Open Journal of Legal Science 法学, 2023, 11(6), 6404-6411
Published Online November 2023 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2023.116919

Hans汉斯

自动驾驶算法安全法律规制的现状、挑战与应对

戴　尧

扬州大学法学院，江苏　扬州

收稿日期：2023年9月21日；录用日期：2023年10月8日；发布日期：2023年11月28日

摘　要

自动驾驶汽车的发展已经进入瓶颈期，更多企业开始转变以传统硬件为核心的观念，开始发展可以实现自动驾驶功能的算法系统。自动驾驶的算法安全问题也成为了自动驾驶汽车商业化过程中必须面对和解决的难题，这其中包括技术、网络和伦理三方面的自动驾驶算法安全问题。因此，需要对传统以人类驾驶员为核心的立法和监管框架进行变革，构建一个以自动驾驶算法为核心的安全框架，形成一个包含自动驾驶算法技术安全、网络安全和伦理安全的安全标准。新的框架应当注意平衡算法的安全性和创新性，保持技术的中立，努力推进自动驾驶汽车迈向商业化应用。

关键词

自动驾驶系统，安全标准，网络安全，伦理风险管理

Current Status, Challenges, and Responses to Legal Regulation of Autonomous Driving Algorithmic Safety

Yao Dai

Law School of Yangzhou University, Yangzhou Jiangsu

Received: Sep. 21st, 2023; accepted: Oct. 8th, 2023; published: Nov. 28th, 2023

Abstract

The development of self-driving cars has entered a bottleneck, and more companies have begun to change the concept of traditional hardware as the core, and have begun to develop algorithmic

文章引用: 戴尧. 自动驾驶算法安全法律规制的现状、挑战与应对[J]. 法学, 2023, 11(6): 6404-6411.
DOI: 10.12677/ojls.2023.116919

systems that can realize the function of autonomous driving. The algorithmic safety of autonomous driving has also become a difficult problem that must be faced and solved in the process of commercialization of autonomous driving cars, which includes the safety of autonomous driving algorithms in the three aspects of technology, network and ethics. Therefore, it is necessary to make changes to the traditional legislative and regulatory framework centered on human drivers, to construct a safety framework centered on autonomous driving algorithms, and to form a safety standard that encompasses the technical safety of autonomous driving algorithms, cyber safety, and ethical safety. The new framework should pay attention to balancing the safety and innovation of algorithms, maintaining technology neutrality, and striving to advance self-driving cars towards commercialized applications.

Keywords

Autonomous Driving Systems, Safety Standards, Cybersecurity, Ethical Risk Management

1. 技术发展及其法律规制现状

自动驾驶汽车的研究与开发已经成为世界潮流，发展自动驾驶的开发者和制造商普遍认为自动驾驶汽车可以大大降低交通事故发生概率，保障道路上人员的安全，同时也提高了通行效率，为残疾人和老年人提供便利的出行服务，且有可能成为最伟大的私人交通革命。根据国际汽车工程师协会(SAE International)提出的“驾驶自动化技术分级标准”，其中L1和L2称为“驾驶员辅助系统”(Driver Support System)，驾驶员需要时刻注意驾驶环境，在出现问题时需要进行接管解决问题，L3~L5 称为“自动驾驶系统”(Autonomous Driving System)，驾驶员的注意程度逐渐降低，接管的次数也会逐渐减少。根据 2021 年 5 月，SAE 和 ISO (国际标准化组织)联合发布最新分级标准明细，L3 至 L5 级的自动驾驶能力逐步提高，其中 L5 级的自动驾驶汽车可以实现完全自动驾驶，即不需要人类驾驶员，就可以在任何条件下都能完成所有的驾驶任务[1]。就我国而言，2022 年 3 月公布的《汽车驾驶自动化分级》(GB/T 40429-2021)标准与一般国际通行的标准不同，我国的标准将自动驾驶能力分为 L0~L5 六个等级，该标准参考了我国自动驾驶汽车发展的具体现状，更符合国内汽车市场的发展模式，同时也体现出我国自动驾驶汽车领域与国际接轨的思路。

