

区块链赋能智能汽车个人数据保护的实现路径

贺中原 骆诗婷

湖南工业大学, 湖南省株洲市, 412007;

摘要: 智能驾驶汽车发展带来个人数据保护新挑战, 数据边界模糊等致多方面问题, 且现行法律难提供有效规范保障。其面临数据处理风险隐患、安全难保障、知情同意机制失灵、维权机制缺失等困境。本文通过区块链技术其中心化、匿名性、不可撤销性、可追溯性等特征为解决智能驾驶汽车个人数据保护问题提供了新的思路和方法, 并提出建构个人数据修改权利、多元监管的完善路径。有望实现智能驾驶汽车个人数据安全合理利用, 推动产业健康发展。

关键词: 智能驾驶; 个人数据保护; 区块链; 隐私

DOI: 10. 64216/3080-1486. 25. 06. 036

引言

在当今数字化高速发展的时代, 数据已成为重要的资产, 其安全保护和合理利用备受关注。从构建智能网联汽车数据共享生态的目标来看, 现行法律大多制定于前数字时代, 无法为智能网联汽车数据治理提供法律上的规范、引领和保障作用。从汽车数据实践来看, 与汽车数据访问关系密切相关的法律主要包括民法、竞争法、个人信息保护法等。汽车用户则希望通过《个人信息保护法》实现其对个人数据的保护。因此, 本部分旨在阐明以上法律在智能汽车数据治理方面存在的困境, 并进一步指出现行法律在促进法律规范与技术支持相互融合方面的不足之处。

1 我国智能驾驶汽车中个人数据保护的现实困境

1.1 个人数据界限模糊

一辆智能驾驶汽车在其运行过程中需要使用大量的数据, 其数据的获取通过安装的传感器进行传输, 包括内部环境数据与外部环境数据。但智能汽车收集的车辆数据并非都是需要保护的个人信息, 它们只有在指向自然人且该自然人已被识别或可被识别的情况下, 才转变成个人信息。这些数据来源广泛且相互关联, 其复杂程度增加了对“个人信息”界定的难度。不同类型数据的融合使用使得数据之间的界限更加模糊。随着技术的发展, 原本难以识别个人身份的数据可能通过新的算法或数据关联变得可识别。匿名化处理的数据在某些情况下也可能被重新识别, 这使得数据的“个性化”边界处于动态变化之中, 给个人信息保护带来不确定性。

1.2 数据安全难以保障

智能驾驶汽车系统中的数据存储面临着被黑客攻击和数据泄露的风险。一旦黑客入侵车辆的存储系统, 可能获取大量用户的个人信息, 包括驾驶习惯、出行路线等敏感信息, 这些信息可能被用于非法目的, 如精准诈骗等。在车与车、车与基础设施、车与云端之间的数据传输过程中, 数据可能被窃取或篡改。在车与云端的数据传输中, 如果通信链路没有足够的加密措施, 攻击者可能拦截并篡改传输中的数据, 向智能驾驶汽车发送错误的指令, 导致交通事故等严重后果。

1.3 知情同意机制失灵

智能驾驶汽车在运行过程中持续收集大量数据, 许多数据收集行为对用户来说是不可见的。一些数据收集是为了实现智能驾驶汽车的基本功能, 但部分数据收集可能超出了用户的预期。如果车辆收集的道路环境数据可能被用于其他商业目的, 而用户在使用车辆时可能并未明确知晓并同意这种数据使用方式。在实际操作中, 用户往往只能选择接受或拒绝预先设定的一揽子数据收集和使用条款, 缺乏对具体数据处理活动的个性化同意选项。普通用户难以充分了解其个人信息数据将如何被使用、共享和存储, 以及可能面临的风险, 这可能导致用户在不知情的情况下同意了一些不合理的数据处理行为。

1.4 数据维权机制缺失

智能驾驶汽车数据处理过程复杂, 涉及多个主体, 包括汽车制造商、软件开发商、数据服务提供商、运营商等。在数据侵害事件发生时很难证明数据泄露的具体环节和责任主体, 因为数据可能在多个主体之间流转和

使用,在数据处理过程中经过多次转换和整合,这使得在出现问题时难以追踪数据的流向和确定责任的源头。数据的易破坏性和易篡改性也增加了举证的难度。一旦数据被泄露或篡改,原始数据可能被销毁或修改得难以恢复,使得用户无法提供有效的证据来支持自己的诉求。

