

个人信息的过度收集与反垄断法的补充保护——以自动驾驶技术为例

严梓晨 刘露

江西财经大学，江西南昌，330013；

摘要：随着科学技术的高速发展，企业获取个人信息的能力不断增强，手段逐渐丰富。自动驾驶技术的发展离不开个人信息的收集。例如，需要通过面部监控对驾驶者的状态进行评估，以提前做出预警。在此过程中不可避免地需要收集用户的面部特征等信息。车企的收集行为为个人信息的保护提出了巨大的挑战。《民法典》《个人信息保护法》在一定程度上保障了个人信息的安全，但无法做到全面保护。随着自动驾驶行业的不断洗牌淘汰，领头车企掌握了巨量的个人信息，并用于商业竞争，市场出现结构性失衡。因此，讨论《反垄断法》介入的合理性及使用场合具有重要的理论价值和紧迫的现实需要。

关键词：自动驾驶技术；数据垄断；个人信息保护；反垄断法

DOI：10.69979/3029-2700.25.03.052

1 自动驾驶技术发展背景及带来的法律风险

1.1 自动驾驶技术发展背景

二十一世纪是人工智能技术高速发展的时代，随着人们对便捷、高效的智能生活追求的日益提高，人工智能技术与各个行业相结合。汽车行业在人工智能技术的助推下，正加速由机械化向智能化转变。2014 年 1 月，国际汽车协会（SAE）发布 J3016 标准，定义了从自动驾驶自动化（L0）到完全自动驾驶自动化（L5）等 6 个自动驾驶自动化等级。截至 2024 年，国际前沿自动驾驶技术已经发展到 L3 阶段（有条件自动化），正在向 L4（高度自动化）快速迈进。中国作为自动驾驶技术发展强国，也紧跟国际步伐——2021 年 8 月我国发布《汽车驾驶自动化分级》。由此可见，中国自动驾驶技术已经出现了划时代的革新，需要制定相关规定予以定义与划分。

可是近几年，部分车企被曝出大量收集个人信息。2021 年 4 月初，特斯拉被黑客曝光一组由车内摄像头拍摄的高清画面。其首席执行官马斯克也承认，特斯拉会通过车内摄像头观察驾驶员是否疲劳驾车和注意路况，并给予一定的提醒。个人信息安全再度受到广泛关注。

1.2 自动驾驶技术收集个人信息现状

2023 年 4 月，有媒体报导称在 2019 至 2022 年期间，有九名前特斯拉员工通过内部消息系统分享了一些车主车载摄像头记录的隐私视频和图像。具体包括用户的

车内对话、车内活动等。仅仅过去一个月，特斯拉又发生一起涉及影响超过 7.5 万人的数据泄露事件。美国缅因州总检察长办公室发布通知称，这是“内部不法行为”的结果。调查显示，有特斯拉的员工违反规定，挪用超过 100GB 的信息。国内自动驾驶汽车用户仍然面临类似风险，我国某车企在方向盘上安装传感器，该传感器可以检测驾驶者的心率、面部表情等。公司声称是为了检测驾驶者的行驶状态，保障行驶安全。

需要承认的是，信息收集无法避免，自动驾驶技术的实现离不开对外界信息的收集和分析。作为自动驾驶汽车关键技术的车载测技术和地面侧技术均需要信息感知（图像及激光感知）、车载摄像头、调度系统等通过对外部地理特征、道路状况、天气情况、车与车间的关系等和内部驾驶者精神状态、面部特征等生物信息的收集来实现自动驾驶。

2 现存法律的保护措施以及不足之处

2.1 现存法律对个人信息的保护

《中华人民共和国民法典》与《中华人民共和国个人信息保护法》为个人信息保护提供法律保障。

《民法典》作为民事领域的基础性法律，有关个人信息保护的条文主要集中在第四编“人格权”中的第六章“隐私权和个人信息保护”。其中，第一千零三十五条明确了个人信息处理者在处理个人信息时应当遵守合法、正当、必要原则，不得过度处理。第一千零三十

七条和第一千零三十八条指出了信息主体的权利和信息处理者的义务。但是,《民法典》仅仅对个人信息保护做出了原则性规定和双方权利义务的基础划定,难以应对复杂的司法实践问题。

