数据合规倒逼国外车企在中国花费额外成本建立数据中心并建立完善的研发团队。2021年5月，特斯拉官方通过社交媒体宣布公司已经在中国建立数据中心，以实现数据存储本地化，并将陆续增加更多本地数据中心。根据公告显示，所有在中国大陆市场销售车辆所产生的数据都将存储在境内，并向车主开放信息查询平台。因为大量中国的行驶数据无法出境，外国车企还将不得已在中国本地建立一支完善的自动驾驶研发团队，利用相关数据开发适用于中国路况的自动驾驶方案。

对汽车智能化最大的挑战来源于对数据质量的担忧。《规定》的出台在一定程度上有悖于自动驾驶技术的发展。自动驾驶作为人工智能技术的分支，主要依赖于机器学习的自动驾驶模型。自动驾驶模型根据驾驶时采集的行驶环境数据做出动作策略从而控制车辆自动地执行相应的动作。模型的训练需要海量的数据，尤其是自动驾驶这种复杂的人工智能特别需要大量的路况数据以及原始图像数据，以便模型能够更加准确对障碍物、线路、交通信号等进行识别。在新规之下，数据的采集和储存都有诸多限制，很多隐私信息和数据将会被过滤掉，进而影响用于训练的数据质量。

Q5：智能汽车行业如何破局？

■ **面对政策限制，汽车厂商车外摄像头采集到的信息可进行图像脱敏处理。而车内数据可以通过信息本地储存，或是使用红外雷达代替车内高清摄像头的方式实现数据合规。**

从技术层面，图像脱敏处理是可以通过算力支持和OTA在线升级完成。首先政策上需要明确的是，中国政府并没有规定车载摄像头不允许使用和用于图像采集的。政策的出台只是在采集过程中加了个脱敏前提。对于新上市的车型，摄像头的安装已考虑数据合规问题。例如新上市的上汽智己 L7，配备了三颗总计一亿五千万像素的Carlog智能车载摄像系统，可以针对人脸等外部敏感信息进行模糊化处理以应对数据合规。对于一些老款车型，由于在上市之前没有考虑数据合规问题，需要后期进行软硬件的升级。硬件方面需要车型搭载4-5TOPS算力以上的座舱芯片以应对脱敏处理。如果硬件足够，那么只需要通过OTA升级在算法上实现对敏感信息的识别和处理工作。

为应对数据合规车内监控数据可以改为本地储存，或考虑使用红外雷达代替车内高清摄像头。根据欧盟法规，从2022年7月起所有具备 L2及以上自动驾驶系统的车辆将强制装配疲劳分神预警系统（DDAW）。2024年7月之后，所有的新车将强制安装此功能。中国政府也已经强制要求商用车车型安装DMS（防疲劳预警系统）。因此，无论是比亚迪、宝马等传统车企还是蔚来、小鹏等造车新势力都在车内安装了摄像头用于监测驾驶员疲劳驾驶和辅助自动驾驶。2021年5月特斯拉发布公告称，车内摄像头会在自动驾驶过程中检测并提醒司机注意力不集中。但是摄像头收集到的数据只会存储在本地，除非车主启用数据共享。这一措施也得到包括蔚来在内的很多车企的积极响应，纷纷跟进车内监控数据本地处理，处理完毕后立刻删除的措施。除此之外，红外雷达可以通过驾驶者的轮廓和行动轨迹来判断驾驶者的状态，或许可以成为高清摄像头的完美替代。相较于高清摄像头，红外雷达只会记录完全模糊的轮廓而不是清晰的影像，不会窃取用户的隐私，可以为车主提供更高的隐私保护。

图表6：汽车传感器对比

传感器	摄像头	红外	超声波	激光	毫米波雷达
成本	中	优	优	差	中
距离绝对精度	优	差	中	优	优
测速精度	中	差	差	中	优
测量距离	优	差	差	优	优
穿透性	差	差	中	差	优
全天候	差	差	中	差	优
隐私保护	差	优	优	优	优
稳定性	优	中	差	优	优

■ **数据的安全保障离不开从主机厂、零部件供应商、政府监管机构以及信息安全供应商的紧密合作。**

在汽车数据安全领域，第三方企业可以为汽车厂商提供完整的数据安全产品和解决方案。随着汽车数据安全相关政策的陆续出台，未来几年，汽车数据安全市场将迎来指数式增长。不少企业看准机会，凭借多年行业经验，纷纷布局汽车数据安全领域。中国的为辰信安、云驰未来等公司已经为智能汽车数据安全推出了一系列产品以及解决方案。以为辰信安为例，企业为智能汽车提供网络安全解决方案，方案涵盖IVI、TBOX、智能座舱、自动驾驶系统等车辆内部零部件，以及服务平台和移动设备等智能汽车网联系统全要素，为智能汽车网联系统建立起整体防御体系。

