数字经济下美国与外国对手 ICTS 交易监管及法律限度
——基于 TikTok 案和微信被禁案的分析

张怀岭

摘　要：伴随着地缘政治的变化和美国推行“脱钩”“去风险”政策，在数字经济领域美国对外国投资者监管的法律工具日益多元化。在规范和执法实践上，美国政府滥用 IEEPA 框架下的紧急状态国家安全保障授权，强化与外国对手 ICTS 交易监管工具，导致我国科技企业的经营面临巨大的法律风险。同时，该监管权虽在实体审查标准与执法程序上存在法律限度，但其权力边界需要基于个案事实由司法机关界定。我国应在统筹推进国内法治和涉外法治的要求下完善应对策略。微观层面，应完善数字经济领域企业数据合规机制，积极利用美国宪法框架下的司法救济机制应对违法歧视性措施；宏观层面，坚持总体国家安全观，在对等原则下强化我国以《反外国制裁法》为基础，以外资安全审查、网络安全审查等制度为重要内容的反制裁、反干涉制度体系。

关键词：与外国对手交易；数字经济；国际紧急经济权法；涉外法治体系

［中图分类号］D971.2；D912.29　［文献识别码］A　［文章编号］2096-6180（2023）05-0015-19

伴随着地缘政治与经济的变化，如何在保持经济对外开放的同时维护国家安全是近年来欧美各国外资监管法律改革关注的问题。数字经济下国家安全的保障更加复杂并引发以美国为代表的国家日益严重的数字保护主义，监管工具呈现新的特征和发展趋势。实践中，与外国对手（foreign adversary）的信息通讯技术与服务交易（下称 ICTS 交易）审查这一新型法律工具已经对我国科技企业的经营产生严重冲击，而且与美国外资审查委员会（CFIUS）主导的外资国家安全审查等既有法律工具既相互补充又相互竞争。对此，学界既有研究无论是在规范层面还是在典型个案执法与司法层面均尚存在不足，不仅难以有效指引企业微观层面的法律应对，而且缺乏在“统筹推进国内法治和涉外法治”的视野下构建我国的总体应对方案。鉴于此，本文首先结合规范变革和典型个案分析数字经济领域美国与外国对手 ICTS 交易监管工具的强化趋势与“国家安全”

［作者简介］张怀岭，法学博士，西南财经大学副教授。

［基金项目］成都市哲学社会科学规划项目（青年项目）“美国与外国敌手交易监管立法及对四川企业的影响研究”（项目批准号：2022C27）；国家社会科学基金一般项目“对等原则视域下我国外资‘国家安全’审查国别因素研究”（项目批准号：19BFX159）。

内涵的扩张。其次，在探讨与外国对手 ICTS 交易的监管措施核心内容的基础上，结合美国法既有判例分析行政机关监管权的基本权利限制以及司法机关对“国家安全”判断的审查权。最后，在“统筹推进国内法治和涉外法治”的视角下从微观和宏观两个层面提出中国的因应策略。

一、数字经济下与外国对手交易监管强化及“国家安全”的内涵扩张

（一）与外国对手交易监管规范强化

1. 特朗普政府 ICTS 交易监管行政令及细则

2019 年以来，美国总统基于《国际紧急经济权法》（International Emergency Economic Powers Act，IEEPA）、《国家紧急状态法》（National Emergencies Act，NEA）等国内法认定所谓“外国对手”直接或间接控制的信息通讯技术与服务在美国的运行导致美国主体敏感数据遭受威胁并威胁到美国国家安全。以这一国家安全威胁认定为基础，美国一方面通过总统行政命令宣布国家紧急状态，同时又以总统行政命令与商务部实施条例相结合的形式直接干预与外国对手之间的特定 ICTS 交易。2019 年 5 月，时任美国总统特朗普颁布了《保障信息通讯技术与服务供应链安全的行政命令》（下称《第 13873 号行政令》）〔1〕，授权美国商务部对包括中国在内的外国对手在信息通讯技术与服务领域的特定交易进行审查并采取禁止或者附条件批准等限制性措施。作为该行政令的实施细则，美国商务部于 2019 年 11 月 27 日颁布第 65316 号条例〔2〕，经公众评议程序和修订，现行实施条例自 2021 年 3 月 22 日生效（下称《特朗普行政令细则》）。〔3〕

2. 拜登政府对 ICTS 交易监管规范的修订

与对特朗普时期颁布部分法令的命运不同，美国总统的更迭并未改变其强化数字领域外资监管的立法趋势。拜登总统不仅允许《特朗普行政令细则》如期生效，而且同样以 IEEPA 等法律的授权于 2021 年 6 月颁布了《保护美国公民敏感数据不受外国对手侵害的行政令》（下称《第 14034 号行政令》）。内容上，该行政令以特朗普政府《第 13873 号行政令》及其实施条例为基础。随后，为了保障上述拜登行政令的实施，美国商务部于 2021 年 11 月 26 日颁布了《保障信息通讯技术与服务安全条例（建议稿）》（86 FR 67379，下称《拜登行政令细则》），对原《特朗普行政令细则》进行相应的修订和细化。

3. 规制与外国对手 ICTS 交易的新法草案

2023 年 3 月，由美国参议院两党数名参议员提出的一项立法草案得以公布。这部名为《信息与通讯技术风险紧急状况限制法案》（RESTRICT Act，下称《限制法案》）〔4〕旨在通过授权商务部

〔1〕 The White House, *Securing the Information and Communications Technology and Services Supply Chain*, U.S. Government Publishing Office (15 May 2019), https://www.govinfo.gov/content/pkg/FR – 2019 – 05 – 17/pdf/2019 – 10538.pdf.

〔2〕 U.S. Department of Commerce, Securing the Information and Communications Technology and Services Supply Chain, 84 FR 65316.

〔3〕 U.S. Department of Commerce, Securing the Information and Communications Technology and Services Supply Chain, 15 CFR Part 7.

〔4〕 Congress of the United States, *RESTRICT Act*, CONGRESS.GOV (7 March 2023), https://www.congress.gov/118/bills/s686/BILLS – 118s686is.pdf.