在产业发展上，自动驾驶汽车已从研究阶段进入加速部署和应用阶段，2022 年中国自动驾驶开发平台市场增速达 106% [1]。自动驾驶汽车正在加速融入道路交通系统，催生出全新的商业模式和服务策略，无人驾驶的公交车、出租车、物流车等新型驾驶车辆正不断涌现，但实现 L5 级自动驾驶的还有很长一段路要走，需要算法进一步的升级和进步。业内普遍认为，自动驾驶车辆将在 2025 年前后实现爆发式增长；到 2035 年，道路上行驶的大部分车辆都可以实现自动驾驶。

面对迅猛发展的自动驾驶汽车产业，不仅需要构建具有前瞻性的自动驾驶算法安全框架，还需要在此基础上加强对自动驾驶算法的安全监管，形成规范、合理的监管路径，才能实现人类希望自动驾驶汽车便利日常生活的愿望。根据毕马威(KPMG) 2020 年发布的《自动驾驶汽车成熟度指数》(Autonomous

[1]SAE Levels of Driving Automation™ Refined for Clarity and International Audience, SAE International (May 3, 2021), https://www.sae.org/blog/sae-j3016-update.

Vehicles Readiness Index)报告，我国在其中排名第 20 位[2]，排名较为靠后，我国排名靠后的一大原因与当前国家和地方政府相关立法层级低、规定不够完善，对自动驾驶算法安全问题没有系统性的回应等有关。就我国而言，目前对自动驾驶汽车的监管呈现以下几个特点。

第一，重点规范自动驾驶汽车的道路测试。根据 2021 年 11 月颁布的《智能网联汽车道路测试与示范应用管理规范(试行)》，国家重点规范了自动驾驶汽车的测试场地的申请，测试主体与驾驶人及车辆，测试牌照发放等各地难以统一的碎片化问题，提升了测试的效率和规范化程度。第二，尝试确定自动驾驶汽车的合法地位。当前立法没有正式规定自动驾驶汽车的合法地位，仅通过 2021 年 4 月公布的《道路交通安全法(修订建议稿)》尝试填补这一空白，但回避了“自动驾驶汽车”的合法性问题。第三，汽车数据安全和网路安全开始得到重视。近年来随着丰田汽车漏洞、特斯拉车主维权、滴滴收集和泄露用户隐私等舆论事件的发酵，监管部门开始加强对汽车联网、自动驾驶汽车行驶数据和汽车传感器采集到的路面信息和行人信息的监管。例如，工业和信息化部印发《车联网网络安全和数据安全标准体系建设指南》，《汽车整车信息安全技术要求》(征求意见稿)和《智能网联汽车自动驾驶数据记录系统》(征求意见稿)，这些文件从不同角度对用车人数据保护、自动驾驶系统记录的数据和数据安全和防护标准体系提出了若干规定，但这些规定主要还是针对汽车整体的网络安全和数据安全，并未对自动驾驶算法安全方面专门的网络安全和数据安全有具体的规定。

综上，我们可以看出当前自动驾驶汽车领域的立法主要侧重于道路测试、准入示范应用、汽车整体数据和网络安全等方面，尚未形成对以人工智能为发展方向的自动驾驶算法的安全监管框架。因此，从鼓励自动驾驶汽车发展的角度出发，我国下一阶段自动驾驶汽车应注意自动驾驶算法的安全，行政机关要主动对监管方法进行完善和改进，立法者要不断提高自动驾驶汽车的立法层级。如此才能构建出自动驾驶算法安全监管框架，应对自动驾驶算法出现的种种安全挑战。

