Dispute Settlement 争议解决, 2021, 7(3), 98-104
Published Online September 2021 in Hans. http://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2021.73013

Hans汉斯

智能网联汽车数据跨境流动的法律规制

张韬略[1]，涂辉招[2]

[1]同济大学法学院，上海
[2]同济大学交通运输工程学院，上海
Email: ztl@tongji.edu.cn

收稿日期：2021年8月9日；录用日期：2021年9月7日；发布日期：2021年9月10日

摘　要

智能网联汽车在运行过程中会产生并处理类型各异的海量数据。智能网联汽车数据跨境流动不仅涉及国家安全、社会发展和产业战略，而且涉及企业知识产权保护和个人信息保护。我国在构建智能网联汽车数据出境的法律制度时，必须立足本国利益，紧跟国际潮流，在对智能网联汽车行业的数据特点尤其是数据分级分类进行充分论证的基础上，建构数据出境的安全审查规则和多元化的出境规制模式，努力兼顾多方法益的平衡。

关键词

智能网联汽车，数据跨境流动，数据出境，法律规制

Legal Regulation of Cross-Border Flow of Data of Intelligent Networked Vehicles

Taolue Zhang[1], Huizhao Tu[2]

[1]Law School, Tongji University, Shanghai
[2]College of Transportation Engineering, Tongji University, Shanghai
Email: ztl@tongji.edu.cn

Received: Aug. 9th, 2021; accepted: Sep. 7th, 2021; published: Sep. 10th, 2021

Abstract

Intelligent networked vehicles will generate and process massive data of various types during operation. The cross-border flow of these data not only involves national security, social development and industrial strategy, but also involves the protection of corporate intellectual property rights and personal information. When constructing a legal system for export of these data, China

文章引用: 张韬略, 涂辉招. 智能网联汽车数据跨境流动的法律规制[J]. 争议解决, 2021, 7(3): 98-104.
DOI: 10.12677/ds.2021.73013

must base on its own interests and keep up with the international trend. A data export system based on the data characteristics and data classification of intelligent networked vehicle industry, security review rules and diversified export regulatory models shall be established to strive for the balance of multiple players.

Keywords

Intelligent Networked Vehicles, Cross-Border Flow of Data, Data Exportation, Legal Regulation

1. 引言

智能网联汽车是车联网与智能车有机结合的新一代汽车，由搭载有先进的传感器、控制器、执行器等装置，融合了现代通信与网络技术，智能网联汽车能够实现车端与人、车、路的智能信息交换共享，实现安全、舒适、节能、高效的行驶，最终甚至可以替代人类驾驶员的操作。作为能够感知环境并做出合理行动决策的智能交通工具，智能网联汽车在运行过程中会产生并处理大量数据，并与其他终端进行数据交互。根据今年两会上全国人大代表、上汽集团董事长陈虹所透露的信息，一辆自动驾驶测试车辆每天产生的数据量最高可达 10 TB。海量数据的产生、采集、交互甚至跨境流动，在促进智能网联汽车技术和产业高速发展的同时，也带来了严峻的数据安全问题。2021 年 4 月 19 日的特拉斯维权事件，同年 6 月 30 日滴滴出行在美国悄然上市所引发的国家数据安全审查，都反映了规制智能网联汽车行业数据跨境流动的迫切性。

2. 数据跨境流动的利弊和规制模式

数据跨境流动是指数据从一个国家、地区和国际组织流动到另一个国家、地区和国际组织。根据数据流动的方向，数据跨境流动包括数据出境和入境，其中数据出境为法律规制的重点。数据跨境流动有其必然性。在国际贸易中，货物、服务、人员、资金的流动必然会伴随着数据的出入境。从国家层面来看，这类数据跨境流动有助于国家之间开展国际、区域的经贸合作，开展司法、执法合作，打击跨国犯罪活动。从企业层面来看，与经营相关的数据跨境流动可以积极降低企业的跨国经营成本，支撑企业的跨国经营，促进跨境交易，驱动互联网和数字经济的发展。

