DOI: 10.16538/j.cnki.jsufe.2021.05.010

比较法视角下的我国“车联网”数据治理路径选择

赵海乐

（吉林大学 法学院，吉林 长春 130012）

摘　要： 当前，我国“车联网”数据治理须顾及个人信息保护、数字市场发展、国家安全三方面利益，但现行法律并未界定“车联网”数据权属与个人信息保护方式，且拟设定的数据出境审查制度是否足以保护国家安全仍待探讨。欧盟对此的治理路径为：以保障终端设备通信自由扩大“车联网”信息保护范围；通过数据确权与欧盟境内数据自由流动促进欧洲数字市场发展；通过“国家安全例外”的设计保障欧盟成员国以国家安全为由进行数据治理的权力。与欧盟相对，美国将“车联网”数据治理交由车企进行行业自律，以自由竞争促进数字经济；通过限制“外国敌对者”获取美国敏感个人信息实现国家安全保障。对我国而言，有必要在对敏感信息进行最高标准保护的同时，对非敏感个人信息实现分层保护、共享利用；同时通过数据出境审查、外商投资负面清单、外资安全审查化解“车联网”数据跨境流动的国家安全风险，实现智能汽车产业发展、个人信息保护与国家安全的三方共赢。

关键词： 车联网；数据治理；个人信息保护；数字市场；国家安全

中图分类号： D996.4　　**文献标识码：** A　　**文章编号：** 1009-0150(2021)05-0139-14

一、引　言

当前，“车联网”已成为汽车产业与智慧城市建设的重要连结点，也成为数字经济的重要一环。车载终端设备将车辆与互联网相连，实现对车辆实时工作情况的采集、存储、发送，对车主驾驶偏好和操作安全进行实时记录，并对路况、交通情况进行拍摄与汇集。这一技术不仅能够为用户创造个性化体验、保证驾驶安全，其生成与汇总的大数据也能够有效服务于汽车生产商改进产品、防范城市拥堵等一系列商业与社会目标。

然而，正如任何新兴事物的产生均会映射法律规制的滞后，“车联网”的出现，同样引发了诸如个人隐私保护、非个人信息归属、数据安全与国家安全等一系列问题。2021年对此最突出的体现，就是特斯拉、滴滴出行、满帮集团先后引发的法律风波[①]。一方面，企业在“车联网”背

收稿日期： 2021-07-11

基金项目： 国家社会科学基金重大项目“中国参与制定国际劳工标准新规则研究”（19ZDA136）；吉林大学劳动关系专项研究课题“国际贸易规则重构对职工权益实现影响研究”（2021LD010）。

作者简介： 赵海乐（1985—），女，黑龙江七台河人，吉林大学法学院副教授。

①中共中央网络安全和信息化委员会办公室：《市场监管总局与中央网信办等五部门约谈特斯拉公司》，http://www.cac.gov.cn/2021-02/08/c_1614355732930891.htm，最后访问时间：2021年8月31日。中共中央网络安全和信息化委员会办公室：《网络安全审查办公室关于对“滴滴出行”启动网络安全审查的公告》，http://www.cac.gov.cn/2021-07/02/c_1626811521011934.htm，最后访问时间：2021年8月31日。中共中央网络安全和信息化委员会办公室：《网络安全审查办公室关于对“运满满”“货车帮”“BOSS直聘”启动网络安全审查的公告》，http://www.cac.gov.cn/2021-07/05/c_1627071328950274.htm，最后访问时间：2021年8月31日。

景下主张其数据权利，就不可避免地会与车主个人信息保护产生冲突。在特斯拉事件当中，车企曾数次拒绝向车主提供行车数据；其后虽同意提供但又将全部数据在互联网上公开[①]。这两种反应显然均非处理行车数据的科学方式。另一方面，即便“车联网”背景下产生的行车信息被匿名化而不属于个人信息，车企对数据的掌握、利用与跨境传输也完全可能产生对国家安全的侵害。“车联网”完全可能对重要军事设施进行高精度测绘，对于人流、车流的大数据记录也可能形成对关键基础设施的变相定位。掌握上述信息的不仅是传统车企，还可能是网约车平台企业和货运平台企业。滴滴出行与满帮集团网络安全审查事件就是又一例证。

“车联网”数据治理，同时反映了个人信息、数字经济与国家安全三者之间的关系之争，也进而提出了我国智能汽车产业发展亟需解决的一系列问题：“车联网”数据究竟归属于谁？如何在坚持个人信息保护的同时实现数字市场蓬勃有序的发展？企业对数据的支配权怎样行使，才不至于对国家安全产生负面影响？

对于上述问题，我国立法虽进行了一系列回应，但总体而言仍不足以提供完美的解决方案。首先，我国目前并没有对“车联网”数据进行确权，因而依靠明确的所有权规则消弭争议并不现实。根据《民法典》第111条，“自然人的个人信息受法律保护”。然而，“车联网”产生的数据是否属于个人信息尚有疑问。这主要是由于，《民法典》第1034条对个人信息的界定，是“能够单独或者与其他信息结合识别特定自然人的各种信息”。鉴于车主与驾驶人可能完全不一致，“车联网”究竟能否有效识别出特定自然人的身份尚有疑问。即便除去“车联网”产生信息的个人与非个人信息之争，仅仅将其作为“数据”加以看待，我国《民法典》同样未从物权或财产权角度对其权属进行规制，仅抽象性承认数据可能构成财产权客体：“法律对数据、网络虚拟财产的保护有规定的，依照其规定”。在数据确权规则仍然缺位的今天，“车联网”产生的数据势必无法进一步确权。[②]

其次，对于可能被认定为个人信息的“车联网”行车数据，我国法律同样欠缺对其的保护性规定。我国目前虽然具有对自然人隐私权保护的规定，但“车联网”数据并不总是与隐私相挂钩。2021年4月的特斯拉事件当中所涉的行车信息仅仅包括速度、刹车等技术性信息，这些并不与驾驶人“私密空间”“私密活动”相关，因而很难构成《民法典》第1032条第二款当中所界定的“隐私”。而对于不属于隐私的“个人信息”，理论上对此的处理和公开需经自然人同意（《民法典》第1035条），但此种“同意”很可能随车辆购买的隐私条款而被动授予。举例来讲，在特斯拉（中国）的官方隐私政策当中就明确提及，“我们可能会收集来自或关于您Tesla车辆的各种信息”，其中包括远程信息处理日志数据、远程分析数据、安全分析数据等；且，至少依据该隐私政策的表述，消费者无法自行在其车辆上拒绝对上述信息的收集。虽然消费者理论上可能通过联系特斯拉公司实现这一目标，但隐私政策当中同时表明，拒绝信息收集将导致无法获得软件和固件定期更新等一系列功能，甚至导致“车辆的功能降低、严重损坏或无法操作”。[③]与此类似，滴滴出行APP同样具有车内录音录像功能。录音功能的开启是使用滴滴服务的前提条件，且录音完成后将直接上传至平台云端。[④]此功能虽有助于维护乘客人身安全，但同样属于强制获取乘客同意。

