美国审查 TikTok 数据安全带来的启示与思考*

许皖秀, 左晓栋

(中国科学技术大学 公共事务学院, 安徽 合肥 230026)

摘要: 近日, 美国媒体、国会对 TikTok(抖音海外版)接连发出质疑, 认为这家在美运营的中资背景企业获取美国数据, 破坏美国数据安全。相较于以往, 此次攻击反映出中美网络空间对抗博弈进入以数据安全为主题的新阶段。预判美国可能对我国高科技企业实施进一步遏制, 通过分析美国对 TikTok 数据安全监管的原因、具体措施及其政策方向, 为我国的数据安全监管工作提出建议。

关键词: TikTok; 数据安全; 数据跨境流动; 数据本地化

中图分类号: G203

文献标识码: A

DOI: 10.20044/j.csdg.2097-1788.2022.02.001

引用格式: 许皖秀, 左晓栋. 美国审查 TikTok 数据安全带来的启示与思考[J]. 网络安全与数据治理, 2022, 41(2): 3-7, 29.

Enlightenments and reflections of the American review TikTok data security

Xu Wanxiu, Zuo Xiaodong

(School of Public Affairs, University of Science and Technology of China, Hefei 230026, China)

Abstract: Recently, the United States media and Congress have questioned TikTok (Douyin Overseas Edition) one after another, arguing that this Chinese-backed company operating in the United States obtains the United States data and undermines the United States data security. Compared with the past, this attack reflects that the Sino-US cyberspace confrontation game has entered a new stage with the theme of data security. Anticipating that the United States may further curb my country's high-tech enterprises, This paper analyzes the reasons, specific measures and policy directions of TikTok data security supervision in the United States, and makes suggestions for China's data security supervision.

Key words: TikTok; data security; cross-border data flow; data localization

0 引言

近年来, 随着中美战略竞争态势加强^[1], 美国以国家安全为借口对中国高科技企业的压制愈演愈烈^[2]。从严格封控对华技术转让、关键技术出口, 再到对华为^[3]、中兴等中资企业施加单方面的贸易制裁, 美国对中国高科技企业的发展虎视眈眈。2022年8月, 特朗普政府以“维护美国国家安全”为由, 要求各大应用商店封禁字节跳动公司旗下的TikTok短视频软件, 这一事件在美国引发一片哗然。这一行为在经历数月的各方博弈后, 以拜登政府2021年6月9日签署的撤销行政令宣告终结^[4], 但美国政府对TikTok的敌视并没有因此结束。此次美

国媒体 BuzzFeed 与国会议员对 TikTok 的攻击卷土重来, 甚至远远超过特朗普政府时期的打击强度。美国政府所谓的 TikTok 威胁数据安全的依据是什么? 下一步将要采取哪些措施来遏制中资背景企业的发展? 美国的政策对我国的数据安全监管有哪些启示与借鉴, 这是值得研究的重大问题。

1 美国审查 TikTok 事件回顾

1.1 BuzzFeed 报道

2022年6月17日, 美国新闻聚合平台 BuzzFeed 报道称, 在其获得的 80 余次 TikTok 内部会议音频显示, 字节跳动的中国员工在 2021 年 9 月至 2022 年 1 月期间“不断访问”美国 TikTok 用户的非公开数据。该报道认为 TikTok 高管在国会作了虚假陈述, 隐瞒了中国政府可以获取美国数据的事实。具体而

* 基金项目: 国家社会科学基金重大项目(21&ZD166)

言,其抨击点聚焦四个方面:

一是受保护数据范围过窄。TikTok 拟将所有受保护的美国用户数据转移存储到甲骨文公司位于得克萨斯州的云服务器上,而 TikTok 公司本身不再留存数据。由于“受保护信息”的具体范围由 TikTok 与美国外国投资委员会(CFIUS)谈判确定,而该保护范围一直悬而未决,当前拟定范围不包括用户的公开评论、IP 属地等非敏感用户信息,存在保护范围过窄的情况。

二是数据能够被中国国内访问。该报道提出,虽然 TikTok 正在与甲骨文达成协议,将美国用户数据的物理存储位置从新加坡迁移至美国,由此来确保这些数据不受中国法律约束,但根据该报道的调查和 TikTok 公司内部工作人员的透露,TikTok 母公司字节跳动的中国员工仍能访问美国用户数据,数据转移至美国并不会消除“数据最终仍会落入中国情报机构手中”的顾虑。