2 区块链赋能智能驾驶汽车个人数据保护的技术路径

区块链作为一种新兴的分布式数据库技术,以链条的方式将各个节点进行连接,能够实现各节点数据信息之间的交互共享,其应用明显区别于传统汽车数据管理技术,不仅能够节约人为数据管理成本,还能有效解决传统汽车数据管理存在的问题,大大提高数据的可信度以及安全性,实现数据融合共享。

2.1 哈希运算建构智能驾驶汽车个人数据安全存储机制

哈希算法是一种将任意长度的数据转换为固定长度哈希值的函数。在智能驾驶汽车个人数据保护中,通过哈希算法对车辆采集的各类数据进行加密处理,将数据转换为不可逆的哈希值进行存储。对于车内人员的生物特征数据(如指纹、面部识别信息等),在采集后立即通过哈希算法进行加密,使得原始数据无法被还原,只有经过授权的用户使用特定的密钥才能验证哈希值是否匹配,从而保护数据的安全性。哈希算法的单向性和抗冲突性确保了数据的保密性。即使攻击者获取了哈希值,也无法通过逆向计算得到原始数据,大大降低了数据泄露的风险。同时,不同的数据输入将产生不同的哈希值,有效防止了数据篡改,因为一旦数据被修改,其哈希值将发生变化,从而可以及时发现数据的异常。

2.2 联盟链建构智能驾驶汽车个人数据安全治理机制

当前,汽车数据服务资源分散,数据流通渠道多,数据在运维过程中难以保留完整的数据操作及流通记录,导致发生数据安全事件后难以维权。而联盟链是一种介于公有链和私有链之间的区块链形式,由多个特定的机构或组织共同维护。在智能驾驶汽车个人数据安全治理中,联盟链可以由汽车制造商、数据服务提供商、相关监管机构等组成联盟共同管理。汽车制造商负责提供车辆数据,数据服务提供商负责数据的存储和处理,监管机构负责监督数据的合规性,各方在联盟链中共同协作,确保数据的安全和合理使用。按照访问者功能和需求进行权限分级,只有必须涉及到个人数据的才能参与验证和存储,对于无需使用个人数据的访问者无法获

取用户数据,保障了数据的隐私性和安全性。

联盟链还具有增强数据的可追溯性的特点,联盟链上的每一笔数据交易都被记录在区块链上,且不可篡改,便于追溯数据的来源和流向。在发生数据安全事件时,可以通过联盟链快速定位问题的源头,采取相应的措施进行处理,同时也有助于责任的认定和追究。

2.3 智能合约建构智能驾驶个人数据访问机制

智能合约是一套以数字化形式定义的承诺,包括合约参与方可以在上面执行这些承诺的协议。在智能驾驶个人数据访问机制中,智能合约可以规定数据访问的规则和条件。当用户需要访问自己的历史行驶数据时,智能合约会验证用户的身份和访问权限,只有符合条件的用户才能获取数据。智能合约的执行是基于预先设定的规则,一旦满足条件,合约将自动执行相应的操作,无需人工干预。智能驾驶汽车检测到车辆发生故障时,智能合约可以自动触发数据共享机制,将相关故障数据发送给指定的维修服务提供商,但在发送之前,会再次验证维修商的身份和权限,确保数据的安全共享。同时,所有的数据访问操作都记录在区块链上,可供审计和监督,提升数据使用的透明度与安全性,用户可以清楚地了解自己的数据被谁访问以及访问的目的。

2.4 时间戳技术建构智能驾驶个人数据维权机制

时间戳技术是对数据产生的时间进行标记和认证的技术。在智能驾驶个人数据维权中,当数据产生时,时间戳技术会为其加盖精确的时间标记,并将其记录在区块链上。一旦数据被标记时间戳,其时间信息就被固定下来,任何后续的修改或篡改都将被区块链记录,从而为数据的真实性和完整性提供了有力的证据支持。由于时间戳技术提供了可靠的时间证据,在司法维权过程中可以减少争议和纠纷,加快案件的处理速度。法院可以直接依据区块链上的时间戳记录和相关数据进行判决,无需花费大量时间进行证据的核实和鉴定,降低了维权成本,提高维权效率,保护了用户的合法权益。

3 区块链赋能智能驾驶汽车个人数据保护的法律法规

智能驾驶个人数据的治理是一项复杂且繁重的工作,需构建风险预防、技术补强与法律规制相结合的体系。因此,在区块链智能驾驶汽车个人数据保护的过程中,法律应作出以下几点回应:

