国家安全视域下我国数据安全法的制度构造

张继红

摘　要：全球化的数据开放与流动对国家安全带来了巨大冲击，国家数据安全制度已经成为一国安全法律制度的重要组成部分。《数据安全法》的出台恰逢其时，贯彻《国家安全法》所提出的总体国家安全观，以法律形式建构我国基本数据安全管理制度，确立了保障数据安全与促进数据发展的立法主旨，捍卫了本国数据主权及其对内对外的管辖效力。在数据分类分级基础上，以“重要数据”的识别为抓手，建构一体两面的跨境数据流动机制，并与《网络安全法》相互协调，为建设有序、公正、合理的数据安全治理新制度夯实基础。

关键词：国家安全；数据安全；数据分级分类制度；跨境数据流动

中图分类号：X915.3；TP309.2　　**文献标识码：**A　　**文章编号：**1009-2447（2021）03-0096-08

当前，全球化的数据开放与流动对国家安全带来了巨大冲击，从各个主权国家相互指责对方的网络攻击，到美国《澄清境外数据合法使用法案》（CLOUD法案）引发的蝴蝶效应，一定程度上反映了在数据空间背后主权国家彼此之间激烈的冲突和博弈。随着国家数据安全风险来源的日趋多样化、复杂化，国家数据安全制度构建已然不可或缺。如果说在全球数字经济大发展的背景下守住不发生重大风险的底线是一种被动防御措施的话，那么明确我国数据安全法的价值定位，构建并完善我国数据安全法的制度体系，以法律形式捍卫国家数据主权安全更是一种积极的应对态度。

在此背景下，我国也加快了数据领域的立法进程。《数据安全法（草案）》分别于2020年7月、2021年4月向社会公开征求意见。在听取各方意见的基础上，2021年6月10日《数据安全法》正式通过，并于2021年9月1日起施行。从体例结构上看，《数据安全法》共七章55条，是我国数据安全领域的基本法。该法的出台，以法律的形式强化数据安全制度，确立了个人、组织、数据交易中介机构、重要数据处理者以及有关部门的数据安全保护义务和职责，对于完善我国数据安全治理体系建设具有重要意义。

一、数据安全法的价值定位

进入物联网、大数据时代，数据与土地、技术、劳动力、资本等传统生产要素相并列，成为新的核心资源，被称为“新时代的石油”，迸发出巨大的价值潜力。作为首部以“数据安全”为主题的法律，必然有着自己的价值取向与选择，即以法律形式建构基本数据安全制度，在保障数据安全的同时促进数据的开发利用。

（一）“数据”“信息”与“资料”三者辨析

“数据”一词本身的内涵及外延界定是《数据安全法》的逻辑起点。其中第3条第1款对什么是“数据”做了界定，这也是第一次以立法形式对数据作出的概念阐释。数据与信息、资料，三者概念经常出现混淆，特别是数据与信息，在我国现有法律规范及学理分析中经常性出现不同的表述和混用，也对实务层面的法律适用带来很大的困扰。

从元认识论的角度，“数据”是通过数字、表

基金项目：2018年度国家社科基金项目“交易安全视阈下大数据交易监管法律研究”（18XFX015）

作者简介：张继红，上海政法学院教授，上海全球安全治理研究院研究员，研究方向为数据法、金融法。

格、图形等对事实的客观记录。[①]在数字化转型的历史背景下，数据实质上就是以记录、描述、重现客观情况。[②]国际标准化组织将数据看作信息、事实的一种表达形式，可以通过人工或自动化处理。事实上，数据不仅包括数据控制者利用网络、传感器等采集或生产的原始数据（未经加工的原始素材，基于事实和观察），还包括经过分析、加工、计算、聚合形成的衍生数据等数据产品。大数据时代，数据大都以电子形式出现。在网络空间和计算机系统中，物理空间中的多种表现都为“数据”所取代，即以二进制信息单位0和1表示。与传统的有体物相比较，数据特别是电子形式的数据本身具有无形性的特征，且可以借助互联网从一个节点到另一节点，甚至跨地域、跨国界的快速传输。

