社会科学进展
2025 年 5 月第 7 卷第 5 期

智能网联汽车数据安全治理困境及解决路径

——以个人信息数据为视角

向丽雅　周　蜜

上海政法学院，上海

摘　要 | 智能网联汽车已日益取代了传统汽车成为汽车产业未来的发展趋势，智能网联汽车在运行过程中会产生大量汽车数据，《汽车数据安全管理若干规定（试行）》将这些数据分为个人信息数据和重要数据两类，其中，个人信息数据与人身利益紧密相关，一旦泄露，不仅会对我们的个人隐私安全造成威胁，甚至会对公共安全和国家安全造成严重损害。随着汽车智能化和网联化水平的不断提升，在给大众带来更舒适、便利驾乘体验的同时，也暴露出数据安全风险隐患，尤其是在个人信息数据安全治理领域，智能网联汽车面临着个人数据边界模糊、传统知情同意制度难以直接应用于汽车个人信息数据处理规制、数据共享中存在个人信息数据安全风险等问题，这些问题对现有的汽车数据安全治理制度体系提出了新挑战。为应对这些问题，需要进一步厘清汽车数据中个人信息数据的界限，根据汽车数据的独特性对传统知情同意制度进行合理调整，并完善数据共享中个人信息数据安全保障机制，从而实现对汽车数据中个人信息数据安全治理体系的完善。

关键词 | 智能网联汽车；个人信息数据；数据安全；数据治理；个人数据

随着人工智能、云计算、大数据、区块链等多项前沿技术的突破，传统汽车行业迎来了一场前所未有的产业革命，智能网联汽车的市场占比正快速提升。所谓智能网联汽车，是指通过先进的传感器、控制器、执行器等装置，以及高速计算机网络，实现车与车、车与路、车与人、车与云之间的连接和信息交互，从而实现自动驾驶、车辆状态监控、路况信息共享等功能的汽车。传统汽车智能化和网联化的基本途径就是通过大量数据信息“喂养”的算法学习，从而实现汽车操作系统和道路交通系统的智能化，因此，数据成为智能网联汽车发展的关键性技术资源。从当前现状来看，智能网联汽车具有广阔的市场发展前景，据预测，到2030年，全球智能网联汽车市场规模有望达到1.5万亿美元。中国作为全球最大的汽车市场，其在智能网联汽车领域的快速发展，无疑极大地拉动了我国汽车行业的经济产值增长，但也带来了日益凸显的数据安全隐患。随着智能网联汽车的大规模普及，汽车数据的边界逐渐扩大，体量不断激增。智能网联汽车上自带的大量摄像头、雷达、传感

通讯作者：向丽雅，上海政法学院研究生，研究方向：民商法。
文章引用：向丽雅，周蜜．智能网联汽车数据安全治理困境及解决路径——以个人信息数据为视角［J］．社会科学进展，2025，7（5）：436-441.
https://doi.org/10.35534/pss.0705075

器、智能座舱等数据采集设备，在每天的运作中产生大量数据，其中汽车驾驶人、乘客、车主，以及车外行人的个人信息数据占据了很大一部分，因此保障个人数据安全在汽车数据安全治理中占据了重要地位。然而，从具体事件来看，汽车数据安全的治理现状不容乐观，个人数据安全问题屡屡发生。特斯拉、蔚来汽车、通用汽车、福特、大众、丰田、沃尔沃等汽车厂商都曾卷入过数据泄露风波。黑客通过攻击这些车企的网络服务器，非法获取其采集存储的数据，对汽车用户的个人信息安全造成严重影响。类似事件的不断发生，引发了行业对智能网联汽车领域个人数据安全的重视，近年来，我国相继出台了一系列有关数据安全的法律规范及标准，初步构建起智能网联汽车数据安全保护体系。在法律层面，《网络安全法》《数据安全法》和《个人信息保护法》这三部重要单行法分别从不同的角度为智能网联汽车的数据安全治理提供了原则性规定，其中《网络安全法》主要是以网络系统为侧重点，《数据安全法》以数据本身为侧重点，《个人信息保护法》则直接聚焦于数据安全中的个人信息安全。智能网联汽车数据作为数据项下的一个具体种类，具备适用上述法律的合理性，但由于汽车数据本身的特殊性，上述法律中的一些具体规定并不能完全适用于汽车数据领域，这为智能网联汽车数据领域相关规章、指导性文件及标准的出台提供了逻辑前提。在部门规章层面，国家网信办等五部门于2021年10月施行《汽车数据安全管理若干规定（试行）》，直接就智能网联汽车数据安全问题作出了回应。同时，国家工信部也相继颁布实施了《关于加强智能网联汽车生产企业及产品准入管理的意见》《关于加强车联网网络安全和数据安全工作的通知》以及《关于车联网网络安全和数据安全标准体系建设指南的通知》等部门规范性文件，将智能网联汽车数据安全治理相关的原则规定进一步细化并落实到具体设计中。在标准层面，《信息安全技术个人信息安全规范》（GB/T35273–2020）以及《信息安全技术汽车数据处理安全要求》GB/T41871–2022等标准的落地为该领域的安全治理提供了实践上的引导和规范。综上可以看出，我国对智能网联汽车的数据安全治理持高度重视的态度，且已经初步形成包含法律、部门规章以及国家标准等多位阶效力的制度体系。