■ **总体而言，《规定》的出台意义重大，智能汽车数据采集的无序扩张时代已经结束。未来智能汽车行业的健康发展需要一把“标尺”，能指引正确的方向并明确各方参与主体责任与义务。目前，中国市场还没有形成一套成熟的方案，一切还在循序渐进的探索过程中。可以预见的是，根据目前的一些解决方案来看，智能驾驶辅助等一系列人工智能新技术并不会因为法规而停滞不前。**

来源：太平洋汽车、速数智联、为辰信安官网、头豹研究院

方法论

- 头豹研究院布局中国市场，深入研究19大行业，持续跟踪532个垂直行业的市场变化，已沉淀超过100万行业研究价值数据元素，完成超过1万个独立的研究咨询项目。
- 头豹研究院依托中国活跃的经济环境，研究内容覆盖整个行业发展周期，伴随着行业内企业的创立，发展，扩张，到企业上市及上市后的成熟期，头豹各行业研究员积极探索和评估行业中多变的产业模式，企业的商业模式和运营模式，以专业视野解读行业的沿革。
- 头豹研究院融合传统与新型的研究方法论，采用自主研发算法，结合行业交叉大数据，通过多元化调研方法，挖掘定量数据背后根因，剖析定性内容背后的逻辑，客观真实地阐述行业现状，前瞻性地预测行业未来发展趋势，在研究院的每一份研究报告中，完整地呈现行业的过去，现在和未来。
- 头豹研究院密切关注行业发展最新动向，报告内容及数据会随着行业发展、技术革新、竞争格局变化、政策法规颁布、市场调研深入，保持不断更新与优化。
- 头豹研究院秉承匠心研究，砥砺前行的宗旨，以战略发展的视角分析行业，从执行落地的层面阐述观点，为每一位读者提供有深度有价值的研究报告。

法律声明

- 本报告著作权归头豹所有，未经书面许可，任何机构或个人不得以任何形式翻版、复刻、发表或引用。若征得头豹同意进行引用、刊发的，需在允许的范围内使用，并注明出处为“头豹研究院”，且不得对本报告进行任何有悖原意的引用、删节或修改。
- 本报告分析师具有专业研究能力，保证报告数据均来自合法合规渠道，观点产出及数据分析基于分析师对行业的客观理解，本报告不受任何第三方授意或影响。
- 本报告所涉及的观点或信息仅供参考，不构成任何证券或基金投资建议。本报告仅在相关法律许可的情况下发放，并仅为提供信息而发放，概不构成任何广告或证券研究报告。在法律许可的情况下，头豹可能会为报告中提及的企业提供或争取提供投融资或咨询等相关服务。
- 本报告的部分信息来源于公开资料，头豹对该等信息的准确性、完整性或可靠性不做任何保证。本报告所载的资料、意见及推测仅反映头豹于发布本报告当日的判断，过往报告中的描述不应作为日后的表现依据。在不同时期，头豹可发出与本报告所载资料、意见及推测不一致的报告或文章。头豹均不保证本报告所含信息保持在最新状态。同时，头豹对本报告所含信息可在不发出通知的情形下做出修改，读者应当自行关注相应的更新或修改。任何机构或个人应对其利用本报告的数据、分析、研究、部分或者全部内容所进行的一切活动负责并承担该等活动所导致的任何损失或伤害。

头豹研究院简介

- 头豹是中国领先的原创行企研究内容平台和新型企业服务提供商。围绕“协助企业加速资本价值的挖掘、提升、传播”这一核心目标，头豹打造了一系列产品及解决方案，包括：**报告/数据库服务**、**行企研报定制服务**、**微估值及微尽调自动化产品**、**财务顾问服务**、**PR及IR服务**，以及其他以企业为基础，利用大数据、区块链和人工智能等技术，围绕产业焦点、热点问题，基于丰富案例和海量数据，通过开放合作的增长咨询服务等
- 头豹致力于以优质商业资源共享研究平台，汇集各界智慧，推动产业健康、有序、可持续发展

备注：数据截止2022.6

四大核心服务

企业服务

为企业提供**定制化报告**服务、**管理咨询**、**战略**调整等服务

云研究院服务

提供行业分析师**外派驻场**服务，平台数据库、报告库及内部研究团队提供技术支持服务

行业排名、展会宣传

行业峰会策划、**奖项**评选、行业**白皮书**等服务

园区规划、产业规划

地方**产业规划**，**园区**企业孵化服务

报告阅读渠道

头豹官网 —— www.leadleo.com 阅读更多报告

头豹APP/小程序 —— 搜索“头豹” 手机可便捷阅读研报

头豹交流群 —— 可添加企业微信13080197867，身份认证后邀您进群

详情咨询

客服电话

400-072-5588

上海

王先生：13611634866

李女士：13061967127

深圳

李先生：13080197867

李女士：18049912451

南京

杨先生：13120628075

唐先生：18014813521