禁止外国的科学技术以及外国企业在美国应用抑或经营来保障美国的国家安全。尽管这一法案很大程度上是针对 TikTok，但是该法案的主导者之一民主党参议员沃纳（Sen. Mark Warner）明确表示，该立法采取“一种全面的和基于风险的路径来积极地应对那些潜在危险科学技术”，尤其是所有被美国确定为所谓“外国对手”国家的公司。此外，九位美国议会议员向美国国会提交了一项新的法案（2021 年 ACES 法案），拟针对性地强制字节跳动出售特定资产，并要求 CFIUS 审查字节跳动与美国企业的商业关系。[5]

趋势上，ICTS 交易审查这一新型国家安全审查工具的规范体系逐渐完备，规范内容更加细化和具有针对性，为商务部在实践中强化审查执法奠定了规范基础，而这一监管工具的强化直接导致我国数字经济领域领军企业在美国的投资与经营活动遭遇严重障碍。

（二）与外国对手交易审查实践强化

以前述生效规范为基础，美国总统以及美国商务部先后颁布了针对中资企业的禁止性行政令以及干预措施，这直接导致字节跳动的 TikTok、腾讯的微信等中国企业开发的互联网应用软件在美国的正常使用遭受巨大影响。

首先，TikTok 同时遭遇了两种以维护国家安全为目的的监管审查，即 CFIUS 主导的外资国家安全审查和商务部主导的与外国对手 ICTS 交易审查。2017 年，字节跳动以近 10 亿美元的对价全资收购了 Musical.ly 并将其与字节跳动旗下产品 TikTok 合并。2019 年，CFIUS 以政治敏感内容审查和个人信息存储存在问题为由启动对 TikToK 的审查。尽管在此过程中 TikTok 向 CFIUS 保证其所获取个人数据完全存储在美国，中国政府对 TikTok 内容没有任何管辖权，并按照 CFIUS 的要求推动在加利福尼亚建立专门负责数据管理的团队，由其批准并监督中国工程师访问 TikTok 数据库的活动。但是，CFIUS 于 2019 年 6 月正式启动调查并随后函告 TikTok，声称其收购 Musical.ly 的交易对美国构成国家安全风险。TikTok 基于与甲骨文公司之间的数据安全合作向 CFIUS 提出名为“德克萨斯方案”（Project Texas）的用户数据保护方案，至今尚未得到后者的最终批准。

然而，在 CFIUS 进行的国家安全审查决定尚未终结的情况下，2020 年 8 月，时任美国总统特朗普直接援引 IEEPA 授权签署第 13942 号行政令，宣布将在 45 日之后禁止美国任何个人或者实体与 TikTok 及其母公司字节跳动进行交易。[6] 此后，特朗普再次签署行政令，要求字节跳动在 90 日内剥离在 TikTok 的所有权益和资产，并要求字节跳动销毁通过 TikTok 或 Musical.ly 获得的任何数据及副本。[7] 8 月 24 日，TikTok 以特朗普行政令以及美国商务部实施细则越权与违宪为由

〔5〕 Congress of the United States, *ACES Act of 2021*, CONGRESS.GOV (7 May 2021), https://www.congress.gov/bill/117th-congress/house-bill/3057.

〔6〕The White House, *Addressing the Threat Posed by TikTok, and Taking Additional Steps to Address the National Emergency with Respect to the Information and Communications Technology and Services Supply Chain*, Federal Register (6 August 2020), https://www.federalregister.gov/documents/2020/08/11/2020－17699/addressing-the-threat-posed-by-tiktok-and-taking-additional-steps-to-address-the-national-emergency.

〔7〕 The White House, *Regarding the Acquisition of Musical.ly by ByteDance Ltd.*, Federal Register (14 August 2020), https://www.federalregister.gov/documents/2020/08/19/2020－18360/regarding-the-acquisition-of-musically-by-bytedance-ltd.

提起诉讼。9 月 27 日，美国哥伦比亚地区联邦法院认定总统令超越了 IEEPA 的授权并且原告若不能获得禁令救济将会遭受不可恢复的损害，从而裁定暂缓执行将 TikTok 从苹果和谷歌应用商店下架的行政命令。[8] 2021 年 6 月，美国总统拜登宣布撤销特朗普时期的多项禁令，包括对 TikTok 的禁令。

其次，在对 TikTok 颁布禁令之后，基于类似的原因，尤其是微信对国家安全、外交政策以及经济的威胁，时任美国总统特朗普 2020 年 8 月 6 日发布《关于应对微信所致国家安全威胁以及采取进一步措施应对 ICTS 供应链国家紧急状况的行政令》（下称《第 13943 号行政令》）[9]，禁止与微信的交易并指令美国商务部认定禁止交易的类型与范围。2020 年 9 月 18 日，美国商务部通过发布《关于执行第 13943 号行政令对禁止交易的认定》，广泛地禁止一系列对于维护微信功能不可或缺的互联网交易。这些措施将导致美国的用户无法下载或者更新微信应用，无法支付或者接收微信转账，从而导致该应用事实上对用户毫无用处，进而最终实现在美国关闭微信的效果。

然而，美国政府对包括 TikTok 在内的中企在美 ICTS 交易安全担忧并未因司法机关的质疑和总统的更迭而消失。恰恰相反，拜登政府依然延续特朗普政府的政策立场，在司法机关确定的边界范围内，颁布一系列行政令和法规来应对所谓与外国对手 ICTS 交易的国家安全风险。这种政治上的担忧和敌意在美国国会众议院于 2023 年 3 月 23 日针对 TiKTok 举行的听证会上得到淋漓尽致的体现。[10] 事实上，美国参议院、众议院以及多个政府部门陆续颁布禁令，禁止在政府的设备上使用 TikTok 应用。[11] 同样基于所谓的国家安全担忧，美国威斯康星、北卡罗来纳等州已经颁布禁令[12]，禁止几乎在所有政府设备上使用 TikTok 应用。执法实践上，美国商务部等执法部门呈现出对所有对美国公民敏感信息和国家安全构成威胁的中资企业互联网应用等产品和技术强化监管的趋势，范围也扩大到包括华为等在内的中国科技企业在美提供的产品或服务。[13]

（三）数字经济下“国家安全”的新内涵

“国家安全”构成美国行政机关（CFIUS 或商务部）干预外国投资者经济活动的依据和标准，而其内涵在数字经济下呈现新的内容，从最初聚焦国防军事安全、国防安全扩展到能源安全、经济安全，再到如今的数据安全以及信息科技安全，确保美国在科技领域的领先地位。

---

〔8〕 TikTok Inc. *v.* Trump, 490 F. Supp. 3d 73 (2020).

〔9〕 The White House, *Addressing the Threat Posed by WeChat, and Taking Additional Steps to Address the National Emergency with Respect to the Information and Communications Technology and Services Supply Chain*, Federal Register, https://www.federalregister.gov/documents/2020/08/11/2020－17700/addressing-the-threat-posed-by-wechat-and-taking-additional-steps-to-address-the-national-emergency.