1　汽车数据中个人信息数据安全的治理困境

1.1　个人信息数据的界限模糊

2021年颁布实施的部门规章《汽车数据安全管理若干规定（试行）》（以下简称《汽车数据规定》）将汽车数据分为个人信息数据和重要数据两大类，在个人信息数据项下又进一步细分为一般个人信息和敏感个人信息两类，且该规定对不同种类汽车数据的展示采取了不完全列举加兜底规定的方式。尽管这在一定程度上有助于厘清不同种类汽车数据的界限，但由于智能网联汽车本身具有参与主体多方性等特征，导致了智能驾驶中数据来源广、数据种类多，这极大地增加了对个人信息数据进行准确识别的难度。根据《汽车数据若干规定》的规定，首先，个人信息数据主体包括车主、驾驶人、乘车人、车外人员等相关人员；[①]其次，个人信息数据需要满足“已识别”或“可识别”的标准，“已识别”是指通过该信息某一自然人得以在特定人群中被辨识、定位，“可识别”是指某一自然人虽然当前还未被辨识定位，但单独通过该信息或者联合该信息与其他辅助信息有实现前述目的的可能性。最后，匿名化处理后的数据排除于个人信息数据的范围之外。上述规定看似明晰，实际上在智能网联汽车的驾驶场景中，对于哪些数据可以识别到特定自然人缺乏明确的判断标准。在汽车数据中，车主、驾驶人、乘车人、车外人员等主体的身份信息、居住信息、人脸信息、声音信息、浏览偏好信息等属于个人信息数据，对此不存在认定争议，因为上述信息与自然人的人身关联度较高，特别是生物识别特征等信息几乎可以直接定位特定自然人。但对于车辆行驶里程数据、车辆维修数据等由车辆衍生的数据是否属于个人信息数据，存在认定模糊性。一般情况下这些数据仅能联系到具体车辆，不能识别到特定自然人，但由于人与车之间存在关联性，通过这些数据与其他的辅助数据相结合，也可以联系到某一特定的自然人。在特定情况下，这些数据也存在构成个人信息数据的可能性。然而，数据作为一种新型生产要素，具有利用价值与流通价值，如果不加区分地将上述相关数据全部认定为个人信息数据，会导致个人信息数据的范围无限扩大，增加数据流通和利用的成本和难度，不利于发挥数据的要素作用。并且，《个人信息保护法》和《汽车数据若干规定》均将匿名化处理后的数据排除在个人信息数据范畴之外，这也导致了个人信息数据的边界模糊。匿名化处理指的是对个人信息进行技术处理后，仅从该信息本身或者结合其他信息无法指向特定个人，且处理后的信息无法被复原。匿名化技术目前已经成了重要的数据安全保障措施之一，尽管其在多年的发展进程中已经形成了相对成熟的技术解决方案，比如泛化、压缩、分解、置换以及干扰等，但是在当前的技术条件下对个人信息数据真正做到完全匿名化几乎是不可能的。且数据识别技术亦处于不断的发展革新中，过去或当前公布的匿名化处理后的数据很可能在不久之后通过新的技术、新的模型可以重新联系到某一特定自然人，此时该数据又重新

① 《汽车数据安全管理若干规定(试行)》第三条第四款：个人信息，是指以电子或者其他方式记录的与已识别或者可识别的车主、驾驶人、乘车人、车外人员等有关的各种信息，不包括匿名化处理后的信息。

https://doi.org/10.35534/pss.0705075

回归到个人信息数据的范畴之内。因此，智能驾驶场景下个人信息数据的识别，并非静态、一成不变的过程，同一类型数据是否属于个人信息数据，在不同时间段内、不同应用场景下可能有不同判断结果。个人信息数据边界的模糊性造成识别障碍，导致无法对相应数据实施应有保障，最终威胁和损害个人信息数据主体的隐私安全。

