新时代我国的数据安全风险及治理方案探析

王　林
(西北政法大学 反恐怖主义法学院(国家安全学院),陕西 西安 710063)

摘　要:为了有效维护数据安全,特别是跨境流动数据的安全,平衡数据安全与发展,有必要探索新时代数据安全治理的中国方案。我国数据安全中存在数据泄露、数据主权侵害和数据霸权等风险点。为了维护我国的数据安全、促进数字经济发展,有必要将治理理念引入数据安全,构建数据安全治理共同体;将数据安全纳入总体国家安全,坚持系统思维,协调好数据安全与其他领域安全的关系;完善数据安全治理法律法规体系,加强数据安全治理顶层设计,完善数据安全标准体系建设;构建数据安全治理国际话语权,积极参与数据安全相关国际规则的制定,反击外国数据霸权;与时俱进、创新数据安全治理措施,引入数据信托和数据合规制度。

关键词:数据安全;国家安全;治理共同体;数据发展;数据信托;数据合规

中图分类号:TP309.2;D820　　**文献标识码**:A　　**文章编号**:1008-7699(2022)03-0026-07

一、我国面临的数据安全风险

2021 年 7 月 2 日,国家互联网信息办公室发布公告,对“滴滴出行”实施网络安全审查。而国家互联网信息办公室发布公告的背景是,2021 年 6 月 30 日,互联网平台公司“滴滴出行”在美国纽约证券交易所上市。在大数据技术被广泛应用的情况下,作为一个掌握海量个人数据和公共数据的企业,虽然目前官方还没有发布针对“滴滴出行”的详细调查报告,但是从 2021 年 7 月 2 日国家互联网信息办公室发布的简短公告来看,“滴滴出行”被网络安全审查主要是与数据安全有关,特别是与数据的跨境流动安全有关。对“滴滴出行”等企业实施的网络安全审查的实质是对数据安全的审查,网络只不过是数据的一种载体,网络数据是数据在网络时代的一种表现形式。因此,对“滴滴出行”等企业的数据安全审查具有转折性的标志意义,标志着我国政府在维护总体国家安全的大背景下,越来越关注数据伦理、数据安全和数据流动问题。[1]数据安全不但是一种状态,即确保数据处于有效保护和合法利用的状态;数据安全还是一种能力,即保障持续安全状态的能力。数据安全治理的方案探索成为理论和实务界共同关注的课题。

与美国等西方发达国家相比,我国无论在数字技术发展、数据挖掘还是数字经济发展等方面,都还有进步的空间,而且我国的数据安全风险也在近年来才开始显现。我国数据安全的风险主要体现在以下方面。

第一,数据泄露。一方面,数据泄露会损害数据企业的声誉,使用户丧失对其的信任感;另一方面,数据泄露也会侵害用户的合法权益,特别是侵害用户的个人信息权和隐私权,而个人信息权和隐私权在数字化时代是每个公民最基本的权利。根据泄露数据的危险源不同,可以将数据泄露威胁分为内部威胁和外部威胁。内部威胁的危险源是企业、单位的内部人员,外部威胁的危险源是企业、单位的外部人员。

第二,数据主权侵害。由于数据的流动性,传统的国家疆界被打破,同时国家主权的内涵也发生了变化。因此,不但要关注传统的、有形的主权安全,也要关注非传统的、无形的数据主权的安全,采取措施保障数据主权安全。随着各领域全球化的推进和全球数字经济的发展,数据全球范围内的跨境流动不可避

收稿日期:2021-10-19
基金项目:中国法学会部级法学研究课题(GLS(2020)ZZ003)
作者简介:王　林(1980—),男,河南正阳人,西北政法大学反恐怖主义法学院(国家安全学院)讲师,法学博士.