①新华网：《“失控”的特斯拉！智能汽车的新维权之路该何去何从？》http://www.xinhuanet.com/fortune/2021-04/25/c_1127371141.htm，最后访问时间：2021年8月31日。

②南方都市报：《特斯拉公开事故前一分钟行车数据，是侵犯隐私还是行使权利？》，2021年4月23日，https://www.163.com/dy/article/G8A7P9PA05129QAF.html. 最后访问时间：2021年7月10日。

③ 特斯拉中国：《隐私》，https://www.tesla.cn/about/legal#choice-transparency，最后访问时间：2021年7月10日。

④ 滴滴：《个人信息保护及隐私政策》，https://www.didiglobal.com/law，最后访问时间：2021年8月1日。

最后，不论行车数据是否被匿名化、是否构成个人信息，企业对此的商业开发均可能引发国家安全之忧。此种国家安全威胁的产生，首先是由于数据完全可能主动或被动流转至境外。例如，根据特斯拉隐私政策，消费者使用其产品或服务即代表其同意将个人信息“转移至居住国以外的国家/地区，包括美国”[①]。滴滴出行引发国家安全审查，直接原因也在于其赴美上市完全可能因美国证券交易委员会要求披露某些数据。随后的“运满满”“货车帮”引发国家安全审查也是基于同一事由。而一旦数据被转移至境外，就可能被他国政府或组织利用。例如，车载设备可能完成高精度测绘；大数据分析可能揭示我国涉密单位、党政机关等重要敏感区域的人流车流数，甚至完成对我国关键基础设施位置与状况的推断。如果考虑到滴滴出行拥有海量乘客个人信息数据库、“运满满”“货车帮”与物流关键基础设施信息紧密相关，这些与行车数据结合会进一步加剧信息出境对我国国家安全的威胁。

对此，我国国家互联网信息办公室于2021年5月12日发布的《汽车数据安全管理若干规定（征求意见稿）》当中，特别提出了“重要数据”的概念并要求将此境内留存，否则运营者将负有通过国家网信部门组织的数据出境安全评估的义务。不过，这并不是我国首次提出“境内留存”与“数据出境安全评估”。早在2017年4月11日，国家互联网信息办公室颁布的《个人信息和重要数据出境安全评估办法（征求意见稿）》就曾提出重要数据出境的安全评估；但直至2021年《汽车数据安全管理若干规定（征求意见稿）》出台，对于何为重要数据仍未形成统一标准，且上述征求意见稿也尚未获得通过。而即便将上述未生效法律文件视为正式法律渊源，此处也仍然留有一个问题：境内留存是否能够完全纾解国家安全之忧？

以上三点分析共同意味着，个人信息保护、数字经济、国家安全三者的关系如何处理，是我国“车联网”数据治理亟需考量的内容。目前，对此的国内研究主要围绕大数据财产权、个人信息商业利用、机器生成数据权益归属等议题展开，[②]且对数据确权[③]问题关注较为集中；但专门针对“车联网”数据本身的研究数量较少，相对偏重对欧盟和欧洲国家立法的综述和对个人信息保护的论述。[④]对于如何实现“车联网”数据充分利用和防范国家安全风险则鲜有论及。相对而言，国外研究对“车联网”数据本身的关注更加集中，但研究基础是美欧既有法律实践，其国家利益立场天然有别于中国，[⑤]也无法为我国提供行之有效的法治建设方案。总之，国内研究

① 特斯拉中国：《隐私》，https://www.tesla.cn/about/legal#choice-transparency，最后访问时间：2021年7月10日。

② 参见：龙卫球：《再论企业数据保护的财产权化路径》，《东方法学》2018年第3期；汪晓华：《企业数据财产权与用户个人信息权益之冲突与协调》，《西南民族大学学报（人文社科版）》2020年第10期；邢会强：《大数据交易背景下个人信息财产权的分配与实现机制》，《法学评论》2019年第6期；李晓宇：《智能数字化下机器生成数据权益的法律属性》，《北方法学》2021年第2期；郭如愿：《大数据时代个人信息商业利用路径研究——基于个人信息财产权的理论检视》，《科技与法律》2020年第5期。

③ 对此的论述参见：何柯、陈悦之、陈家泽：《数据确权的理论逻辑与路径设计》，《财经科学》2021年第3期；许可：《数据权属：经济学与法学的双重视角》，《电子知识产权》2018年第11期；安柯颖：《个人数据安全的法律保护模式——从数据确权的视角切入》，《法学论坛》2021年第2期；程啸：《论大数据时代的个人数据权利》，《中国社会科学》2018年第3期；李爱君：《数据权利属性与法律特征》，《东方法学》2018年第3期。

④ 近五年来的典型研究成果包括：张韬略、蒋瑶瑶：《智能汽车个人数据保护——欧盟与德国的探索及启示》，《德国研究》2019年第4期；张韬略、蒋瑶瑶：《德国智能汽车立法及<道路交通法>修订之评介》，《德国研究》2017年第3期；邱遥堃：《行踪轨迹信息的法律保护意义》，《法律适用》2018年第7期；邓辉：《论我国智能驾驶汽车中的个人信息保护》，《电子科技大学学报（社科版）》2020年第1期。

⑤ Wolfgang Kerber，Data Governance in Connected Cars：The Problem of Access to In-Vehicle Data，9（2019）Journal of Intellectual Property，Information Technology and Electronic Commerce Law. Daniel J.Fagnant，Kara Kockelman，Preparing a nation for autonomous vehicles：opportunities，barriers and policy recommendations，77（2015）Transportation Research Part A：Policy and Practice. Kerber，Wolfgang and Frank，Jonas，Data Governance Regimes in the Digital Economy：The Example of Connected Cars（November 3，2017）. Available at SSRN：https://ssrn.com/abstract=3064794.最后访问日期：2021年8月1日。