从信息科学的角度看，“资料”和 “数据”表述基本一致，都是以可识别的符号序列对事物本身加以表述，可以使口头或书面，并且不以文字为限。[③]无论是词源还是从实际应用上来看，两者并无根本性差异。至于“资料”这一说法，只是学者对“data”的另一种译法而已，英文中并无“资料”的专门译法。

信息则是经过一定技术处理后有价值的内容，在一定程度上减少了不确定性。相较而言，数据侧重于一种客观表达，而信息的着眼点在于内容与人的互动关系。“无数客观事物的信息，正是通过人的眼、耳、鼻、舌、身这五个官能‘传递’给人们，经过人们大脑去粗取精、去伪存真的加工，人们才认识了世界”。[④]显而易见，信息和数据呈现出一个事物的不同方面，信息是标识的内在含义，数据是表象化的标识本身。[⑤]简言之，信息是数据表达的内容，数据是信息的载体和外在表现形式。与信息相比，显然数据涵盖的范围更为广阔。

在《数据安全法》出台之前，我国《网络安全法》《民法典》《护照法》《居民身份证法》《刑法修正案（九）》《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》《个人信息安全规范》等法律规范都基本适用了“个人信息”一词来指称与个人相关的信息资料内容。《数据安全法》首次从法律层面对“数据”进行了含义解释，即电子或其他方式对信息的记录，第一次明确区分了数据与信息。也就是说，“记录”是数据的根本性特征。只要是“对信息的记录”，无论以电子还是书面或其他形式，不论该数据上所承载的是个人信息、企业信息抑或政务信息，都是《数据安全法》所要规制的对象。

（二）贯彻总体国家安全观的数据安全治理体系

“安全”是《数据安全法》的第二个关键词，也彰显出该法最根本的价值出发点，即维护国家安全。其中，第4条明确要求“维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力”。数据安全源于我国《国家安全法》，属于国家安全体系建设中的重要组成部分。在数据作为新型生产资料和国家重要战略资源的今天，数据安全的重要价值和意义愈加凸显。[⑥]早在2014年，习近平总书记在中央国家安全委员会第一次会议中就明确提出要建立国家安全体系。2015年修订后的《国家安全法》便贯彻吸收了这一“总体安全观”的理念和精神，将“统筹内部安全和外部安全、国土安全和国民安全、传统安全和非传统安全、自身安全和共同安全”作为安全工作的重要内容，国家安全已经辐射政治、经济、文化、军事等各个领域。

作为《国家安全法》的下位法，《数据安全法》的制度价值统合于国家安全这一总体国家安全观。一方面，国家应对重要数据拥有实际的控制支配权，避免被其他国家或组织非法操控、干扰、窃取或泄露；另一方面，确保数据的宏观安全，防控因数据处理而引发的国家主权、公共利益以及企业和公民的权益受损威胁。同时，贯彻国家安全制度中的全流程安全管理机制，《数据安全法》建立了事前“风险评估、报告、信息共享、监管预警机制”，事中“安全审查监管机制”以及事后“应急处置机制”。

然而，通信、网络技术的快速发展，在带来便捷性的同时亦引发了新的国家安全风险。以云计算为例，其突破了对传统电脑物质载体的存储要求，直接将数据存储于云端，也无须信息技术的硬件支持。[⑦]大量存储于国界之外的云端数据，直接影响了国家对其国内数据的控制。事实上，数据作为技术的产物，控制核心技术意味着控制了数据资源，这也导致了国家与国家之间由于信息技术的不均等引

发的数据主权层面的博弈。也就是说，一方面，信息技术强国利用其技术优势，不仅对其本国数据进行了有效控制，还对其他国家的数据进行肆无忌惮的收集、监测、分析和挖掘，其中“棱镜门事件”无疑是美国安全部门窃取国外数据的典型例证。而且，美国还垄断着全球互联网的战略资源，[8]拥有全球影响力最大的网络运营商和通信服务商，[9]在高科技领域和用户数量方面具有无法比拟的强大支配力。另一方面，大多数发展中国家及最不发达国家困囿于技术水平有限，无法与美国为代表的技术强国相抗衡，不能有效保障自身的数据安全和国家利益。