三是 TikTok 可能会从推荐算法入手,煽动美国民众并进行社会动员。该报道基于所有中国企业都会受控于中国政府操控的不实指控,担忧中国政府有较大可能性通过软权力指挥字节跳动,要求字节跳动总公司指示 TikTok 调整视频推荐算法,散播不实言论影响美国民众认知,从而实现美国的舆论引导和社会动员。

四是试图影响美国政策制定,为中国企业大开方便之门。该报道指出,TikTok 希望能借助此次与 CFIUS 谈判契机,影响拜登政府正在制定的海外 APP 数据安全监管法规,为其他中国公司在美国开展业务创造便利条件,从而挤压美国国内企业,达到通过企业输入影响美国国家安全的目的。

1.2 TikTok 在美数据安全问题的历史脉络

自特朗普政府时期起,美国政商两界、媒体和智库一些人员持续污蔑 TikTok 将海外收集的美国用户数据交给中国政府,威胁美国公民隐私和国家安全^[5]。

2019 年 11 月,CFIUS 启动对中国字节跳动公司收购 Musical.ly 音乐短视频应用的审查。2019 年 11 月至 2020 年 7 月间,美国参议院召开针对中国的听证会,拟推动立法封禁 TikTok。2020 年 7 月,参议院国土安全和政府事务委员会讨论并投票通过《禁止在政府设备上使用 TikTok 应用法案》。同期,美国众议院投票通过将“在政府设备中禁用 TikTok”条

款纳入 2021 财年《国防授权法案》修正案。2020 年 8 月,时任总统特朗普签署 2 份行政命令,要求限制 TikTok 在美国境内的下载、更新和运营,并要求字节跳动在 90 天内剥离 TikTok^[6]。此禁令一直未生效,但 CFIUS 随后对 TikTok 展开国家安全审查。

2021 年 6 月 9 日,拜登政府发布行政令,撤回特朗普时期的 TikTok、微信禁令,但维持了 CFIUS 审查。其并非放松管制,而是要求针对“外国敌手”开发的软件应用出台一揽子限制措施,打击力度超过特朗普执政时期。

目前,美国商务部已出台信息通信技术和和服务(ICTS)交易的暂行最终规则,审查美国企业和中国企业的 ICT 相关交易是否会导致美国个人敏感数据面临“不当或不可接受的风险”。据报道,美国司法部也在酝酿新的法律,以阻止 TikTok 等中国背景应用程序收集和访问美国公民敏感数据。

1.3 TikTok 德克萨斯项目

为回应美国政府对数据安全的关切,TikTok 与拜登政府达成了一项“充分保障用户数据安全和美国国家安全利益”的最终协议,即德克萨斯项目。

该协议的实质是,TikTok 采用“数据托管加第三方审计”的模式与甲骨文公司合作,将美国用户的受保护数据存储于位于德克萨斯州的甲骨文数据中心,并且授权甲骨文作为“看门人”审计和监督数据的流动和访问。所有美国用户流量均被路由至甲骨文云基础设施。TikTok 后续拟删除美国和新加坡数据中心的备份。

2 TikTok 审查事件最新进展

在过去的一个月里,TikTok 审查事件的关注度再度陡增,超过 20 多名美国国会议员相继对 TikTok 发难,对 TikTok 威胁美国用户数据安全提出质疑。

6 月 23 日,以科顿为首的数名共和党参议员致函财政部部长耶伦,要求在 7 月 22 日前,就特朗普 TikTok 行政令的执行情况以及拜登政府针对 TikTok 进行的安全审查进展回答一系列问题。

6 月 24 日,美国联邦通信委员会共和党籍委员卡尔致函苹果和谷歌 CEO,称因为“北京可以不受限制地访问敏感的美国用户数据”,TikTok 没有遵守苹果和谷歌的规则,要求苹果、谷歌应用商店下架 TikTok。佛罗里达州参议员斯科特随即在推特上发文表示支持。

6 月 27 日,布莱克本等 9 名美国国会参议员致

函 TikTok 首席执行官周受资,要求其于 7 月 18 日前对 BuzzFeed 报道所涉相关问题进行澄清。对此, TikTok 进行了较为妥善的应对,以公开信形式回复了 9 名参议员的提问。

7 月 5 日,美国国会参院情报委员会主席华纳和副主席卢比奥联名以委员会名义致函联邦贸易委员会(FTC),引用 BuzzFeed 报道,指控“TikTok 在其数据安全、数据处理和公司治理实践方面一再作出虚假陈述”,并要求开展调查。