2021 年 11 月 1 日施行的《个人信息保护法》是专门针对个人信息保护的特别法。它在《民法典》的基础上,进一步细化了个人信息保护的具体规则,明确了个人信息处理的合法性基础(如同意、合同履行、法定义务等)、敏感个人信息的特殊保护规则、跨境传输规则、个人信息处理者的义务(如个人信息保护影响评估、数据安全措施等)法律责任(包括行政处罚和民事赔偿)等。信息主体对其个人信息的处分体现为自己使用、自己决定是否为他人使用,以维护其人格自由发展。首先,用户享有知情权和同意权,有权知悉其个人信息被收集、使用的目的、方式、范围等以及决定是否同意处理其个人信息。自动驾驶汽车公司应当明确告知相关内容,未经许可不得收集用户的个人信息。同时用户可以撤回同意,撤回后公司应当立即停止处理并且删除个人信息。其次,用户享有访问权和更正权。用户有权随时查询自己的个人信息,当发现个人信息有误时,可以要求处理者及时更正以保证信息的准确性。最后,用户享有删除权。当处理目的已经实现、信息主体撤回同意或者出现其他法定事由的,处理者应当及时删除并通知第三方停止使用。此外,用户可以行使数据可携带权,请求将个人信息转存至用户指定的个人信息处理者。该存储地址既可以是用户的私人设备,也可以是云空间。

为响应国家法律要求,市面上主流自动驾驶汽车品牌 and 购买者之间的用户协议中包含了个人信息保护相关条款。例如:小鹏汽车 2024 年 11 月 25 日生效的《小鹏汽车网络平台隐私政策》。该政策较为清晰地告知了个人信息收集和使用;个人信息的对外提供、转让、公开披露;个人信息的储存等事项。其中第五条列举了用户的权利,具体包括对个人信息(账号头像、昵称、性别、生日、用车城市、兴趣偏好、职业信息等)的查阅、更正、补充和删除;撤回个人信息的同意授权;复制、转移个人信息;申请注销账号等权利。蔚来汽车《蔚来汽车隐私政策》向用户明确告知如何收集、储存、使用、管理、保护个人信息。

2.2 客观收集的垄断属性和被收集的个人信息法律保护之局限

《民法典》《个人信息保护法》主要通过规定信息主体和信息处理者对个人信息“使用”的权利和义务来保护个人信息。《个人信息保护法》是个人信息保护领域的专门规范,通过构建“告知——同意”架构来增强信息主体对其个人信息的“使用”能力。但是,随着市场主体力量的壮大,市场出现结构性失衡,持续性不平等信息关系被推到极致,信息主体实际上失去了对个人信息的控制。加之这种对“使用”的控制也极其有限,个人信息的公共属性决定了,个人信息的控制最多可以做到控制自己不联系他人或者如何联系他人,但并不能控制信息本身被他人如何使用。法学界学者们将目光聚焦于对个人信息处理行为的规制,却忽略了个人信息的大量收集本身具备的数据垄断隐患和法律风险。正如前文所述,必要性信息的收集是必不可少的。其次,自动驾驶汽车的平均安全使用寿命是 4-6 年,虽较于传统汽车平均 13 年的寿命更短,但是公司仍然可以保证在这 4-6 年内购车用户的忠诚度。加之全国掌握自动化驾驶技术的公司数量较少,掌握领先技术的公司更是少之又少。每年千万级的购车需求和极为有限的品牌选择,直接导致了头部公司在相对稳定的期间内会得到百万甚至千万的用户。不仅如此,按照一般消费习惯,当车主适应了一个品牌的汽车后往往会选择继续购买本品牌的高级款型,逐渐形成稳定的客户群体。其是否具备数据垄断属性以及应对之策值得探究。

3 《反垄断法》补充保护的法理分析

反垄断法处理市场力量问题。将个人信息保护纳入《反垄断法》的基础在于,个人信息损害行为与市场力量的形成和运用有关。数字技术对传统市场结构、商业模式、竞争格局和消费者行为产生的深刻影响和变革。这种数字市场的颠覆效力不仅改变了企业的运营方式,还重塑了整个经济生态。在数字经济时代,个人信息成为企业竞争的重要资源和市场力量的核心要素。

3.1 个人信息成为市场竞争的核心资源

支配地位是市场力量的具体体现之一,如今数据驱动商业模式成为许多数字平台的首选。数字平台通过收集和分析用户数据,提供个性化服务,从而获得竞争优势。而过度的数据收集和与网络效应结合的市场颠覆,直接导致了支配地位的产生和滥用的可能性,最终实现“赢家通吃”。加之汽车客观使用年限和用品牌效应,

