智能汽车个人数据保护
——欧盟与德国的探索及启示*

张韬略　蒋瑶瑶

摘　　要：智能汽车的运行依赖于大量数据的收集，这给个人数据保护带来一定风险。数据类型、数据主体和责任主体的复杂性也使智能汽车数据保护面临法律适用的独特难题。本文研究欧盟、德国智能汽车相关的个人数据保护立法成果和经验，并立足于我国立法现状，探讨欧洲经验对我国的借鉴意义。我国目前数据立法偏重数据安全，对个人数据保护重视不足，但后者乃智能汽车产业重要竞争力之一，必须重视。我国在强化数据安全的同时，应努力澄清个人数据保护的基础概念、原则和权责，厘清知情同意机制与数据处理的其他合法性基础的边界，平衡自动驾驶所涉的各方利益。

关 键 词：智能汽车；　德国；　欧盟；　自动驾驶；　隐私；　个人数据；　知情同意

作者简介：同济大学　法学院　副教授　上海　200092
同济大学　法学院　硕士研究生　上海　200092

中图分类号：D95；　D951.6
文献标识码：A
文 章 编 号：1005－4871(2019)04－0092－22

引　言

与隐私保护一样，个人信息和数据的保护从其诞生开始，就与技术发展有着密不可分的联系。最初被学者称为“独处权”的隐私权是为了回应即时摄影的出现和

* 本文是教育部人文社会科学研究规划基金项目（编号：14YJC820077）“中美信息技术产业专利危机及专利制度优化比较研究”、“同济大学欧洲研究双一流建设基金”和同济大学交通学院交叉学科培育项目“自动驾驶时代的道路交通法律问题研究”的研究成果之一。

当时媒体对个人私生活的介入和侵犯。[①] 计算机技术兴起所导致的广泛且简易的个人信息收集和处理则催生了“个人信息”的概念，隐私权也因之扩展为对个人信息的积极控制权利。[②] 而随着网络和自动化信息处理技术对大众日常生活的全面渗透，个人数据保护的理念也日渐被许多国家接受并上升为一项基本人权。1980年，经合组织（OECD）发布《关于隐私保护与个人数据跨境流动的指南》，提出隐私和个人数据保护的知情、接入、目的限制等重要原则，影响了经合组织成员国的立法和个人数据保护模式，[③]随后逐渐为许多非经合组织国家所接受。

智能汽车技术的快速发展对个人数据保护提出了新的挑战。智能汽车又名自动驾驶汽车、智能网联汽车，由于具备降低能耗、减少交通事故、提高道路交通容量和承载力等技术优势和极大的商业价值和市场前景，在近年成功吸引了巨资研发投入，受到众多国家产业政策的扶持。智能汽车的使用势必产生大量个人数据，这些数据在为企业带来巨大经济利益的同时，也引发了社会对隐私和个人数据保护问题的担忧。特别是智能汽车的数据处理、利用过程涉及主体繁多、数据种类复杂，而且事关交通安全，从而具有强烈的公共利益属性，这些都对通用的个人数据保护规则在该新兴领域的具体适用提出了新的挑战，使得智能汽车领域的个人数据保护问题具有单独讨论的价值和必要性。

下文首先分析智能汽车对个人数据保护提出哪些挑战，然后梳理德国和欧盟相关立法，归纳其如何基于现有法律制度回应上述挑战，最后分析我国立法现状和欧盟、德国经验对我国的借鉴价值。文章选取欧盟和德国为比较视角主要基于两点考虑。第一，它们有成熟的个人数据保护制度。欧盟通过《欧盟基本权利宪章》将个人数据保护列为基本人权之一，并借助最初的数据保护指令（《关于个人数据处理和自由流通中保护个人数据的指令（95/46/EC）》，下文简称“95指令”）和2018年开始适用的《通用数据保护条例》（GDPR），构建了一套较完善的个人数据保护规则体系，俨然是全球数据治理的引领者。第二，它们在近年开展智能汽车立法时，对数据保护问题有深入的探讨，其中不乏值得借鉴的经验。

一、智能汽车的个人数据保护问题

（一）持续、大量数据的处理带来个人数据保护的风险和隐患

① Samuel D. Warren/Louis D. Brandeis, “The Right to privacy”, *Harvard Law Review*, No. 5, 1890, pp. 193－220, here p. 195－196.