7 月 22 日,民主党议员乔希·戈特海默和共和党议员布莱恩·菲茨帕特里克联合提出一项新法案——《打击社交媒体有害行为法案》(简称“CHATS”),将矛头直指 TikTok 与其他“可能危害年轻用户”的应用。这项新的法案将包括举报犯罪行为及与其关联的社交媒体平台,并将修改联邦调查局过去一成不变的犯罪行为举报制度。同时,这两位议员也向 TikTok 首席执行官周受资致信,要求其在 12 月 1 号之前,就 TikTok 如何保护青少年隐私、向海外分享美国用户数据等问题予以回复。

可以预见,近期一系列的事件仅是美国政客制裁 TikTok“车轮战”的开始,美国政府对 TikTok 的审查将延续并进一步趋严,TikTok 与 CFIUS 就国家安全的协议谈判将更为困难。而拜登政府正在制定的海外 APP 的监管法规也可能迫于压力提出更为严苛的要求。基于此,有必要对美国政府针对 TikTok 数据安全监管措施进行具体分析。

3 美国针对 TikTok 数据安全监管措施

3.1 美国关注数据安全监管的原因

第一,数据安全与国家安全的进一步紧密^[7],美国试图确保数据安全领域内的绝对控制力。有过“棱镜”项目经验的美国极为清楚,数据安全是国家安全的重要组成部分,类似“剑桥分析”事件更显示出社交平台对政权稳定和国家平稳运行可能产生的巨大影响。因此,中国企业旗下社交应用在美国成为比肩脸谱、推特的重要数据平台,无疑引发了美国政界和智库对数据安全的恐慌和担忧。在科顿致函财政部部长耶伦的信中,强调“TikTok 当前方案无法解决特朗普行政令中指出的国家安全风险”,因为“隐患不仅存在于数据领域,更关乎一家中国企业对美国社交媒体的所有权”,强调拜登政府不能只关注数据存储问题。

第二,维系美国在全球数据规则制定中的话语权和影响力。以数据为核心的数字经济已经成为经济发展的新引擎,国际贸易实质上是数据跨境流动^[8]。数据安全已成为国际规则制定的核心议题,美国为维持其在国际政治经济格局中的霸主地位,正力图掌控数据规则制定权。TikTok 进入美国市场后,其迅速扩张的市场份额与日益庞大的社会受众,触动了美国部分政客与互联网企业的既得利益,通过打压 TikTok 等企业,意图削弱中国在全球数据规则制定中的话语权和影响力。

第三,网信企业全球影响力是国家竞争软实力的重要组成部分,网络安全议题始终是美对华遏制的优先选项。通过对中国网信企业进行制裁、封禁^[9],美国进一步扩散对华恐慌情绪,打压中国科技竞争力、维护其全球科技领导地位。从“清洁网络计划”开始,美国长期炮制中国数据安全威胁论,将经贸问题政治化,试图在 IT 领域对华进行升级遏制,彻底清除所谓“中国元素”。

第四,封杀外国应用程序有助于保护本国市场。国家利益到哪里,信息化就覆盖到哪里。网信企业的良性发展,既关乎企业自身的良好运行,也关乎国家科学技术的发展与综合国力的提升^[10]。对美国而言,TikTok 的成功,冲击了美国老牌社交媒体的市场地位(如表 1 所示)。因此,部分企业采取游说政府和公开抨击等举措,意图促使美国当局对 TikTok 进行打压,最终目的必然是将 TikTok 驱逐出美国市场,维系其自身利益。

表 1 2021 年度 TikTok 与其他社交软件用户数据对比

	月活跃用户	月活跃用户 增长率/%	用户增长率 (美国地区)/%
TikTok	近 10 亿	40.80	18.30
Pinterest	近 20 亿	29.19	3.10
Twitter	近 2 亿	13	0.20
Instagram	近 10 亿	3.70	3.70
Facebook	近 29 亿	7	0.80