仍需在一般性数据治理规则研究的基础之上，进一步聚焦“车联网”数据治理问题，加强对个人信息保护、数字经济、国家安全三方关系的讨论；国外研究从美欧立法实践出发，其研究相对深入但仍需结合我国国情进行扬弃。因此，本文的分析，将以本部分已进行回顾的、我国“车联网”数据治理法律缺陷为基础，通过对美欧相关实践与学术研究进行比较法研究，探寻人权、市场、安全三者的平衡之策。这将有利于实现智能汽车产业发展、个人信息保护与国家安全的三方共赢。“车联网”数据治理的有法可依，同样将有助于推进数字经济领域法治现代化进程。

二、欧盟进路：个人信息范围扩张与信息出境限制

对于“车联网”数据治理的比较法研究将从欧盟进路开始。这不仅仅是由于我国个人信息保护很大程度上与欧盟进路相似，也是由于，就“车联网”问题而言，欧盟已具有了专门的规则。欧盟同样会面临个人信息保护—数字经济—国家安全三重考量，而欧盟处理此问题的思路在于扩大个人信息保护范围、以数据确权推进数字经济，以限制数据跨境流动维护国家安全。

（一）“车联网”语境下的个人信息保护

对欧盟而言，“车联网”规制首先包括技术标准，如欧盟2019年第2019/2144号条例就是对于车联网技术的强制性规定，如应当遵循隐私保护原则，具有强制关闭智能速度服务功能，强制安装行车事件记录装置以存储匿名关键车辆信息等要求；[①]同时，也会包括对于车联网数据保护的专门规定。

欧盟对“车联网”信息的规制，首要特点在于将绝大多数“车联网”信息作为个人信息进行保护。例如，2020–2021年间，欧洲数据保护委员会（EDPB）就两次发布《车联网和移动设施个人信息处理指南》，[②]在序言中明确表示，车联网产生的大部分信息均可归为个人信息。某些信息尽管并不直接与姓名相连，但至少会与“驾驶人”或“乘客”相关，若进一步信息查询就可通过车架号获知车主的真实信息。[③]《通用数据保护条例》与欧盟2002年《电子隐私指令》均会对此适用。后者的适用，甚至并不以“车联网”信息能够联结至特定自然人为前提。任何能够与外界通讯的终端设备均有权获得隐私保护。[④]此处对“终端”的强调，是由于欧盟全部个人信息保护法律的合法性渊源均来自于《欧洲基本权利宪章》第7–第8条对于私人生活和通信自由的保护，而终端设备只要能够与外界保持通讯，则通讯内容必然属于“通信自由”所保护的范畴。[⑤]“车联网”信息也同样如此。

在确定了“车联网”信息除非匿名化则均应作为个人信息得到保护之后，对于“车联网”信

① Regulation（EU）2019/2144 of The European Parliament and of The Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers，and systems，components and separate technical units intended for such vehicles，as regards their general safety and the protection of vehicle occupants and vulnerable road users，amending Regulation（EU）2018/858 of the European Parliament and of the Council and repealing Regulations（EC）No 78/2009，（EC）No 79/2009 and（EC）No 661/2009 of the European Parliament and of the Council and Commission Regulations（EC）No 631/2009，（EU）No 406/2010，（EU）No 672/2010，（EU）No 1003/2010，（EU）No 1005/2010，（EU）No 1008/2010，（EU）No 1009/2010，（EU）No 19/2011，（EU）No 109/2011，（EU）No 458/2011，（EU）No 65/2012，（EU）No 130/2012，（EU）No 347/2012，（EU）No 351/2012，（EU）No 1230/2012 and（EU）2015/166.

② EDPB.（March 2021）. Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications，Version 2.0.（hereinafter referred to as “EDPB Guidelines 2.0”）.

③ I*bid*，paras.3.29.

④ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector（Directive on privacy and electronic communications）. 需说明的是，此《电子隐私指令》的升级版《电子隐私条例》目前尚未正式通过。本文因而援引《电子隐私指令》的最新版本——2009年版。

⑤ I*bid*，Recital，para. 24.

息的具体保护方式，首先要遵循《通用数据保护条例》对于个人信息保护的一般性规定：个人信息与终端信息的流通，如无遵从法律要求、履行合同所必需的法定理由，就必须获得信息主体的明示同意方可进行。此“同意”必须特定、清晰、合法。不仅如此，对信息的索取还必须符合数据最小化原则，即非必要不收集不处理。除此之外，欧盟车联网指南特别强调，三类个人信息应当进行额外保护，即位置信息、自然人生物识别信息以及能够反映驾驶人刑事犯罪或其他违法行为的信息。位置信息是由于其与自然人私生活（如兴趣爱好、工作与家庭地址、宗教信仰、性取向）紧密相关；生物识别信息是由于可以直接识别个人身份；而第三类信息则是由于，对刑事犯罪的起诉与惩罚直接涉及一国司法公正，此过程中的调查取证直接涉及犯罪嫌疑人的基本权利。因此，《通用数据保护条例》第10条专门对此进行了规定：对涉及犯罪与非法行为的个人信息处理应当在政府机关控制下进行，且应当保证信息主体的权利与自由不受侵犯。基于此，上述三类信息的处理应当在车内进行，尽量不将此数据传输至车外并避免上传至云端；对信息的处理必须在信息主体知情的情况下进行，汽车生产商还应采取积极措施避免此类信息的非法获取、修改或删除。[①]

（二）便利欧洲数字市场发展的非个人信息确权

以上分析固然体现了欧盟对个人信息保护的严格态度，但这并不意味着汽车生产商、销售商与保险公司等均无权获得“车联网”产生的各种信息。从理论上讲，任何个人信息均可经匿名化形成非个人信息。而在欧盟法项下，区别于个人信息保护的严格权利导向，非个人信息向来是以充分利用为立法准则。例如，与欧盟《通用数据保护条例》几乎同时生效的非个人信息规制条例，其全称为《欧盟非个人信息自由流动框架》（下文简称《框架》）。较之于前者名称当中的“保护”二字，后者名称当中的“自由流动”就已很大程度上表明了欧盟的态度。此《框架》序言第3段当中进一步表明，对于数据的本地化要求，是对欧盟“四大自由”当中的资本与服务自由流动的侵犯。[②]因此，《框架》核心立法目标在于，确保非个人信息在欧盟境内自由流动，禁止欧盟各成员国无故施加信息本地化要求。

此处需注意的是，欧盟对非个人信息自由流动的要求，仅为“欧盟境内”的自由流动而非真正意义上的“数据跨境流动”——全球自由传输。这是由于，欧盟的利益诉求一方面在于发展欧洲数字市场，但另一方面在于保证数字市场中的利益为欧洲企业而非美国互联网巨头享有。因此，欧盟在2017年欧洲数字经济动议[③]当中，尤其强调如下三方面内容：其一，欧盟数字市场的蓬勃发展需要减少数字本地化壁垒，加强数据流动。但此种流动仅限于欧盟境内流动。对于非个人信息传输至欧盟以外的国家，欧盟允许对此进行限制。其二，欧盟通过对于“机器生成数据”的保护以实现价值最大化为基本目标，且坚决反对数据生成者对此主张排他性财产权利。从知识产权角度来讲，欧盟并不承认匿名化机器生成数据具有任何知识产权属性，仅在数据库编纂者对数据获取、证实和内容编排具有实质性贡献的情况下方授予其特别权利。[④]而对于匿名化的机器生成数据，欧盟同样反对其构成《商业秘密保护指令》当中的商业秘密，原因在于

①郭晓燕、李拥军：《公众参与立法的功能异化与矫正路径》，《齐鲁学刊》2021年第2期。同时参见 EDPB Guidelines 2.0，paras.67-68。

② Regulation（EU）2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union（Text with EEA relevance）.