1.2 个人信息数据处理中传统的知情同意规则失效

《个人信息保护法》的出台对个人信息处理活动的规制具有重要意义，其引入了个人信息处理活动的核心原则——知情同意原则。知情同意指的是自然人在充分了解个人信息处理的目的、范围、方式等关键性信息的基础上，自愿、明确地向信息处理者表示同意的行为。特定情况下还可能对自然人作出同意的形式有要求，即单独同意或书面同意。[①]由此推断，在《个人信息保护法》语义下，信息处理者对个人负有充分告知义务，然而关于告知方式《个人信息保护法》仅作原则性规定，要求信息处理者应当以显著方式、清晰易懂的语言向个人告知信息处理的目的、方式、存储期限，以及处理的信息种类等。对于何种方式属于显著方式没有进一步详细的规定。《汽车数据若干规定》出台以后对“显著方式”进行了不完全列举，包括但不限于通过用户手册、车载显示器界面、语音播报、汽车使用相关应用程序等方式，这相较于《个人信息保护法》的笼统规定具有一定程度上的进步意义。然而，在智能网联汽车个人信息数据的处理活动中，知情同意规则仍然面临着无可避免的现实困境。第一，智能网联汽车的驾驶场景涉及多方数据主体，包括车主、驾驶人、乘客、车外行人等相关人员，在上述人员中，仅车主具有事先阅读隐私政策或用户协议从而作出同意的可能性及合理性，其余人员在知情同意规则的落实上都存在操作的可行性不足的问题。首先，就驾驶人而言，在车辆租赁服务和代驾服务的应用场景下，驾驶人是车辆的承租人和代驾服务的提供者，此时就出现了车主和驾驶人不一致的情形，此种情形下驾驶人无法基于知情同意原则拒绝智能网联汽车相关数据处理者对其个人信息数据的处理活动。其次，就乘客而言，乘客的乘坐行为具有单次性和随机性，难以期待数据处理者在每一位乘客的搭乘行为开始前都通过签订用户协议或者同意隐私政策的方式获得个人信息处理的合法性来源。最后，尤其是对于车外不特定行人来说，提前阅读用户协议或隐私政策从而作出事先同意是最不可能实现的。第二，实际使用中很多用户协议或隐私政策存在条款冗杂、语言晦涩难懂等问题，大部分的汽车用户由于自身专业知识有限和缺乏完整阅读的耐心等原因，通常不会对该用户协议或隐私政策的内容加以研究，判断其是否符合信息处理的合法、正当、必要和信息安全保障等原则，而仅仅是简单勾选同意选框。这也为之后智能网联汽车厂商任意处理个人信息数据、损害汽车用户个人信息安全的行为提供了免责事由。

1.3 数据共享中存在个人信息数据安全风险

数据共享对发挥数据的要素作用、实现数据的利用价值具有重要现实意义，智能网联汽车领域的数据共享从宏观层面可促进自动驾驶技术发展，推动汽车产业创新，数据共享能促进汽车厂商、第三方服务提供商以及科研机构之间的合作，加速新技术的研发和完善，推动汽车产业的创新发展；从微观层面上有利于提升用户的驾乘体验感，增强智能网联汽车的安全性能。汽车厂商与地图导航、车辆保险及车辆维修等第三方服务提供商之间的数据共享，可通过分析用户驾驶习惯和偏好，为车主提供个性化服务，如推荐最佳路线、定时提醒车辆维修保养等，从而提升用户的驾乘体验感。同时，通过共享车辆运行数据，可以实时监控交通状况，包括车流量、道路障碍物、异常驾驶行为等，从而及时发现潜在的安全风险，有效减少或避免交通事故的发生，提高智能网联汽车的安全性能。然而，由于智能网联汽车在驾驶环境中产生的汽车数据包含了大量的个人信息数据，因此在数据共享中也给个人信息数据的安全治理带来了巨大风险，如个人信息被恶意泄露或非法利用等。当前，智能网联汽车领域的数据共享主要面临如下几方面的困难，第一，共享前提难以满足。智能汽车数据共享前提是授权和信息披露，具体来说，以汽车厂商与第三方服务提供商之间的数据共享为例，当涉及用户个人信息数据的共享时，第三方服务提供商不仅需要得到汽车厂商的授权，同时也需要获得该汽车用户的授权，即所谓的双重授权。这就要求汽车厂商与第三方服务提供商均需要对汽车用户承担一定的信息披露义务，即充分告知该汽车用户有关个人信息数据共享的目的、内容、方式、期限及潜在的风险等。然而在现实中，大部分汽车厂商与第三方服务提供商进行数据共享时未满足上述前提条件，很多汽车用户在毫不知情的情况下，其个人信息数据就在汽车厂商和第三方服务提供商之间默认流通使用了。第二，共享的主体范围过于广泛。根据《汽车数据若干规定》，汽车数据的处理者包括汽车厂商、零部件供应商、第三方软件服务提供商、经销商、维修机构以及出行服务企业等，由此可见汽车数据共享的主体存在多元化的特点。在现实的汽车数据共享关系中，