考虑到美国在数据安全角度不断遏制中国高科技企业发展,有必要针对此次 TikTok 事件,具体分析美国的数据安全监管措施。

3.2 美国数据安全监管措施

一是将数据安全升级到国家安全角度,并以此

为由对中资高科技企业进行安全审查。从对华为进行芯片断供、封禁 5G 产品,再到以泄漏美国用户数据为由,要求 TikTok 退出美国市场,实质上是将商业竞争升级到国家安全层面来进行。数据安全是中美博弈背景下压制中国科技企业的最新手段。在 TikTok 事件中,美国通过新闻媒体报道渲染,不断地针对中资企业进行所有权和政治背景调查,煽动美国内群众情绪和认知,企图以这种方式封杀外国尤其是中国互联网公司,从而保护本国的应用市场。

二是对用户数据进行分类,提出“受保护数据”概念。美国议员在向财政部部长、联邦贸易委员会致函时,都提出了“受保护数据”概念,并认为 TikTok 现有的隐私政策和保护力度不足以保护数据安全。通过提出新的数据分类概念,强调数据安全对于国家安全的重要性,要求中国高科技公司重点保护美国敏感个人信息(如电话、出生年月等)的安全,以便加强对中国互联网公司的数据安全监管。“受保护数据”的范围目前还没有确定,现有记录表示不会包括公共评论、用户公开的个人资料等,但目前甲骨文公司与 CFIUS 对此拒绝予以置评。

三是要求 TikTok 建立“管用分离”的用户数据存储模式,以防美国用户数据流入中国。该方案的用户数据存储模式是与美国第三方公司合作,建立一个低风险的境外企业数据存储系统。对于“受保护数据”,美方要求 TikTok 公司与甲骨文云服务商合作,把搜集到的美国用户信息存储在德克萨斯数据中心,而不能存储在位于中国的总公司字节跳动。此前存储在新加坡的数据,将在与甲骨文达成协议工作完成后,全部予以删除。对于“受保护数据”的访问权限,只能授权特定的美国员工,而不能是中国员工。

四是启动由 CFIUS 负责的国家安全审查,组建第三方专业技术团队对 TikTok 数据安全技术措施进行评估。在 2019 年起,CFIUS 牵头开始负责对 TikTok 的数据安全问题进行审查。在德克萨斯项目当中,CFIUS 专门负责 TikTok 与甲骨文数据存储的协议推进和内容进行监管,并且数据访问协议的内容将由甲骨文和 CFIUS 合作协定,TikTok 无参与权,以此来保证两家企业在政府机关的监管下展开合作。在 TikTok 审查事件当中,美国要求建立一支由美国人组成的第三方专业数据安全团队,评估 TikTok

公司的数据安全技术措施,即多次提到的“美国 USTS 数据团队(United States Technical Services team)”。对于存储在甲骨文云服务器上的“受保护数据”,仅授权给 USTS 的特定人员查看。而 USTS 之外的任何人访问美国用户数据,都应当受到强大的数据访问协议的限制。

五是利用法律手段监管数据安全。除了在政府层面制定一系列的数据安全监管措施外,美国还加快了针对数据安全法律责任的立法工作。民主党议员乔希·戈特海默和共和党议员布莱恩·菲茨帕特里克共同提出《打击社交媒体有害行为法案》,拟调整美国联邦调查局原有的犯罪举报制度,将社交媒体平台纳入举报对象,以此增加 TikTok 在数据合规、青少年隐私保护方面的法律责任,形成美国全社会层面的监督监管。

同时,美国最新提出两份数据安全法案,开始加强对“数据经纪生态系统”的监管。第一部法案是 6 月 15 日提出的《健康和位置数据保护法》,加强了对美国公民位置与健康两类数据的特别保护,在执法层面授予相关部门与受害者两类人群的诉讼权利。该法案旨在禁止数据经纪人出售或传输美国人的位置与健康数据。第二部法案是 6 月 23 日提出的《2022 保护美国人数据免受外国监视法案》,开展对数据的分类和跨部门合作,对于敏感个人数据(如位置和 health 数据)采取禁止出售或传输的管理规定,对于易被利用的数据采取建立黑白清单的方式来保护国家安全。制定黑白清单的考虑因素包括该国的数据保护水平、强迫公民提供数据的情况以及与美国是否开展过敌对的情报行动等。

4 我国可借鉴的数据安全监管措施

美国政府在数据安全监管层面对华动作不断,应该如何应对?其中有哪些值得借鉴?今后,我国在数据安全监管中可以考虑采用以下措施:

一是从国家安全层面进一步深化对重要数据和个人信息认识,完善数据分类分级管理制度。我国《数据安全法》提出建立数据分类分级制度,目前已经确定为一般、重要和核心三级。此外,我国《个人信息保护法》确立了个人信息保护制度。在此基础上,我国《网络数据安全条例(征求意见稿)》提出,国家对个人信息、重要数据和核心数据均进行重点保护。为此,我国先后开展了《重要数据识别指南》《网络数据分类分级指南》等国家标

准的制定工作。在制定过程中,有很多声音认为我国标准规定过严,甚至质疑标准编制组将“国家安全”概念扩大解释。但从美国“受保护数据”概念的提出来看,其对国家安全与数据安全作了更为紧密的关联,甚至如用户出生年月、电话号码等都被赋予了国家安全内涵。从俄乌冲突中西方社交媒体精准定位俄罗斯士兵身份等一系列事件看,个人信息以及商业领域信息越来越具有了国家安全属性。下一步有必要借鉴“他山之石”,对重要数据的范围作出更科学和更符合国家安全需求的界定,并从防范国外情报威胁角度完善我国个人信息保护的相关规定。

二是细化网络安全审查制度,明确建立外资机构在华运营的数据安全审查机制。我国《网络安全法》最初提出网络安全审查制度时,主要规范的是关键信息基础设施运营者采购网络产品和服务的行为。《数据安全法》设立了数据安全审查制度,为此国家互联网信息办对《网络安全审查办法》作了相应修订,将数据安全审查要求纳入网络安全审查之中,明确对可能影响国家安全的数据处理活动进行审查,其主要场景是中国企业赴国外上市前应主动申报,接受审查。其他情况下的网络安全审查,则由国家网络安全审查办公室主动发起,无需申报。CFIUS 的外国投资国家安全审查向来被视为中国网络安全审查制度的重要借鉴。此次 CFIUS 对 TikTok 的审查,从侧面说明了对外资企业处理中国数据进行常态化审查存在合理性和必要性。CFIUS 的具体审查措施,如关注数据协议、合作方式、数据访问模式等,均提供了借鉴。

三是健全数据本地化存储制度,提出数据“管用分离”的监管要求。美国政府要求 TikTok 公司与美国云服务商合作,将“受保护数据”全部储存在甲骨文控制的德克萨斯数据中心,体现了对数据安全的绝对追求。与之相较,我国《网络安全法》虽然提出关键信息基础设施运营者收集产生的重要数据、个人信息应在境内存储,但在实践中,监管部门的精力仍主要在数据出境安全管理上,尚未对数据本地化存储政策作进一步研究。而且,《网络安全法》并未涉及国外企业在我国境内收集处理数据的活动。与要求境内、境外一些企业实施本地化存储的基本要求相比较,更为严格的措施是要确保数据只能存储在我国政府信任且可控的境内数据中心,且

数据访问者应当严格限定为中方人员。仅仅将中国用户数据存储在中国境内,从国家安全角度来看,保护力度仍然不够。为此,我国应在数据本地化存储制度框架下,明确“管用”分离要求。即企业在我国境内开展业务时收集到的中国用户数据必须托管给中国企业,且签订的数据安全合作协议应由政府部门审查通过。外资企业不得留存、备份数据。要注意的是,此举针对的不是所有外资企业和所有数据,而应严格限定在国家安全领域。

四是对境外企业的数据处理活动开展算法、源代码的透明审查。TikTok 公司最近发布公告,宣布将建立一个数据透明中心,接受美国政府对其算法、源代码的审查。当年,华为、中兴等企业为了自证清白,也向美国国会提出了审查请求。华为公司为了在英国开展业务,还与英国政府合作建立了网络安全中心,主要目的是开放源代码供英国安全机构审查。美国微软公司也曾在中国建立源代码开放实验室,在严格条件下向特定中国企事业单位开放源代码浏览权限。但总体而言,类似的透明审查能否奏效?如何实施?如何保障各方合法权益?这些问题尚没有定论。随着人工智能的迅速发展,关于算法的审查也提上了议事日程,形势发展显示,一个国家应当建立对源代码和算法的安全审查设施,并提出源代码和算法开放制度要求。我国至少应形成这方面的对等反制能力。要注意的是,这项制度也不是针对所有的外国企业产品,而是聚焦于重要敏感数据的处理方面。