免。由于数据特别是国家关键数据是稀缺资源，各个国家对数据的争夺也进入了白热化。如果我国享有所有权的数据被他国占有，这是对数据主权的侵害，也是对国家主权的侵害。我国政府对“滴滴出行”实施网络安全审查，也是出于避免关键基础数据被外国非法占有的考虑，积极维护我国的数据安全和国家安全。

第三，数据霸权。数据霸权是霸权主义在数据领域的集中体现，美国凭借其在数据技术、综合国力等方面的优势，一方面控制数据安全标准的制定权，另一方面强制他国企业转移数据。例如，美国要求台积电等半导体企业在 45 天内，交出公司相关数据，包括库存、销售及客户等商业机密。[2]

可见，我国所面临的数据安全风险是非常现实和紧迫的。出于应对数据安全风险的考虑，我国的立法机关出台了《数据安全法》，使维护数据安全的实践有了基本的法律依据。总体来说，我国探索数据安全治理的实践和理论都刚刚起步，不但要借鉴他国、其他地区的优秀经验，也要创造出适合中国国情的模式，走出一条有中国特色的数据安全治理道路。

二、数据安全治理的中国方案

（一）将治理理念引入数据安全

与管制、管理的概念不同，治理是目前全球都在研究和实践的治国理政方式。无论是国家治理，还是社会治理，治理体系和治理能力的现代化都是治理追求的目标。作为国家安全治理重要部分的数据安全治理，同样要追求治理体系和治理能力的现代化，要改变“自上而下”的单向的政府对数据安全的监管，变成既有“自上而下”的监管也有“自下而上”的数据安全治理共同体的构建这种双向流动的局面。《数据安全法》中“建立健全数据安全治理体系”的表述就是在法律上对数据安全治理理念的确认，在数据安全中引入治理理念主要有以下呈现。

1.构建数据安全治理共同体

构建治理共同体是治理与管理的最大区别之一，治理共同体的构建也反映出治理模式强大的吸纳力，构建治理共同体可以将各种力量聚合起来，最大程度减少对抗和内耗。数据安全治理共同体包括但是不限于数据权利人、数据控制人、数据处理人、数据受益人、数据监督人等，他们是治理共同体，也是利益共同体，他们各司其职、协调配合。构建数据安全治理共同体要突破传统的治理共同体外延，传统的治理共同体只是包括国内主体，但是考虑到数据的特点，特别是数据的跨境流动性，因此一国的数据安全离不开其他国家和组织的配合，一国的数据安全也是经过包括其他国家、组织主体等要素博弈后均衡发展的结果，全球范围内的数据安全也是各国博弈的结果。拜登政府在 2021 年 6 月 15 日发布的《打击国内恐怖主义国家战略》中也提到要构建反恐社区，这里的反恐社区其实就是反恐治理共同体。这个反恐治理共同体不但包括联邦政府、地方政府、部落、社区、公民社会、企业、研究机构等，还包括国际组织和美国的盟友。美国对反恐治理共同体外延的界定，可以给我国的数据安全治理共同体的构建提供一定的借鉴。《数据安全法》对数据安全治理共同体作出了规定，而且 2020 年 9 月 8 日，我国政府在“全球数字治理研讨会”上提出了《全球数据安全倡议》。倡议提出，“我们欢迎政府、国际组织、信息技术企业、技术社群、民间机构和公民个人等各主体秉持共商共建共享理念，齐心协力促进数据安全”。

2.均衡数据安全和数据发展

有学者将数据主权、数据保护和数据流动称为数据跨境流动中的“三难问题”。[3]在数据跨境流动中，其核心就是在保护数据安全、维护数据主权的前提下，保障数据正常的跨境流动，充分挖掘数据的经济效益。没有数据流动，发展数字经济就成为无本之木、无源之水。均衡数据安全和数据发展是治理思想中均衡发展的要求，也是综合施策、标本兼治的要求，是两点论而不是一点论，是用联系的视角而不是孤立的视角看待问题。均衡数据安全与数据发展，也是安全与发展这对矛盾在数据安全治理中的具体体现，安全是发展的保障，而发展可以促进安全，将安全提升到一个更高的层次。