由于数据跨境流动具有上述优点，在数字经济兴起初期，尤其在倡导贸易自由的大环境之下，各国大多允许数据自由流动。但是，随着信息技术的高速发展和人类社会生活的数据化，各国逐渐认识到数据背后具有巨大的经济、政治和国家安全利益。数据一旦被肆意利用和滥用，很可能损害数据出口国的公共利益甚至国家安全。因此，在数据跨境流动尤其数据出境的问题上，各国逐渐形成了针对不同类型数据的跨境流动治理模式，其限制程度各异。

第一，针对影响国家安全的先进技术的数据，实施出口管制。掌控并输出先进技术有助于提升、巩固企业在国际市场的竞争地位，但在全球一体化背景下，也可能导致技术快速扩散从而影响到国家安全。因此技术发达国家往往会对部分先进技术实施出口管制，相应的，与这部分技术相关的数据也会受到出口管控。一些国家出于保护国家安全、联合国制裁等原因，对电信和信息安全类的技术以及相关数据进

行出口管制，就是典型例子。以美国为例，其《出口管制条例》按照技术类别、管控理由等因素，编制受管控技术的“出口管制分类编码”(ECCN)，然后结合技术数据出口的目的国、最终用户、最终用途等进行综合判断。受管控的技术范围包括基础技术例如计算机和软件技术，也包括新兴的技术例如人工智能、机器学习、网络监控技术等等，并由美国政府实时加以调控。

第二，针对战略性或有重要价值的数据，要求本地化存储。为了保障国家、地区或者行业的安全，有的国家要求具有战略意义的数据例如涉及政府、国防、能源等数据必须存储在本国，禁止出境。以美国为例，服务美国国防部门的云计算服务商必须遵守本地化存储要求，美国联邦税务信息也必须由在美国领土设置的信息系统加以存储、处理和传输。发展中国家例如印度尼西亚，同样要求网络运营商必须将其控制的能源、政府和国防等战略数据存储在本国[1]。可见，对战略性或有重要价值的数据采取保护主义，要求本地化存储，是发达国家和发展中国家的普遍性做法。

第三，针对个人数据跨境流动，采取多元的规制模式。前述两类数据的出境在各国都受到明显地限制，相比之下，各国对个人数据跨境流动的控制则松紧不一，体现了不同国家在各自经济、技术、法律制度差异之下的不同选择。在这些特征各异的立法模式之中，一端是以个人数据跨境流动自由为导向并辅以本地化例外的自由开放模式，另一端是以限制个人数据跨境流动为原则并辅以出境备案或审查制度的保护主义模式。但是，所谓的自由开放模式或者保护主义模式也仅仅是粗放式的概括，在相同模式之下，不同国家规制数据出境的具体做法仍有区别，背后体现了不同的文化背景和价值取向[2]。

以欧美的开放模式为例。美国作为一个具备高度发达的信息、数据处理和分析技术的科技强国，保障个人数据跨境流动自由显然能给其带来巨大的经济和战略利益，而且美国国内隐私保护分散立法的特点也决定了美国更倾向于将个人数据的流动交由行业、市场进行治理。因此，美国主导的国际贸易协定不仅强调数据自由流动，而且推崇市场、行业的商业价值。例如，早年在美国影响之下通过的两个法律文件——1980 年经合组织(OECD)发布的《隐私保护与个人数据跨境流动指南》以及 2004 年亚太经合组织(APEC)发布的亚太地区第一份关于跨境数据流动的区域性指导文件《APEC 隐私框架》，都积极倡导数据自由流动以及行业自律。2016 年正式签署的《跨太平洋伙伴关系协定》(TPP)明确其目标是“在保障个人信息保护等合法公共政策目标的前提下，促进全球数据自由流动”，并在电子商务领域，限制缔约国有关“数据本地化存储”的规定。随后，以 TPP 为蓝本的《全面与进步的跨太平洋伙伴关系协定》(CPTPP)以及《美国－墨西哥－加拿大》(USMCA)，也都包含了开放程度较高的跨境数据流动条款。例如，CPTPP 将“禁止数据本地化”设置为一般原则，但也允许各国出台国内法规以保护国家机密和通信安全。而 USMCA 更进一步，直接去除了将计算设施放置在一国境内或者使用一国境内计算设施的本地化要求。

