Open Journal of Legal Science 法学, 2022, 10(5), 794-800
Published Online September 2022 in Hans. http://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2022.105101

Hans汉斯

论我国数据安全保护的实践与思考

方　悦

宁波大学，浙江　宁波

收稿日期：2022年7月8日；录用日期：2022年7月22日；发布日期：2022年9月8日

摘　要

数据作为国家一项重要的战略资源，是各国进行利益博弈的重要领域。随着大数据时代的到来，数据安全保护逐渐成为各国争议的焦点问题。由于中国在数据治理领域起步较晚，仍然存在立法不完善、技术创新能力弱、国际合作不足、治理不力等问题。中国需要全面、系统地分析影响数据安全的各种主要风险因素，明确数据安全和数据自由的界限，明确网络数据主权的归属，构建合理的数据安全治理制度体系。

关键词

数据安全保护，法律属性，国际条约

On the Practice and Thinking of Data Security Protection in China

Yue Fang

Ningbo University, Ningbo Zhejiang

Received: Jul. 8th, 2022; accepted: Jul. 22nd, 2022; published: Sep. 8th, 2022

Abstract

As an important strategic resource of countries, data is an important area for all countries to play interest games. With the advent of the era of big data, data security protection has gradually become the focus of controversy among various countries. As China started relatively late in the field of data governance, there are still some problems, such as imperfect legislation, weak technological innovation capacity, insufficient international cooperation, and ineffective governance. China needs to comprehensively and systematically analyze various major risk factors affecting data security, clarify the boundary between data security and data freedom, clarify the ownership of network data sovereignty, and build a reasonable data security governance system.

文章引用: 方悦. 论我国数据安全保护的实践与思考[J]. 法学, 2022, 10(5): 794-800.
DOI: 10.12677/ojls.2022.105101

Keywords

Data Security Protection, Legal Attributes, International Treaty

1. 引言

科学技术的发展使得数据逐渐趋于复杂，数据处理活动繁杂，安全风险扩大。近年来，各国在数据安全上对中国企业实施制裁，如印度查封了 59 款中国 App；美国的净网行动以及特朗普政府针对抖音海外版 TikTok、微信的禁令。而国际上尚未形成对数据安全保护的统一的国际条约，实际上，自 2020 年以来，中国已相继签署《区域全面经济伙伴关系协定》(RCEP)和《中欧双投资协定》(BIT)，并向国际社会发起《全球数据安全倡议》，又积极申请加入《全面与进步跨太平洋伙伴关系协定》(CPTPP)。中国需要全面、系统地分析影响数据安全的各种主要风险因素，准确把握全球数据安全趋势，进一步优化中国在全球数据安全治理中的战略选择。

2. “数据安全”保护面对的挑战

2.1. “数据安全”的法律属性辨析

在谈起数据安全保护问题前，首先要明确保护的对象，即“数据”的基本概念和基本属性。在立法上，数据和信息并没有十分严格的区别。从数据和信息的外延来看，数据只是信息表达的一种方式，除数据外，信息还可以通过其他方式来表达。[1]在法律上，数据和信息的区分并不十分严格。数据传递只是数据信息对外表达信息的另外一种传递方式，除传送数据自身外，信息自身还同时可以被通过各种其他传送方式传递来被表达。在这种情况下，数据安全和信息安全息息相关，因此在数据安全保护中对信息安全进行规制是理所应当的。事实上对“数据”的定义在理论界和实务界一直存在着较大的分歧。在域外方面，被各国立法所推崇的欧盟《一般数据保护条例》(以下简称 GDPR)从个人数据方面对数据的概念做出了明确。[1] 而在国内，在《数据安全法》颁布之前，我国对数据的定义在各种法律、法规及规章中都有提及。[2] 其次在于数据安全的基本法律属性，早期数据安全主要集中在个人信息泄露以及对隐私权的保护，因此各国关于数据安全保护往往从个人数据保护立法角度出发。但是目前只能从国际私法理论上来对数据信息安全进行具体规制，关于怎样对一些非隐私方面的公共数据如何进行法律保护，各国还没有达成共识。而且私法上对于个人数据的法律保护常常还涉及到公法上对公共资产安全管理和维持网络社会秩序安全等其他方面法律的相对价值加以考量。因此法律对数据隐私的有效保护也不仅建立在个体私权意识层面，还应当通过整个国家公权力制度层面上来对数据信息安全问题进行保护。虽然现在国内外理论界对“数据安全保护”的具体概念内涵在理论界定层面上还是略有差异，但就总体框架上的定义来看，可以将其定义为国际行为体对数据从产生、收集、处理、存储、修改、流动使用等每个活动环节上提供有效的信息安全及保护，也包括对数据的封锁和擦除。

