总体国家安全观视域下数据安全立法探讨

胡尔贵
(西南政法大学 国家安全学院,重庆 401120)

[摘 要]随着数据技术和数字经济的发展,数据已经成为重要的社会资产和战略资源。数据安全与国家安全和国家主权息息相关。完善数据安全立法已经迫在眉睫。但是,检视我国现有数据安全相关法律制度,我们不难发现,我国数据安全立法进程、立法渊源、立法理念、立法效果都与维护我国数据安全和国家安全的现实需要存在明显的差距。为更好地发挥数据安全法在维护国家安全中的积极作用,应当在我国的数据安全立法中,进一步突出总体国家安全观的立法指导思想地位,确立数据主权不可侵犯原则,认清数据应用发展与国家安全的辩证关系,构建科学完整的数据安全法治体系,助推我国的国家安全治理体系和治理能力现代化。

[关键词]总体国家安全观;国家安全;数据安全;立法建议
doi:10.3969/j.issn.1673-9477.2020.03.010
[中图分类号]D616 [文献标识码]A [文章编号]1673-9477(2020)03-052-06

伴随着大数据时代的到来,数据经济发展带来的数据安全及其对国家安全的影响日益凸显。加快数据安全立法,推进新时期国家安全法治建设是全面推动总体国家安全观发展与实践之重要内容。[1]习近平总书记明确要求要切实保障国家数据安全,“建设数字中国、发展数字经济,既需要技术支撑,也需要法律保障。”[2]但是,反观我国数据安全立法现状,难以满足维护国家安全的现实需要。为此,我国明确提出要制定《数据安全法》,并将其列入了十三届全国人大常委会2020年立法规划“第一类项目”。鉴于《数据安全法》是维护和塑造我国国家安全的一部重要法律,本文拟从总体国家安全观这一视角,就我国的数据安全立法提出个人拙见,以期抛砖玉。

一、数据安全立法与维护国家安全的关系

习近平总书记强调:“安全与发展是一体之两翼、驱动之双轮。安全是发展的保障,发展是安全的目的。”[3]数据发展和数据安全密不可分。法治是数据安全的重要保障手段之一,已逐步成为共识。西方发达国家大多早已运用法律手段解决国家安全等重大政治问题。只有正确认识和理解了数据安全立法与国家安全的关系,才能处理好数据发展、数据立法、国家安全三者的关系,树立数据安全立法的科学观念。

(一)数据安全立法是保护国家数据战略资源的重要保障

随着大数据、物联网、人工智能的发展,越来越多的“物”的存在方式都会以数据形式体现。人类的活动会不断产生数据,形成海量数据。这些海量数据就是“物”的数据存在方式,具有无限的潜在价值。在数字经济发展的初期,人们关注的主要是数据与公民个人权利保护的关系、促进数字经济产业发展等问题,对于数据对国家安全的关系认识不够。殊不知,由海量数据构成的大数据正日益成为国家基础性战略资源。[4]即使对于看似仅涉及个人隐私的简单个人信息资料,如果将不同人的个人信息资料汇聚起来分析,其中必然蕴藏着最新的社会动态、科技发展、经济形势、安全威胁、敌我态势等各种政治、经济、文化、安全等信息。此时的数据不仅关乎隐私权,还涉及国家信息安全,二者互为表里。[5]

世界各国正在通过不断完善数据安全立法争夺他国数据资源,有的国家甚至正在依仗技术优势推行数据霸权。如欧盟于2018年5月25日通过的《通用数据保护条件》(简称“GDPR”)就以最严格的个人数据保护为名,通过立法确立了“长臂管辖”原则,不仅对欧盟国家境内设立法人实体的企业有管辖权,还对虽未在欧盟国家境内设立法人实体但只要为欧盟境内个人提供商品或服务、为欧盟境内法

[投稿日期]2020-07-10
[基金项目]西南政法大学校级重点资助项目(编号:2015XZZD-12);重庆市哲学社会科学规划项目(编号:2019TBWT-ZD37)
[作者简介]胡尔贵(1972-),男,重庆忠县人,教授,硕士生导师,研究方向:侦查学、国家安全学。