相比之下，虽然欧盟主导或签订的贸易协定和区域性立法同样将促进数据跨境自由流动作为基本原则，但由于欧盟将个人隐私和数据保护确定为“基本人权”，对数据跨境流动提出更高的要求，所以欧盟立法具备了有别于美国的价值取向和制度特色。例如，欧盟与印度尼西亚等国磋商的自由贸易协定的数据流动条款同样禁止成员国通过设置数据本地化存储和处理等条件限制数据跨境流动。但 2018 年生效的《一般数据保护条例》(GDPR)在“致力于保障成员国之间个人数据的自由流动”(序言)的同时，非常强调个人数据跨境流动的数据输入国必须具备充分的保护水平。据此，欧盟先后废止了与美国签订的《安全港协议》以及《隐私盾协议》，因为自愿参与上述协议的美国企业无法遵守相关的数据保护义务。可见，欧盟相比美国，在个人数据出境方面提出了更高的要求，个人数据保护的充分性保障制度，构成了欧盟规制数据跨境流动的鲜明特色和重要因素。另外应该注意的是，虽然欧美模式大力倡导个人数据的跨境自由流动，但是它们依然允许一国依照公共政策采取某些限制措施和履行监管义务，这就为国际条约保留了相当的自由度或灵活度。

3. 我国数据出境法律制度的主要特色

意识到数据流动规制的重要性，我国近年也在积极推进相关立法。但不同于欧美的开放模式，我国立法对数据出境的态度十分谨慎。总的来说，具有如下特点：

第一，由国家法律、行政法规和国家标准三级规范组成的规则体系。位于最高层级的国家法律规定了数据出境应遵循的基本原则，例如《国家安全法》《网络安全法》《数据安全法》以及《个人信息保护法》。位于第二层级是配套的行政法规，例如国家互联网信息办公室(网信办)的《网络安全审查办法》《个人信息和重要数据出境安全评估办法(征求意见稿)》《关键信息基础设施安全保护条例》《个人信息出境安全评估办法(征求意见稿)》《汽车数据安全管理若干规定(试行)》等等。第三层级是细化的国家标准，例如全国信息安全标准化技术委员会(信安标委)针对信息安全技术所起草的《公共及商用服务系统个人信息保护指南》《数据出境安全评估指南(草案)》《个人信息安全规范》等等。目前，许多配套的部门规章和国家标准都尚未正式出台，公开渠道仅能看到“征求意见稿”建议的相关规则，但立法者释放出来的信号已经对市场起到了部分指引作用。

第二，以本地化存储为原则，必要的数据出境应进行安全评估。根据我国上述立法及草案，确保国家、网络和数据的主权和安全，保障我国公民的隐私、数据权利是数据出境的前提。我国《国家安全法》第 25 条规定，国家应该“实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控”，以维护国家网络空间主权、安全和发展利益。为了落实“数据的安全可控”，《网络安全法》第 37 条明确规定，关键信息基础设施的运营者有义务在境内存储运营中收集和产生的个人信息和重要数据，如果因业务需要，确需向境外提供的，应当进行安全评估。值得注意的是，网信办的《个人信息和重要数据出境安全评估办法(征求意见稿)》在构建数据出境安全评估制度时明确规定，“所有网络运营者”在境内收集和产生的个人信息和重要数据都应当在境内存储(第 2 条)，而且其他个人和组织的数据出境的安全评估工作，同样参照执行(第 16 条)。这意味着，本地化存储原则适用于各行各业的不同实体，不区分网络运营者或者非网络运营者，如果将我国境内收集和产生的个人信息和重要数据提供给境外机构、组织、个人的，都应当符合必要性原则，并且遵守法定的安全评估程序。正因为如此，国际社会有观点认为我国采用了数据保护主义的立法模式。