(二)数据安全纳入总体国家安全

总体国家安全观理论的提出在我国新时代国家安全思想的发展历程中具有划时代的意义,总体国家安全观是习近平新时代国家安全思想的理论骨架。在我国从“站起来”到“富起来”再到“强起来”的过程中,在不同的阶段,面临的国家安全形势是不同的,对安全的认识和把握也是不同的,对安全和发展的侧重也不同。第一阶段:从新中国建立到改革开放。新中国成立后,我国面临严峻的国家安全形势。在外部被西方国家敌视和孤立,新生的人民政权还不稳定;在内部也面临国民党旧政权残余势力、特务、土匪等各种敌对势力的破坏,社会不稳定因素交叉、交织。虽然当时新生的人民政权也重视经济的发展、民生的改善,通过制定“五年计划”的方式发展国民经济,但是与经济发展相比,安全占据更重要的地位,而且后期由于“以阶级斗争为纲”政策的提出,国民经济发展遭受巨大破坏。第二阶段:从改革开放到十八大。改革开放的总设计师邓小平同志认识到当时世界发展的主流是和平与发展,将改革开放设定为基本国策,坚持以经济建设为中心,通过发展经济,提升综合国力,强化保障自身安全的能力,使中国成为维护世界和平的重要力量。在这个阶段,发展与安全的天平更多是向发展倾斜,更加注重发展对安全的推动作用和发展的基础作用。第三阶段:十八大以来的新时代。经过改革开放 30 多年的发展,我国的经济实力和综合国力都得到巨大提升,但是发展的红利却不能完全弥补安全的赤字。我国面临的安全问题日益凸显,传统安全的威胁一直存在,同时恐怖主义、生态危机等非传统安全问题也开始出现,严峻的安全形势会侵蚀来之不易的发展成果,发展需要安全环境的保障。新时代的国家安全思想要求统筹发展与安全,二者缺一不可,发展是安全的基础,安全是发展的条件。总体国家安全观既是世界观也是方法论,其核心内涵是“五大要素”和“五对关系”,将整体思维、综合思维和系统思维注入维护国家安全的体制和机制。总体国家安全观的提出在我国维护国家安全的历史上具有划时代的意义,总体国家安全观是我国维护国家安全实践的最根本指导思想。把握总体国家安全观的前提是深刻认识总体国家安全观提出的背景,对我国国家安全的内涵和外延、时空领域、内外因素要结合国家安全的实际情况进行整体思考。

《数据安全法》明确规定,“维护数据安全,应当坚持总体国家安全观”。将数据安全纳入总体国家安全也是系统思维的要求,系统思维要求构建大安全格局,而数据安全正是大安全格局的重要一环。在网络时代,数据和网络紧密结合,数据安全和网络安全紧密相连;在信息时代,个人信息也是个人数据的重要组成部分,很难将数据安全、网络安全和信息安全完全分割开来。总体国家安全也是一个开放、动态的体系,又衍生出海外利益安全以及太空、深海、极地、生物等不断拓展的新型领域安全。虽然上述所列举的安全领域并没有数据安全,但是总体国家安全观通过“等”字的立法模式,将数据安全这种在性质上相近的国家安全领域囊括进去。

维护数据安全,应当坚持总体国家安全观。一方面,要把握好数据安全与其他国家安全领域的关联性。例如数据安全与科技安全的关系,要维护数据安全,就要大力发展数据的收集、存储、使用、加工、传输等技术。只有科技安全了,才能为数据安全提供科技保障。另一方面,坚持总体国家安全观还要处理好自身安全和共同安全的关系。由于数据自身的无实体边界性,数据的流动特别是跨境流动就不可避免。在维护自身数据安全的同时,还要关注外部的数据安全,外部的数据安全事件会反过来影响我国的数据安全,构建全球范围内的数据安全共同体就非常必要。维护数据安全,坚持总体国家安全观,还要关注数据安全治理的领导体制问题。中央国家安全领导机构在整体上领导数据安全治理工作,起到统筹协调的作用。就目前的国家安全领导体制来讲,中央国家安全领导机构是指中央国家安全委员会,而国家网信部门负责统筹协调网络数据安全工作。2021 年 7 月 16 日,公安部、国家安全部、自然资源部、交通运输部、税务总局、市场监管总局等部门就是在国家网信办的统筹协调下进驻滴滴出行科技有限公司,开展网络安全审查的。[4]