2. 自动驾驶汽车的算法安全挑战

2.1. 自动驾驶算法的技术安全挑战

美国作为自动驾驶汽车领域发展的典型代表，正积极探索和建立新的安全标准和审批机制以适应自动驾驶汽车的飞速发展。美国 NHTSA 在 2017 年发布的《自动驾驶汽车政策指南 2.0》和 2020 年 12 月发布的《自动驾驶系统安全框架》(Framework for Automated Driving system Safety)中都强调自动驾驶汽车安全自我评估、自我认证和自我监管[3]。德国则与美国的注重监管不同，根据 2021 年 5 月德国出台的自动驾驶法案，我们可以发现德国更加注重对技术要求和型号审批程序等事前准入要求的规定[4]。就我国而言，当前的规范性文件如，2021 年 8 月工信部发布的《关于加强智能网联汽车生产企业及产品准入管理的意见》、2022 年 8 月 8 日发布的《自动驾驶汽车运输安全服务指南(试行)》等规范性文件开始借鉴了一些国外经验，对自动驾驶系统的安全性、可靠性以及稳定性提出了一些要求，包括数据安全、网络安全等[5]。但相关的自动驾驶系统安全性要求比较笼统、欠缺前瞻性，不能形成统一的框架，不能满足一般

[2] 毕马威的“自动驾驶汽车成熟度指数”的衡量指标包括：1) 政策和立法；2) 技术和创新；3) 基础设施；4) 消费者接受度。See 2020 Autonomous Vehicles Readiness Index, KPMG, https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/07/2020-autonomous-vehiclesreadiness-index.pdf, accessed August 21, 2021.

[3] Automated Driving Systems 2.0: A Vision for Safety, NHTSA, https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/13069aads2.0_090617_v9a_tag.pdf, accessed June 3, 2022. Framework for Automated Driving System Safety, NHTSA, https://www.federalregister.gov/documents/2020/12/03/2020-25930/framework-for-automated-driving-system-safety, accessed August 21, 2021.

[4] Patrick Ayad, Susanne Schuster & Katharina Göpferich, Germany Takes a Pioneering Role with a New Law on Autonomous Driving, LEXOLOGY (August 2 2021), https://www.lexology.com/library/detail.aspx?g=7347621e-e032-476a-a06c-ae2dc33dac3f.

[5] 参见《工业和信息化部关于加强智能网联汽车生产企业及产品准入管理的意见》，来源：http://www.gov.cn/zhengce/zhengceku/2021-08/12/content_5630912.htm，2021 年 9 月 3 日访问。参见《自动驾驶汽车运输安全服务指南(试行)》(征求意见稿)，来源：https://www.gov.cn/xinwen/2022-08/14/5705346/files/7e2c6f6a04884124bcfd71668619de82.docx，2023 年 7 月 6 日访问。

的自动驾驶系统的技术安全要求。在笔者看来，自动驾驶汽车系统在未来的发展过程中相关政策制定者需注意以下三个层面的技术安全问题。

第一，明确自动驾驶的安全门槛。安全问题是自动驾驶汽车首先需要注意的关键性问题，作为自动驾驶汽车系统重中之重的自动驾驶算法安全问题自然需要被具体的规定进行保护和规制。但自动驾驶算法的安全门槛不能以交通事故的发生率和死亡率来确定，应从实际情况出发结合一般人类驾驶员的水平来进行综合衡量，得出一个较为合理科学的标准[6]。例如，2017 年德国发布的自动驾驶汽车伦理报告中强调，如果自动驾驶能够比人类驾驶更能够降低风险，那么自动驾驶技术就应该发展[2]。

第二，规范自动驾驶算法安全性能的检验流程。由于自动驾驶汽车算法的不可解释性、结果的不确定性、自我学习能力强和由于改进不断增加的复杂性，所以评估自动驾驶汽车的算法安全性难度大大提高。所以传统的审批方式，如型号审批、自我认证或者豁免机制等方式并不适用于衡量自动驾驶汽车的算法安全性。根据美国库兰德公司的研究，如果通过传统的道路测试来验证自动驾驶算法的安全性能高于一般人类司机，至少需要自动驾驶汽车行驶 5000 亿英里[7]。仅仅依靠这样单一的测试方法，自动驾驶汽车真正实现规模化、产业化将遥遥无期，所以自动驾驶汽车的制造者和立法者需要有针对性地研究寻找算法安全性的测试方法，如模拟测试、开放道路测试、特定场景测试或者基于事故场景还原的仿真测试等[8]，同时还需要保证这些测试方法的有效性、可行性、公正性和不被操控性。最后，还以结合虚拟现实技术与生成式人工智能等最新技术，增强测试场景的真实性，进一步增强算法的安全性和可靠性。