① 《中华人民共和国个人信息保护法》第十四条第一款：基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。

通常缺乏对上述主体的准入规制，即未明确规定个人信息数据可以在哪些数据处理者之间进行共享。第三，共享的个人信息数据的范围不确定。智能汽车在运行过程中获取和产生了大量个人信息数据，首先，哪些数据属于个人信息数据本身就存在界限模糊的问题，其次，在已确定的个人信息数据范畴内，哪些个人信息数据属于可以共享的对象、基于何种目的可以共享以及在多大程度上可以共享都存在极大的不确定性。第四，缺乏可行的个人信息数据共享模式。当前智能网联汽车厂商与第三方服务提供商之间主要依靠签订合作协议共享用户数据，这种共享模式也存在明显的弊端，比如缺乏合理的数据访问控制机制，过于注重数据的开放性和流通价值，忽略了对个人信息数据安全的保护。这种单一的数据共享模式既不利于对个人信息数据的合理利用，又因缺乏第三方监管机构，容易导致个人信息数据在共享过程中被滥用。

2　汽车数据中个人信息数据安全治理的解决路径

2.1　结合具体情境对个人数据的界限判定

立法语言表述的不确定性以及匿名化技术发展的局限性使得个人信息数据与非个人信息数据之间的界限具有模糊性。同时，智能网联汽车数据具有种类多、来源广、体量大等特征，运用列举方式对汽车数据中的个人信息数据加以明晰在事实层面不具可操作性。尽管个人信息数据界限的模糊性不可避免，但在汽车数据安全治理中，确定某类汽车数据是否属于个人信息数据却具有重大意义，因为对个人信息数据的保护和管控较其他类型数据更为严格。那么，如何合理确定个人信息数据的边界？可综合数据与人的“距离”及“连接”加以判断。在智能网联汽车运行中，存在“车”和“人”两个数据中心，由此可以大致将汽车数据分为三大类。第一类是完全以“车”为中心形成的数据，车辆的基本信息数据（如车辆的种类和型号数据）、车辆的外部环境数据（如交通信号灯分布数据、道路分布数据、天气数据等）都不属于个人信息数据的范畴。第二类是以“人”为中心产生的数据，包括汽车用户的个人身份信息数据（姓名、性别、年龄、身份证号等）、个人在驾驶过程中形成的人脸数据、声音数据、指纹数据等生物识别特征数据以及使用车内第三方应用软件形成的浏览偏好等数据，均属于个人信息数据的范畴。第三类是“人”和“车”共同作用的数据：车辆维修数据、行驶路线数据，以及车辆的行驶里程数据等，这类数据是否属于个人信息数据存在争议。此时需要引进一个相对确定的判断标准，即判断该类别数据是否可以单独或者与其他数据相结合识别到唯一车辆，如果可以识别到唯一车辆，从而通过人与车的联系识别到特定自然人，则属于个人信息数据。以车辆行驶路线数据，一般情况下根据车辆的行驶路线可以识别到特定车辆，但是如果已经采取匿名化处理技术使得该特定车辆无法联系到某一特定自然人，则不属于个人数据。因此，在判断某一数据是否属于个人信息数据时不能脱离具体情境泛泛而谈，要结合数据适用的具体场景，同一类型的数据在不同的情境中可能会属于不同的分类范畴，从而适用不同的保护规则。至于匿名化处理后数据可能被重新识别再次回归个人信息数据范畴，从而导致个人信息数据与非个人信息数据难以区分这一问题，目前我们可以从技术和法律制度两个层面来尝试解决。首先从技术层面来说，可以通过匿名化技术的发展革新增加重新识别的难度；其次从法律制度层面来说，可以借鉴欧盟的“合理可能”标准，因为绝对的匿名化难以做到，所以我们可以综合重新识别所需时间、成本等因素判断，在采取了所有可能的方法的情况下，如果还是不能识别到数据主体，则可以认定该数据符合匿名化标准，不属于个人信息数据。