〔10〕 Hannah Murphy, *TikTok Chief Faces Hostile Congress in Bid to Fight off US Ban*, Financial Times (4 March 2023), https://www.ft.com/ content/6f0b931f－10c3－4f85－9f30－5d9977aab459.

〔11〕 Jordan Freiman, *House Bans TikTok on Government Devices*, CBS News (27 December 2022), https://www.cbsnews.com/news/tiktok-ban-government-devices-house-of-representatives-congress/.

〔12〕 截至 2023 年 4 月，已经有 34 个美国联邦州颁布类似禁令。

〔13〕 Alexander Alper, *U.S. Probes China's Huawei Over Equipment Near Missile Silos*, Reuters (21 July 2022), https://www.reuters.com/world/us/exclusive-us-probes-chinas-huawei-over-equipment-near-missile-silos－2022－07－21/.

首先，“国家安全”内涵扩张体现在 CFIUS 主导的国家安全审查机制的变革上。美国外资审查制度缘起可追溯到 1917 年颁布的《与敌贸易法》（Trading with the Enemy Act，TWEA）。该法第 5 条赋予总统在战争期间或者其他紧急情况下对涉及国家安全的交易行为进行调查的权利。[14] 此后，外资审查制度经历了三次改革，每次改革都有其特定的地缘政治与经济背景，并与美国外交战略政策的变化以及遏制其他国家崛起密切相关：第一次改革以《埃克森 – 弗洛里奥修正案》（Exon-Florio Amendment）颁布为标志。20 世纪 80 年代日本经济的迅猛发展以及日本企业收购大量美国公司等诱因促使国会制定《埃克森 – 弗洛里奥修正案》。法案列举了衡量外资并购是否对国家安全造成威胁应当考虑的因素，除第五项之外，其余四项都与国防安全相关。[15] 第二次改革以 2007 年《外国投资与国家安全法》（Foreign Investment and National Security Act，FINSA）出台为标志。其背景是，“9 • 11”事件之后，中东主权财富基金在美投资以及其他发展中国家在美国市场的大规模并购引发美国对经济安全的担忧。另外，“中油海收购优尼科”“DPW 并购 P&O”等具有象征意义的个案也成了推动 FINSA 颁布的重要因素。[16] FINSA 在《埃克森 – 弗洛里奥修正案》的基础上，增加了六项国家安全审查标准，除最后一项为兜底性条款，前五项均为国家经济性安全因素。第三次改革则以 2018 年《外国投资风险审查现代化法》（Foreign Investment Risk Review Modernization Act，FIRRMA）[17] 出台为标志。针对中美地缘政治的变化以及中国在经济科技领域崛起的现状，FIRRMA 通过针对性地强化美国外资安全审查制度来遏制中国的科技发展，强化对数字产业的投资审查，将商业问题、数据存储问题政治化，从而服务于数字保护主义与国际数据主导权的目的。

其次，ICTS 交易监管逻辑重心在于儿童、青少年等美国公民群体的“敏感个人信息”“数据安全”以及预防外国对手通过社交媒体应用非法获取和利用这些信息，从而威胁到美国的安全。这种监管逻辑的起点是信息通讯技术与服务供应链对于国家安全的重要意义：一方面，信息通讯技术与服务对美国经济、关键基础设施以及紧急服务具有重要支撑作用；另一方面，其对美国存储、处理和转移大量数据（包括敏感个人信息）的能力具有关键意义。因此，确保 ICTS 供应链的安全、韧性与可靠性对于国家安全至关重要，而美国主体购买、安装或使用由外国对手所有、控制或者管辖之主体提供的信息通讯技术与服务会导致相关外国对手获得利用美国信息通讯技术与服务潜在的脆弱性，并对美国主体的数据（包括个人可识别生物信息或者其他敏感个人数据）的保密性、完整性和（如通过拒绝访问）可获取性构成威胁。[18] 可见，ICTS 交易监管逻辑的核

〔14〕 郑雅方：《美国外资并购安全审查制度研究》，中国政法大学出版社 2015 年版，第 16 – 17 页。

〔15〕 比如交易是否涉及美国国防所需国内产品、是否会涉及向支持恐怖活动的国家转让军需物资等。

〔16〕 Joshua W. Casselman, *China's Latest Threat to the United States:The Failed CNOOC-Unocal Merger and Its Implications for Exon-Florio and CFIUS*, 17 Indiana Intellectual & Comparative Law Review 155, 163 (2007).

〔17〕 Foreign Investment Risk Review Modernization Act of 2018, H.R.5515 – 538.

〔18〕 Department of Commerce, *Securing the Information and Communications Technology and Services Supply Chain*, Federal Register, https://www.federalregister.gov/documents/2021/01/19/2021 – 01234/securing-the-information-and-communications-technology-and-services-supply-chain.

心是将“个人信息安全”“数据安全”纳入“国家安全”范畴，并进而认定外国对手国家（例如中国）所有或控制的社交媒体应用（例如抖音或微信）在美国的广泛使用对美国国家安全构成“不当或者不可接受之风险”。

二、ICTS 交易审查的主要内容

（一）ICTS 交易审查的实体规则与审查程序

特朗普政府《第 13873 号行政令》及其实施条例规定了与外国对手 ICTS 交易审查的核心内容，主要包括监管的逻辑起点、适用范围、监管权的内容和程序性规定的核心规则。

1. ICTS 交易监管的逻辑起点

作为 ICTS 交易监管干预的逻辑起点是基于以下“发现”：其一，外国对手日益频繁地制造和利用美国信息通讯技术与服务领域的脆弱性来从事恶意的网络活动，而信息通讯技术与服务能够存储、流通大量敏感信息，支撑关键基础设施以及提供重大紧急服务。其二，在美国境内不受限制地获取或者使用外国对手拥有、控制、管辖或者有权指示之主体设计、开发、生产或者提供的信息通讯技术与服务增强了外国对手制造以及利用美国该领域脆弱性的能力并导致潜在性的灾难后果，因此对美国的国家安全、外交政策和经济构成“非同寻常的威胁”。〔19〕

2. ICTS 交易监管的适用范围与内容

适用范围的界定对于准确理解监管权的范围和边界至关重要。首先，《第 13873 号行政令》对确定适用范围的部分关键性概念进行了立法界定，包括“信息通讯技术或服务”“实体”“外国对手”“主体”“美国主体”等。其中，ICTS 是指“任何硬件、软件（包括互联网软件应用），或者其他产品或服务，包括云计算服务；这些技术与服务旨在实现或便于实现信息或数据的处理、存储、恢复功能，或通过电子形式（如电磁、磁、光子）来实现通讯，包括传输、存储或展示”。〔20〕可见，ICTS 这一概念涵盖了外延极为广泛的技术与服务，诸如互联网系统、无线网络、移动电话、计算机、卫星系统、人工智能、量子计算和云计算。〔21〕相应地，ICTS 交易是指任何对一种信息与通讯技术与服务采取的并购、进口、移转、安装、交易或者使用行为，包括数据传输、软件更新、维修以及为消费者下载 App 提供平台或者数据存储等。此外，作为审查对象的 ICTS 交易还应当涉及以下六种类型技术中的一类，即“关键基础设施”“网络基础设施与卫星”“敏感个人信息处理”“监控、家庭网络与无人机系统”“通讯软件”以及（人工智能、量子计算、精密机器人等）“新兴技术”。〔22〕

〔19〕 Executive Order 13873 of May 15, 2019, Preface.