第三，人机交互中技术安全问题。在自动驾驶的过程中存在两个主要因素影响人类司机接管的安全性。一是接管表达方式，自动驾驶系统可以通过人类可感知的方式传递请求接管的信息，形成一个数字化交互界面。但单纯依靠数字交互界面提醒人类司机还不够充分，因为人类司机有时不能及时处理相关信息，进而导致危险发生。二是人类司机的反应时间，这个时间可能受到多种因素的影响，包括司机的注意力集中程度、先前多次手动接管的经验、系统提醒的程度等。所以，不同的驾驶人员对接管请求的反应快慢各不相同，这要求我们找寻一种基于个人表现采取定制化接管请求的提醒路径。总之，自动驾驶的技术安全问题不容小觑，必须开发出能够充分考虑不同驾驶人员心理、认知因素和身体情况的综合性模型，这是自动驾驶技术面向大众之前所必须面对和解决的一个挑战。

2.2. 自动驾驶算法的网络安全挑战

网络安全作为影响自动驾驶汽车发展应用的关键性因素[3]，其自身遇到的风险和威胁将直接影响到自动驾驶汽车的安全。首先，自动驾驶汽车由于其高度联网的特性，与传统汽车相比更容易受到网络攻击。自动驾驶系统对汽车行驶有很大的控制权限，这意味着如果自动驾驶汽车的算法受到网络攻击，失灵后所造成的后果也会及其严重，所以当自动驾驶系统受到网络攻击失灵时，人类的干预就显得极为重要。其次，通过自动驾驶汽车的网络攻击汽车的主体更加多样化。自动驾驶汽车的生产高度智能化，需要在生产、维修、监管等不同环节提供相应的端口和权限，不同的主体就可以通过对应的端口实现对自动驾驶汽车的访问和控制。如果这些主体受到网络攻击，黑客就通过这些端口控制自动驾驶汽车系统，影响到自动驾驶汽车的正常运行，所以要严格规范和监督自动驾驶汽车访问和参与者，以面对更严峻的网络安全风险。然后，自动驾驶汽车可以通过网络被多种方式攻击不同的零部件。自动驾驶汽车系统可以控制汽车大部分的组件，黑客就可以采取多种方式，如操控方向盘、抹除仪表盘数据、使传动功能失

[6]Marjory S. Blumenthal *et al*., Safe Enough: Approaches to Assessing Acceptable Safety for Automated Vehicles, RAND, https://www.rand.org/pubs/research_reports/RRA569-1.html, accessed August 21, 2021.
[7]Nidhi Kalra & Susan M. Paddock, Next Stop, Neptune? RAND, https://www.rand.org/pubs/infographics/IG128.html, accessed August 21, 2021.
[8]Laura Fraade-Blanar *et al*., Measuring Automated Vehicle Safety, RAND, https://www.rand.org/pubs/research_reports/RR2662.html, accessed August 21, 2021.

效等手段达到攻击汽车的目的，这些攻击会对自动驾驶系统产生致命的影响，甚至危及行车人和乘车人的生命安全，所以不容小觑，需要加以防范。最后，自动驾驶汽车的网络安全风险还具有影响范围广和深层次的特点，很容易导致全面且多层次的危害后果。在范围上，当前自动驾驶汽车的软硬件高度结合，自动驾驶汽车需要搭载专门的自动驾驶系统，如果这一系统被侵入，黑客可以侵入所有搭载该自动驾驶系统的车辆，这样就可以达到控制所有相关自动驾驶汽车的目的。为此，2017 年 7 月，特斯拉 CEO 警告说，对于自动驾驶汽车最大的忧虑是“黑客可以实现车队规模攻击”[9]。在深度上，自动驾驶汽车被黑客侵入控制后，会造成不同层次的后果。最直接的是由车辆碰撞产生的财产损失，更严重的就是行车人的数据和自动驾驶汽车采集到的周边信息被窃取。这些数据对车企、系统开发商、政府部门等都有极大的价值，正因如此这些数据成为黑客攻击和获取非法收入的理想目标。