针对无国界边界的数据空间，一国对数据进行有效控制的路径不能也无法仿效美国利用技术优势的单边控制主义，而应通过与其他国家的公平互利合作加以实现。在国际社会语境下，开展国际合作、坚持主权平等，维护共同安全和利益是所有国家的义务和使命。数据主权合作理应体现国家间的平等性、双赢性、互利性，不能以损害甚至牺牲其他国家利益为代价来满足本国的发展，所有国家不分强弱大小，都有平等参与制定数据领域国际规则的权利。《数据安全法》亦秉承这一原则，其中第11条提出“国家积极开展数据安全治理、数据开发利用等领域的国际交流与合作，参与数据安全相关国际规则和标准的制定，促进数据跨境安全、自由流动”。此外，基于公平目标，国际社会应对广大发展中国家特别是最不发达国家提供数据技术支持，以提升其控制和管理本国数据的能力，防范外来的数据霸权、恐怖主义等数据安全威胁。

二、数据安全法的管辖效力

按照传统国家主权理论，主权是国家与生俱来的对内最高统治权力和对外独立的权力。国家主权延展至数据空间，主要表现为两个方面：一是对数据的管辖权，即国家对本国数据的治理；二是当国家遭受外部数据窃取、监控或攻击时进行防御的权利。随着通信及网络技术的发展，数据已经成为一国的基础性战略资源，由于其所承载的信息还关涉文化、价值、意识形态等内容，各国都积极主张对本国数据的生产、开发和利用等权利。加之，一个国家不可能独占性地控制与其领土、企业以及公民等的所有数据，数据的跨境存储、利用及传输往往会涉及多个国家及地区，数据控制者、使用者、处理者在地理位置上也存在事实上的分离甚至是跨国界，这也引发国家之间数据主权的深层次冲突。

数据管辖权作为国家主权的重要表现形式，是指一国对其数据生成、存储和传输的物理设备以及相关服务等享有维护、管理和利用的权利。[10]国家对数据管辖权的行使也遵循传统的国家管辖权原则，即属地管辖、属人管辖、保护性管辖和普遍性管辖等原则。我国《数据安全法》第2条则遵循了属地管辖、属人管辖和保护性管辖原则。即，只要在中国境内开展数据处理活动及其安全监管，无论是中国境内的组织、个人还是中国境外的组织、个人，都适用本法。如果境外的组织或个人虽然没有在我国境内开展数据处理活动，但是其内容或性质会损害我国的国家安全、公共利益或其他公民、组织的合法权益，执法机构仍有权依据数据安全法追究上述主体的法律责任。

从目前数据领域的立法规范看，我国基本采用了较为谨慎的“被动型防御”策略，即强调对重要数据的出境管控，而并不积极主张数据的跨境调取。对于来自外国司法或者执法机构的调取数据请求，我国遵循的是“条约优先、平等互惠”原则，采取逐一报送主管机构批准的控制机制。为了使报告义务真正落地实施，《数据安全法》还规定了法律责任条款（第48条第2款）。同时，为规范重要数据出境活动，《数据安全法》第31条采用“二分法”的方式，对于关键信息基础设施的运营者在境内运营中收集和产生的重要数据出境，适用《网络安全法》的规定[11]；其他数据处理者的重要数据出境，则由国家网信部门会同国务院有关部门制定。为了细化《网络安全法》第37条规定，国家网信办分别于2017年和2019年出台两版有关信息数据出境安全评估办法〔《个人信息和重要数据出境安全评估办法（征求意见稿）》与《个人信息出境安全评估办法（征求意见稿）》〕，[12]这也从侧面反映出个人信息出境与重要数据出境在安全评估原则及规则内容等方面存在重大差异，宜采取单独立法的模式。