2.2　对传统知情同意规则的创新性发展

智能网联汽车运行中产生的个人信息数据，相较于普通的个人信息而言，汽车数据中的个人信息数据具有数据主体多元化、来源广泛化、类型复杂化、内容实时更新等特征，在智能驾驶环境下，数据主体多样且有随机性，数据类型复杂且具实时性，因此不能完全照搬《个人信息保护法》中的知情同意规则。但这也并不是说知情同意规则完全不能适用于汽车数据中个人信息数据的处理活动，而是指应当在原有的架构基础上结合汽车数据的特点进行变通性规定和创新性发展。《汽车数据若干规定》在这一方面相较于《个人信息保护法》已经做出了一定程度上的细化、完善和创新，但是仍然存在很多不足之处。因此，笔者认为应当结合《个人信息保护法》《汽车数据若干规定》以及《信息安全技术个人信息处理中告知同意的实施指南》GB/T42574–2023（简称“42574标准”）等法律规范及标准中的相关规定，针对不同数据主体采取个性化告知与同意机制。第一，对于车主而言，由于其与汽车厂商或者经销商之间存在买卖等前置合同关系，因此可以通过在汽车买卖合同或者维修服务合同中以独立条款的形式进行提示，也可以通过车载显示器的弹窗提示或者第三方应用软件的提示等。涉及敏感个人信息的处理时，应当通过车载显示器的弹窗多次弹出提示、指示灯常亮提示、即时的语音播报提示等显著的提示方式。此外，一般情况下车主对智能网联汽车的使用具有固定性，因此针对那些高频率、重复式的场景，可以赋予用户设置同意次数、同意期限等多样化的同意机制，但是要注意将个人同意接受一般服务条款与同意接受个人信息数据处理条款相区分，不能将二者混为一谈。第二，对于车辆承租人和代

https://doi.org/10.35534/pss.0705075

驾等临时驾驶人而言，可以采取车载显示面板弹窗提示以及第三方应用程序告知的方式予以提示，由于这类数据主体具有临时性和随机性，因此应当在每次用车前重新获得同意。第三，对于乘车人而言，可以通过打车应用软件弹窗提示进行告知，当乘车人是儿童等特殊群体，无法用应用软件进行告知时，可以由车主代为授权以保障汽车基本功能的启动。第四，对于其他同行车辆车主和不特定的车外行人而言，无法取得其事前的明示同意，因此，只能采取推定同意的方式，即在安装了数据处理设施的道路入口设置显著的提示标志，若该主体仍然进入该区域，则推定该主体对数据处理活动做出了同意的表示。此外，对于智能网联汽车中拍摄到的车外行人的人脸图像数据等，在满足安全驾驶功能的基础上采取删除或者对人脸信息进行轮廓化处理等匿名化处理技术。智能网联汽车运行中对这类数据的处理主要是基于保障驾驶安全的目的，因此在采取匿名化技术以后无需取得数据主体的同意，处理完成以后也不应对其进行存储。

2.3 完善数据共享中个人信息数据安全保障机制

数据共享有利于提高数据资源利用率，优化数据市场资源配置，但也涉及数据安全和隐私保护。实施智能网联汽车数据共享战略时，需平衡数据共享效率与汽车用户个人信息数据安全保护，进一步完善安全保障机制，为智能汽车数据共享保驾护航。具体来说，主要从以下方面进行完善。第一，完善汽车数据中个人信息数据的分类分级授权规制和信息披露规制。《汽车数据若干规定》将个人信息数据分为一般个人信息和敏感个人信息两类，针对这两类不同的个人信息数据，应当采取不同的数据共享授权规则。当数据共享的内容是一般个人信息时，数据处理者只需得到个人的一般性授权，当数据共享的内容是敏感个人信息时，数据处理者以及数据共享关系中的接收者均应当得到个人的明确授权。同时，智能网联汽车厂商和第三方服务提供商随着数据共享关系发展的阶段不同，其扮演的角色也不同，因此要区分不同阶段不同责任主体的信息披露义务的内容和信息披露程度，其中信息披露的内容应当包括数据共享的目的、共享数据的类型、数据接收方的信息及潜在风险，信息披露的标准应当达到足以使数据主体充分了解的程度。第二，限定个人信息数据共享的对象范围。个人信息数据共享关系中涉及了包括车主、驾驶人、乘车人、车外行人、汽车厂商以及第三方服务提供商等多方主体。尤其是存在大量的第三方服务提供商，这些第三方服务提供商在数据安全保障方面的能力良莠不齐，如果不加区别允许所有的第三方服务提供商成为数据共享对象，这将会引发严重的个人信息数据安全风险。为了实现对数据共享过程中安全风险的事前防范，应当对个人信息数据共享对象的安全保护能力进行审查评估，只有通过了相应的安全资质审查才能赋予其个人信息数据访问权限及共享资格。