(三)完善数据安全治理法律法规体系

在依法治国的大背景下,数据安全治理也要依法进行,科学立法是数据安全依法治理的第一步。强

化数据安全方面的立法是很多国家的通常做法，我国目前数据安全治理的法律法规体系主要包括《国家安全法》《网络安全法》《数据安全法》《网络安全审查办法》《个人信息保护法》等，整体来说还是比较完备的。但是上述法律法规出台的时间比较晚，总体来说都还没有经过实践的充分检验，还需要一定时期的磨合。为了完善数据安全治理的法律法规体系，需要在以下两个方面加强。

1.加强数据安全治理顶层设计

欧盟发布《欧洲数据保护监管局战略计划(2020—2024)》，旨在从前瞻性、行动性和协调性三个方面继续加强数据安全保护，以保障个人隐私权。美国发布《联邦数据战略与2020年行动计划》，确立了保护数据完整性、确保流通数据真实性、数据存储安全性等基本原则。[5]34 虽然我国提出的《全球数据安全倡议》呼吁“各国应以事实为依据全面客观看待数据安全问题，积极维护全球信息技术产品和服务的供应链开放、安全、稳定”，但是其毕竟只是个倡议，没有约束力，而且是用于调节国家间的数据流动关系，缺乏对内效力。在《全球数据安全倡议》框架下，我国和阿拉伯国家联盟共同提出了《中阿数据安全合作倡议》，共同应对数据安全风险挑战。和《全球数据安全倡议》一样，《中阿数据安全合作倡议》在治理约束力和效力范围方面都不能完全满足我国数据安全治理的需求。为了加强我国数据安全治理的顶层设计，我国有必要在官方层面制定《数据安全国家战略》，在宏观上、长远上为我国的数据安全治理提供指导。中共中央政治局分别于2015年和2021年审议通过了《国家安全战略纲要》《国家安全战略(2021—2025年)》，这两个国家安全战略可以为《数据安全国家战略》的制定提供宏观指导。

2.完善数据安全标准体系建设

“安全发展、标准先行”，标准化工作是保障数据安全的重要基础。《数据安全法》要求相关行业组织按照章程，依法制定数据安全行为规范和团体标准；推进数据开发利用技术和数据安全标准体系建设。为落实《中华人民共和国网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》《电信和互联网用户个人信息保护规定》等法律法规要求，指导电信和互联网行业数据安全标准化工作，2020年，工业和信息化部组织制定了《电信和互联网行业数据安全标准体系建设指南》。

总体来说，我国数据安全领域的行业标准还不够完善，在交通、金融、自然资源、卫生健康、教育等部门还没有数据安全行业标准，需要尽快补齐这个短板。在数据安全标准指南建设方面，欧盟发布了《为保持欧盟个人数据保护级别而采用的数据跨境转移工具补充措施》，西班牙数据保护局发布了《默认数据保护指南》，[5]34 其他国家、地区的优秀成果和经验可以助力我国的数据安全标准体系建设。

(四)构建数据安全治理国际话语权

数据安全是国家安全的重要领域，我国目前的国家安全面临着非常严峻的形势。特别是以美国为首的西方国家利用民主、自由、人权等所谓的普世价值在香港、新疆、西藏等问题上给我国设置障碍，以恐遏华、以疆制华，妄图阻碍中华民族的伟大复兴。美国为何能在国家安全问题上屡屡给我国制造麻烦，而且在客观上的确给我国带来了损害。例如特朗普政府对我国发动贸易战，实施所谓的“极限施压”，打压以华为为代表的高新技术企业，制裁我国的政府机构和官员，出现上述现象的主要原因有两点。第一，美国泛化国家安全概念，将非政治问题政治化。由于国家安全的政治性特征，各个主权国家很难在法律上统一国家安全概念的内涵和外延，国家安全就容易出现泛化的现象，国家安全也就容易沦为美国推行霸权主义、强权政治的工具。在将非政治问题政治化方面，典型的表现就是将新冠肺炎疫苗政治化，而且美国妄图将科学问题政治化，鼓吹新冠肺炎病毒溯源，以达到栽赃陷害我国的目的。第二，美国掌握了国家安全领域的国际话语权，这也是最主要的原因。由于历史的原因，二战后，美国通过北约组织、布雷顿森林体系、意识形态输出等工具和手段，牢牢控制了军事、金融和文化等领域的国际话语权，在全世界推行霸权主义和强权政治。