与之形成鲜明对比的是，以美国和英国为代表的西方国家积极谋求跨境数据管辖权，在跨境数据

调取方面采取“主动获取”策略，并明确赋予执法机构向其海外企业调取数据的法定权力，为其跨境数据的访问和获取扫清障碍。

早在2001年恐怖袭击之后，为了切断基地组织及其他恐怖组织的资金流，根据《国际紧急经济权利法案》美国政府启动了恐怖分子资金追踪计划（Terrorist Finance Tracking Program, TFTP），秘密地从国际银行间转账的环球银行金融电信协会（SWIFT）获取金融数据。[13]而最终促使美国扩大执法机构的境外数据获取权的直接原因，就是始于2013年微软与美国司法部之间的重大隐私权案。当时负责调查一起毒品走私案的检察官们获得了一份搜查令，要求微软提供保存在都柏林的微软服务器上的、该案嫌疑人的相关电子邮件。微软质疑美国政府签发的搜查令是否涵盖了存储于爱尔兰服务器上的邮件数据。司法部则认为，由于微软总部设在美国，所以检察官们有权获得这些数据。[14]在联邦最高法院对该案做出裁决之前，美国国会在短时间内便通过了《澄清境外数据合法使用法案》（CLOUD法案），并于2018年3月23日由特朗普总统正式签署。

CLOUD法案赋予美国政府调取存储于他国境内数据的合法权利，即在数据主权判断标准这一问题上，法案适用了“数据控制者标准”，不管数据是否在美国境内存储，只要该数据控制者属于美国企业，即便是在海外的美国机构，其执法机构也可以单方面向其主张获取该数据。[15]但对于“适格外国政府”调取存储在美国境内的数据，CLOUD 法案第五部分做了规定，包括三方面：一是由美国国会来认定“适格外国政府”，评判的标准和要求具有较强的主观色彩，如该外国政府是否有完善的个人隐私或数据保护法制，是否尊重人权等；如果被认定为“适格外国政府”后，还需要与美国签署双边协定；二是如果“适格外国政府”调取位于美国境内的数据时，该法案提出了比较苛刻的条件，如该外国政府的调取行为，应与严重犯罪行为密切相关，需提供确定的账号、住址等；三是调取令须有国内法的合法依据，并受本国司法机关或其他监督机构的审查监督等。[16]事实上，能够成为“适格外国政府”要求就不低，即便符合条件可以向美国政府申请调取数据，该行为还受到重重约束和限制，其所遵循的差异性标准可见一斑。

显而易见，在数据主权问题上，美国采取对内对外“双重标准”：一方面严格限制其他国家对存储于美国数据的获取，另一方面美国执法机构却可以合法地调取存储于美国境外的数据。CLOUD法案最显著的变化，就是以“数据控制者标准”取代地域边界，实质上抵销了其他国家试图通过数据本地化以保护自身数据安全的努力，而美国则可以通过其遍及全球的互联网巨头公司牢牢地将数据主权控制在自己手中。

虽然英国在境外数据获取方面也采取主动策略，但相比美国激进的“双重标准”，英国则采取了更加温和的合作态度。2018年，英国审议了《犯罪（境外提交令）法案2018》。该法案授予了英国执法机构依据英国法庭命令，在与英国签订相关国际协议的国家或地区直接获取境外数据的权力。该法案通过建立“境外提交令”机制，赋予英国执法机构向英国法官申请该命令，以直接要求企业提交境外数据的权力。需要注意的是，根据该法案的规定，“境外提交令”仅在与英国签订了相关国际协议的国家或地区才有效。应该说，该法案为英国通过双边或多边国际合作协议模式开展执法机构境外数据获取确立了基本框架。

与此同时，司法机关域外管辖权扩张的情形也不少见，如加拿大公司Equustek Solutions Inc.（以下简称ESI）诉谷歌公司案。该案件源于ESI要求谷歌删除侵权的网站链接，但谷歌只删除了在加拿大领域内的链接，其他国家领域内的链接依然存在，ESI公司认为仅仅这样是远远不够的，因此向加拿大法院起诉要求谷歌公司删除在全球领域内的所有链接。加拿大法院支持了ESI的诉请，在全球范围内发布禁令，开创了法院域外管辖权的先例，[17]但这也引发了数据主权冲突风险。