人实体提供数据服务的企业有管辖权。通过这种立法规定,就可以最大限度地获取他国数据资源。

各种数据正在成为新时代的核心社会资源和重要社会财富,同时也成为支撑国家安全与发展的重要战略资源。随着我国数字经济发展步伐越来越快,我国已经成为世界上数据储量最大、信息最丰富的国家。据阿里巴巴董事局主席兼首席执行官张勇于在 2019 年阿里巴巴投资者大会上的发言所说,阿里巴巴数字经济体的客户就接近 10 亿,数据规模可见一斑。随着我国的掘起,以美国为首的西方发达国家正在凭借其在网络空间和数据技术上的优势,不遗余力地攫取我国的数据资源,争夺数据控制权。因此,加快数据安全立法进程,有效遏制数据资源流失或被他国掠夺,是维护国家安全与发展的迫切要求。

(二)数据安全立法是维护国家数据主权的重要武器

互联网实现了数据传播的无界性、广泛性,使得任何国家在任何时候都有可能获得任何其它国家的数据。因此,获取、占有、控制数据以及从海量信息中获取战略情报成为了维护国家安全的重要预警手段。当一国拥有他国数据的规模与分析能力达到一定程度与水平时,就有可能对他国的国家安全形成足够的威胁。这充分体现出了数据所具有国家主权性。

据“棱镜门”曝光的信息,美国政府为了监控其它国家,就借助谷歌、微软等 9 家跨国公司将在境外合理收集的数据转移至国内。[6] 这一事件给世界各国敲响了维护数据主权的警钟,各国纷纷立法限制或禁止本国数据向境外流动。2016 年初,欧美在废除“安全港”协议后又签署了“隐私盾”协议,该协议在数据跨境传输上对美国进行了限制并要求美国政府作出相应承诺。

数据具有主权性,数据主权已经成为国家主权的重要内涵,数据安全关乎国家安全。因此,如何维护我国的数据主权,保证我国的数据安全,是我国在维护国家安全方面的一个无法回避的现实难题。为此,我国应当借鉴国外的立法经验,加快数据安全立法进程,建立符合我国国情的数据跨境流动制度,运用法律武器捍卫我国的数据主权。

(三)数据安全立法是防范化解国家安全风险的重要手段

当前,各种新技术的应用使得数据收集无时无处不在,这必将导致个人敏感数据与非敏感数据难以区分,国家机密与非国家机密的难以界定。而通过数据分析和数据挖掘,可以从碎片化的、不具有敏感性的数据中分析出敏感的、可识别的信息。所以,对于任何一个国家来讲,在数据收集和运用中的安全风险也就接踵而来。有时在某个领域、小范围内的数据处理或运用不当,就可能带来不可预见的大范围内的巨大风险,进而引发系统性风险。随着数据时代的到来,数据安全越来越超越个体安全范畴,收集和运用海量数据所带来的国家安全风险越来越大。

世界各国都在不断完善数据安全法律制度,防范数字经济发展中可能出现的安全问题。2018 年,美国 Facebook 数据事件使得大众意识到大数据风险不仅是个人和企业层面的保护问题,更与政治权力相勾连,事关社会稳定和国家政治安全。西方 33 国缔结的《瓦森纳协定》明确将与管制商品和技术清单内容直接相关的各类技术数据纳入受管控范围,对儿童色情、恐怖主义信息等非法内容进行管控。[7] 韩国不仅重视对国家信息安全和信息基础设施的保护,还对个人的隐私及通信权益做出明确规定,形成了较为完备的信息安全立法体系。[8]

数据安全风险日益凸显,并正在成为影响我国国家安全与稳定的重大风险因素。长期以来,我国的国家治理存在“重发展轻安全”的倾向,这也在一定程度上造成了我国在发展数字经济的过程中对数据安全重视不够。法治是国家治理体系和治理能力的重要依托。[9] 为防范和化解我国在数据领域面临的重大风险,必须推动数据安全立法工作,以法治手段防范和化解数字经济发展可能带来的国家安全风险,做到安全与发展并重。这也是贯彻落实总体国家安全观的必然要求和具体体现。