[1]GDPR 第 4 条第 1 款规定：“个人数据是指向一个已识别或可识别的自然人(数据主体)的信息。”
[2]如《中华人民共和国民法典》第 127 条、《中华人民共和国网络安全法》第 76 条以及《中华人民共和国电子商务法》第 25 条都提及了“数据”的概念。

2.2. 全球“数据安全”问题的困境

数据权利是指主体以某种正当的、合法的理由要求或吁请承认主张者对数据的占有，或要求返还数据，或要求承认数据事实(行为)的法律效果。[2]由于数据存在着分享的特性，这要求数据必须通过传播来实现自己的经济价值。而在传播过程中，自然关系到数据传播中所带来的影响——对个人信息、公共利益以及国家安全所带来的影响。当前，各国际行为体机构对全球数据的安全保护并未能够形成完全统一高效的国际治理体系框架，全球数据的安全治理规则长期停留于国际单边、双边条约以及经贸规则中。但是，数据安全保护关系到全体公民经济生活以及国家安全发展等方面。因此，全球数据安全保护方面的治理问题也早已经引起国际社会的重视：1990 年，以联合国名义发布了《计算机处理的个人数据文档规范指南》公告，对个人数据信息治理活动给予了规范性指导。此后，美国经济合作与发展组织公约(OECD)组织、美国亚太经济合作组织协定(APEC)组织和世界贸易组织规则委员会(WTO)等组织纷纷积极开展了多边经济规制协调行动，致力于加快把多边数据安全战略合作行动体系向国际纵深推进。然而，面对风险性增加和不确定性问题日益倍增下的国际数据安全保护现状，关于保障全球数据安全的多边治理规则的制定以及一揽子解决方案等却依然未能取得重大实质性进展，当前复杂的数据国际协调合作的机制问题仍然广泛散落在于各类多边、区域性组织体系以及全球经贸规则之中。其中欧盟 2018 年 5 月 25 日生效实施的 GDPR 就为全球数据安全隐私保护树立了一个典范。个人信息保护向来是数据治理的重要方面，目前全球共有 127 个国家制定了个人信息保护相关法律。[3]随着互联网的兴起，数据共享的途径越来越便利。与此同时，数据全球化也引发了世界各国对数据安全和数据主权的担忧。随着全球数字经济时代来临的时代到来，日益严峻的全球性数据基础设施安全管理问题与越来越错综复杂的国际局势矛盾相互碰撞交织，导致当今世界各国围绕影响着数据安全规则体系制定的矛盾也不断升级激化，进而可能引发更为全球性重大的互联网数据安全治理新问题。与此同时，个别西方国家的滥用数据及霸权主义等行为也导致国际层面对于数据安全规则体系的完善制定问题难以达成普遍共识，全球数据信息安全问题治理过程仍然进度十分缓慢。

2.3. 我国“数据安全”立法面临的挑战

而对于我国而言，随着我国不断推广和落实“互联网+”战略，数据共享为我国国民的生活带来了极大的便利。与此同时，中国高度重视数据安全的相关议题，陆续出台了《网络安全法》、《个人信息保护法》等一系列关于数据安全保护的法律法规以及规范性文件。随着《数据安全法》的颁布与施行，我国关于数据安全保护的立法更加趋于完善。《数据安全法》为全球数据安全治理贡献中国智慧和中国方案。[3]但数据安全依旧面临很多难点：首先随着网络科技的越来越发达，数据安全治理所面临的环境将越来越严峻。二是各国关于数据立法上是存在差异的，这给数据跨境流通的保护带来不小的挑战，数据犯罪很可能利用他国的法律来对中国的数据法进行法律规避，这给我国主权会带来严重的威胁。三是在于数据主权问题，由于现在科技越来越发达，各种加密手段不断发展，在对非法数据问题上，面临的一个重要问题就是数据主权归属。数据往往通过网络进行交易，而一旦对数据来源无法查找时，相关责任主体如何认定呢？因此关于我国数据安全保护问题依旧有必要进行探讨。