〔20〕 Executive Order 13873 of May 15, 2019, Sec.3 (c).

〔21〕 Stephen P. Mulligan, *The Information and Communications Technology and Services (ICTS)Rule and Review Process*, CONGRESS. GOV (26 October 2022), https://crsreports.congress.gov/product/pdf/IF/IF11760.

〔22〕 Stephen P. Mulligan, *The Information and Communications Technology and Services (ICTS)Rule and Review Process*, CONGRESS. GOV (26 October 2022), https://crsreports.congress.gov/product/pdf/IF/IF11760.

交易主体上，所谓“外国对手”是指“任何长期从事或者严重危害美国国家安全或者美国主体安全的外国政府或者非政府主体”。[23] 对此，《特朗普行政令细则》规定了外国对手的具体范围，包括中国（含香港特别行政区）、古巴、伊朗、朝鲜以及委内瑞拉政治人物马杜罗。针对一项 ICTS 交易是否涉及特定外国对手，美国商务部结合以下因素来判断：一是交易的当事人或者供应商的总部或者其他设施是否位于外国对手控制的国家；二是交易当事人与外国对手的个人或者职业关联；三是交易当事人总部或者经营地所在之外国对手国家的法律法规的规定。[24] 总体上，审查的重点是交易当事人与被界定为外国对手国家的关联。[25] 除了当事人与外国对手的关联，作为审查对象的 ICTS 交易还应当涉及受美国法管辖之财产或者主体从事的活动，并且外国国家或个人对于相关财产享有利益。

其次，针对监管权的内容而言，上述行政命令授权美国商务部采取审查措施，包括针对被禁止的交易确定交易终止的时间和方式，颁布适当的实施规则以及行使其他为实施该行政命令所必要的所有 IEEPA 授权总统行使的权力。[26] 针对实施规则的内容，该行政命令进行示例性列举，诸如确定外国对手所涵盖的国家或者主体范围，认定外国对手拥有、控制、管辖或者有权指示之主体的范围，认定应当特别严格审查的涉及特定技术或者国家的交易范围，建立交易许可程序，建立概括性禁止或者豁免的交易类别制度以及建立缓解措施协商机制。

作为前述国家安全威胁的应对措施，《第 13873 号行政令》宣布“国家紧急状态”并授权美国商务部对以下交易采取限制性措施：其一，相关交易涉及外国对手拥有、控制、管辖或者有权指示的主体所设计、开发、生产或者提供的信息通讯技术或服务；其二，该交易：（1）对美国信息通讯技术或服务的设计、完整性、制造、生产、分配、安装、运行或者维持构成“不当的破坏或者颠覆风险”；（2）对美国关键基础设施或者数字经济的安全或者可靠性构成可能引发“灾难性效果”的“不当风险”；（3）对美国的国家安全或者美国主体的安全构成其他“不可接受的风险”。美国商务部可以直接禁止相关交易，或者依职权制定或者与交易方协商能够缓解所认定威胁的措施，并将之作为批准相关交易的前提条件。[27]

3. ICTS 交易监管的例外情形

美国商务部主导的 ICTS 交易审查不适用于美国主体对属于美国国家产业安全计划（NISP）范围 ICTS 的并购以及 CFIUS 正在进行或者已经完成的国家安全审查的交易。原因在于，国家安全已经通过其他形式得以保障。实践中，商务部主导的 ICTS 交易监管与 CFIUS 主导的国家安全审

〔23〕 Executive Order 13873 of May 15, 2019, Sec.3.

〔24〕 Stephen P. Mulligan, *The Information and Communications Technology and Services (ICTS)Rule and Review Process*, CONGRESS.GOV (26 October 2022), https://crsreports.congress.gov/product/pdf/IF/IF11760.

〔25〕 Anthony Rapa, *The ICTS Supply Chain Rules: Towards a U.S. –China Tech Decoupling?*, JDSUPRA (9 August 2022), https://www.jdsupra.com/legalnews/the-icts-supply-chain-rules-towards-a – u – 4390528/.

〔26〕 Executive Order 13873 of May 15, 2019, Sec.2.

〔27〕 Executive Order 13873 of May 15, 2019, Sec.1.

查更加具有类比性，均以维护国家安全为目的而对特定外国主体的交易进行干预，并且适用范围存在重合。但是，两种监管工具的侧重点不同，国家安全审查聚焦于“外国投资者”对美国主体实施的重大公司重组或者并购交易，而 ICTS 交易更加关注具体的商业销售交易。〔28〕

（二）ICTS 交易审查的审查程序

《特朗普行政令细则》详细规定了商务部对 ICTS 交易审查的程序，包括提交程序、初步审查、初步决定以及最终决定四个环节。

首先，提交程序是商务部 ICTS 交易审查程序的起点，具体包括三种启动方式：一是商务部收到表明有理由启动审查的信息；二是应其他联邦政府部门的请求；三是商务部依职权自行决定启动。在此阶段，商务部对相关交易是否属于审查范围进行评估，可以要求当事人提供信息或者否决提交申请。

其次，在初步审查程序中，商务部针对受管辖 ICTS 交易是否构成《第 13873 号行政令》所规定的“不当或者不可接受之风险”。在认定存在此风险的情况下，商务部应当与其他政府部门进行协商，并在此基础上作出初步决定。类型上，可以是批准决定、禁止相关交易的决定或者附缓解条件的批准决定。针对该初步决定，交易当事人可以向商务部提交说明进行回应。在当事人进行回应的情况下，商务部应当启动第二次政府部门间协商，并在考虑当事人说明以及其他因素的情况下作出最终决定，包括禁止性决定、批准性决定或者附缓解条件的批准决定。此外，美国商务部的《拜登行政令细则》进一步明确了以下事项的程序规则：（1）ICTS 交易是否构成“不当”或“不可接受”风险的认定程序；（2）发布 ICTS 交易禁令的程序；（3）指令 ICTS 交易的时间安排以及终止方式的程序；（4）可以缓解 ICTS 交易风险因素的程序。〔29〕