二、我国数据安全立法现状检视

在大数据领域,当大数据逐渐有可能成为资源和产业时,在“发展是第一要务”这一惯性思维的作用下,人们首先看到了繁荣数字经济对于发展的重要性,对安全问题的认识明显不足。在“重发展轻安全”观念的影响下,我国过去在进行数据领域的法律制度设计时安全理念明显缺失。这导致现有的所有数据法律制度无论在内容上还是在形式上,都与维护我国的数据安全和国家安全的现实需要还存在明显的差距与不足。

(一)从立法进程看,立法步伐严重滞后

认真检视我国数字经济发展及相关立法的实践

历程,我们不难发现,我国有关数据安全的立法很不充分,立法进程严重滞后。一方面,我国在数据领域的安全立法起步相对较晚。我国于1994年2月18日颁布的《中华人民共和国计算机信息系统安全保护条例》才在国家层面做出了有关"保护信息安全"的规定。前西德的黑森州在1970年通过世界上第一部《数据保护法》,该法其实是倾向于从政府安全的角度进行立法。[10]此后欧美各国相继都出台有关数据安全方面的立法。这反映出我国对数据安全问题的认识和思考比西方国家落后了20多年。另一方面,我国在数据领域立法中涉及安全的法律制度很不成熟、很不完善。最明显的体现就是,在很长一段时间里,尽管我国的数据立法本来就为数不多,但其中更是鲜有关于数据安全的规定,更不用说直接涉及国家安全的规定。总体来讲,数据安全领域的立法进程十分缓慢,不能较好地满足维护国家安全的现实需要。

从国家层面的规定看,曾一度不够重视数据安全。国务院于2015年8月颁布了《促进大数据发展行动纲要》中仅提出了"切实加强对涉及国家利益、公共安全、商业秘密、个人隐私、军工科研生产等信息的保护",并未就安全立法提出要求。[11]该纲要作为我国近年来促进大数据发展的总纲,涉及大数据及其运用的长远发展,却对安全问题一笔带过。直到2019年5月,国家互联网信息办公室公布的《数据安全管理办法(征求意见稿)》才作为第一个比较系统强调"数据安全""国家安全"的官方文件开始征求意见,这在一定程度上也反映了我国数据安全立法的现状。

从地方层面的规定来看,情况也不乐观。2016年3月1日《贵州省大数据发展应用促进条例》作为全国第一部大数据地方性法规正式颁布,该条例主要是扶持大数据行业发展,对大数据安全规定较少。2017年5月颁布的《浙江省公共数据和电子政务管理办法》虽是全国第一部有关公共数据的省级政府规章,但仅有一条提及信息安全。这充分反映出了无论是国家层面还是地方层面,我国对于数据安全立法普遍认识不够,严重影响了立法进程。

(二)从立法渊源看,法律制度不成体系

近几年来,虽然随着人们的数据安全意识不断增强,一些政策法规的制定过程中不断开始出现调整数据安全的具体规定,但是,从总体来看,涉及数据安全的相关规定具有较强的随意性,立法表现形式比较散乱,没有从安全管理角度对数据的全生命周期进行系统设计,没有形成严谨的法律制度体系,呈现出明显的碎片化特征。

首先,法律层面的规定仅点到为止。《网络安全法》虽然于2017年6月正式实施,成为我国第一部网络安全法律方面的基本法,但是,该法对数据安全的规定比较片面,对公共大数据安全有所提及,却没有对公共大数据信息安全作出专门系统规定。截止目前,另外两部涉及数据安全的《数据安全法》和《个人信息保护法》尚处于立法规划阶段。