3. 我国数据安全保护的实践

3.1. 国内立法上的发展

随着经济社会的快速发展，大数据时代的到来，数据逐渐成为一个国家的战略性资源，数据安全逐渐成为国家安全的一部分。按照国家总体安全观的要求。数据安全是关系到国家安全的至关重要的一环。

[3]参见中国网信网，http://www.cac.gov.cn/2021-06/15/c_1625341228851523.htm。

2020 年 12 月，中共中央印发的《法治社会建设实施纲要(2020~2025 年)》中明确规定了国家要建立健全数据安全管理制度、研究制定个人信息保护法。目前典型的关于数据安全的法规包括：2021 年刚发布的《数据安全法》和《个人信息保护法》，同时 2016 发布的《中华人民共和国网络安全法》中也对网络数据安全作出了系统的规定，此外国家网信办发布的《网络安全审查办法(修订草案征求意见稿)》也专门增补了数据安全相关要求，正式发布后也将是各关键信息基础设施数据处理者所应重点遵守的法规之一. 另外还有很多其他法规(如《中华人民共和国民法典》《中华人民共和国测绘法》《中华人民共和国证券法》等)也涉及数据安全相关规定，其中 2021 年 6 月 10 日通过的《数据安全法》，这部法律是数据领域的基础性法律，也是国家安全领域的一部重要法律。这部法律成为我国开展数据活动的适用法律，它不仅包括境内的适用，同时对境外的数据保护也具有域外适用效力。[4]这在一定程度上对《网络安全法》起到了补充作用。当前数据已经成为最具有价值的战略资源，数据跨境流动已经成为常态，在此背景下，将数据安全保护涉及到域外也是具有十分现实的意义。其次本法中对于数据的定义具有里程碑的作用。在此之前，各种法律对数据的定义含糊不清，也存在着与信息混淆的法条。而这部法律中对数据的界定在一定程度上克服了其他定义中存在的边界不明的缺陷。

3.2. 国际数据安全保护中的“中国方案”

如何在国际上舞台上发挥中国的力量，提出解决“数据安全”问题的中国方案是我国近几年所前进的方向。中国数据安全规则的构建既要维护我国的利益，也要兼顾他国所关切的方面；既要符合我国传统的法律体系框架，也要遵守国际法的基本原则。而实际上，自 2020 年以来，中国已相继签署《区域全面经济伙伴关系协定》(RCEP)和《中欧投资协定》，并向国际社会发起《全球数据安全倡议》，又积极申请加入《全面与进步跨太平洋伙伴关系协定》(CPTPP)，呼吁各国秉持发展和安全并重的原则，平衡处理技术进步、经济发展与保护国家安全和社会公共利益的关系。[4]中国作为数据大国，一直秉持着加强国际间数据安全治理合作的理念，积极推行与各国之间的交流合作。加入这些国际条约，能够在尊重他国数据主权的前提下和利益诉求的基础上，进而推进全球数据有序流动。但是如何能够有效的与各国践行这些数据安全的条约仍旧需要努力。自从 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》提出数据跨境流动的法律命题之后，各国开始对数据跨境流动采取法律措施，目前世界上形成了以美国、欧盟为代表的两大治理范式。[5]这种区域间的立法模式对于国际之间的数据安全保护治理具有很好的借鉴意义。这两种模式都提出了“长臂管辖”的规则。欧盟出台的 GDPR 被称之为“史上最严个人信息保护法规”。其严苛程度不仅体现在高标准个人信息保护责任，还极大地扩张了欧洲个人信息保护监管机构的管辖范围。[6]在 GDPR 数据条例中，无论数据的处理行为是否发生在欧盟内，只要其对数据的处理者和控制者是设立在欧盟内，那么其就在欧盟管辖范围内。甚至不在欧盟内时，出于对数据的监管，GDPR 依旧可以适用。这种“长臂管辖”规则之下，会对数据主权国带来严重的侵犯。就个人的数据主权来说，数据隐私权是其中较为重要的部分。在隐私权方面，欧盟与美国的法律呈现出不同的特点。欧盟的隐私法更关注保护“尊严”，而美国的隐私法更强调保护“自由”。[7] 2019 年 3 月，美国国会研究局发布了《数据保护法概况》报告。这份报告虽然采取了“数据保护”一词，但是其主要个人数据行为规范。对于“数据保护”的含义，报告指出，作为一个立法概念，“数据保护”融合了数据隐私和数据安全两大领域。前者包括如何控制个人数据的收集、使用等方面；后者包括如何保护个人数据免受未经授权的访问与使用，以及如何解决未经授权访问的问题等方面。[8]从以上关于欧盟 GDPR 和美国《数据保护法概况》来看，国际各国为了本国的利益，在立法上会强调他国数据的自由流动，而对其本国的数据则采取严格的保护措