3 结语

智能网联汽车时代，个人信息数据安全构成了汽车数据安全的重要组成部分。近年来智能网联汽车领域频频发生的个人数据泄露和非法利用事件，已引发大众对汽车数据安全治理的高度重视。汽车数据中的个人信息数据具有数据量庞大、数据种类多、影响范围广等特点，对个人信息数据的安全风险进行治理是当前发展智能网联汽车产业亟待完成的任务。本文以《汽车数据安全管理若干规定（试行）》的出台为背景，指出了汽车数据中个人信息数据安全治理面临的困境，从厘清个人信息数据界限、针对不同数据主体实行个性化告知同意机制，以及完善数据共享中个人信息数据安全保障机制三条路径探索了智能网联汽车时代走出个人信息数据安全治理困境的可行办法，为智能网联汽车产业数据安全治理体系的完善提供了思考。

参考文献

[1] 孙晋，周灿．网络运营商数据监控行为的法律边界——以云存储服务商为例[J]．长江论坛，2022（12）．
[2] 徐子淼．智能网联汽车数据处理的法律规制：现实、挑战及进路[J]．兰州大学学报（社会科学版），2022（2）．
[3] 赵舒捷．智能网联汽车数据安全的风险、冲突与规制：基于总体国家安全观的规范建构[J]．数字法治，2023（4）．
[4] 黄凯男．英国智能网联汽车数据治理框架及其启示[J]．科技创业月刊，2023（6）．
[5] 齐爱民，张哲．识别与再识别：个人信息的概念界定与立法选择[J]．重庆大学学报（社会科学版），2018（2）．
[6] 徐子淼．智能网联汽车数据处理的法律规制：现实、挑战及进路[J]．兰州大学学报（社会科学版），2022（2）．
[7] 高完成．智能汽车数据共享的困境与法律应对[J]．河南财经政法大学学报，2023（6）．
[8] 郑佳宁．知情同意原则在信息采集中的适用与规则构建[J]．东方法学，2020（2）．
[9] 程啸．论数据安全保护义务[J]．比较法研究，2023（2）．
[10] 宋琦，武波，刘永东．关于智能网联汽车数据安全治理框架的探究[J]．网络安全与数据治理，2024（3）．

Data Security Governance Dilemmas and Pathways for Resolution in Intelligent and Connected Vehicles: A Focus on Personal Information Data

Xiang Liya Zhou Mi

Shanghai University of Political Science and Law, Shanghai

Abstract: Intelligent connected vehicles have increasingly replaced traditional vehicles as the future development trend of the automotive industry. During their operation, intelligent connected vehicles generate a large amount of vehicle data. The "Several Provisions on Automotive Data Security Management (Provisional)"classifies these data into two categories: personal information data and important data. Among them, personal information data is closely related to personal interests. Once leaked, it not only poses a threat to our personal privacy security but also causes serious damage to public and national security. With the continuous improvement of the intelligence and connectivity levels of automobiles, while bringing more comfortable and convenient driving and riding experiences to the public, it also exposes data security risks and hidden dangers. Especially in the field of personal information data security governance, intelligent connected vehicles face problems such as ambiguous boundaries of personal data, the difficulty of directly applying the traditional informed consent system to the regulation of personal information data processing in automobiles, and the existence of personal information data security risks in data sharing. These problems pose new challenges to the existing automotive data security governance system. To address these issues, it is necessary to further clarify the boundaries of personal information data in automotive data, make reasonable adjustments to the traditional informed consent system based on the uniqueness of automotive data, and improve the personal information data security guarantee mechanism in data sharing, so as to achieve the improvement of the personal information data security governance system in automotive data.

Key words: Intelligent and connected vehicles (ICVs); Personal information data; Data security; Data governance; Personal data

https://doi.org/10.35534/pss.0705075