因此，合理界定数据管辖权行使的范围是数据主权合作的重要前提。我国《数据安全法》在其管辖效力问题上，不仅要管住重要数据出境这一关，明确相应的数据出境限制措施及制度安排。[18]更重要的是，面对来自境外的数据调取要求，出于国家安全的考量，理应作出相应的规范，以约束他国过分膨胀的公权机构的数据获取要求，亦需在法律层面

明确涉及跨境数据调取相关主体的义务与责任。同时，还应特别强调，即便是在境外的数据活动，只要是危害到我国的国家安全、公共利益、企业和公民权益的，都应在我国法律的管辖范围内。对于数据恐怖主义等影响国际社会稳定和秩序的国际犯罪行为，则可遵循普遍性管辖原则。鉴于广大发展中国家的数据技术水平有限，无法通过自身力量管辖域内外数据来应对上述行为，就需要在国际社会上寻求集体合作的安全机制，在集体自卫权基础上实施跨国惩治。

三、数据安全法的核心制度：数据的分级分类

在全球经济一体化的背景下，数据的跨境流动日趋频繁，在带来经济利益的同时也会蕴含数据泄露风险，更有甚者直接对国家安全和数据主权造成威胁。但如果完全禁止数据跨境流动又会引起其他国家的政治敌视，被贴上“保护主义”的标签。如何在确保国家安全的基础上建构有效的数据跨境流动制度，如何能够实现重要数据的保护与非重要数据的自由流通之间的平衡。其中，数据分类分级制度就是解决上述问题的关键，不仅可以防止重要数据的泄露或非法利用，还可以确保非重要数据的跨境自由流动，最大限度地发挥数据的经济价值。

在《大数据产业发展规划（2016—2020年）》中，已经将分类分级作为数据管理要点。数据分类分级制度是构建整个数据安全管理机制的前提和基础，数据分类是为了区分不同数据类别和管理对象，指向监管目标，而数据分级则是根据不同级别实施不同程度的保护，指向具体的保护措施。从顺序上看，数据先分类再分级，即在数据分类的基础上按照重要程度和危害程度再分级，以实现不同级别匹配相应的数据安全保障措施。[19]应该说，对数据进行数据分类分级管理，可以对不同类别和不同级别的数据采取不同的安全和保护措施，将安全保护措施和监管力量聚焦到重要数据、核心数据，以尽可能释放数据红利。如果不加区分地采取一刀切的监管措施，必然会阻滞数据的合理使用，也不利于数字经济的健康发展。重要数据的保护强度显然高于其他级别的数据。重要数据的概念、范围和监管，也是目前普遍关注的焦点问题。

在《数据安全法》公布之前，《数据安全管理办法（征求意见稿）》以及《数据出境安全评估指南（征求意见稿）》都曾经尝试对什么是“重要数据”进行相应的界定和列举，但都没有清晰明确的分类分级标准。[20]前者给出了“重要数据”的定义，并列举哪些不是重要数据；后者则在附录A中列举了人口健康、金融、征信、交通运输、邮政快递、地理信息、国防军工、化学工业、有色金融、装备制造等27个门类的重要数据名录和主管部门，并附加了兜底性规定，授权行业（领域）主管部门可根据行业（领域）发展、评估实践，判断是否存在其他重要数据并及时更新指南。

《数据安全法》第三章明确了数据安全制度的具体内容，数据分类分级制度是最重要的安全保障机制。《数据安全法》第21条对数据分类分级制度做了框架性规定，以加强对重要数据的法律保护。其中，按照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、公共利益或者公民、组织合法权益造成的危害程度，作为数据分类分级的原则性标准。在此基础上要求各地区、各部门确定本地区、本部门以及相关行业、领域的“重要数据保护目录”。

与2020年7月公布的一审稿不同的是，《数据安全法》明确了重要数据目录的认定权属于国家事权，由“国家数据安全工作协调机制统筹协调有关部门制定重要数据目录”。一审稿曾将重要数据目录认定权力下放到地方和部门，与《数据出境安全评估指南（征求意见稿）》授予行业主管机关确定重要数据名录的思路有明显差异。如果重要数据的目录认定权下放到各个地方，容易出现某一类数据各地方认定的类别并不一致的问题，不同地方的重要数据范围可能存在较大差别，由此引发适用层面上的混乱。《数据安全法》正式文本则及时回应这一问题，将重要数据目录的认定权归属于中央，更符合我国现阶段数据产业发展的实际需求。与此同时，《数据安全法》还创造性地提出“国家核心数据”这一概念，[21]由此在数据分类分级制度基础上，形成了一般数据、重要数据、国家核心数据的基本