[4]《数据安全法》第 2 条规定：“在中华共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。”

施。这种单方单边和霸权的做法是不利于国际数据安全保护立法规则的构建的。而中国如何在如此复杂的国际局势下找到自己的定位，积极与国际安全保护制度接轨，这是当今亟需解决的问题。

4. 我国数据安全保护的策略思考

4.1. 平衡数据利用与数据安全保护

在《全球数据安全倡议》中，我们再次呼吁：在各国应坚持重视发展和安全的原则，平衡技术进步、经济发展、国家安全和维护社会公共利益的关系。目前，随着数据大国的“数据战”崛起，特别是以美国为首的全球数据霸权斗争和数据单边主义正在盛行，因此中国在积极参与捍卫全球数据安全权利的诉讼过程中，必须时刻坚持要保护自身国家经济安全、公共利益和个人隐私，同时考虑到数据隐私保护问题和数据跨境流动。特别是中国要在数据利用和数据安全上找到利益平衡点。确定平衡点需要注意的一点是，过度限制数据流通，保护数据安全无助于发挥数据的社会价值和经济价值。但是，为了追求数据共享的经济价值，数据应用中的数据控制主体可以随心所欲。因此，立法必须限制与国家、企业和个人安全相关的数据在数据流通中，但在限制的同时，必须根据自己的发展需要开放国家之间的数据共享。如上所述，中国在全球范围内积极推进对数据安全的保护，在立法过程中，中国一贯重视尊重其他国家的数据主权和利益要求。有效促进全球数据安全的有序流动。因此，在当前复杂的国际形势下，中国必须实时应对全球数据安全领域新规则的变化，及时评估国际行为体的利益衡量和数据安全重点。这不仅可以有效地参考国外的立法创新，而且更有利于及时调整国内规范，科学地有效应对全球数据安全带来的挑战。

4.2. 明确网络数据主权的归属

网络数据主权是指我国网络空间系统中所谓的数字国家主权，是由一国有对我们本国的网络数据信息进行独立管理分配和合法利用后的一项独立法律自主权，同时它不受外界他国法律干涉侵犯和侵扰。当前网络数据权属问题是有关数据安全保护的一大困境，因为数据权属存在争议，数据产权无法精准的确立。具体而言，不同种类的数据在权利和内容上是存在差异的，在数据流通过程中，数据权利并不会完全的归属于一个主体。不同的数据主体之间的利益诉求是不同的，这就引发了数据主权上的冲突。其次，数据在流动监管时遇到的工作环境都是相当十分严格复杂严峻的，且数据跨境的监管也并没有制定统一规范的相关国际标准，因而对于实现全球数据流动安全跨境监管网络全领域覆盖、进行跨国数据跨境安全的监管与定责管理以及依法开展国际数据信息跨境和流动交易安全跨国监管面临的现实难得也都差异较大。数据安全在国际形势方面，大数据国家间的竞争博弈式发生改变，如若无法掌握数据主权，他国别有用心的数据干预必然会危害国家安全和国家主权。中国提出的互联网数据主权规则体系应该继续以互联网主权国家独立、平等相待和交流合作理念为基础指导。一个主权国家间无论综合国力强弱，无论存在互联网数据技术水平怎样的重大差异，都仍然应该共同平等自主享有互联网络数据主权。同时，制定中国全球数据主权规则时应注意以联合国网络空间命运共同体理念实践为理念指导，以多边合作国际共治原则理念为思想基础，促进未来全球数字经济健康发展，构建出国际普遍通行意义的网络数据主权领域合作机制规则。欧盟和我国美国出台的国际数据主权规则体系可以借鉴为制定中国规则提供比较有益经验的借鉴。中国应积极探索符合数据发展和国家利益的内容，提出具有中国特色内容的数据主权国际立法合作的方案。