第三，积极借鉴域外立法经验，探索个人数据跨境流动的利益保护与平衡机制。受到欧盟 GDPR 等域外立法的影响，我国近期立法在数据出境方面加大了对个人信息保护的力度。例如，根据 2019 年公布的《个人信息和重要数据出境安全评估办法(征求意见稿)》，个人信息出境前，网络运营者应当向所在地省级网信部门申报个人信息出境安全评估(第 3 条)，网信部门在进行安全评估时应重点审查数据出境是否符合国家有关法律法规和政策规定，网络运营者获取个人信息的合法正当性、网络运营者与境外接收者对个人信息主体合法权益的保护能力、个人信息出境合同的可执行性等。也即如果网络运营者缺乏保护个人信息的能力，或者有保护不力的历史甚至数据泄露、数据滥用等事件时，网信部门可以停止网络运营者的数据出境行为，以维护个人数据主体的利益。此外，为促进数据流动，协调不同的利益诉求，我国近期立法也积极吸收了域外立法经验。例如，《个人信息保护法》第 38 条规定，个人信息处理者因业务等需要，确需向境外提供个人信息的，除了通过国家网信部门组织的安全评估之外，还可以采取类似 GDPR 的认证制度和标准合同制度，也即：1) 按照国家网信部门的规定经专业机构进行个人信息保护认证；2) 按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务。从政府部门的安全评估，专业机构的认证，到当事人之间的标准合同，这几项评估条件实际是由紧到松，在一定程度上与数据的重要程度相对应，也因此跟数据分类分级制度契合起来。例如，如果关键信息基础设施的运营者收集的个人数据构成了重要数据，则其跨境流动依法只能按照国家网信部门会同国务院有关部门

制定的办法进行安全评估。如果不涉及重要数据，那么就不排除其他能够保障个人信息保护水平的法律工具的适用，例如数据保护水平的认证、有约束力的公司规则以及标准合同等等。

第四，以数据分级分类为基础，但具体行业的数据分类出境规则尚不明朗。我国《网络安全法》规定，网络运营者必须采取数据分类、重要数据备份和加密等措施(第 21 条第 1 款)，并要求关键信息基础设施的运营者对“重要数据”和“个人信息”进行本地化存储(第 37 条)，但并没明确重要数据的概念。信安标委发布的国家标准《数据出境安全评估指南(草案)》(第二稿)进一步明确了重要数据和个人信息(包括个人敏感信息)的定义、范围和识别标准，并在指南附录“重要数据识别指南”中列举了石油天然气、石化、电力等 27 个行业的重要数据类型、范围，要求各行业主管部门明确本行业重要数据定义、范围或判定依据，根据行业发展变化，及时更新或替换指南中相关内容。刚刚通过的《数据安全法》第 21 条更明确地规定，国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。根据该条规定，除了个人信息和重要数据，还有“国家核心数据”，也即关系国家安全、国民经济命脉、重要民生、重大公共利益等数据。对国家核心数据，要实行更加严格的管理制度。对重要数据，各地区、各部门还应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。可见，目前我国法律至少明确了国家核心数据、重要数据、个人数据(包含个人敏感数据)三类数据，并且要求国家、行业和经营者根据数据对国家安全、经济社会发展和个人权益的重要性，实施数据的分级分类管理。但是，诸如智能网联汽车等行业的数据分级分类办法以及出境管制规则仍在酝酿起草或者评审阶段，相关规则并不清晰。

4. 智能网联汽车数据的分类分级

数据的分类分级保护必须结合具体行业的数据来源、数据处理方式及其法律内涵进行分析，否则可能失去实际意义。在这方面，汽车行业、理论界和立法机构已经进行了一些有益的探索。

从数据来源的角度来看，智能网联汽车的数据可以分为用户数据、车辆技术数据和交通环境数据。用户数据指用户在使用智能网联汽车时产生的具有个体倾向性的数据，例如用户的通讯簿、导航目的地等数据。借助这些数据，汽车制造商可以完善用户体验或开展有针对性的市场营销。车辆技术数据是由汽车传感器产生并用于控制汽车决策和运动的数据。掌握这些技术数据，汽车开发商可以优化智能网联汽车的技术，提升汽车的安全性、鲁棒性等功能。交通环境数据则是指来自汽车外部的交通、地理和气候等交通环境数据。这类数据有助于智能网联汽车更灵敏、快捷和安全地融合到周围的交通环境之中。