2.3. 自动驾驶算法的伦理安全挑战

自动驾驶汽车的理想情况是确保道路上的人员都获得相同程度的安全保障，但算法的主观性和片面性就必定会带来不公平的歧视，由此引发了伦理上的争议[10]，大众产生了对自动驾驶算法的伦理安全问题的担忧。自动驾驶的算法不像一般的自动化软件，需要在许多不确定的情况下做出不同的决策。在发生事故时，人们往往对自动驾驶汽车的要求会高于对一般人类驾驶人员的要求，希望自动驾驶算法可以解决类似“电车困境”的难题。但由于种族差异化的原因，导致自动驾驶算法的道德指导原则难以形成共识。因此，有人便提出了一个风险成本函数。该函数考虑了总体风险的最小化、最坏情况的优先级和对人平等对待的程度，该函数适用于公共道路上发生的所有情形的伦理问题[11]。2017 年德国“自动与网联驾驶伦理委员会”，制定了一份包含二十项伦理原则的报告[4]，核心内容大致包括三类。第一类对基本价值进行排序，明确保护人类的优先级；在不可避免的事故发生时，禁止基于年龄、性别、身体条件等进行歧视。第二类，要求自动驾驶汽车对相关控制者进行详细记录，为事故发生时确定责任提供证据支持。第三类，强调通过算法防范伦理困境，降低对道路上弱势使用者的风险。从这些函数和伦理原则报告中，我们可以寻找适合自己的伦理标准，并结合我国实际发展情况，制定符合我国国情，具有中国特色的法律法规，以应对自动驾驶技术发展中遇到的安全挑战。

3. 自动驾驶算法安全的法律规制的构建

在全球范围内，西方的一些发达国家都在积极制定与自动驾驶汽车有关的政策和立法，致力于构建自动驾驶汽车的监管框架，逐步将监管重心从规范道路测试转向实现商业化应用[5]。

我国也需要加快制定相关政策和法律，推动自动驾驶真正实现落地商用。目前，北京、上海、深圳、武汉等城市已经出台了地方性的法律法规，但由于级别较低，适用范围较小，给自动驾驶实现商用形成了不小的阻碍。同时，国家层面的立法，例如，《道路交通安全法》《公路法》等法律的主要适用还是人类驾驶员，并未进行及时的扩充和新增，对自动驾驶汽车产生的侵权责任以及自动驾驶汽车的算法安全等具体问题，都没有进行规定。

根据《智能汽车创新发展战略》提出的“到 2025 年实现有条件自动驾驶的智能汽车达到规模化生产，实现高度自动驾驶的智能汽车在特定环境下市场化应用”的目标，传统适用于人类驾驶人员的法律和监管框架已经落后于时代，不能应对自动驾驶汽车及其引发的一系列法律、道德和监管问题。为了实现自

[9] 李志勇：《车联网数据安全开始影响产业发展进程》，来源：http://www.xinhuanet.com/tech/2021-07/09/c_1127637056.htm，2023 年 1 月 23 日访问。

[10] Responsible Innovation in Self-Driving Vehicles (Policy Paper), GOV.UK (August 19, 2022), https://www.gov.uk/government/publications/responsible-innovation-in-self-driving-vehicles/responsible-innovation-in-self-driving-vehicles#governance.

[11] Maximilian Geisslinger *et al.*, Autonomous Driving Ethics: from Trolley Problem to Ethics of Risk, Springer (April 12, 2021), https://link.springer.com/article/10.1007/s13347-021-00449-4.

动驾驶汽车与当前道路交通体系的融合，其核心是对自动驾驶算法进行监管规制，构建新的法律制度和监管框架，这个框架主要包含系统的安全标准和审批准入、网络安全法律规定、伦理安全管理三个维度。