4.3. 构建科学系统的数据安全治理制度体系

“宜细不宜粗”的数据安全立法风格是提高数据安全立法效力的关键因素。[9]从整个全球数据犯罪

治理领域来看，包括中国在内的欧洲许多重要国家现今基本上都已处在对数据及其安全法律治理新体系加以探索发展和逐步完善创新的阶段。中国数据安全治理制度体系主要由《网络安全法》《数据安全法》《个人信息保护法》这三部法律规章所构成。这些信息安全法律法规草案的顺利出台基本顺应住了当下国内外技术形势日新月异的技术发展，已经可以初步基本形成国际数据与安全产业治理法规的法律总体制度框架，但未来在立法实践的操作推进中也还急需进一步立足于全球视野，进一步规范细化各国数据及安全法律治理规范细则，为实现中国深度融合参与的全球数据产业安全及治理战略建立良好对话和基础。具体而言，一是要考虑根据不同类型的数据，提出了不同层次的数据安全标准要求。全面调查分析“关键数据”工程项目面临潜在的社会安全防范形势问题与重大风险，建立隐患分级及分类等级保护措施制度，有一定针对性有效地研究提出各项安全综合防控体系要求。二则是政府要通过对数据资产的数据全业务生命周期中进行数据全程的安全及风险状况评估监测和保密审查等监管，重视从数据内容的信息产生、形成、采集过程和传输存储全过程等多个环节上可能随时产生潜在的信息系统安全和漏洞暴露以及相关安全问题风险，做到安全提前风险预警，并加快建立国内统一完整的信息数据的安全及相关信息安全标准。三则是规定要同时对地方政府、企业、个人组织和公民其他各类组织依法在国家维护计算机数据存储安全事务中行使的具体权利义务职责作出更明确详细的相关规定。在严格赋予各类数据主体对数据信息的自由所有权、使用权、财产权、人格权、访问权、被遗忘权和信息可携权等其他诸多自由权利内容的权利同时，还要严格明确各方维护互联网数据信息内容安全运行的各自职责分工和相应义务，做到了责任权利要求相统一。

4.4. 积极开展并促进数据领域的国际交流与合作

互联网时代，数据在只有在流通过程中才能充分发挥其潜在的价值。而未来随着科技全球化步伐的日益推进，数据技术的更大规模和跨境信息流动趋势已经会成为行业常态。互联网技术快速的迅速发展也使得同世界各国社会的互依存合作程度将日益得到加深，国际社会已经日益演变成为这样一个代号“一荣俱荣、一损俱损”的网络命运共同体。在全球面对着这些国家层出不穷的互联网数据存储安全威胁问题时，没有任何这样一个国家能够独自地去妥善处理好数据储存安全及保护等问题。虽然各个国家对于跨境数据流动在数据安全保护规则制定中存在一定的差异，但积极开展国际间的交流与合作是当前促进全球数据安全成功的关键点。如果各国不采取合作的话，数据跨境流动会成为数据安全保护规则制定的最大阻碍，当然也不利于数据潜在价值的发挥，同时也会影响到企业的稳定运营。同时，为了确保最大限度充分地合理发挥全球数据基础设施的协同创新潜能和潜在生产力优势，主权国家领导人应继续基于高度包容性、互操作性强和充分公平和透明公开的共同原则，就促进全球数据网络安全及其治理进程的八项核心原则深入达成基本共识，并着手制定若干共同规则。中国在数据安全领域内开展的国际交流与合作是有待加强的，而且现行立法上存在着与现行国际规则并不统一。在此形势下，中国提出应重点加快立法探索与建立国际标准相适应新的网络安全国际统一治理合作机制、全球数字规则标准以及安全统一治理新框架。一方面，中国国家应当首先积极并主动积极地坐下去主动参与全球数据和安全领域治理、数据自由开发以及利用问题的相关多边磋商或着重点双边协议谈判，在共同尊重现有他国数据主权边界和自身利益相关诉求的基本前提指导下，尽快协商确立出统一有序的国际双边数据或相关多边组织跨境数据有序流动管理规则，减少国际不确定影响因素，进而加快形成全球各国均能够取得普遍充分认可支持的多边数据自由保护运行机制，实现跨境数据高效安全合理有序规范的双向流动；另一方面，在大力促进跨境数据信息跨境快速流动服务的发展同时，对关键敏感的数据采取必要的限制。中国作为数据大国，应在国际数据安全保护、数据开发利用规则制定上发挥自己的话语权，向世界展现中国智慧，这也有利于抵御个别国家的“数据霸权”。