数据类别，不同类型的数据将采用不同的数据安全保护措施。这也意味着如果落入重要数据、国家核心数据的范畴，数据处理者需要履行组织及人员保障、定期风险评估等“加重义务”。

关于数据的分类分级制度，由于不同行业及领域所涉数据的属性也不尽相同，在《数据安全法》出台之前，大都由相关行业主管部门负责该领域的数据分类分级工作，并制定了相应的法律规范及行业标准。例如，《科学数据管理办法》（2018）第10条规定，“由科学数据中心负责科学数据的分级分类、加工整理和分析挖掘”。《工业数据分类分级指南（试行）》（2020）第8条，“根据不同类别工业数据遭篡改、破坏、泄露或非法利用后，可能对工业生产、经济效益等带来的潜在影响，将工业数据分为一级、二级、三级等3个级别”。中国人民银行于2020年发布《个人金融信息保护技术规范》4.2，“根据信息遭到未经授权的查看或未经授权的变更后所产生的影响和危害，将个人金融信息按敏感程度从高到低分为C3、C2、C1三个类别”。应该说，数据分类分级管理已在一些重点行业和领域进行了有益的尝试。与之相类似，澳大利亚也按照重要性程度对政府数据进行分级标识，分为不需要额外安全保护的数据和需要额外安全保护的数据。而对于后者，澳大利亚则采取了保护性标识与不同管理措施结合的方式。保护性标识类型包括三种：安全分类标识；传播限制标识以及警告标识。其中，“警告标识主要用于可能影响国家安全的特定分类数据，是在保护性标识基础上进行的额外要求的特殊标识类型。当然，相关机构可出台符合自身情况的分类指南以指导工作人员对数据进行分级”。[22]

需要注意的是，2020年9月23日中国人民银行发布并施行的《金融数据安全 数据安全分级指南》（JR/T0197—2020），“根据金融业机构数据安全性遭受破坏后的影响对象和所造成的影响程度，将数据安全级别由高到低划分为五级”。其中，对金融领域的重要数据进行了描述，即“重要数据是指通常主要用于金融业大型或特大型机构，金融交易过程中重要核心节点类机构的关键业务使用，一般仅针对特定人员公开，且仅为必须知悉的对象访问或使用”。附录C还进一步对“重要数据”进行了概念界定，并列举了其外延范围，即“重要数据可包括宏观特征数据、海量信息汇聚得到的衍生特征数据、行业监管机构决策和执法过程中的数据，以及关键信息基础设施网络安全缺陷信息等”。在此基础上，对“重要数据”进行了范围上的排除，明确了“企业生产经营和内部管理信息、个人信息”不是重要数据。应该说，该指南为金融数据的具体分类提供了标准，不仅可以在最大程度上发挥非重要数据的流通价值，还为相关监管机构开展数据安全检查与评估工作提供了依据。

数字经济时代，只有在保证国家安全的前提下实现数据的自由流动，才契合国家最根本最长远利益，这就从本质上要求从立法层面完善以分类分级为基础的数据管理制度，谨防重要数据和国家核心数据外泄，并保障其他数据的依法有序流动，形成一体两面的数据跨境流动规则。申言之，在数据出境方面，应建立起数动态追踪机制和安全风险评估机制，特别是对个人信息和重要数据明确安全评估措施，追踪其传输流向、地域、规模及使用情形，建立数据安全的检测预警机制和应急处置机制。