3.1. 新的自动驾驶系统安全标准和审批准入机制

国家必须将“安全第一”作为自动驾驶汽车发展的最基本原则，制定新的、具有前瞻性的安全标准，将传统法律注重汽车硬件安全的标准，转向以自动驾驶算法为核心的安全标准，允许汽车通过自身传感器和控制系统，代替传统驾驶舱、后视镜的新型设计。目前，美国的 NHTSA 已经在 2022 年更新了“联邦机动车安全标准”(FMVSS)，其中对于没有手动控制装置的自动驾驶汽车，相关乘员的安全保护标准进一步提高，这是实现自动驾驶算法的新的安全标准的第一步[6]。此外，由于当前自动驾驶技术正处于快速的演变中，新的安全标准应对具体设计提出强制性规定，主要还是应该聚焦汽车的安全性能，保持技术的中立性。

一般国家，如中国、欧盟、韩国等国对自动驾驶汽车的审批准入主要采取审批机制，包括汽车的 OTA 更新；而美国等国主要强调制造商通过自身的标准，进行自我认证，政府等部门进行事后监管的机制。这些严格的审批和准入机制，延缓了自动驾驶技术的发展，汽车厂商需要花费大量的时间进行审批，新的技术和算法不能立即投入使用，具有严重的滞后性。笔者认为，我们可以采取关键事项审批和一般事项自我认证相结合的机制，提高了自动驾驶汽车的审批速度，为促进技术创新，增强我国自动驾驶汽车的国际竞争力提供了政策保障。

3.2. 网络安全法律规定

网络安全是自动驾驶算法安全的重要组成部分，政策制定者需要注意到最新的网络安全问题。通过法律的强制性规定，将网络领域影响自动驾驶算法安全的行为进行规范，构建一个全新的网络安全框架，将传统网络安全原则与最新网络安全原则相结合，从根本上保障自动驾驶汽车的算法安全。

第一，建立自动驾驶汽车的专用网络和认证机制，只有通过专用网络的汽车并进行认证才能允许销售和使用。如今，汽车网络与手机网络共用同一频段和信号，黑客可以通过手机网络大范围入侵接收该信号的汽车，降低了网络入侵的难度，增加了汽车网络被侵入和控制的风险。自动驾驶算法只能较低层级地控制汽车，不能防止汽车网络被侵入从而被更高的优先级接管汽车，对道路上的车辆和行人造成风险。通过专用网络，可以降低网络数据的复杂性，同时这些汽车都经过了网络认证。即使被黑客侵入网络，由于没有经过认证，数据构成也相对简单，很快就可以发现入侵者，快速解决网络安全问题。

第二，明确自动驾驶汽车的网络安全防护等级和技术措施。通过立法等强制性手段要求制造商建立明确的网络安全等级，根据不同的风险，对不同的网络安全问题进行分类监管，对高等级的问题提供重点防护，保证自动驾驶系统的正常运行。同时，采取多种网络安全措施，包括算法加密、流量监控、威胁监控、强化网络监控服务、建立可靠的识别和鉴别机制等技术措施，降低自动驾驶汽车被侵入的风险性。

第三，建立数据共享平台，实现行业和政府之间数据的高效分享，相互促进。将行业内自动驾驶汽车采集到的道路数据与政府部门共享，帮助政府部门完善道路数据，对道路上发生的交通事故提供及时预警。反之，政府可以向自动驾驶汽车行业提供相关事故发生原因、发生地点和时间段等数据，为行业算法进一步优化提升提供数据支持。此外，行业内部也可以互相分享和解决自动驾驶算法遇到的困境和难题。总之，建立自动驾驶数据共享平台，对于提升自动驾驶的算法，促进自动驾驶行业的发展具有重大意义。

3.3. 加强自动驾驶算法的伦理安全管理

自动驾驶算法不仅需要面对技术难题，更要面对伦理难题。在面对不可避免的事故发生时，一个公认的自动驾驶算法道德标准往往可以发挥定分止争的作用。但这个道德标准不能由汽车制造商来制定，因为这些制造商对创新和商业利益有着狂热的追求，他们不能站在一般的公共安全角度出发考虑，形成客观、公正可被一般人接受的道德标准。这个标准需要立法者、制造商和政府共同努力，从不同角度探索这个标准。有公信力的立法者应发挥带头作用，从宏观角度指引如何保证自动驾驶算法的伦理安全；广泛的参与者要发挥能动作用，从细节出发结合自身特色形成保证自动驾驶算法的伦理安全的管理方法；坚定的管理者要发挥监管作用，及时发现和解决自动驾驶算法可能出现的伦理问题。具体来说：