3.1 保留个人对区块链数据的修改权利

区块链不可篡改性是其安全性和透明性的重要保

障,但同时其对个人信息权影响甚巨。个人信息权即自然人依法对其个人信息进行控制和支配并排除他人干涉的权利,它是自然人对其个人信息享有的人格权的总称。依据相关法律法规,如《个人信息保护法》等,明确个人在区块链环境下对其数据的更正和删除权利。

在智能驾驶汽车场景中,用户有权要求更正区块链上存储的不准确或不完整个人数据;对于自身不再需要或违反法律法规的数据,用户亦有权要求删除。智能驾驶汽车制造商及数据服务提供商应设立专门的用户服务平台或接口,为用户提交数据更正、删除请求提供便利。若数据控制者未及时处理或无正当理由拒绝处理用户的合理请求,应承担相应法律责任。通过提升汽车生产商、网络经营者保护个人隐私的能力与主动性,以弥补传统“告知—同意”机制的缺陷。在此过程中,法律更需注重多元价值的平衡,其制度设计应聚焦个人隐私保护与适应新兴技术变迁之间的利益衡量。

3.2 隐私保护转化为数据财产权保护

从本质而言,数据在民法范畴内应是一种具有物质性、确定性、自主性且非人身性的存在。智能驾驶汽车相关的数据保护亦涵盖于这一特定且宏观抽象的范畴之内。汽车数据作为权利目标,其自然属性与现存民事权利的自然属性有所不同,它既具备财产权的性质,又兼具个人人格的权属性,故而有学者将其称为一种特殊的民事权利。因此,需要由法律将用户对其个人数据的权益确认为一种财产权并予以保障。

用户可以授权数据服务提供商使用其数据,并获得相应的经济补偿。在数据交易的过程中,用户应能够对其数据的使用范围和方式进行限制,可以选择仅允许数据用于特定的研究目的,而禁止用于商业营销活动,以平衡数据财产权的行使和隐私保护的需求。用户作为数据的所有者,有权根据自己的意愿决定数据的用途,这有助于在保障用户隐私的基础上,实现数据财产价值的合理开发和利用。同时,法律应提供相应的机制和救济途径,当用户的隐私或数据财产权受到侵害时,能够及时获得赔偿和保护。

3.3 强化数据监管

构建专门的数据共享监管机构。面对人工智能时代数据行业明显的混业经营态势,有必要依托传统分业监管模式下各行业固有监管机构在行业知识、行业特征、行业监管经验及监管渠道等方面的天然优势,在各行业固有监管机构之下设置专门的数据监管部门。

强化数据监管责任。“一切有权力的人都容易滥用自己的权力,直到他遇到界限才会休止。”因而,在赋予监管机关权力的同时,应该加强数据监管责任机制建设,通过立法明确各级监管机构的职责权限,规定不认真履行监管职责的机构及人员应承担的法律责任,从而促进数据共享监管体系有效运行。

4 结语

智能驾驶行业正处于高速发展阶段,数据体量将迎来井喷式增长,相关数据的处理行为及其规制已成为制约行业健康发展的关键议题。当前,我国针对智能驾驶领域数据的专门规范尚显匮乏,亟需立足行业实践,依托技术创新、法律完善与行业自治的协同发力,构建多维度数据治理体系,系统探索并优化数据风险防控机制与治理模式。

参考文献

- [1] 参见杜明强.:《无人驾驶汽车运行中隐私权保护困境与进路》,载《河南财经政法大学学报》2021年第4期,第30页。
- [2] 参见陈晓林:《无人驾驶汽车对现行法律的挑战及应对》,载《理论学刊》2016年第1期,第128页。
- [3] 参见郑佳宁:《知情同意原则在信息采集中的适用与规则构建》,载《东方法学》2020年第2期,第202页。
- [4] 参见郑阳:《区块链在数字图书版权治理中的应用研究》,载《图书馆工作与研究》2022年第12期,第34页。
- [5] 参见陈奇伟、聂琳峰:《技术+法律:区块链时代个人信息权的法律保护》,载《江西社会科学》2020年第6期,第173页。
- [6] 参见李青:《区块链技术中的个人信息保护问题研究》,载《上海法学研究》2022年第5卷(2022世界人工智能大会法治论坛文集),第192页。
- [7] 参见施建锋等:《区块链智能合约交易并行执行模型综述》,载《软件学报》2022年第11期,第99页。
- [8] 参见齐爱民:《信息法原论》,武汉大学出版社2010年版,第80页。
- [9] 参见季卫东:《数据保护权的多维视角》,载《政治与法律》2021年第10期,第8页。

作者简介:贺中原(1999年10月—),男,汉,河南省南阳市,法律硕士,湖南工业大学,412007
骆诗婷,湖南工业大学