② 丁晓东：《个人信息私法保护的困境与出路》，载《法学研究》，2018年第6期，第194－206页，这里第197页。

③ OECD, *Thirty Years after the OECD Privacy Guidelines*, 2011, p. 11, http://www.oecd.org/sti/ieconomy/49710223.pdf, 访问日期：2019－08－27.

智能汽车的运行是一个持续的、伴随着大量数据收集和处理的过程。以导航系统为例，智能汽车在操控车辆之前，经过信息搜集、分析、决策等一系列过程，其中每一个步骤都需要与实时数据库进行数据交换。[①] 这一过程潜伏着个人数据保护的风险和隐患。一方面，持续和大量的数据处理使个人数据主体更容易被识别和追踪。如何在其中各个环节贯彻个人数据保护的基本原则，充分尊重并切实保护数据主体的权利，需要业界拿出一套合法合规且成本可行的方案。另一方面，持续的数据处理和交换加大了个人数据泄漏的风险。一旦某个环节被病毒攻击，就可能造成大量个人数据的泄漏，带来难以挽回的损害。这也对智能汽车的数据安全保护体系提出了更高的要求。

（二）数据的复杂性使得“个人数据”与“非个人数据”的界限变得模糊

适用个人数据保护法的前提是定义“个人数据”的范围。典型立法例在界定“个人数据”内涵时一般采用富有弹性的表述，例如GDPR第4条第1项规定，“个人数据”可关联到与“已识别或可识别的自然人”有关的任何数据，但具化到某一情景，哪些数据是可识别到个人的数据，仍有一定的模糊性。况且，原本难以识别到个人的数据或者已经匿名化处理的数据，随着新技术的出现和运用，往往会具备识别到个人的可能性。智能汽车领域就属于这样的情况。当智能汽车收集、处理的数据是直接涉及自然人的数据，例如位置、账号和身份数据时，这类数据的法律属性当然不存在争议。但如果是有关车辆控制和运行方面的数据，例如涉及行车路线、运行参数、维修信息、服务需求等等，其法律属性就有些模糊了。这对“个人数据”法律概念的具体适用至少提出了两层问题：第一，哪些车辆数据可以识别到具体的车辆？第二，如果可以识别到具体车辆，是否必然等同于识别到具体个人？例如，车辆设备状况数据、运行状况数据、存储在车辆内部的累计里程数是否属于个人数据，或在何种情况下属于个人数据。显然，只有先对智能汽车运行的过程中收集和处理的不同数据进行充分的甄别，才能够充分评估个人数据保护法可能适用的范围。

（三）个人数据主体的多样性为知情同意机制的实施带来挑战

根据通行的立法例，数据主体的知情同意是获得数据处理合法性的主要来源。数据控制者应履行充分告知的义务，数据主体也应作出自由、明确、清楚的同意，否则同意是无效的。这要求数据主体是明确的、可联络的，并且收集同意和数据处理之间应存在一定的时间间隔，以便数据主体在知晓数据处理的相关信息之后，再做出同意的意思表示。但在智能汽车领域恰恰存在操作的困难。智能汽车收集的数据可能涉

① Stefan Vacek/Tobias Gindele/J. Marius Zollner, “Using case-based reasoning for autonomous vehicle guidance”, in *2007 IEEE/RSJ International Conference on Intelligent Robots and Systems*, San Diego, CA, 29 October – 2 November 2007, pp. 4271 – 4276, here pp. 4271 – 4272.