（三）拜登政府对 ICTS 交易监管规范的修订

美国总统的更迭并未改变其强化数字领域外资监管的趋势。以《第 13873 号行政令》及其实施条例为基础，美国总统拜登以 IEEPA 等法律的授权为基础颁布的《第 14034 号行政令》对前者进行了部分修订和细化。

其一，继续维持“紧急状态”。《第 14034 号行政令》决定，《第 13873 号行政令》宣布的“紧急状态”应当维持，尤其是外国对手控制的互联网软件应用在美国的广泛应用构成对美国国家安全、外交和经济的威胁。〔30〕该“紧急状态”源于一系列因素，包括外国对手持续性地盗窃或以其他方式获取美国主体的数据，并对美国的国家安全、外交政策和经济构成“非同寻常和极端的威

〔28〕 张怀岭、邵和平：《对等视阈下外资安全审查的建构逻辑与制度实现》，载《社会科学》2021 年第 3 期，第 43 页；Stephen P. Mulligan, *The Information and Communications Technology and Services (ICTS) Rule and Review Process*, CONGRESS.GOV (26 October 2022), https://crsreports.congress.gov/product/pdf/IF/IF11760.

〔29〕U.S. Department of Commerce, Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications, 15 CFR Part 7.

〔30〕 Executive Order 13873 of May 15, 2019, Preface.

胁”。其中，互联网软件应用通过在美国的 ICTS 设备（诸如智能手机）上运行可以访问和捕获大量用户信息，并可能导致外国对手得以访问这些数据进而构成巨大的风险。为应对上述威胁，该行政令要求美国商务部提供采取额外的立法和行政措施的建议，来应对外国对手拥有、控制、管辖或有权指令的主体设计、开发、生产或者提供的互联网软件应用。

其二，具体化安全评估的考量要素，增加互联网软件应用的风险评估。《第 14034 号行政令》认定，有必要将应对 ICTS 领域国家紧急状态的措施进行具体化。美国政府应当审慎地以事实为基础来评估这些威胁，并应对国家安全、外交政策和经济活动所面临的“不当”或者“不可接受”风险，包括对美国核心价值观和基本人权自由的维护与彰显。基于此，该行政令撤销了特朗普时期的三项行政令以及相关实施措施，包括对 TikTok 的禁令（《第 13492 号行政令》）、对微信的禁令（《第 13493 号行政令》）以及 2021 年 1 月 5 日第 13971 号《应对中国公司开发或控制应用或其他软件导致风险的行政令》。

在评估互联网软件应用的风险时，除了考虑《第 13873 号行政令》及其实施条例所规定的风险因素，还应当考虑以下潜在的风险因素：（1）由支持外国对手军事、情报和核扩散活动之主体所有、控制和管理；（2）运用互联网软件应用进行监控活动，从而为间谍活动提供便利；（3）受外国对手胁迫或指派之主体所有、控制或者管理的互联网软件应用；（4）从事恶意网络攻击主体控制的互联网软件应用；（5）收集数据的范围和敏感度；（6）互联网软件应用的用户数量和敏感度；（7）经确认的风险已经或者可以通过独立的可认证措施予以应对的程度。针对安全审查的考量要素，美国商务部于 2021 年《拜登行政令细则》中增加规定额外的风险审查要素，以便其认定涉及互联网软件应用的 ICTS 交易是否构成“不当”或者“不可接受”的风险，尤其新增列入使得外国对手可以访问敏感个人数据以及对互联网软件应用缺乏彻底和可靠的第三方审计等内容。

此外，《第 14034 号行政令》要求美国商务部持续性地评估以下涉及互联网软件应用的交易，包括：（1）对美国信息通讯技术和服务的设计、可靠性、制造、生产、销售、安装、运行或维护构成不当的破坏或者颠覆风险的 ICTS 交易；（2）对美国的关键基础设施或数字经济的安全和弹性构成不当的灾难性后果风险的 ICTS 交易。

三、与外国对手 ICTS 交易审查的基本权利限制

IEEPA 框架下，美国总统以及商务部等行政机关享有对于外国对手交易的极大干预权，但依然受到美国宪法以及行政程序法的限制。然而，这些法律对于行政监管权的限制是借助于一般性条款来实现的，其边界存在不确定性，需要司法机关结合个案事实予以厘定。以下结合“TikTok 诉特朗普案”[31]（下称 TikTok 案）和“微信用户联盟诉特朗普案”[32]（下称微信案）来分析司法机关的裁判逻辑。

〔31〕 TikTok Inc. *v.* Trump, 507 F. Supp. 3d 92 (D.D.C. 2020).

〔32〕 U.S. WeChat Users Alliance *v.* Trump, 488 F. Supp. 3d 912 (2020).

（一）“Winter 要件”作为一般性审查规则

在“TikTok 诉特朗普案”和“微信用户联盟诉特朗普案”中，原告均针对行政机关的限制性干预措施向法院申请临时性救济禁令，并且两个审理法院都是在所谓“Winter 要件”判例法规则的框架下审查是否应当给予原告临时性禁令的救济，阻止行政机关限制性措施的执行。按照判例法规则，临时性禁令是一种例外情况下的救济措施，申请方必须能够明显地举证证明满足以下条件：（1）基于法定权利具有“胜诉的可能”；（2）若不能够获得救济将面临“不可逆的损害”；（3）各种“利益衡量”支持发布救济措施；（4）临时性禁令也符合“公共利益”。在政府是被告一方的情形下，将“对被告方的损害”与“公共利益”两个要件合并。其中，“胜诉可能性”构成 Winter 要件中最为核心的内容。

（二）“TikTok 诉特朗普案”中审理法院的立场

在本案中，原告 TikTok 及其中国母公司字节跳动提起诉讼，主张美国政府的行为违反了《美国行政程序法》、宪法第一修正案以及第五修正案的正当程序条款；超越了 IEEPA 框架下总统以及商务部部长的权限；违反了宪法第五修正案的征收条款，并向法院申请临时性禁令救济。