在我国由“富起来”进入“强起来”的阶段，作为维护世界和平、促进世界发展的重要力量，要在国际上发挥更大的影响力，为世界的和平与发展作出更大的贡献，我国有必要成为国际规则的制定参与者，而不

仅仅是国际规则的遵守者。特别是在坚持“道路自信、理论自信、制度自信、文化自信”的大背景下,我们更有必要在国家安全领域构建中国的话语权,具体到数据安全治理领域也是如此。

1.积极参与国际交流与合作

在经济、政治、科技全球化的时代,任何一个国家都不可能孤立起来搞建设、谋发展。在维护数据安全的过程中,我国也要积极参与国际交流与合作。一方面,要积极参与数据安全治理的国际交流与合作,吸收外国数据安全治理的成功经验为我所用,完善我国的数据安全治理体系。另一方面,要积极参与数据开发利用领域的国际交流与合作。数据安全治理与社会综合治理等其他领域治理的最大区别是技术性。数据安全治理会用到大数据、人工智能、区块链等新技术,数据开发利用关涉数据采集、传输、存储、处理、交换、销毁等全生命周期环节。我国目前在数据实践利用方面有一定的优势,但是在数据开发基础理论方面与世界上有些国家相比,还有一定的差距,要补齐数据开发利用的技术短板。

2.参与数据安全相关国际规则和标准的制定

参与数据安全相关国际规则和标准的制定,一方面是为了反击数据霸权、科技霸权,建立我国的数据安全治理国际话语权;另一方面是为了促进数据跨境安全、自由流动。数据的跨境流动关涉数据主权问题,数据主权是一个国家对数据的运用能力,能使该国在国际政治上领先,也可以使其因数据跨境流动而丧失主权。与传统的国家主权相比,数据主权被赋予了数字化的特征。我国目前在数据跨境管理体系国际博弈中还处于被动地位,有必要基于公共数据权益打造中国模式,维护我国的数据主权和数据安全。[6]

3.反击外国数据霸权

数据霸权是霸权主义的一种表现形式,是指一个国家依仗在数据领域的技术优势和话语权,在数据交易、数据流通、标准制定等方面给予其他劣势国家不合理的、歧视性待遇和强迫性交易等行为。为了应对美国的无理制裁,我国及时出台了《反外国制裁法》,利用法律手段反制外国的干涉、制裁和长臂管辖。徒法不足以自行,法律的生命力在于实施。《反外国制裁法》制定得再完备,如果不能被各方当事人遵守或者僵化执行法律条款,也无法发挥法律的效力。在利用《反外国制裁法》反击外国数据霸权的过程中,要注意以下事项。

(1)原则性与灵活性相结合

用法律手段打击国外反华势力对我国的无端制裁,用法治思维和法治方式应对重大风险挑战,维护国家主权、安全和发展利益,是我们必须坚持的原则,在这些问题上不能有任何的妥协。在坚持原则性的前提下,还要与灵活性相结合,毕竟法律是灰色的,而实践之树常青。在非原则性问题上可以灵活处理,如果采取协商等方式可以化解矛盾和争端,也不是一定要采用两败俱伤的反制手段。但是无论是原则性还是灵活性,最终的落脚点都是维护我国的国家利益和民众利益。

(2)急用先行与全面布局相结合

所谓“急用先行”,是指根据实践和形势需要,采取专项立法形式,增强反外国制裁立法的针对性和可操作性。“急用先行”有进行试点的意味,而且采取专项立法的形式可以提高反制裁的精准度。在全面布局思想的指导下,逐渐在各个领域布局,在各个专项立法完备的情况下,最终形成层次分明、布局合理的反外国制裁法律法规体系。商务部的《阻断外国法律与措施不当域外适用办法》其实就是反外国制裁法在反长臂管辖领域的专项立法。反外国制裁法是一个法律法规体系,不但包括其基本法《反外国制裁法》,还包括其他相关的法律、行政法规和部门规章等。