占有支配地位的自动驾驶汽车公司会在相当长的一段时间内对用户进行“锁定”，以维持其支配地位。

3.2 个人信息的非价格竞争维度

在零价交易中，消费者的个人信息成为交易的主要成本，而在非零价交易中，个人信息也是消费者的成本类型之一。有学者将《反垄断法》的立法目的解释为“对市场权力形成的制约”，也有学者将其解释为“保护消费者福利”。但其本质上都是对市场力量和对竞争秩序的关注。一般而言，在同类相似商品中低个人信息需求的产品更容易获得消费者的青睐，个人信息隐私保护的**市场需求反向刺激经营者提供满足用户隐私偏好的产品来提升市场竞争力，经营者的市场竞争力部分既体现为个人信息保护水平的高低。然而，少数经营者对个人信息的**大量收集形成的垄断会打破企业间有关减少个人信息收集的良性竞争。消费者逐渐单一化的可选项使得经营者在个人信息收集**中掌握主动权。聚焦于自动驾驶领域，个人信息的垄断意味着汽车公司可以在法律规定的底线之上以各种名义在用户协议中增设有关个人信息许可收集使用的条款。这将会严重损害消费者的合法权益。

（三）现实的合规灰色地带。在数据交易中，往往存在合法交易的灰色地带。例如，许多平台通过冗长的隐私政策将“同意数据共享”隐含在用户协议中，用户往往未仔细阅读即点击同意，陷入默认同意的陷阱中。此外，匿名化不等于不可识别。企业可能将用户数据匿名化后交易，规避直接的个人信息保护法规。这些事实直接导致个人信息被大量收集的现实情况。

4 《反垄断法》补充保护的可行性

《反垄断法》保护个人信息符合立法目的。《反垄断法》第一条规定“为了预防和制止垄断行为，保护市场公平竞争，鼓励创新，提高经济运行效率，维护消费者利益和社会公共利益，促进社会主义市场经济健康发展，制定本法。”不难看出，本法的立法目的多元，既为了控制市场力量又为了消费者权益还为了维护公平正义的市场竞争秩序。但毫无疑问，“预防和制止垄断行为，保护市场公平竞争”是其直接目的和动因。也就是说，反垄断立法的直接目的在于保护竞争。在如今的数字市场中，个人信息作为重要的要素。就自动驾驶汽车领域而言，大量的个人信息被集中于极小部分的企业

上，不仅会导致消费者权利的受损，更会导致市场机制的失灵。通过网络效应和锁定效应，这些企业可以利用已有的大量个人信息不断巩固自己的优势地位，再通过自己的优势地位不断获取更多的用户，收集其个人信息。这种循环最终会致使个人信息的非价格竞争因素被打破。竞争机制的失灵直接导致组织可能滥用市场支配的地位——随意提高或降低隐私保护水平。此时，《反垄断法》介入可以维护市场主体在个人信息保护水平层面的竞争，不会打破《反垄断法》保护竞争的直接目的。

保护手段合理有效。《反垄断法》可以对滥用市场支配地位造成的个人信息损害施加多种形式的救济措施。例如，禁止实施集中；拆分还原——采取限期处分资产等措施恢复到集中前的状态等。当前法律对自动驾驶汽车公司收集个人信息的客观现状没有有效的治理手段，多是从用户角度规定其权利以及个人信息处理者的义务，且相关术语定义尚不明确，个人信息处理者有较大的解释空间，很难形成有效治理。《反垄断法》的介入可以有效解决当前问题，通过明确的禁止性规定，直接打击过度处理的行为。在行为端，针对滥用市场支配地位收集的个人信息，反垄断执法机构可以责令停止实施并没收违法所得。违法收集的个人信息有被解释为违法所得的空间。有效解决了个人信息被过度收集可能带来的隐患。在监察端，反垄断执法机构可以依法对涉嫌违法的市场主体实施审查和调查，若市场主体采取故意隐匿、销毁、转移证据等手段试图逃避监管，相关机构有权责令整改、罚款，构成犯罪的，依法追究其刑事责任。

5 《反垄断法》保护的实现路径

有学者认为利用《反垄断法》保护个人信息会带来许多问题。例如，可能会过度扩张该法的适用范围，增加执法难度；可能会加大企业合规审查的难度，影响法律的稳定性和可预见性；可能会导致法律适用边界的模糊，法律监管重叠甚至是规则冲突。因此，路径的设计既要应对数据垄断对市场的威胁，又要避免《反垄断法》的泛化适用。笔者尝试通过“标准完善+有限扩张”的路径实现法律目标和社会效益的统一。