一是限制措施是否超越 IEEPA 授权的认定。美国总统和商务部是否超越了 IEEPA 的授权构成本案核心的问题。法院认定，原告已经证明了相关禁令可能超越了合法性界限。理由在于，尽管 IEEPA 的授权非常广泛，包含了宣布国家紧急状态以及禁止特定与第三国或其主体之间威胁国家安全的交易；但是，该法也同时规定了两项限制条件，即“对总统的授权不包括直接或间接地对以下事项进行规制的权限”：（1）信息或信息资料的输入或输出。法定类型上包括但不限于出版物、电影、摄影、艺术作品以及新闻推送。[33] 本案中，TikTok 用户交换的信息构成“信息和信息资料”，多数内容属于或者类似于“出版物、电影、摄影、艺术作品以及新闻推送”。而美国商务部禁令的目的则是限制以及最终完全禁止美国用户在该平台评议以及在 TikTok 上留有个人信息，从而至少构成对于美国主体信息资料转移的间接规制。TikTok 构成 IEEPA 意义上的“传播途径”，类似于法定列举类型中的“新闻推送”。（2）不涉及价值转移的“个人通讯”。法院认定，商务部禁令不可否认地将产生禁止美国用户通过 TikTok 分享个人通讯的后果，并且禁令“通过要求从应用市场中移除 TikTok 的应用，并完全关闭 TikTok 会摧毁这一在线社区”。针对美国政府认为 TikTok 上的通讯事实上具有经济价值的主张，法院认定，大量的 TikTok 视频、公共评论以及好友之间关于短视频的私人信息并不具有任何经济价值。

二是“不可逆之损害”要件的认定。“不可逆之损害”要件要求临时性禁令救济的申请人证明损害是“确定、巨大、现实的（而非是理论上的）以及即将发生的，从而明显亟需例外性的救济

〔33〕 International Emergency Economic Powers Act, 50 U.S.C. § 1702 (b) (3).

措施来预防损害”。[34] 法院认定，相关行政令颁布之时，TikTok 是美国用户数量增长最快的 App。禁止从应用市场下载会直接阻碍新用户的流入并可能导致用户流入替代性的平台，从而侵蚀 TikTok 的竞争力。如果禁令生效，但日后被认定非法，会对 TikTok 的用户基础造成不可挽回的损害。

三是利益衡量。针对当事人不同权益与公共利益的衡量，法院认定，本案中“政府的利益是公共利益”。[35] 但是，针对政府的抗辩，即“临时性禁令救济将会取代并阻碍总统在如何最佳应对国家安全威胁上的决策，而这一领域司法机关通常尊重总统的判断”，审理法院援引判例规则认为，司法机关当然必须尊重行政部门“对事实的评估”以及“国家安全和外交事务的敏感性和重要性”。本案中，针对 TikTok 所构成威胁的具体证据以及这些禁令是否是应对这些威胁的唯一有效措施缺乏充分的依据。政府“不可能从这样一种禁令中遭受损害”。[36] 理由在于，“对于非法政府行为的继续并不存在公共利益”，反而，“对于令政府部门遵守涉及其设立和运行的联邦法律存在重大公共利益”。[37]

（三）“微信用户联盟诉特朗普案”中法院的立场

本案中，原告质疑《第 13943 号行政令》的合法性，主张该行政令的限制性措施违反了宪法第一、第五修正案以及《宗教自由复原法》，违法行使 IEEPA 下总统以及商务部的权力，违反《美国行政程序法》的规定，并申请法院颁发临时性禁令救济，但是，并未质疑作为宣布紧急状态并构成该禁令基础的《第 13873 号行政令》的合法性。与 TikTok 案中一样，审理法院将 Winter 判例规则的四项要件作为审查标准，具体包括：（1）基于法定权利胜诉的可能；（2）未能获得临时性禁令救济情况下将遭受不可逆损害的可能；（3）多种权益的衡量有利于原告；（4）临时性禁令救济符合公共利益。[38] 同时，审理法院援引判例规则，在其他临时性救济要件获得满足的情况下，若原告对案件的正当性提出严重质疑并且权益侵害程度的衡量明显有利于原告的情况下，法院发布临时性禁令救济是“适当的”。[39]

一是“胜诉可能性”要件的认定。法院认定，商务部所禁止的交易事实上会排除其关键的通讯平台，延迟或者减少言论，等同于对于言论的审查或者对于言论的事前限制，进而存在侵害原告宪法第一修正案所保障的权利的嫌疑。而且，针对政府存在替代性平台的抗辩，原告也证明了对于华裔美国人或者汉语社区（由于语言的限制）不存在事实上的替代平台或者应用。

此外，对言论自由所采取的内容中性、“时间地点或方式”型限制在以下情况下才满足中级审查的要求：（1）限制措施是“精准制定的”；（2）限制措施有助于政府的重大利益的实现，且与言

〔34〕 Power Mobility Coal *v.* Leavitt, 404 F. Supp. 2d 190, 204 (D.D.C. 2005).

〔35〕 Pursuing America’s Greatness *v.* Fed. Election Comm., 831 F. 3d 500, 511 (D.C. Cir. 2016).

〔36〕 R.I.L-R *v.* Johnson, 80 F. Supp. 3d 164, 191 (D.D.C. 2015).

〔37〕 League of Women Voters of U.S. *v.* Newby, 838 F. 3d, at 12.

〔38〕 Winter *v.* Natural Res. Def. Council, Inc., 555 U.S. 7, 129 S. Ct. 365, 172 L. Ed. 2d 249, 21 Fla. L. Weekly Supp. 547 (2008).

〔39〕 Alliance for Wild Rockies *v.* Cottrell, 632 F. 3d 1127, Id.1134–35 (9th Cir. 2011).

论的内容无关；（3）给通讯自由留有充分的渠道。〔40〕其中，“精准性”的要件要求限制措施不得超越政府促进合法利益实现之必要范围从而对言论自由构成重大负担。同时，与“以内容为基础对言论自由的限制措施”的要求不同，内容中性限制并不要求相关限制措施是实现政府利益可能措施中对权利人限制最小或者侵害最小的措施。〔41〕尽管“国家安全”这一总体利益是重大的，但是政府并未提交有说服力的证据说明对微信的关闭有助于应对上述国家安全担忧。另外，明显存在其他非完全禁止的替代性措施（如在政府设备中禁用微信），或者采取其他措施来应对数据安全。〔42〕

二是其他“Winter 要件”的认定。针对“不可逆之损害”，（限制措施）直接的威胁是通讯平台的消失，从而在不能获得临时性禁令救济的情况下会导致不可逆的损害。根据判例法，宪法第一修正案之自由（即便仅是短期）的丧失毫无疑问地构成不可逆之损害。〔43〕因此，法院认定，在没有明显替代品的情况下关闭通讯渠道会不必要地构成对言论自由的严重限制，而不是促进政府利益的实现。此外，针对美国政府所提出的“微信禁令会对人权保护产生积极效果”抗辩，法院认为：“言论自由是美国民主的基石。我们的国父们用宪法第一修正案来保护这一神圣的权利……近年来，在线平台的增长引发如何将宪法第一修正案的理念应用于现代通讯科技的问题。如今很多美国人（包括原告）通过社交媒体以及其他在线平台来追踪新闻、保持与朋友和家人的联系以及分享对时事的观点。结果，这些平台在诸多方面构成了 21 世纪的‘公共广场’。”〔44〕基于此，即便在担忧重大国家安全和外交政策的情形下，也存在对宪法第一修正案之法定权益侵害之严重质疑。