其次,行政法规层面的规定未涵盖数据的全生命周期。从理论上讲,按照依法治国的要求,要确保大数据时代的数据安全,立法应当对数据的采集、存储、应用、传输、销毁等全生命周期进行全面系统的规制,既要规定一般意义上的数据安全问题,又要规定数据主权安全等问题。但是,从涉及我国数据安全的行政法规制定来看,却主要集中在为《网络安全法》制定配套规范,如国家互联网信息办公室、全国信息安全标准化技术委员会主要在推动实施《网络产品和服务安全审查办法(试行)》《个人信息和重要数据出境安全评估办法》《信息安全技术数据出境安全评估指南》等。直到2019年5月,国家互联网信息办公室才公布《数据安全管理办法(征求意见稿)》,试图对数据收集、数据处理使用、数据安全监督管理等进行全流程规制,但迄今也未颁布。

再次,地方法规层面的规定为数不多。2018年《贵阳市大数据安全管理条例》作为全国首部大数据安全管理地方性法规,是落实和细化《中华人民共和国网络安全法》的有关规定和要求,聚焦大数据安全,提出了数据对国家安全的意义,[12]是对数据安全立法的有益探索。2019年8月《天津市数据安全管理办法(暂行)》作为全国第一部数据安全的省级专门性地方立法开始施行。这两部地方法规分别作为省会城市和省级政府的首部调整数据安全的法规出现,而且从立法时间来看均属近期立法。由于,数据安全立法在地方法规层面的状况可见一斑。

(三)从立法理念看,国家安全理念缺位

数据安全既与个人隐私有关,又与国家安全相关。因此,世界各国有关数据安全立法目标深化到国家主权与国家利益的维护,内容越来越丰富。但是,从我国目前有关数据安全的规定来看,数据安全立法理念存在缺位现象,尤其是对总体国家安全观认识不到位。

一方面,从宏观高度把握总体安全不够。安全的内涵十分丰富,既有宏观安全,也有微观安全。总

体国家安全观强调地就是宏观安全、总体安全,就是要从国家安全的宏观高度理解和认识安全问题。但从现有的数据安全相关法律制度来看,着眼微观安全较多,有关个人信息保护规定较多,对个人信息安全保护相对充分一些,对宏观安全照顾不足。如《全国人大常委会关于加强网络信息保护的决定》《消费者权益保护法》《刑法》《民法总则》和《网络安全法》均有关于个人信息保护的不少规定,但是,却少有从维护国家安全高度对数据安全进行规定。比如《网络安全法》的第四章虽名为“网络信息安全”,但侧重于对个人信息的保护,并未对数据合法利用和安全管理作出充分的规定。

另一方面,对公共数据和政府数据安全重视不够。从国家互联网信息办公室推动《个人信息和重要数据出境安全评估办法》的制定过程来看,也反映出了我国社会在数据信息安全方面缺乏公共集体意识和国家安全意识。该办法早在 2017 年 4 月就向社会公开征求意见,明确了数据出境安全评估的重点在于数据出境及出境数据汇聚可能对国家安全、社会公共利益、个人合法利益带来的风险等,但却因争议较大至今尚未通过。[13]

(四)从立法效果看,安全风险难以化解

由于涉及数据安全的立法规定不全面、碎片化情形突出,难以相互协调配套,必须影响其可操作性,导致有关法律制度难以实施落地,进而在化解安全风险方面的法律效果大打折扣。在实践中普遍存在“数据不够用、数据不可用、数据不会用、数据不敢用”的情形。[14]最突出的表现有两个方面:

一是数据安全管理责任分散,权责不清,各自为战。由于数据技术的高速发展,人们对数据及数据安全的内涵外延难以准确界定,相应的管理体制也比较混乱,这导致现有立法要么缺乏法律责任条款,要么缺少配套制度,很难确保法律责任落到实处,势必其法律效果。有的规定甚至机械照搬国外立法模式,不能结合我国具体国情做出具有操作性的规定。如《信息安全技术数据出境安全评估指南》将可能危害国家安全、国防利益、国际关系、国家经济秩序和金融安全、国家财产、个人合法权益、国家政治、国土、军事、经济、文化、社会、科技、信息、生态、资源、核设施安全的数据均囊括为“关键(重要)数据”,这虽然全面,但却没有明确的解释区分,缺乏失操作性,给政府执法和企业守法造成困难。