5.1 标准完善——数据垄断的滥用市场支配地位属性

依据我国《反垄断法》规定，在认定企业是否滥用

支配地位时，首先需要界定相关市场，包括相关产品市场和地域市场。自动驾驶汽车企业的经营范围遍及全球，没有相对准确的地理边界，相关地域市场难以界定；而相关商品市场同样难以界定，数据驱动型的市场相较于传统市场而言是动态变化的，并且掌握尖端自动驾驶技术的企业通常科技力量雄厚，涉猎多方领域。通过数据整合构建数据生态系统，其可将某一市场掌握的数据使用于另一市场。各个市场相互影响，难以形成明确的相关商品市场。为解决上述问题，应当扩展“相关市场”的内涵，增设“相关数据市场”。数据类型多种多样，并非所有的数据都应当纳入相关数据市场领域。

“相关数据”应当定义为对竞争具有实质影响的数据。其认定应当围绕“价值捕捉策略”展开，形成更加关注横向和纵向互动的定位工具。数据价值的体现是一个动态的过程，其包含了数据的收集、数据的分析、数据的利用和用户反馈。在这一过程中，相关数据市场可以划分为三个子市场——数据捕获子市场、数据存储子市场和数据分析子市场。

5.1.1 数据捕获子市场

自动驾驶技术对信息的捕获大致可以分为主动捕获和被动捕获。主动捕获是指自动驾驶汽车利用激光雷达、摄像头、超声波传感等设备，实施感知车内及周围环境，捕捉路况环境、行人、其他车辆以及车内人员的面部特征、表情、精神状态等信息。例如，车载侧技术可以利用微型摄像头捕捉驾驶人的面部信息、表情等生物信息；地面侧技术收集驾驶人经常行驶的路段以及起终点，掌握驾驶人的居住地、工作单位、通勤距离以及其他个人信息。被动捕获主要是通过用户的主动输入或主动产出而收集的信息。例如，驾驶人在使用车载系统时，系统被动地得知用户的偏好设置、音乐选择、通话记录等信息，或者在车内与家人谈话时，系统被动地接收这些信息。

5.1.2 数据存储子市场

自动驾驶汽车公司根据收集信息按照实时性、敏感性、使用场景等不同划分标准分类存储信息。针对驾驶者的实时操作数据，例如刹车、加速、转弯等以及行车记录的短期缓存数据，例如短时间记录的车辆周边环境等通过车载硬盘（SSD）存储于车载终端。而长期的用户行为数据，例如驾驶者的驾驶习惯、驾车精神状态监测记录、语音指令记录等都被存储于车企的云平台。

5.1.3 数据分析子市场

并非所有的存储数据都有价值，车企利用相关技术进行数据冷热分层并加以分析，利用收集的信息为用户画像，分析用户的“可能偏好”，并可以“描绘”驾驶人，大致掌握其收入情况、职业、家庭情况等敏感个人信息。车企以大量的用户画像为基础，可以快速捕捉并满足用户的新型需求，增加用户量，提升自己的市场竞争力。再利用网络效应和锁定效应反哺数据获取子市场，形成数据壁垒。

5.2 有限扩张——明确《反垄断法》介入信息保护的场景

从《反垄断法》的立法目标出发，“利用市场支配地位滥用个人信息破坏市场竞争”是其判断的核心标准。单纯的个人信息过度收集不应当受到《反垄断法》的规制。因此，应当构建数据垄断破坏竞争的评估标准，可以通过“数据控制力评估（包括客观数据独占性、数据可替代性和数据动态积累能力）+损害竞争”模式进行分析。

1. 数据控制力。（1）客观数据独占性。独占指人们对其享有所有权的物进行排他的占有、使用、处分的行为。对于在自己的生产活动中产生的数据，企业具有天然的独占权利，这是一种私权利。但是对于利用先进技术收集而来的数据是否当然的享有独占性值得讨论。有学者认为数据来源于车企的经营活动，并且经过了用户的授权同意，具备独占性。还有学者认为用户对信息收集的相关条款属于强迫同意，加之个人信息具有公共属性，车企不当然享有所有权，而是享有了该部分数据的用益物权。笔者认为，这里的独占是一种客观上的独占，即车企通过用户协议强制用户授权其收集信息或者利用用户草率同意协议的特点让用户在不知情的情况下同意车企收集其个人信息，并且条款中往往会有“独家授权”的内容。无论是何种方式，车企都客观上排他占有了用户的个人信息。一个车企的用户量越大，独占数据的基数也就越大。（2）数据可替代性。数据可替代性是指某一数据集是否能够被其他数据（同类或异类）以同等效果替代，以实现相同的商业或技术目标。一个结果往往可以通过不同的数据组合分析得到，可当只有利用特定的数据才能得到需要的结果时，该数据具有不可替代性。企业掌握的此类数据越多，其对该领域数据的控制能力越强。此类数据往往具有实时性、场景依赖