四、“国家安全”决定的司法审查：现状与走向

除了宪法保障的基本权利限制之外，IEEPA 框架下的与外国对手 ICTS 交易审查和国家安全审查工具所适用的审查标准同为“国家安全”，因此，司法机关对于 CFIUS 以及美国总统的“国家安全”决定是否抑或多大程度上享有司法审查权的立法与判例也可以类比适用于对 ICTS 交易的审查决定。

（一）FIRRMA 之前的司法立场：“罗尔斯案”

美国外国投资委员会在对管辖交易进行审查期间或审查终结后，可以依据对相关交易的风险评估情况，采取“中止交易”“将交易提交总统”“通过协议或者设定条件减少国家安全威胁”三

〔40〕 Ward *v.* Rock Against Racism, 491 U.S. 781, 791, 109 S. Ct. 2746, 105 L. Ed. 2d 661 (1989); Pac. Coast Horseshoeing Sch., Inc. *v.* Kirchmeyer, 961 F. 3d 1062, 1068 (9th Cir. 2020).

〔41〕 McCullen *v.* Coakley, 573 U.S. 464, 486, 134 S. Ct. 2518, 189 L. Ed. 2d 502 (2014).

〔42〕 值得注意的是，审理法院否决了原告基于 IEEPA、APA 以及宪法第五修正案的诉讼请求。

〔43〕 California *v.* Azar, 911 F. 3d 558, 581 (9th Cir. 2018); Elrod *v.* Burns, 427 U.S. 347, 373, 96 S. Ct. 2673, 49 L. Ed. 2d 547 (1976).

〔44〕美国宪法司法审查标准中，对“公共场所”言论的限制设定了较之于非公众场所（例如监狱）更加严格的标准。Executive Order 13925 of May 28，2020，85 Fed. Reg. 34，079.

种类型的措施。在 2018 年 FIRRMA 颁布之前，美国立法并未对 CFIUS 和美国总统的安全审查决定规定救济途径，而是仅在《国防生产法案》中规定“总统所采取的行动及其结论不受司法审查”。实践中，在所谓“政治问题原则”（political question doctrine）下，长期以来奉行总统对于国家安全事项的最终决定权，司法不加以干涉。伴随着地缘政治与经济的变化，在缺乏司法制约的情况下，CFIUS 以及美国总统的国家安全审查决定过于政治化，缺乏透明性。缺乏透明性和司法制约的弊端也在针对华为并购美国 3Com 以及 3Leaf 公司等多项中资企业并购交易审查中得到了充分体现。鉴于此，CFIUS 主导的外资安全审查被称为“特朗普政府保护主义的头号武器”和“终极火箭弹”。〔45〕

上述司法立场在“罗尔斯公司诉 CFIUS 案”（下称罗尔斯案）〔46〕中有所动摇，在该案之前没有一个外国投资者通过司法来挑战行政机关的国家安全决定。该案中，原告 Ralls 公司通过诉讼挑战美国监管部门禁止原告收购美国风电场企业的审查决定。本案原告 Ralls 公司在美国设立，但其股东是中国公民且与三一重工具有紧密联系。作为并购标的的四所风电场分别临近抑或位于美国海军的限制空域。尽管同一位置还有其他外国主体所有的风电场，但时任美国总统奥巴马基于 CFIUS 的建议颁布总统令，禁止该项交易并要求原告完全地转让目标公司。针对该项禁令，原告主张 CFIUS 的调查认定和总统令无效，理由是其违反了《美国行政程序法》、美国宪法第五修正案正当程序条款和平等保护条款的规定。美国政府则主张，原告的正当程序指控属于“政治问题”，而“政治问题原则”禁止司法机关对行政机关的政治决策进行司法审查。

该案审理法院一方面坚持“政治问题原则”的判例法规则，并认定行政部门关于存在国家安全威胁的判断不受司法审查。其理由在于，这样的“判断”构成基于“行政部门外交政策的一个政治问题，而司法机关对此既没有资格和条件，也没有责任作出决策”。〔47〕另一方面，审理法院认为，尽管《国防生产法案》中规定“总统针对 CFIUS 的决定而采取的措施和得出的结论”不应受到司法审查，但没有“明确且令人信服”的证据表明，立法者旨在禁止司法部门对宪法诉讼进行审查。因此，上述规定并不是针对以总统所采取措施程序违法为由所提起的宪法诉讼的可诉性为对象，并认定美国政府剥夺了 Ralls 公司因交易完成而取得的财产利益，而这一剥夺行为缺乏正当程序。这意味着，法院有权对美国总统调查或者禁止威胁国家安全之外国投资的程序予以司法审查。〔48〕

（二）“罗尔斯案”的争议以及 FIRRMA 对司法审查权的立场

“罗尔斯案”的判决引发巨大反响和争议，但在此之后，禁止司法机关对行政部门国家安全的

〔45〕Christopher W. Jusuf, *Investments and Security, Balancing International Commerce and National Security with Expanded Authority for the Committee on Foreign Investment in the United States*, 29 Catholic University Journal of Law and Technology 145, 145 – 176 (2020).

〔46〕 Ralls Corp.*v.* Comm. on Foreign Inv., 758 F. 3d 296, 312 (D.C. Cir. 2014).

〔47〕 Ralls Corp.*v.* Comm. on Foreign Inv., 758 F. 3d 296, 314 (D.C. Cir. 2014).

〔48〕 Ralls Corp.*v.* Comm. on Foreign Inv., 758 F. 3d 296, 307 (D.C. Cir. 2014).