(3)被动反制与主动出击相结合

《反外国制裁法》的一个显著特点是“反”,即针对外国的干涉、制裁、长臂管辖采取的反制措施,《反外国制裁法》对列入反制清单中的个人、组织进行的反制具有“被动性”。反制具有“被动性”,一方面与我国长期坚持和平共处五项原则、反对霸权主义和强权政治、构建以国际法和联合国为中心的秩序和体系有关;另一方面,也是为了避免反华势力曲解、污蔑我国的《反外国制裁法》,错误宣扬随着我国综合国力的

提升，我国的对外政策开始向进攻性转变。在新时代的社会大变局下，我们有必要适当调整处理涉外事务的政策，在“被动”反制的同时，也要兼顾“主动”进攻。通过主动进攻的手段，最大限度保护我国的国家利益和民众利益。因此，可以在《反外国制裁法》中增加主动制裁的内容，以顺应局势发展的需要。

（五）创新数据安全治理措施

无论是数据安全治理中国方案，还是数据安全治理中国模式，都有创新数据安全治理措施的要求，这也是中国特色社会主义的应有之义。方案和模式在概念内涵上是基本相同的，笔者在这里不再作过于牵强附会的区分。传统的数据安全治理措施和手段已经不能完全满足数据安全、数据流动和数据开发利用的要求，无法解决数据主体和数据控制者之间不平衡的权力关系，也无法确保数据流通和交易中的隐私和安全。

1.数据信托：一种数据安全治理的新方案

将信托制度引入数据安全治理是数据安全治理领域的有益尝试，也是一种数据安全治理的新方案。数据信托通过建立第三方机构提供独立的数据信托服务，与传统的政府监管不同，数据信托是一种自下而上的方案，其优势就是通过第三方来实现数据主体和数据控制者之间的权力平衡。我国目前在“数据信托”上还处于起步和探索阶段，需要在实践中验证数据信托方案的可行性。考虑到我国数据安全和数据发展的现实情况，要加强数据信托在两个方面的理论和实践探索。第一是数据流通和交易。数据权利到底是一种什么性质的权利存在争议，特别是在大数据时代，我们如何理解和看待个人数据权利，关系到每个公民的人身权利和财产权益。关于个人数据权利，笔者赞成以下观点：个人数据可以成为民事权利的客体，但是个人数据权利并不是绝对权，它与所有权等物权还是存在区别的。个人数据权利要想获得侵权法的保护，需要满足因为个人数据权利被侵害而导致其他民事权利被侵害的条件。[7]在数据新型财产权构建过程中，数据信托可以悬置所有权问题，基于个人或企业的数据财产权益设立数据信托。第二是公共数据的管理。公共数据也具有巨大的经济效益，要探索既确保公共数据安全又合理利用公共数据、保障公众对公共信息资源知情权的道路。[8]

2.数据合规：监督数据安全治理的新模式

数据合规是指企业及其员工的数据活动需要符合规则，不但要符合《网络安全法》《数据安全法》《刑法》等法律，还要遵守民法、经济法、行政法、国际条约等，以及商业伦理和市场规范。要打造具有中国特色的数据合规管理体系，实现行政监督与公司治理、行业自治相结合。[9]数据合规建设主要依靠企业内部的自身规范建设，如果企业自身内部的合规建设失范时，就需要国家、政府层面的推进和监督。

（1）合规建设的企业视角

数据企业要完善企业合规建设，在合规制度、合规部门、合规人员等方面进行完善，企业负责人和管理人员要有遵纪守法的合规意识，要带头合规。要加强企业合规建设的刚性，加大对违规行为的处罚力度，不能通过企业内部规章处理的行为，要及时转交相关的司法机关，追究行为人的违法犯罪责任，同时要扩大合规部门人员的权力。