二是相关规定没有较好地与国际接轨,与国外数据法存在冲突。比如,欧盟 2018 年 5 月实施的《通用数据保护条例》(GDPR)是史上最严的个人数据保护法规,该条例要求获取在华企业的数据或进入其设备系统的访问权限。但我国网络安全法第 37 条规定数据不予出境,企业对于欧盟调查权的行使要求不予执行。二者的冲突既不利于中欧企业之间的合作,也会给我国数据主权带来威胁。

三、国家安全视角下的数据安全立法思路

习近平总书记在中央国家安全委员会第一次全体会议上明确“既重视发展问题,又重视安全问题”,这是中国特色社会主义国家安全理论的最新发展,也是中国特色社会主义新时代“推进国家治理体系和治理能力现代化、实现国家长治久安的迫切要求”。在大力发展数字经济的同时,必须高度重视数据安全风险的防范。数据安全法立法迫在眉睫。结合前文分析,本文在此以维护国家安全为视角,就数据安全立法提出几点拙见:

(一)突出总体国家安全观的立法指导思想地位

数据安全不仅涉及个体安全问题,而且越来越与国家安全密切相关。随着数字经济发展和技术进步,数据越来越成为一个国家的重要社会财富和战略资源,数据在国家安全中的价值将进一步凸显,同时,其所带来的国家安全风险也将更加突出。习近平总书记在中共中央政治局第二次集体学习时强调:“要切实保障国家数据安全。要加强关键信息基础设施安全保护,强化国家关键数据资源保护能力,增强数据安全预警和溯源能力。”加强数据安全立法是维护国家安全的迫切现实需要。当前,在国家安全法这一上位法的统领下,《网络安全法》已经出台,个人信息保护法和数据安全法已经列入立法计划。我们要正确好数据安全法与网络安全法、个人信息保护法的立法关系,应将数据安全法聚焦于“重要数据”的风险预防和管控上。这三部立法要各有侧重,各居其位,相互配合、相互协调、相互补足,形成三角构造,分别对涉及数据、网络空间、个人信息相关活动进行法律调整,共同维护大数据时代我国的网络安全、个人信息安全和国家安全。既保证了法律之间的衔接,又有利于后续执法工作的执行。

为此,应当将总体国家安全观作为数据安全法的立法指导思想,将其立法目标和立法主要内容定位在通过确保关键(重要)数据安全以维护国家安全上,使其成为数据安全领域里维护国家安全的根本法。要站在总体国家安全观的高度,厘清数据安全、网络安全和个人信息安全这几个范畴的关系,科学

界定数据安全的内涵和外延。要站在总体国家安全观的高度,充分认识网络无界性对数据安全所涉时空领域的无限延展性,全面、系统地分析影响数据安全的各种重大风险因素。要站在总体国家安全观的高度,准确把握国际数据安全立法趋势,既符合保护我国数据资源的需要,又能与国际社会有效接轨。

(二)确立数据主权不可侵犯原则

数据时代,数据权决定话语权。如果失去数据主权,国家的政治、经济、文化等数据资源就会被其他数据强国所控制,国家主权也会受到威胁。鉴于美国等强国正在推行数据霸权,强行干涉他国数据主权,而我国现有法律体系尚未提及数据主权,因此确立国家数据主权不可侵犯原则对于维护我国的国家数据主权安全具有现实紧迫性,刻不容缓。数据安全立法应当将数据主权原则作为贯穿数据安全法的一条主线,聚集"重要敏感数据"的风险防控。确立这一原则,必须完善以下几项具体制度:

一是长臂管辖制度。当前无论是 GDPR 还是美国的《合法使用境外数据明确法》(Clarify Lawful Overseas Use of Data Act,简称"CLOUD 法")法均将属地管辖扩展至长臂管辖,扩大其法律的域外效力。为争夺数据话语权,扩张本国法律的适用范围,积极推行符合本国利益诉求的国际社会数据规则体系成为当前国际的立法趋势。[15]我国的数据安全立法工作要因势而变,由"属地"管辖向"属地+长臂"管辖过渡,即只要侵犯到中国境内的自然人、企业和国家的利益,不区分数据处理行为的域界,均有权利获取数据。确立此制度后,可以适当调整我国对待外国数据的策略和态度,适度放开让外国公司来华开展业务的政策规定,可以为我国合法获取他国数据资源提供法律依据。