③ Communication From The Commission To The European Parliament，The Council，The European Economic And Social Committee And The Committee of The Regions，“Building A European Data Economy”，{SWD（2017）2 final}.

④ Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases OJ L 77，27.3.1996.

商业秘密的核心在于“保密”，而数据库显然需要访问以获利。[①]第三，欧盟建议通过设定数据生产者权利打击数据垄断。所谓“数据生产者权利”是指终端设备所有人或者长期使用人对非个人信息的权利。[②]数据生产者有权决定其数据如何使用，这将有效避免机器生成数据被大型企业提前“锁定”进而形成事实上的数据垄断。欧盟2018年《欧盟非个人信息自由流动框架》序言当中也曾论及，数字价值链需建立在各种数据活动基础之上，而数据处理的高效运作又是数字价值链的基石。数据持有者对数据的锁定将阻碍欧盟内部市场的发展。[③]

欧盟上述对非个人信息的法律与政策规定，虽未明确论及“车联网”，但其与“车联网”的关联在于，上述2017年欧洲数字经济动议的主要推进者包括德国政府与其境内大型车企。[④]这意味着，上述动议符合欧洲数字经济发展的需求，也同样符合欧洲车企的利益诉求。

（三）“车联网”数据治理与国家安全

或许是由于欧盟本身并不干预其成员国的国防与安全问题，欧盟对于“车联网”信息与国家安全关系的处理主要是通过对数据跨境流动的干预实现的：

其一，如果“车联网”信息被认定为个人信息，则此部分信息的跨境传输应当遵循与《通用数据保护条例》完全一致的跨境流动标准，即对方国家与欧盟之间已经达成了信息保护“充分性”审查共识，或者对方企业与欧盟企业之间存在标准合同条款和集团公司规则，否则，信息将原则上被禁止流入非欧盟国家。根据欧洲法院此前对“安全港”“隐私盾”两份协议的审查，美国政府个人信息保护的“充分性”认定两次被否决，均是因为美国政府为其国家安全目的对欧盟信息的监控不符合欧盟法的标准。而即便标准合同条款和集团公司规则仅仅是针对非欧盟企业个人信息保护的规则，其中也同样要求，在他国政府可能侵犯欧盟个人信息时，非欧盟企业有义务中止个人信息传输。

其二，即便“车联网”信息属于非个人信息，欧盟促进其境内数字经济发展的举措也未必会允许非个人信息自由流动。上文分析曾经提及，欧盟2018年《框架》原则上禁止对非个人信息的本地化要求。然而，此规则唯一的例外就是公共安全。该框架当中指出，此处的“公共安全”一词包括内部与外部安全，也包括为调查和惩处犯罪的公共安全目的而采取的措施。因此，欧盟成员国可以为了维护社会基本利益而要求数据本地化。对基本利益的威胁可以包括对公共设施运作的威胁、对人民生存的威胁、对国家外交与国家间和平相处的威胁以及对军事利益的威胁。不仅如此，为满足公共安全而施加的数据本地化要求必须符合比例原则，即便是出于公共安全目的限制数据自由流动，也应当手段与目标相适应，且不应超出实现该目标所必需的限度。[⑤]

此处需说明的是，此处的例外是“公共安全”例外而非“公共利益”例外。二者区别在于，环境保护、文化多样性、公共道德等均属于后者但不属于前者。如果将此例外的设计与GATT“一般例外”与“安全例外”相对比可知，上述公共安全例外的适用条件相当严苛。欧盟理论上并不干预其成员国对于何为“安全”的判断，但对“安全”的列举显然并不包括国家经济利益与社会

① Communication From The Commission To The European Parliament，The Council，The European Economic And Social Committee And The Committee of The Regions，“Building A European Data Economy”，{SWD（2017）2 final}，Part. 3.3.

② *ibid*，Part 3.5.

③ Regulation（EU）2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union（Text with EEA relevance）.Recital，para. 2.

④ Peter K. Yu，Data Producer's Right and the Protection of Machine-Generated Data. Tulane Law Review，93（2019）.

⑤ Regulation（EU）2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union（Text with EEA relevance）.Recital，paras.18-19，Article 4.

利益在内。不仅如此，欧洲法院理论上保有了对公共安全措施本身合法性的审查权，且有权宣告一项明显不适当的措施违法。因而这意味着，欧盟维护欧洲共同市场的决心是毋庸置疑的，其对于数字经济的开放态度仅限于欧洲市场。

综上，对欧盟而言，“车联网”数据治理共涉及三方利益：驾驶人、乘客或车主的个人信息保护，欧洲数字市场利益，国家安全利益。对于这三方面利益安排，欧盟的基本思路，是在坚持权利保护为导向的同时，推进欧盟内部的非个人信息自由流动，国家安全问题则是唯一的例外。但对于信息能否流转至欧盟境外，个人信息须受到《通用数据保护条例》项下的各项审查；而对于非个人信息的跨境流动，欧盟则并未给出任何承诺。

三、美国：行业自律与隐私保护并行的立法进路

与欧盟不同的是，对于美国“车联网”数据治理，很难从立法层面进行完整的回顾。这是因为，美国不论是数字经济领域还是个人信息保护领域，很大程度上均遵循着“行业自律”路径。因此，对“车联网”的美国规制进路的分析，将体现为各领域规则的汇总研究。