德国汽车工业协会(VDA)则从智能网联汽车数据的生成、收集的角度，将智能网联汽车数据分为六个种类。第一类是因法律规定而收集的数据，例如在发生严重交通事故时根据欧盟《电子呼叫法案》需要向当地应急机构传输的安全气囊数据和位置数据；第二类是因合同约定而发生的服务数据，例如汽车的远程诊断服务、远程定位等数据；第三类是用户自己的数据或由用户生成的数据，例如司机最舒适的座椅位置、音箱音量、导航目的地、通讯簿数据；第四类是车辆中生成的并展示给司机的数据，例如剩余燃油数据、油耗数据等；第五类是车辆中生成的总量数据，例如平均油耗数据、平均速度数据；第六类是车辆中生成的技术数据，例如引擎等各种汽车组件的运行数据。VDA 这种分类有助于判断汽车数据与个人数据的关联性以及开展相关数据处理的法律根据。例如，前三类与个人数据的关联度较强，而后三类数据通常只涉及一些短暂存储并最终服务于车辆运行的技术数据，与个人数据相关性很小，数据控制者在车辆和产品安全方面可能具有需要优先考虑的合法利益[3]。

从数据背后的法益来看，可以将智能网联汽车相关的数据区分为企业数据、个人数据和对国家具有重要意义的数据。企业数据主要指智能网联汽车运营者在车辆设计、测试、运营等过程中合法掌握的车

辆技术数据、个人数据和交通数据等。根据企业数据的实际状态，运营者可以通过商业秘密、数据库版权等方式对这些数据加以保护。例如，在采取保密措施并符合技术秘密保护条件下，企业数据可以享有《反不正当竞争法》有关商业秘密的保护。个人数据是指包括车主、驾驶人、乘车人、行人等个人信息，以及能够推断个人身份、描述个人行为等各种信息的数据。这类数据的泄露，会危及个人信息利益和隐私利益。而重要数据是指智能网联汽车收集、处理的可能影响国家安全、公共利益的数据。根据《汽车数据安全管理若干规定》第 3 条第 6 款，汽车行业的重要数据包括下述六类可能影响国家安全、公共利益或个人、组织合法权益的数据：1) 军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等数据；2) 车辆流量、物流等反映经济运行情况的数据；3) 汽车充电网的运行数据；4) 包含人脸信息、车牌信息等的车外视频、图像数据；5) 涉及个人信息主体超过 10 万人的个人信息；6) 其他可能危害国家安全、公共利益或者个人、组织合法权益的数据。值得注意的是，企业数据、个人数据和对国家具有重要意义的数据并非是相互排斥的，三者之间可以有交集。例如，根据《汽车数据安全管理若干规定(试行)》，重要数据的类型之一“人脸、车牌等的车外音视频数据”就包含了可以识别自然人的个人数据。同理，企业数据之中也完全可能包含有个人信息和重要数据。

5. 我国智能网联汽车数据出境制度的建构

智能网联汽车数据的多样化，意味着其出境问题不仅涉及国家安全、社会经济发展和产业战略，而且涉及企业知识产权保护以及个人信息保护，因此，我国在构建智能网联汽车数据出境的法律制度时，必须立足本国利益，紧跟国际潮流，对智能网联汽车数据的分级可从数据的三大属性，即保密性、完整性、可用性遭泄露或破坏后，造成的潜在影响后果来分级。基于定性和定量相结合的方法，判断数据遭泄露后对国家、公民、法人实体和其他组织可能造成的危害，乃至对国家安全、社会秩序、人民财产和公共利益等造成的最大后果影响来进行分级。在对智能网联汽车数据分级分类的基础上，建构数据出境的治理方案，努力兼顾多方法益的平衡。

首先，在数据出境的自由度方面，尽管西方欧美国家倡导的数据跨境规制模式以促进数据自由流动为基本原则，但我们应当看到，它们同样不排除针对不同类别的数据，采取各种限制程度的数据跨境流动管理措施，例如本地化副本保留、有条件出境、本地化存储和处理等等。也即，从世界范围来看，数据出境的法律规制模式是多元化的。因此，我国在设计数据出境的法律方案时，应当以本国的国家主权、网络数据安全、产业发展以及本国国民的个人信息保护利益为重，无需担心所谓的“数据保护主义”的指责[4]。