4.5. 建立企业合规制度

目前在我国也已经正式出台实施了《网络安全法》《数据安全法》和《个人信息保护法》文件，确立出了我国数据保护政策的三个基本框架。数据基础设施安全及维护等工作真正的全面开展则有赖力于其他各方面的主体政府的共同努力，尽管在《数据保护法》计划中也明确规定了地方各级主体政府相关的数据监管和职责，但是真要有效实现这些数据基础安全设施的管理，仅仅依靠这些部门进行监督管理显然是不切实际的。企业作为数据处理过程中的重要一环，如何实现个人数据合规和数据跨境流动合规是当前亟待研究的重要课题。企业应当对可能与自身数据业务相关的法律进行梳理，并在数据收集、处理及流通过程中处理好相关的合规工作，以求能及时有效的避免数据安全风险。除此以外，需要做好相关的宣传教育，制定行为规范，以能够实现行业自治。在现代企业投资运营建设过程活动中，应力求尽量做到减少出现或力求避免发生会产生危及社会主义国家安全、公共生产利益和或影响个人生命和企业组织内部合法资产权益行为的投资数据处理活动。在国内层面，企业需要根据现行法律调整其内部管理制度，以确保在收集和使用个人数据方面的合规性。国家也可以尝试探索建立行政合规激励机制和刑事合规激励机制。对于建立有效数据合规的企业，可以减轻行政处罚，达成行政和解，或者不采取影响企业正常经营的强制措施，作为法定减轻或者从轻判处。在国外层面，跨国企业在国际贸易中实现数据合规是一个更加具体和复杂的问题。要实现这个目标，需要很多主体参与。企业要事前开展国际合作，通过企业间签订协议或标准合同搭建合作桥梁。一旦出现合规问题，应积极采取各种措施进行补救。抖音事件是通过沟通解决问题的典型案例。此外，政府应积极维护国内企业的海外利益，阻止长臂管辖权，维护中国的数据主权。

5. 结论

当今数据安全是国家安全的重要保障，相较于传统的数据安全，当前的数据安全更加复杂，动态化。但是需要明确的是数据安全保护本质上是如何平衡数据的安全合法有序的流动与数据监管与限制。国际社会虽然对数据保护进行了关注，但全球数据安全仍然面临诸多现实挑战，包括全球数据安全治理面临标准差异化、规则碎片化和诉求多元化等问题。检视现有立法不难发现中国现有数据安全相关法律法规与维护中国国家安全和数据安全的现实需要存在明显差距。因此未来立法可以在以下方面进行加强，首先需要平衡数据利用与数据安全风险，其次需要明确网络数据主权归属，同时积极与国际社会进行合作，构建科学的数据安全保护体系。

参考文献

[1] 梅夏英. 数据的法律属性及其民法定位[J]. 中国社会科学, 2016(9): 164-183+209.
[2] 李爱君. 数据权利属性与法律特征[J]. 东方法学, 2018(3): 64-74.
[3] 邵晶晶, 韩晓峰. 国内外数据安全治理现状综述[J]. 信息安全研究, 2021, 7(10): 922-932.
[4] 阙天舒, 王子玥. 数字经济时代的全球数据安全治理与中国策略[J]. 国际安全研究, 2022, 40(1): 130-154+158.
[5] 高仲劭. 数据跨境流动的国际治理实践与中国方案[J]. 青年记者, 2021(21): 78-79.
[6] 吴玄. 数据主权视野下个人信息跨境规则的建构[J]. 清华法学, 2021, 15(3): 74-91.
[7] 张晓君. 数据主权规则建设的模式与借鉴——兼论中国数据主权的规则构建[J]. 现代法学, 2020, 42(6): 136-149.
[8] 张臻, 李艳. 美国《数据保护法概况》报告述评[J]. 保密科学技术, 2019(8): 29-35.
[9] 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): 52-66.