（一）美国“车联网”个人信息保护规则

与欧盟类似，在美国法项下，受到保护的“车联网”信息同样包括消费者信息与终端信息。这是因为，美国个人信息保护法律通常会将“个人信息”界定为“可直接或间接识别消费者或家庭”的信息。[①]因此，至少对于非营运车辆而言，“车联网”所产生的绝大多数非匿名信息均属于个人信息。不过，如果仅从个人信息保护范围角度分析，美国“车联网”语境下的个人信息保护范围明显小于欧盟。这是因为，美国并不存在联邦统一的个人信息保护立法，且目前仅有少数州具有个人信息保护立法。而即便是美国州法中影响力最大的《加利福尼亚州消费者隐私法（CCPA）》，其规制范围也仅限于超过一定规模的营利组织，且仅有收集加州居民信息的行为才会受到规制。因此，从联网车辆处获得信息的企业如不满足该法案对规模下限的要求，则完全不需受到个人信息保护法律的规制。这就将相当一部分汽车经销商、服务提供商排除在法律规制范围之外。而即便一个企业规模达到该法案要求，美国法意义上的个人信息处理前提——“告知同意”也并非欧盟式的“明示同意”，而是“默示同意、告知退出（opt-out）”。不仅如此，在《加利福尼亚州消费者隐私法》项下，消费者虽理论上有权起诉企业方并要求其承担对个人信息的侵权责任、加州总检察长也同样有此权力，但信息控制者仅需在30天内加以改正并保证未来不重犯，就很可能无需承担赔偿责任。

美国相当一部分“车联网”个人信息保护规则的义务方是美国政府而非车企或保险公司。例如，美国联邦《1994年驾驶人隐私保护法》原则上禁止政府机关公示机动车照片、车牌号、车主地址、电话、驾驶证号等信息，以防驾驶人被广告推销滋扰；《电子通讯隐私法》禁止第三方非法截获车载通讯工具的通讯信息；2015年《驾驶人隐私法》更是专门对行车事件记录进行了规制，其中将行车事件记录设备中存储的信息均认定为车辆所有人或者承租人的财产。任何第三人除非获得了司法或行政机关的明确授权，否则不得访问其中的信息。政府或行政机关对行车事件记录设备中信息的获取，必须符合相关证据法的要求。[②]除此之外，对于“车联网”生成的位置信息，美国早已通过判例明确认定，政府对此的长期监控构成美国宪法第四修正案当中的

① 典型立法为：The California Consumer Privacy Act of 2018，Section 1798.140. 此规定部分来源于美国宪法第四修正案对于“人民的人身、住宅、文件和财产不受无理搜查和扣押”的要求。

② Driver Privacy Act of 2015，Sec 2.

“搜查”，因而会违反宪法当中对隐私权保护的规定。[①]

除上述规定之外，美国再无对于“车联网”数据治理的法律规制。不过，或许是由于在此领域的消费者隐私保护问题会严重影响消费者使用“车联网”的意愿，美国汽车生产者联合会于2014年发布了《车辆技术与服务隐私原则》，并于2018年进行了修订。其参与方包括美国本田、阿斯顿马丁、宝马（北美）、法拉利（北美）、福特、通用汽车、现代汽车（美国）、起亚汽车（美国）等19家车企。参与该自律性倡议的企业一旦违反该原则，理论上将会受到美国联邦贸易委员会的处罚。[②]此隐私原则表面上与欧盟车联网指南大同小异，但在关键规则设计上均存在明显差异。此种差异体现在收集驾驶人信息的同意方式。此自律规则同样要求，对于地理位置信息、生物识别信息与驾驶人行为信息的收集须适用不同于“默示同意”的规则，但这仅仅包括车企须提供清晰、显著的通知，告知驾驶人信息收集的目的和未来可能分享信息的实体类别。车企仅仅在使用上述三类信息进行市场营销和与非关联第三方分享信息时才需获得驾驶人明示同意，且此种明示同意无需在每次驾驶之前单独给予，在车辆购买、租赁时概括性给予亦可。在特定情形下，该自律规则甚至仅要求车企获取驾驶人默示同意即可。这些情形包括车企保护其自身、车辆所有人、使用人或驾驶人的安全、财产或权利，车企进行并购或产品研发，车企为遵从政府法律或要求而采取某些行动，以及车企协助寻找被盗车辆时提供位置服务。“仅有少数州存在为企业设定义务的个人信息保护法律”[③]

综上，美国“车联网”个人信息保护立法更倾向于对政府行为而非企业行为的规制，仅有少数州存在为企业设定义务的个人信息保护法律，且不论是现行法律还是美国汽车产业自律性规范，均强调车辆所有人或驾驶人的默示同意与个别情况下的明示同意。其个人信息保护范围明显小于欧盟。

（二）美国相关法律对于数字市场的促进

上文分析表明，欧盟促进欧洲数字市场发展的主要手段，是促进非个人信息在欧盟境内自由流动，同时拟通过设定数据生产者权利打击美国互联网巨头对欧洲数据的“掠夺”。与欧盟相比，美国法律对数字市场的扶持明显更为激进。

一方面，美国对于数据自由流动的偏好，已不只是要求非个人信息在某一区域内自由流动，而是扩展至对个人信息与非个人信息全球自由流动的鼓吹。美国从未以维护境内数据市场为目标颁布过禁止本地化存储要求的法律。恰恰相反，美国在国际上向来主张应当废除数据跨境流动的任何壁垒，进而为美国互联网企业顺利进入全球市场创造有利的法律环境。这就意味着，在美国看来，“车联网”数据应当不受限制地流转至美国。

另一方面，美国个人信息保护规则与行业自律规范，均给予了车企更大的数据收集权力。此种权力源自于美国法与行业自律规范当中的个人信息收集“默示同意”规则。车企不需获得消费者明示同意即可获得其相当数量的个人信息，此信息无论随后是否匿名化均将处于车企控制之下。不仅如此，美国车联网自律规则在要求成员方应当对个人信息进行合理、负责任地

① United States v. JONES，Certiorari To The United States Court of Appeals For The District of Columbia Circuit No. 10–1259. Argued November 8，2011—Decided January 23，2012.

② 美国《联邦贸易委员会法》第5条规定，“不公平、具有欺骗性的行为”如果“影响了贸易”，则联邦贸易委员会有权对此进行处罚。此条款也是美国联邦贸易委员会处罚企业不遵循其隐私政策行为的主要法律渊源。参见：FTC，Privacy and Security Enforcement，https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement，最后访问日期：2021年7月11日。

③ Alliance Of Automobile Manufacturers，Inc. Association of Global Automakers，Inc. Consumer Privacy Protection Principles，Privacy Principles For Vehicle Technologies And Services. Established：November 12，2014，Reviewed：May 2018.