二是数据跨境流动保护制度。在坚持数据本地化政策的前提下,对数据跨境转移实施分级保护。对于涉及国家安全、社会重大利益的敏感数据,采取最严格管控措施,严禁跨境转移;对于一般性行业数据和政府公开数据,根据双边、多边协议可以有限制地跨境流动;对于公开的个人数据,原则上可以允许跨境转移。当然,鉴于国际法或国际惯例尚未对数据管辖和数据主权作出规定,应注意与国际接轨,加强国际交流与合作,积极参与国际规则的制定,要让世界听到中国的声音。

三是数据跨境安全风险审查评估制度。数据是否重要敏感、是否具有安全风险,需要由专业人员、按照法定的程序、采取专业的方法进行科学的评估。而且,特别要注意地是,某些数据是否重要敏感、是否具有安全风险不是一成不变的,是会随着数据挖掘技术的发展和人们的认识能力的提高而变化的。因此,要根据数据性质及技术发展状况,对数据出境可能带来的安全风险进行审查评估,非经评估同意,禁止任何数据跨境转移。

(三)认清数据应用发展与国家安全的辩证关系

有一种观点认为,由于数据具有无形化和无界传播性,要有效防范数据可能带来的安全风险,就应当将数据"保护"起来,限制数据开放,禁止数据传输,通过限制数据的应用发展,就能够实现绝对安全。比如,欧盟早期为了保护个人隐私,对数据技术的应用采取了最为严格的限制措施。但是,从结果来看,欧盟这种做法在一定程度上影响了数据技术进步和经济发展,最后它不得不主动走向开放。这充分证明了这种观点的片面性。我们试想一下,在数据技术飞速发展的今天,一个国家如果限制数据技术及数据应用发展,就会阻碍数字经济横向发展,国家经济发展水平和数据技术发展水平一定会相对落后,国家落后就会挨打,就会面临更加严重的国家安全风险,这是任何国家都不愿意承受的结果。

但是,如果人们由此认为,那就应该鼓励数据完全开放,允许数据自由流动,以促进数据技术及数字经济飞速发展,这种观点又走向了另一个极端,也是极其片面的。殊不知,这样毫无限制地推进数据运用发展,就会造成数字经济过度发展,这在一定程度上又会导致短期内大量数据的急剧产生、无序流动。由于数据制度缺乏或跟不上数据发展速度,数据发展将会累积风险,国家安全隐患会越来越大。正如习近平总书记在网络安全和信息化工作座谈会上所提,网络安全是整体的、动态的、开放的,而不是割裂的、封闭的、绝对的。这充分说明了千万不能片面、绝对地看待网络数据和国家安全的关系问题,否则就会顾此失彼。

为此,在我国的数据安全立法中,要辩证看待数据应用发展与国家安全的关系。要正确评估我国在世界上的数据技术发展水平,要结合我国的具体国情和所处的发展阶段确定我国对于数据应用发展"开放"与"限制"的程度,在数据应用发展与维护国家安全之间找到一个恰当的平衡点。

(四)构建科学完整的数据安全法治体系

鉴于数据安全对于维护国家安全的重要性,必须高度重视数据安全立法的科学性,要认真梳理研

究数据技术应用发展实践现状及发展趋势,摒弃“宜粗不宜细”的立法风格[16],全面把握影响数据安全的可能要素,构建一套完整的数据安全法治体系,不留法律真空,确保数据安全法的系统性、完整性和可操作性,提高法律实施的效力和效果。

一是要针对不同类型数据提出不同的安全要求。要在厘清个人数据、重要敏感数据、公共数据、政府数据、商业数据、跨境数据等不同类型数据的内涵外延的基础上,分析“关键数据”面临的安全形势与风险,建立分级分类保护制度,有针对性地提出安全防控要求。