在立法层面，政策制定者不仅应当关注制定自动驾驶算法的一般道德标准，更应关注具体的科技伦理和算法伦理风险管理。2022 年 3 月印发的《关于加强科技伦理治理的意见》中，强调了国家对于科技创新发展的高度重视，对科技伦理治理体系建设的迫切要求。在此背景下，自动驾驶汽车生产企业需要明确自动驾驶算法的伦理规则，健全自动驾驶算法伦理治理的制度，强化自动驾驶算法的伦理审查和自我监管，同时，也要注重对自身技术人员的科技伦理教育和宣传 [12]。通过政策制定者和制造商的共同努力，才能建立更加科学完善的科技伦理治理体系。

在个人层面，应注重发挥企业和行业的主动性，自行管理和实施自动驾驶算法的伦理治理。为此，可以采取一系列措施，如建立专门的自动驾驶算法伦理委员会、制定行业公约、引入伦理技术和管理工具等。通过将相关伦理要求与自动驾驶算法相结合，解决算法歧视、算法黑箱等伦理安全风险，进一步提升自动驾驶算法的可靠性、安全性和稳定性，从而构建更加完善和公平的自动驾驶算法体系。

在监管层面，必须坚持“伦理先行”的治理观念。通过具体的监管规则，规范自动驾驶汽车制造商对自动驾驶算法的伦理安全管理机制，以便及时发现、分析、解决自动驾驶算法的伦理问题。同时，监管部门也要将立法落实到实处，通过出台具体的实施细则和标准，对如何提升企业算法管理的安全性、规范性、公开性和可解释性、人机协同工作、人类物化、算法滥用等伦理风险，给自动驾驶汽车的生产者和从业者提供具体的参考和引导。将科技伦理要求贯穿算法研究、算法开发等自动驾驶算法研究活动全过程，实现科技活动与科技伦理协调发展、良性互动。

4. 结语

自动驾驶汽车的投入和使用，是社会发展的必然趋势。通过建立自动驾驶的算法安全监管框架，可以为自动驾驶汽车的发展提供保障，加快实现自动驾驶汽车的商业化。在构建这个框架时，应当重点关注使用者和社会整体的预期，努力满足这些预期。进而，自动驾驶汽车就能保证使用者的满意程度和安全性，实现信任、透明、稳定等设计价值。基于对上述问题的考虑，本文着重对自动驾驶的算法安全问题进行探讨，创造性地提出一种全新的监管模式，构建算法安全的监管框架，积极应对自动驾驶汽车商业化过程中出现的算法安全问题。只有保证自动驾驶算法的安全，才能推动自动驾驶汽车真正地实现商业化落地。通过本文提出的监管和治理思路，希望可以给政策制定者一些启发，为未来的交通法治创造一个良好的开端。

参考文献

[1] 5.89 亿 IDC: 2022 年中国自动驾驶开发平台市场增速达 106% [J]. 智能建筑与智慧城市, 2023(5): 4.

[2] 叶强. 德国自动驾驶立法评析[J]. 国外社会科学, 2022(2): 73-86+197.

[12] 参见《关于加强科技伦理治理的意见》，来源：http://www.gov.cn/zhengce/2022-03/20/content_5680105.htm，2022 年 6 月 15 日访问。

[3] Dave, R., Boone, E.R.S. and Roy, K. (2019) Efficient Data Privacy and Security in Autonomous Cars. *Journal of Computer Sciences and Applications*, **7**, 31-36. https://doi.org/10.12691/jcsa-7-1-5

[4] 郑戈. 算法的法律与法律的算法[J]. 中国法律评论, 2018(2): 66-85.

[5] 曹建峰. 人工智能治理: 从科技中心主义到科技人文协作[J]. 上海师范大学学报(哲学社会科学版), 2020, 49(5): 98-107. https://doi.org/10.13852/J.CNKI.JSHNU.2020.05.011

[6] 曹建峰. 论自动驾驶汽车的算法安全规制[J]. 华东政法大学学报, 2023, 26(2): 22-33.