使用的同时，强调将信息用于研发是一种合理与负责任的使用方式。在要求车企遵循“数据最小化”要求和数据留存限制的同时，却将“数据最小化”要求界定为“仅为合法商业目的收集”，而非欧盟式的“非必要不收集”；数据留存限制也仅为“留存数据时间不长于合法商业目的所必须”。不论是美国现行立法还是上述自律规则，均未规定匿名化的个人信息的权属问题。美国法中亦不存在数据生产者权利这一概念。这就意味着，在法律无相反规定的情况下，实际掌控数据的车企，将毫无争议地享有对其掌控下数据的所有权。

（三）美国“车联网”数据治理与国家安全的协调

美国通过宣扬数据跨境自由流动，为其互联网企业进入国际市场创造有利条件。与此同时，美国又通过外资安全审查限制他国互联网企业进入美国市场、掌控美国数据，进而同时实现市场保护与国家安全两重目标。美国对国家安全的强调，关注的并非数据存储地，而是数据持有人的身份。最为典型的例子就是2020年特朗普政府对于Tik Tok与微信的经营禁令。[①]此禁令虽然在拜登政府上台后被撤销，但取而代之的2021年6月9日拜登政府新行政命令，在美国白宫网站的官方名称则是《保护美国人敏感信息免受外国敌对者侵犯的行政命令》。其内容同样是“进一步解决2019年行政命令当中所指称的、对美国信息和通讯产业供应链造成的国家安全威胁”，以及，防范外国敌对者持有美国人敏感信息对于美国关键基础设施的安全威胁。其中或许并未明确提及“车联网”字样，但鉴于“信息和通讯技术与服务”包含任何进行信息或数据存储、处理、交流的软硬件，联网车辆显然包含在该行政命令规制范围之内。该行政命令不仅要求在认定存在国家安全威胁的个案当中禁止并购交易，还要求尽快树立标准明晰的法律框架，以确保外国敌对者控制或管辖的人不会获得敏感个人信息。[②]这就意味着，该行政命令一旦正式应用于“车联网”领域，则中国“车联网”企业就可能无法从事在美业务。

四、“车联网”数据治理的关键问题

综合以上分析可知，美欧“车联网”数据治理的核心，均意在个人信息保护、数字市场与国家安全三者之间达成平衡，尽管其具体手段存在差异。美欧制度设计也将为我国未来的“车联网”数据治理提供重要启示。

首先，对美欧实践综合分析可知，虽然美欧国情不同，但“车联网”数据治理均面临完全相同的三重议题。此种状况的原因在于“数据”天然具有三重属性：对车主、乘客而言，数据意味着个人信息；对车企、车联网平台企业而言，数据是数字经济的“石油”，具有重要经济利益；对主权国家而言，“车联网”形成的数据则代表着对国家安全至关重要的情报。数据的三重属性并不因所处国家不同而有所差异，也正是这三重属性决定了“车联网”数据治理的多面性。因此，我国在设计“车联网”数据治理路径时，固然有必要考量我国国情与利益诉求与美欧的异同，但同时也不可忽视数据的任一方面特质，以保证“车联网”数据治理的利益均衡。

其次，个人信息保护制度如何设计，将直接影响数字市场发展与国家安全保护的实现。对于与个人权利关系最为密切的信息，如位置信息与行车事件记录，美欧均给予了最高标准保护，且法律渊源均可追溯至宪法性文件。欧盟相对严格的个人信息保护制度，本质在于对个人信息的确权，以及通过创设“数据生产者”概念，试图保护车辆所有人对信息的初始所有权。此

① Executive Order 13942 of August 6，2020. Addressing the Threat Posed by TikTok，and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain，https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/，最后访问日期：2021年7月11日。

② White House，Fact Sheet：Executive Order Protecting Americans’ Sensitive Data from Foreign Adversaries，June 09，2021.

种思路大体遵循了“财产规则”——预先界定数据权属，并在此基础之上由信息主体与车企协商确定数据后续权属。[①]其目的不仅在于避免信息被大型企业强行“锁定”，进而赋予欧洲数字市场以活力；“确权”与数据跨境流动限制相互配合，还能够有效防范数据被他国获得、进而危及欧盟成员国国家安全。相较于欧盟，由于美国互联网企业足够强大，因此美国“车联网”数据治理更加偏重于对政府权力的限制和对自由市场的放任。美国个人信息保护立法与行业自律性规则对个人信息保护要求更加宽松，这客观上允许美国互联网企业低成本获取“车联网”数据，进而促进美国数字经济发展。其国家安全目标更多通过外资审查完成。以上分析意味着，我国如何设计“车联网”个人信息保护规则，将不仅仅是一个民法问题，而且“牵一发而动全身”，对数字市场与国家安全均产生影响。数据确权有助于打破数据垄断、促进数字市场竞争；对车企获取个人信息的规范化，也有助于防范超范围收集数据，从源头减少数据外流带来的国家安全风险。

最后，数字市场的发展与国家安全保护并不矛盾，二者完全可以同时实现。问题的关键在于如何识别数字市场的驱动力与国家安全威胁的来源。在欧盟看来，促进欧洲数字市场发展的是数据跨境流动，但危及欧盟成员国国家安全的同样是数据跨境流动。正是基于此，欧盟促进欧洲数字市场发展的重要手段是保证个人信息与非个人信息在欧盟内部自由流动；而对于信息向欧盟境外自由流动，欧盟一方面在“充分性”审查当中防范他国的监听行为，另一方面明确为其成员国保留了基于国家安全原因限制数据跨境流动的权力。在美国看来，数据为“外国敌对者”持有而非数据自由流动才是对其国家安全的威胁。美国因而在鼓吹数据跨境自由流动以促进数字市场发展的同时，通过外资审查限制外国企业获取美国数据以保证其国家安全。以上分析表明，对我国而言，数据自由流动或许同样是数字市场的有效驱动力；但是，仍有必要思考的是，究竟什么才会构成对我国国家安全的威胁？对数据跨境流动的规制，能否有效消减国家安全威胁？除此之外，是否还有其他手段用以化解国家安全威胁？只有对此进行识别，方可精准定位我国未来法治设计的指向，以最小的成本保障国家安全。

五、我国“车联网”数据治理的三重进路

上文分析足以表明，数据作为信息、生产要素与情报的三重属性，分别对应“车联网”数据治理中个人信息保护、数字市场与国家安全的三重面向。因此，对我国“车联网”数据治理模式的设计，同样不能将民法、商法、国家安全法相互割裂，而是需要跨越部门法通盘考量制度设计，方可实现三方利益共赢。