性等特点,因此可以从数据生成的方式、数据质量与精度、数据获取的时间成本等角度综合分析。(3)数据动态累积能力。数据的控制力还体现在数据获取的数量上。在数字市场,数据累积能力主要体现为网络效应和锁定效应的发挥。

2. 损害竞争。单纯的数据控制力强并不当然形成数据垄断。只有企业借助其强大的数据控制力干预、破坏正常的市场竞争时,《反垄断法》才有介入的空间。相关机构应当密切关注企业的市场行为,既要结合传统的反垄断框架还需要关注数据经济的特殊性。针对某一具体的行为应该建立完整的竞争损害证据链以证明数据垄断行为导致了价格上升、创新抑制等可以量化的损害,并对此加以处罚。

6 结语

在自动驾驶技术高速发展的时代,数据成为各企业竞争的关键非价格要素。这种对数据的狂热追求直接导致了个人信息面临前所未有的法律风险。车企与消费者签署用户协议授权收集个人信息,利用车内外传感器捕捉包括面部特征、家庭住址、驾驶习惯、家庭成员信息在内的个人信息。我们需要承认收集个人信息的必要性,但同时也应该规制过度收集的现象。在特定场景下《反垄断法》介入补充保护,可以规制市场主体行为,有效保证用户的个人信息安全。《民法典》《个人信息保护法》《反垄断法》三法协同保护个人信息也是时代发展的趋势。

本文通过对车企收集个人信息的现状、相关法律法规的保护、《反垄断法》协同保护的可行性等角度的分析,得出了如下结论:(1)利用《反垄断法》保护个人信息符合本法立法目的,且手段有效,具备可行性。

(2)过度收集个人信息并使用于商业竞争具备垄断的属性,应当扩展“滥用市场支配地位”中相关市场的内涵,扩大“滥用市场支配地位行为”的范围。(3)《反垄断法》的介入是有限的介入,只有当利用个人信息破坏市场竞争时,才有介入的合理性。因此,构建了“数据控制力评估+损害竞争”的分析框架,划清独占与垄断的界限。

参考文献

[1]杨叶:《自动驾驶汽车的数据安全保护研究》,厦门大学,2022年6月

[2]中国小康网:《特斯拉车内摄像头视频画面曝光 马斯克承认特斯拉用摄像头监控车主是怎么回事》, <https://baijiahao.baidu.com>

[3]汽车专业V:《有“内鬼”!特斯拉100GB数据泄露原因查明 影响超7.5万人》, <https://news.qq.com/rain/a/20230822A0201T00>

[4]叶名怡:《个人信息的侵权法保护》,《法学研究》2018年第4期

[5]丁晓东:《个人信息权利的反思与重塑:论个人信息保护的适用前提与法益基础》,《中外法学》2020年第2期

[6]高富平:《论个人信息保护的目的一以个人信息保护法法益区分为核心》,《商法研究》2019年第1期

[7]汪改丽:《论个人信息的反垄断法保护——以“滴滴案”为例》,《交大法学》2024年第2期

[8]Marija Stojanovic, Can Competition Law Protect Consumers in Cases of a Dominant Company Breach

Of Data Protection Rules? 16 European Competition Journal 531, 563 (2020)

[9]吴太轩、肖建华:《个人信息的反垄断法保护:理据证立、实践难题及破解方案》,《电子知识产权》2024年第8期

[10]王晓晔:《论反垄断法的“社会公共利益”》,《中国社会科学院报》2008年6月12日

[11]王晓晔:《我国反垄断法为什么保护竞争》,《法治研究》2024年第4期

[12]顾尧舜:《数据垄断场景下滥用市场支配地位认定标准的完善》,《天府新论》2024年第6期

[13]Ioannis Lianos, Competition Law for the Digital Era: A Complex Systems' Perspective, CLES Research Paper Series, 2019

[14]Vicente Bagnoli, "The Big Data Relevant Market," Concorrenza e Mercato, numero speciale: BIG DATA E CONCORRENZA, 2016

[15]梁铮:《论企业数据独占与共享的法律基础及均衡关系构建》,北京交通大学,2023年6月

[16]商希雪:《超越私权利属性性的个人信息共享——基于〈欧盟一般数据保护条例〉正当利益条款的分析》,《法商研究》Vol. 37, No. 2 (2020)