二是要对数据的全生命周期进行全程安全风险评估和审查监管。要以数据的全生命周期为线索,围绕数据的产生、形成、采集、存储、加密、隔离、访问、验证、使用、下载、处理、分析、传输、保护、备份、销毁、恢复等环节的各种安全漏洞和安全风险进行全面梳理,建立数据安全基础标准、数据安全技术标准、数据安全管理标准和数据安全应用标准,编织严密的数据安全保护网。

三是要对政府、企业、个人和其他组织在维护数据安全中权利义务分别做出明确的规定。在赋予数据主体对数据的所有权、使用权、财产权、人格权、访问权、更正权、反对权、限制处理权、被遗忘权、可携权以及限制自动化决策等诸多权利的同时,明确维护数据安全的职责和义务,做到责权利相统一。

参考文献

[1]李恒. 坚持总体国家安全观指导国家安全法治建设[J]. 江淮法论,2018,(09):45.

[2]吴汉东. 加快建设数字中国 [N]. 人民日报,2018-8-19(05).

[3]习近平. 习近平在第二届世界互联网大会开幕式上的讲话[N]. 人民日报,2015-12-17(1).

[4]张峰. 大数据正日益成为国家基础性战略资源[J]. 通信世界,2016,(14):06.

[5]王顺清,刘超. 欧美个人数据跨境转移政策变迁及对我国的启示[J]. 行政与法,2018,(7):100.

[6]石静霞,张舵. 跨境数据流动规制的国家安全问题[J]. 广西社会科学,2018,(8):129.

[7]刘金瑞.《网络安全法》实施一周年配套立法的回顾与展望[J]. 网事焦点,2018,(7):62.

[8]乔丹. 韩国信息安全法律立法与管理框架[J]. 中国信息安全,2013,(2):67.

[9]冯玉军. 法治是国家治理体系和治理能力的重要依托[N]. 光明日报,2019-12-06(11),http://epaper.gmw.cn/gmrb/html/2019-12/06/nw.D110000gmrb_20191206_2-11.htm.

[10]张金平. 跨境数据转移的国际规制及中国法律的应对———兼评我国《网络安全法》上的跨境数据转移限制规则[J]. 政治与法律,2016 ,(12):137.

[11]田维琳. 公共大数据信息安全立法的内涵、现状与依据[J]. 河南社会科学,2018,(7):86.

[12]王太师. 为国家大数据安全保障探索可复制经验——解读全国首部大数据安全管理地方性法规《贵阳市大数据安全管理条例》[N]. 贵州日报,2018-8-20(8).

[13]刘金瑞.《网络安全法》实施一周年配套立法的回顾与展望[J]. 网事焦点,2018,(7):62.

[14]何友,朱扬勇,赵鹏. 等. 将信息化推向智能化:概论国防大数据[J]. 系统工程与电子技术,2015,(11).

[15]黄道丽,胡文华,大阿来. 安全视角下的大数据治理与合规应对[J]. 保密科学技术,2018,(10):14.

[16]许可. 数据安全法:定位、立场与制度构造[J]. 经贸法律评论,2019,(3):64.

[责任编辑　王云江]

Discussion on data security legislation from the perspective of a holistic view of national security

HU Er-gui

(School of National Security, Southwest University of Political Science and Law, Chongqing 401120, China)

Abstract: With the development of data technology and digital economy, data has become an important social wealth and strategic resource. Data security is closely related to national security and national sovereignty. It is urgent to improve the legislation of data security now. However, reviewing the existing legal systems related to data security in our country, we can easily find that, the legislative process, source, concept and effect of data security can't meet the actual needs of maintaining data security and national security in our country obviously. In order to give full play to the positive role of the data security law in maintaining national security, we should further highlight the guiding ideological status of the holistic view of national security in the data security legislation, establish the inviolability principle of data sovereignty, recognize the dialectical relationship between the development of data application and national security, construct a scientific and integral legal system of data security. This can promote the modernization of governance system and governance ability on national security.

Key Words: a holistic view of national security; national security; data security; proposal for legislation