安全秩序的形成从来不是仅仅依靠内心的自觉遵守及道德力量，其真正的保障内核在于法律规范的确立和维护。在数字科技发展的大背景下，主权国家不仅存在传统军事安全的隐患，更要面临来自非传统安全的风险和挑战，特别是居于数字科技权力顶端的国家的技术威胁，而跨境数据流动的急剧增长又不断冲击着领土、领海、领空在物理空间所构建的传统安全区域。在“数据驱动经济发展”的理念下，各国都在积极开展数据的开发、利用、共享等活动，以求最大限度挖掘数据的经济价值。尤其是以美国为代表的科技强国，明确反对他国数据主权并积极倡导网络自由、数据开放和数据跨境自由流动。面对国际复杂形势，我们更应清醒地意识到，没有数字科技的硬实力和足以与之配套的规则体系制度等软实力，盲目进行数据开放和跨境数据自由流动，只会徒增国家安全风险。我国作为一个网络及数据技术的后发型国家，应高度警惕来自数字空间的新型安全风险。一方面，在本国之内，有必要在法律层面对本国数据的收集、存储、传输、使用、公开等处理行为进行有效监管，明确我国数据的

管辖效力，以保障数据的安全性、真实性和完整性；另一方面，在本国之外，积极通过双边或区域性多边协定方式协调本国与他国之间的数据管辖权冲突，有效管理和控制涉及国家安全利益、公共利益以及公民、组织合法利益的数据，以捍卫国家数据主权。

注释

①参见许可：《数据安全法：定位、立场与制度构造》，《经贸法律评论》2019年第3期。

②参见维克托·迈尔·舍恩伯格等：《大数据时代》，盛杨燕、周涛译，浙江人民出版社2013年版，第28页。

③参见李建新：《两岸四地的个人信息保护与行政信息公开》，《法学》2013年第7期。

④参见郑成思：《信息、信息产权与个人信息保护立法》，法律出版社2004年版，第23页。

⑤参见纪海龙：《数据的私法定位与保护》，《法学研究》2018年第6期。

⑥该法第2条规定，国家安全是指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。第25条，国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，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；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。

⑦Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption and Government Back Doors in the Web 2.0 Era*, Journal on Telecommunications and High Technology Law, Vol. 8, 2010, p361.

⑧全球互联网根服务器有13台，唯一的主根服务器在美国，其余12台辅根服务器中有9台在美国。参见奕文莉：《中美在网络空间的分歧与合作路径》，载《现代国际关系》2012年第7期。

⑨根据“2019全球300个最有价值的电信品牌榜”显示，美国电信运营商继续占据了主导地位，其中AT&T（美国电话电报公司）、Verizon（威瑞森无线公司）分别位居第一和第二位。而在2020年全球十大互联网公司排行榜上，苹果、谷歌、微软、脸书、亚马逊等美国公司也是名列前茅。

⑩参见蔡翠红：《云时代数据主权概念及其运用前景》，载《现代国际关系》2013年第12期。

⑪《网络安全法》第37条规定，关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当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；法律、行政法规另有规定的，依照其规定。

⑫其中，《个人信息出境安全评估办法（征求意见稿）》的核心制度安排，就是通过网络运营者与个人信息接收者签订合同方式明确网络运营者与接收者各自承担的责任和义务。其本质是通过行政监管对合同条款施加内容要求，但仍然存在行政干预过度的嫌疑。参见张继红：《应进一步厘清个人信息出境的权利义务安排——简评<个人信息出境安全评估办法（征求意见稿）>》，载《上海法治报》2019年7月24日B06版“法治论苑”。

⑬2001年10月，美国财政部外国资产控制办公室(Office of Foreign Asset Control)与中央情报局(CIA)合作，向SWIFT发出了调取数据的传票。2001年至2006年期间共发出约64份行政传票，涉及上万个银行转账账户以及个人信息。欧盟和比利时有关机构批评SWIFT违反了欧盟个人数据保护法的规定，有关金融交易的信息只能用于与银行业相关的目的，而不能用做他途，如调查恐怖分子的资金来源。但美国方面认为，这些信息对于反恐斗争至关重要。2007年6月，欧盟与美国就利用SWIFT金融数据用于打击恐怖主义达成协议。See Sharman J C .*Privacy as roguery:Personal Financial Information in an age of Transparency in an Age of Transparency*, Public Administration, 2010, 87(4):717-731.