5 结论

本文深入研究了美国政府遏制 TikTok 事件,特别是分析了美国政府的数据安全举措,目的是完善我国的数据安全政策措施。事实上,政策制定是一个复杂过程,不但要勇于创新,还要聚焦政策可行性及其对贸易的影响。TikTok 审查事件为我国开展数据治理提供了可资借鉴的范例,侧面证明有必要从国家安全需求出发构建数据安全监管制度,特别是在数据分类分级、“管用分离”要求、网络安全审查等方面。

参考文献

- [1] 吴心伯.论中美战略竞争[J].世界经济与政治,2020(5):96-130.
- [2] 刘凤朝,姜滨滨.中国企业跨国并购的国家安全审

(下转第 29 页)

- 2017: 1–13.
- [10] SPARKS E R, TALWALKAR A, HAAS D, et al. Automating model search for large scale machine learning[C]//Proceedings of the Sixth ACM Symposium on Cloud Computing, 2015: 368–380.
- [11] XIAO W, REN S, LI Y, et al. AntMan: dynamic scaling on GPU clusters for deep learning[C]//14th USENIX Symposium on Operating Systems Design and Implementation(OSDI 20), 2020: 533–548.
- [12] JEON M, VENKATARAMAN S, PHANISHAYEE A, et al. Analysis of large-scale multi-tenant GPU clusters for DNN training workloads[C]//2019 USENIX Annual Technical Conference(USENIX ATC 19), 2019: 947–960.
- [13] QIAO W, LI Y, WU Z H. DLTAP: a network-efficient scheduling method for distributed deep learning workload in containerized cluster environment[C]//ITM Web of Conferences. EDP Sciences, 2017, 12: 03030.
- [14] ZHAO H, HAN Z, YANG Z, et al. HiveD: sharing a GPU cluster for deep learning with guarantees[C]//14th USENIX Symposium on Operating Systems Design and Implementation(OSDI 20), 2020: 515–532.
- [15] WU Y, MA K, YAN X, et al. Elastic deep learning in multi-tenant GPU clusters[J]. IEEE Transactions on Parallel and Distributed Systems, 2021, 33(1): 144–158.
- [16] OR A, ZHANG H, FREEDMAN M. Resource elasticity in distributed deep learning[J]. Proceedings of Machine Learning and Systems, 2020, 2: 400–411.

(收稿日期: 2022-04-20)

作者简介:

魏宏原(1996-), 通信作者, 女, 硕士研究生, 主要研究方向: 高性能计算。E-mail: whyyy@mail.ustc.edu.cn。

华蓓(1966-), 女, 博士, 教授, 主要研究方向: 高性能计算。

林飞(1994-), 男, 硕士研究生, 主要研究方向: 高性能计算。

(上接第 7 页)

- 查: 以美国为例[J]. 科学学与科学技术管理, 2010(3): 151–156.
- [3] 任星欣, 余嘉俊. 持久博弈背景下美国对外科技打击的策略辨析——日本半导体产业与华为的案例比较[J]. 当代亚太, 2021(3): 110–136, 168.
- [4] 冯硕. TikTok 被禁中的数据博弈与法律回应[J]. 东方法学, 2021(1): 74–89.
- [5] 程柏华, 龙坤, 秦中南. 美国政府封禁 TikTok 的策略探究——基于安全化理论的分析视角[J/OL]. 情报杂志: 1–8[2022-08-11]. <http://kns.cnki.net/kcms/detail/61.1167.g3.20220615.1030.002.html>.
- [6] 黄钊龙. 特朗普政府时期美国科技战略解析[J]. 南开学报(哲学社会科学版), 2022(3): 86–94.
- [7] 马其家, 刘飞虎. 数据出境中的国家安全治理探

讨[J]. 理论探索, 2022(2): 105–113.

- [8] 王海梅. 数字经济发展水平对进出口贸易和贸易效率的影响——基于江苏与 RCEP 协议国的数据分析[J]. 现代管理科学, 2022(3): 145–53.
- [9] 池志培. 美国对华科技遏制战略的实施与制约[J]. 太平洋学报, 2020, 28(6): 27–42.
- [10] 方滨兴. ITNS 主题专栏: 中国电子“网络安全和信息化”专题[J]. 信息技术与网络安全, 2018, 37(9): 4.

(收稿日期: 2022-08-01)

作者简介:

许皖秀(1999-), 女, 硕士研究生, 主要研究方向: 数据安全、数据跨境。

左晓栋(1975-), 通信作者, 男, 博士, 教授, 主要研究方向: 网络安全法、数据安全法。E-mail: xdzu@ustc.edu.cn。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部

www.pcachina.com