（一）对敏感信息设置最高保护标准

首先，应当坚持对“车联网”数据的分层保护，且对于最为核心的敏感信息设定最高保护标准，如明示许可、数据最小化、存储本地化等。此部分敏感信息可包括足以识别自然人身份的信息（包括生物识别信息在内）、位置信息、行车事件记录信息。行车事件记录信息无论是否属于个人信息，均应考虑其可能涉及驾驶人行为的合法性评判，因而应当从犯罪嫌疑人正当权利保护角度严格规制，如类比或延伸适用我国《宪法》第40条对于通信自由的保障方式：除因国家安全或者追查刑事犯罪的需要，由公安机关或者检察机关按照法律规定的程序对行车事件

① 此处的“财产规则”并不等同于“承认个人信息属于财产权”，而是采用了卡拉布雷西在其法经济学经典论著《财产规则、责任规则与不可让渡性：“大教堂”的一幅景观》中的界定方式。所谓财产规则，是指由政府出面进行确权，权利拥有者可在获得令其满意对价的情况下放弃其权利。参见：Calabresi & A. Douglas Guido. Property Rules，Liability Rules，and Inalienability：One View of the Cathedral. 85 Harvard Law Review，1972，85(6)。

记录进行检查，或因当事人主动提出申请，则任何组织与个人不得对此进行公示。“以人民为中心”是依法治国的核心理念，因而对于人民基本权利的保护绝不可让位于数字市场利益。如有可能，还应扩展“车联网”数据的法律保护范围，在法律未明确将“车联网”数据定性为物权或财产权之前，将此部分信息作为类似于欧盟立法中的“终端信息”或美国立法中的“家庭信息”提供保护。

（二）实现非敏感信息的分层保护与利用

对于非敏感信息，我国应当采用与大数据商业价值、社会价值相平衡的个人信息保护方式。我国学者通常认为，单个数据价值密度低且难以量化，有时甚至毫无经济价值；[①]因此，考虑到数据在数字经济当中的基石性作用，应当充分发挥数据的公共属性，[②]促进个人信息的自由共享。[③]而实现数字经济与个人信息保护平衡的关键，则在于对数据的分层保护，[④]在应受不同程度保护的个人信息与可被信息产业不同程度利用的个人信息之间实现规范衔接。[⑤]事实上，这在《汽车数据安全管理若干规定（征求意见稿）》当中已有体现。其中第四条强调运营者处理个人信息目的应当合法、具体、明确，“与汽车的设计、制造、服务直接相关”。这也客观上表明，该征求意见稿默认了运营者出于商业目的收集、处理个人信息的合法性，且“个人信息”较之于“敏感个人信息”的获取与使用法律门槛更低。因此，如车企能够满足我国个人信息保护“知情同意、合法、正当、必要”的要求，则完全可以对“车联网”信息进行商业利用。除此之外，对于纯机器生成数据，我国目前尚不具备通过知识产权法或财产法进行确权的基础。欧盟式的个人信息确权，目前已经引发了“反公地危机”的担忧。[⑥]我国在《民法典》尚未做好对数据本身进行确权的准备的情况下，如果已经能够针对“车联网”生成的非匿名数据给予类似于个人信息的保护，则无需重复通过财产权方式为数据主体设定更多权利类型。

（三）对国家安全威胁的识别与分阶段化解

对我国国家安全的全方位保护，首先需要对我国国家安全威胁的种类加以识别。上文分析已经表明，“车联网”数据治理与国家安全产生的关联，是数据作为“情报”的属性。此处的“情报”，可能包括“车联网”生成的我国高精度测绘资料、保密部门或党政机关人流车流信息等，也可能包括上述信息与“车联网”所收集个人信息的叠加。而“情报”之所以会带来国家安全威胁，归根结底源自于“车联网”数据由企业主动或被动提交给外国政府、公共机构，如因跨国企业回传母国或中国企业海外上市而应要求提供信息，进而交由外国掌控或脱离我国掌控。此种威胁源于外国政府对情报的掌控，但完全可以始于外资企业对情报的掌控和对其母国属人管辖的遵守。目前来看，我国国家网信办涉入的全部“车联网”数据治理事件，所指向的“外国”均为美国，但未来同样不排除英国、欧盟涉入类似争端的可能。

以上分析意味着，“车联网”数据治理对我国国家安全的威胁共包含三个环节：作为情报的数据脱离车主掌控；此数据被外国企业或外资企业掌控；此数据最终被外国政府获得、利用。

其中，对于第一个环节，上文分析的数据分层保护，如能有效防范“车联网”超范围收集、保存信息，则已经从源头限制了可能危及国家安全的信息被车企乃至于他国政府所获得。而对于第三个环节，我国目前立法主要是从数据出境审查角度进行的。例如，《汽车数据安全管理若

① 任颖：《数据立法转向：从数据权利入法到数据法益保护》，《政治与法律》2020年第6期。

② 韩旭至：《数据确权的困境及破解之道》，《东方法学》2020年第1期。

③ 吴伟光：《大数据技术下个人数据信息私权保护论批判》，《政治与法律》2016年第7期。

④ 陈兵、顾丹丹：《数字经济下数据共享理路的反思与再造——以数据类型化考察为视角》，《上海财经大学学报》2020年第2期。

⑤ 郭如愿：《大数据时代个人信息商业利用路径研究——基于个人信息财产权的理论检视》，《科技与法律》2020年第5期。

⑥ 蒋林君：《欧盟数据生产者权及其对我国的启示》，《湖南科技大学学报（社会科学版）》2021年第2期。

干规定（征求意见稿）》中对于个人信息与重要数据出境设置了审查要求。《网络安全审查办法（修订草案征求意见稿）》第六条、第十条第五款，也要求对于采购活动、数据处理活动以及国外上市，进行“核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用或出境的风险的评估”。而且，掌握超过100万用户个人信息的运营者赴国外上市，必须通过网络安全审查。上述要求严格来讲不等于对数据跨境流动的全面禁止，且审查内容仅为国家安全审查，因而足以实现数字经济与国家安全的平衡。不过，考虑到数据跨境流动并不仅限于企业主动向境外提供或海外上市应要求提供，还可能包括应外国行政或司法机关要求被动提供，例如美国通过《云法案》谋求全球司法长臂管辖，我国仍有必要针对个案设立防范机制，如要求我国境内企业主动报告等，以及时发现并对抗可能出现的国家安全风险。