⑭2016年，纽约第二美国上诉法院作出了一项对微软有利的裁决，认为这些电子邮件超出了1986年美国《存储通讯法案》（Stored Communications Act）规定的国内搜查令的范围。特朗普政府对第二美国上诉法院的裁决表示不服，向联邦最高法院提出了上诉。

⑮但如果服务提供者认为存在以下两种情况，则可以不提供相应信息：消费者或者用户不是美国人且不居住在美国；服务提供者提供信息可能实质性地违反合格外国政府的相关法律。参见洪延青：《美国快速通过CLOUD法案 明确数据主权战略》，《中国信息安全》2018年第4期。

⑯参见翟志勇：《数据主权的兴起及其双重属性》，《中国

法律评论》2018年第6期。

⑰Martin Aquilina.Google Inc.v.Equustek Solutions Inc.,a Commercial Perspective.July 21,2017.at:https://hazlolaw.com/google-inc-v-equustek-solutions-inc-commercial-perspective/

⑱2021年7月初，国家网信办连续发布了对赴美上市企业，诸如滴滴、运满满、货车帮等实施网络安全审查的公告。上述企业的境外上市，可能存在涉及个人信息与重要数据泄露的国家安全风险。2021年7月6日，中共中央办公厅与国务院办公厅专门发布《关于依法从严打击证券违法活动的意见》指出要“完善数据安全、跨境数据流动、涉密信息管理等相关法律法规”，“压实境外上市公司信息安全主体责任”以及“加强跨境信息提供机制与流程的规范管理”。7月10日，国家网信办就修订《网络安全审查办法》向社会公开征求意见稿，其中第6条明确规定“掌握超过100万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查”。以上种种监管动向都表明，关键基础设施运营者、重要和国家核心数据的处理者以及达到规定数量的个人信息处理者在信息与数据全生命周期的处理活动中应始终把国家安全放在首位。

⑲以工业数据为例，工业企业结合生产制造模式、平台企业结合服务运营模式，分析梳理业务流程和系统设备，考虑行业要求、业务规模、数据复杂程度等实际情况，对工业数据进行分类梳理和标识，形成企业工业数据分类清单。在分类基础上，再根据不同类别工业数据遭篡改、破坏、泄露或非法利用后，可能对工业生产、经济效益等带来的潜在影响，将工业数据进行分级。

⑳《数据安全管理办法（征求意见稿）》第38条规定，重要数据，是指一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据，如未公开的政府信息，大面积人口、基因健康、地理、矿产资源等，一般不包括企业生产经营和内部管理信息、个人信息等。《数据出境安全评估指南（征求意见稿）》3.5规定，重要数据是指相关组织、机构和个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展以及公共利益密切相关的数据（包括原始数据和衍生数据）。经政府信息公开渠道合法公开的，不再属于重要数据。

㉑《数据安全法》第21条，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。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。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属于国家核心数据，实行更加严格的管理制度。虽然《数据安全法》并未对“国家核心数据”作出明确的定义，仅仅做了方向性的列举，但不等于说只要牵涉国家安全的都属于核心数据，其外延理应受到严格限定。事实上，也不太可能出现全社会广泛分布国家核心数据的情形。

㉒参见伦一：《澳大利亚跨境数据流动实践及启示》，载《信息安全与通信保密》2017年第5期。

The Institutional Construction of China’s Data Security Law from the Perspective of National Security

ZHANG Jihong

Abstract: Globalized data sharing and mobility has brought about tremendous impact on national security. National data security system has become an indispensable part of a nation’s security law system. Data Security Law was enacted at a proper timing. The implementation of the holistic view of national security stipulated in National Security Law constructs China’s basic data security administration system in the form of law, establishes the legislative mission of safeguarding data security and promoting data development, and defends our data sovereignty and its governing power at home and abroad. Based on data classifying and rating, the identification of “key data” is taken as a crucial task to establish a unified dual cross-border data mobility system. In coordination with Cyber Security Law, it can lay a solid foundation for an orderly, just, reasonable, and new system of data security governance.

Key words: national security; data security; data classifying and rating system; cross-border data mobility