（2）合规建设的国家视角

数据企业对其内部的企业合规建设特别是刑事合规建设存在惰性，需要国家相关部门在外部进行监督和推动，促进数据企业加强和完善数据安全技术和规范制度建设，在保障数据安全的前提下，更好地发展数字经济。考虑到我国的实际情况，要创新企业合规建设的监督机制。检察机关是我国宪法规定的专门的法律监督机关，企业合规建设也是企业要履行的法律义务。检察机关可以通过提出社会治理检察建议的形式，对企业的合规建设进行法律监督。考虑到社会治理范围的广泛性，检察机关发放检察建议要考虑到社会治理类检察建议的权力边界和实施的规范性，避免沦为破坏权力结构平衡的一般法律监督。[10]除了向数据企业制发社会治理类检察建议，检察机关也可以向数据安全的主管行政机关制发公益诉讼检察建议，要求其依法履行监管职责或者纠正违法行使职权的行为，如果相应的行政机关在一定的期限内不依法履行职责或者纠正违法行为，检察机关可以提起行政公益诉讼。

三、结语

在全球化时代,数据流动不可避免具有全球化的特征。同时,数据也是有主权的,各个国家都非常重视维护自己国家的数据主权。丧失了数据主权,一个国家的主权就是不完整的,从这个意义上讲,数据安全也关系到一国的国家安全,数据安全是一种非传统安全。数据全球化和数据主权具有对抗性,但是也具有统一性,二者对立统一的最理想状态是数据安全前提下的数据发展。[11]我国在探索有中国特色的数据安全治理道路过程中,也不能偏离这个宗旨,片面地强调数据安全或者片面地强调数据发展,都不是数据安全治理中国方案的应有之义。

参考文献:

[1]韩洪灵,陈帅弟,刘杰,等.数据伦理、国家安全与海外上市:基于滴滴的案例研究[J].财会月刊,2021(15):1.

[2]美国强制台积电 45 天内交出机密数据[EB/OL].[2021-10-27].https://www.163.com/dy/article/GL27L2M50511A6N9.html.

[3]魏远山.博弈论视角下跨境数据流动的问题与对策研究[J].西安交通大学学报(社会科学版),2021(5):6.

[4]国家网信办等七部门进驻滴滴,开展网络安全审查[EB/OL].[2021-07-27].https://www.guancha.cn/politics/2021_07_16_598702.shtml?s=zwytt.

[5]王伟洁,周千荷.国外数据安全保护的最新进展、特点及启示[J].科技中国,2021(7).

[6]邓崧,黄岚,马步涛.基于数据主权的数据跨境管理比较研究[J].情报杂志,2021(6):119-120.

[7]程啸.论大数据时代的个人数据权利[J].中国社会科学,2018(3):102.

[8]翟志勇.论数据信托:一种数据治理的新方案[J].东方法学,2021(2):76.

[9]颜新华.网络安全视阈下的数据合规:基本理论、问题审视与中国方案[A]//上海法学研究集刊[C],2021(1):28.

[10]王林,王柏洪.社会治理类检察建议的权力边界及规范化[J].广西大学学报(哲学社会科学版),2021(2):138.

[11]何傲翾.数据全球化与数据主权的对抗态势和中国应对——基于数据安全视角的分析[J].北京航空航天大学学报(社会科学版),2021(3):24.

An Analysis of China's Data Security Risks and Governance in the New Era

WANG Lin

(*National Security School, Northwest University of Political Science and Law, Xi'an* 710063, *China*)

Abstract: In order to effectively maintain data security, especially the security of cross-border data flow, and balance data security and development, it is necessary to explore a Chinese solution to data security governance in the new era. This paper analyzes the risks of data leakage, data sovereignty infringement and data hegemony in data security governance, and summarizes the basic connotation of China's data security governance. In order to maintain China's data security and promote the development of the digital economy, it is necessary to introduce governance concepts into data security and build a data security governance community, to incorporate data security into overall national security and coordinate the relationship between data security and security in other areas, to strengthen the construction of the laws and regulations regarding data security governance, and to strengthen the top-level design of data security governance and promote the construction of data security standards; meanwhile, it is vital to improve our international discourse power in data security governance, to actively participate in the formulation of international rules related to data security, and combat foreign data hegemony; what's more, we are expected to keep pace with the times, to innovate data security governance measures, and introduce data trust and data compliance systems.

Key words: data security; national security; governance community; digital development; data trust; data compliance

(责任编辑:江 雯)