其次，若要在确保国家安全、网络和数据安全的同时，促进数据的流动以实现各方利益的平衡，关键在于建立合法、合理、动态的智能网联汽车行业的数据分类分级治理制度。该制度应该针对不同的数据类型，在国家、行业和经营者三个层面，从数据收集、处理到出境各个环节，实现有差别的管控。国家层面主要提供法律制度的供给，也即通过立法、司法和执法活动，实现对市场主体的指引。目前，从《网络安全法》《数据安全法》和《个人信息保护法》来看，目前我国立法基本明确了国家核心数据、重要数据、个人数据(包含个人敏感数据)三类数据，并且要求国家、行业和经营者根据数据对国家安全、经济社会发展和个人权益的重要性，实施数据的分级分类管理。而配套的法规和标准草案尤其是《汽车数据安全管理若干规定(试行)》又进一步明确了其中“重要数据”的定义和主要类型。但是，在目前三个位阶的法律规范之中，许多规范数据出境的法规规章和标准也都没有生效，相互之间可能存在契合的问题。例如，《数据安全法》提出了全新的概念“国家核心数据”，并要求进行更加严格的管理。但此前配套网络安全法的所有涉及数据出境的规章和标准，都仅以重要数据和个人信息两类数据来构建数据出境的安全审查制度，并没有涉及“国家核心数据”。而汽车行业的重要数据和个人数据的安全审查以及

其他出境途径的具体差异点，仍有待行业指南的细化。因此，我国必须加快立法，并且协调好不同的法律、行政法规和标准之间的关系，给市场提供更加明确的指引。

再次，鉴于智能网联汽车数据的复杂性，在个案之中，判断智能网联汽车数据的法律类型及其级别，尤其是相关数据对国家安全、社会发展和个人权益的重要性，必然是一个动态的过程。这就需要我们构建一个弹性的、动态的数据出境安全审查机制。该审查机制在贯彻汽车数据本地化存储以及出境安全审查机制时，应当充分考虑我国参与的或者与其他国家和地区、国际组织缔结的条约、协议有关数据出境的规定，应当充分考虑到数据处理活动的持续性，以及技术因素对数据重要性的影响。因此，相关法律法规或者标准在明确运营者的范围及其保障数据安全的义务和责任时，应当建立动态的审查机制。例如，出台具有前瞻性的行业重要数据指南并根据现实情况做不定期的更新和调整，不定期抽查运营者向境外提供个人信息或重要数据的类型、范围，持续监督境外接收者按照约定的目的、范围、方式使用数据的情况等等。

第四，从智能网联汽车运营者的角度来看，为了提高跨国经营的效力，降低相关的法律风险，必须在智能网联汽车的设计、生产、销售、运营、管理各个环节都确保数据合规，从而为数据出境的必要性审查和安全评估打下制度层面的合法基础。具体而言，企业应当在管理制度上落实网络安全等级和数据分级分类保护制度，并将其贯彻到数据处理(收集、分析、存储、传输、查询、利用、删除以及向境外提供)的各个阶段。以个人数据为例，智能网联汽车运营者在处理(包括出境)个人信息或重要数据时，应当确保目的合法、具体、明确，应与汽车的设计、制造、服务直接相关；在最初收集个人信息时，就应当取得被收集人同意，或者在难以获取同意的情况下进行匿名化或脱敏处理；在处理数据时，必须遵循车内处理原则、匿名化处理原则、最小保存期限原则、精度范围适用原则、默认不收集原则、数据本地化存储原则等等。

基金项目

本文获得上海市科委重点计划课题“智能驾驶治理原则及机制研究”(项目编号：20511101703)以及科技部重点专项项目子课题“自动驾驶电动汽车应用关键技术及法律社会问题研究”(项目编号：2018YFB0105202-05)资助。

参考文献

[1] 张衡. 跨境数据流动的国际形势和中国路径[J]. 信息安全与通信保密, 2018(12): 21-26.

[2] 何渊. 数据法学[M]. 北京: 北京大学出版社, 2020: 171-189.

[3] 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[J]. 德国研究, 2019, 34(4): 92-113.

[4] 高富平. 关于中国数据出境管制政策的建议[EB/OL]. 澎湃新闻. https://www.thepaper.cn/newsDetail_forward_2458980, 2018-09-20.