最后，对于上述第二个环节——数据为外国企业或外资企业所掌控，这虽仅仅为国家安全威胁产生的环节之一，且并不必然会带来国家安全威胁，但对此的规制同样不能放松。例如，在外商投资负面清单的制定过程当中，可以在某些可能涉及大量个人信息或敏感信息的行业对外资准入进行限制。这也是我国当前负面清单尚未纳入考量的内容。举例来讲，在我国2020年版外资准入负面清单当中，第七部分“信息传输、软件和信息技术服务业”就并无限制外资进入敏感信息产业或接触敏感信息的规定；第九部分“科学研究和技术服务业”虽原则性禁止外资进入测绘类产业，但对于特斯拉汽车足以完成的高精度测绘行为却完全没有进行限制。“车联网”相关产业理论上也并不属于负面清单的任何一类。此种状况在未来是否需进行改变，还有待我国商务部门与国家安全部门会商后决定。如不便改动负面清单，也可以启用我国目前业已确立的外资安全审查制度，对信息泄露风险进行国家安全评估。鉴于国家安全审查完全可以进行附条件许可，如允许外资企业进行并购或绿地投资的同时，要求其剥离某些“车联网”敏感业务或不得从事某些特定业务，外资安全审查并不必然会与投资自由相冲突。

六、结　语

“车联网”是物联网技术在交通系统当中的典型应用，其不仅代表着经济新动能，也同时意味着个人信息与国家安全的未知风险。“车联网”数据治理，同时代表着个人、经济、社会与国家利益的平衡，具有个人信息保护、数字市场与国家安全等三重面向。美欧相应规则构建起步相对较早，且均希望发挥“车联网”数字市场功能，但二者利益取向不同，具体路径也全然不同。欧盟从欧洲公民基本权利出发，意在限制美国互联网巨头轻易占领欧洲数字市场，以实现“人权”与“主权”双赢；美国更加偏重市场调节作用，同时通过外资审查排除外国投资者参与美国市场竞争。不过，在美欧博弈当中，美欧均注重对公民通信自由与终端信息的保护，且均提出了对“车联网”数据的分层保护标准。

对我国而言，“车联网”数据治理需要将数据作为整体，跨越部门法通盘考量来进行制度设计。对敏感信息的最高标准保护能够有效保障人民基本权利不受侵害，对非敏感个人信息的分层保护有利于数字经济发展，但须同时遵循个人信息保护的“知情同意、合法、必要”原则，以从源头避免情报外流。与此同时，数据出境审查、外国跨境电子取证的风险识别、外商投资负面清单的设计与外资安全审查对数据安全的关注，均有助于防控国家安全风险。

主要参考文献：

[1] 陈兵，顾丹丹. 数字经济下数据共享理路的反思与再造——以数据类型化考察为视角[J]. 上海财经大学学报，2020，(2).

[2] 郭如愿. 大数据时代个人信息商业利用路径研究——基于个人信息财产权的理论检视[J]. 科技与法律，

2020,(5).
[3] 韩旭至. 数据确权的困境及破解之道[J]. 东方法学,2020,(1).
[4] 蒋林君. 欧盟数据生产者权及其对我国的启示[J]. 湖南科技大学学报(社会科学版),2021,(2).
[5] 龙卫球. 再论企业数据保护的财产权化路径[J]. 东方法学,2018,(3).
[6] 任颖. 数据立法转向:从数据权利入法到数据法益保护[J]. 政治与法律,2020,(6).
[7] 吴伟光. 大数据技术下个人数据信息私权保护论批判[J]. 政治与法律,2016,(7).
[8] Calabresi G, Melamed A D. Property rules, liability rules and inalienability: One view of the cathedral[J]. Harvard Law Review, 1972, 85(6): 1089–1128.
[9] Yu P K. Data producer's right and the protection of machine-generated data[J]. Tulane Law Review, 2019, 93(4): 859–929.

Data Governance of Connected Vehicles from a Comparative Law Perspective

Zhao Haile
(*School of Law, Jilin University, Jilin Changchun* 130012, *China*)

Summary: Currently, China's data governance of connected vehicles needs to balance the interests among personal information protection, the development of digital market and national security. However, the existing law does not clarify the right of data generated by connected vehicles or the method of personal information protection. Moreover, the proposed cross-border data transfer review mechanism may not be sufficient to protect national security. EU, by means of active legislative and judicial approaches, takes the approach of enlarging the data protection scope of connected vehicles by safeguarding the right of communication of terminal equipment. By clarifying data rights and promoting the free movement of data within its border, EU removes barriers to the digital economy and blocks the monopoly of European market by US internet tycoons. These in turn promote the development of EU digital market. By means of public security exception, EU safeguards the right of its member States to regulate the digital industry through public security concerns. In contrast, the US largely confers the right to regulate connected vehicles to industrial self-discipline and promotes digital economy through a free market approach. The State Laws of the US offer a much narrower protection of personal information. The US also brings safeguards to its national security through restricting the right of "foreign adversaries" to access US sensitive personal information, since it has been reluctant to regulate the cross-border transfer of data. A study of EU and US approaches indicates that the data governance of connected vehicles needs to balance those three aspects because the concept of data has three attributes: personal data, productive factor as well as intelligence. The design of personal information protection would directly impact the development of data market as well as national security. The development of data market does not necessarily contradict with the protection of national security, and they can have a balanced development with scientific identification of the driving force of digital market and the origin of threat to national security. As to China, the three attributes of data correspond with the three aspects of connected vehicle data regulation.

Consequently, the institutional design needs to overcome the restriction of different departments of law and be integral. While it is advisable for China to invoke stringent protections of sensitive personal information, non-sensitive personal information should receive categorized protection and data sharing should also be facilitated. Meanwhile, cross-border data transfer review, negative list of foreign investment as well as foreign investment review may contribute to the elimination of national security risks incurred by the cross-border transfer of connected vehicle data. Only in this way can the industrial development of smart vehicles, personal information protection and national security be balanced and promoted.

Key words: connected vehicles; data governance; personal information protection; digital market; national security

（责任编辑：倪建文）

(上接第49页)

competition. The study finds that when the industry competition becomes more intense, the CEO-CFO social relationship has a stronger role in promoting the investment efficiency of enterprises. This article provides empirical evidence for how social relationships affect the information communication of the senior management team, and helps to understand the impact of the social network of the senior management team on corporate investment behavior. With the continuous improvement of China's institutional environment, financial work has played a key role in the continuous growth of enterprises. More and more CFOs are involved in major corporate decisions. Some listed companies even require the successor CEOs to have professional background of CFOs. Therefore, the research conclusions of this article are also helpful to understand the important role of CFOs in corporate investment decision-making and have certain enlightenment for enterprises to build a reasonable management team.

Key words: social relationships; information communication; financial background; investment efficiency

（责任编辑：倪建文）