决定进行审查的判例法规则一直未受到挑战。伴随着 CFIUS 对外国投资的国家安全审查干预权在立法和实践层面不断扩张，甚至超越其管辖权，导致外国（尤其是中国）投资者在美投资面临巨大的法律不确定性和歧视性对待。〔49〕这种不确定性和歧视性对待在 2016 年福建宏芯收购德国半导体企业爱思强（Aixtron）的交易中得到淋漓尽致的体现。该案中，目标公司是德国公司，但在美国有附属企业并在美国国防工业的导弹系统发展中发挥重要作用。时任美国总统奥巴马对于该交易采取了极为罕见的措施：在德国联邦经济部已经批准（即针对该交易发布“不存疑证明”）的情况下，美国政府一方面禁止福建宏芯收购爱思强，另一方面将福建宏芯可能将爱思强的技术用于中国的核计划告知德方〔50〕，进而导致德国联邦经济部取消之前的批准，重新启动对该交易的国家安全审查。最终，并购方被迫放弃了该交易。〔51〕

在此背景下，美国学界主张法院应当依据“正当程序”的要求对外国投资审查决定实施有限度司法审查的呼声日益强烈；甚至有意见认为，“罗尔斯案”的判例应当被推翻，司法机关应当有权对行政部门的国家安全决定进行司法审查，以维护美国宪法所保障的个体权利。〔52〕也有观点认为，“罗尔斯案”开启了司法干预国家安全和外交事务的危险先例，且不能忽视已被广泛接受的“政治问题原则”，即司法机关没有能力对国家安全问题作出决定，否则违背美国宪法的权力分立原则。〔53〕

作为对上述法律争议的部分立法回应，2018 年 FIRRMA 明确纳入了“司法审查”制度。具体而言：一方面，原则上美国总统依据 FIRRMA 采取的行动或者得出的结论不受司法审查。另一方面，规定基于挑战总统采取的行动以及得出的结论而提起的民事诉讼仅限于在哥伦比亚特区联邦巡回上诉法院提起。在此类民事诉讼中，如果法院认为行政机关所持有的信息（包括机密或者其他法律所保护的信息）对于案件裁决是必需的，该信息应单方面和秘密地提交法院，法院应当对这些信息保密。〔54〕可见，“罗尔斯案”的判例法规则依然有效：在外资安全审查制度中，司法机关无权对行政部门的国家安全决定进行司法审查，但法院有权对程序事项以及 CFIUS 对事实的认定进行审查。

---

〔49〕 Norman P. Ho, *Asian-American Jurisprudence and Corporate Law:Politicization, Racialization, Foreignness, and the U.S. CFIUS Foreign Direct Investment Review Mechanism*, 4 Widener Journal of Law, Economics & Race 1, 1 – 20 (2012).

〔50〕 Die Chinesen werden nochmal aufgehalten, FAZ v.24.10.2016, https://www.faz.net/aktuell/wirtschaft/unternehmen/wirtschaftsministerium-stellt-aixtron-uebernahme-durch-chinesen-in-frage – 14495317.html; Guy Chazan, *Germany Withdraws Approval for Chinese Takeover of Tech Group*, Financial Times (24 October 2016), https://www.ft.com/content/f1b3e52e – 99b0 – 11e6 – 8f9b – 70e3cabccfae.

〔51〕 张怀岭：《德国外资并购安全审查：改革内容与法律应对》，载《德国研究》2018 年第 3 期，第 59 页。

〔52〕 Isaac Lederman, *The Right Rights for the Right People?The Need for Judicial Protection of Foreign Investors*, 61 Boston College Law Review 703, 703 – 748 (2020).

〔53〕 Christopher M. Fitzpatrick, *Where Ralls Went Wrong:CFIUS, the Courts, and the Balance of Liberty and Security*, 101 Cornell Law Review 1087, 1087 – 1114 (2016).

〔54〕 张怀岭、邵和平：《对等视阈下外资安全审查的建构逻辑与制度实现》，载《社会科学》2021 年第 3 期，第 50 页。

五、统筹国内与涉外法治视域下中国的应对方案

美国外资监管中与外国对手 ICTS 交易审查严重冲击我国数字经济领域科技企业的正常经营，并威胁到我国的供应链安全。对此，我国应当以习近平法治思想为指导，统筹发展与安全，通过贯彻落实“统筹推进国内法治和涉外法治”的要求，提高制度化应对涉外法治风险的能力。一方面，在微观层面应完善数字经济领域企业数据合规机制，积极利用第三方审计机构对企业数据安全、应用安全进行常态化认证，并在个案中针对违法歧视性措施积极利用美国宪法框架下的司法救济机制。另一方面，在宏观层面，则须在对等原则下强化我国以《中华人民共和国反外国制裁法》（下称《反外国制裁法》）为基础，以《中华人民共和国外商投资法》（下称《外商投资法》）、《中华人民共和国网络安全法》等规范为重要组成部分的涉外法治体系。

（一）完善数字经济领域企业数据合规机制及第三方认证

企业合规机制构成完善的公司治理机制的必要组成部分。然而，近年来“中兴事件”等以极端的形式暴露了我国科技企业在涉外合规机制建设与运行中存在的缺陷。在域外针对性和歧视性立法不断强化的背景下，尤其是在数字经济领域，企业的数据合规建设更加迫切和必要。数据安全已经构成国家安全的重要组成部分，而数据竞争背景下实现数据控制和数据安全是近年来美国强化数字经济领域外资监管的重要动因。与外国对手 ICTS 交易审查作为监管工具强化了对中资企业在数字经济领域投资与经营的干预。与外资国家安全审查着力于预防和阻止中资企业通过并购等方式取得美国目标企业的技术和数据不同，与外国对手 ICTS 交易审查则在于确保美国企业在数字经济领域的领先地位，保护个人敏感信息等数据，防止数据外流。

完善数字经济领域我国科技企业的数据合规机制的基础是，我国科技企业应当准确理解美国与外国对手 ICTS 交易监管的适用范围（尤其是受管辖交易的类型）、审查标准（是否对国家安全构成“不当或者不可接受”风险）以及监管部门附条件批准情况下所规定的“组织条件”和“行为条件”。在不违反我国法律的前提下，将上述监管规范转化到企业内部合规机制中，并确保其在实践中得到有效实施，而非仅停留在“纸面合规”上，避免出现类似于“中兴事件”中被美国监管部门发现相关合规承诺或者措施虚设后引发更严厉的监管后果。

实践中，美国司法机关也认可合规措施对于完全禁止性决定的替代作用。例如，在微信案中，审理法院主张，外国对手控制或影响之企业通过运营信息通讯 App 所引发的国家安全威胁并不必然只能采取“关闭”措施才能消除，而是可以采取其他替代性措施来应对。这些“其他措施”包括企业数据合规机制下严格按照美国法要求制定企业数据收集、存储、处理以及传输等行为准则，确保其透明与可靠。对此，中资企业应当积极利用独立第三方机构对自身合规组织的有效性以及产品与服务在个人敏感信息保护、数据安全保障等有效性进行认证或者审计。在组织措施方面，中资企业应当设立专门的企业数据合规部门，配备专业人员，并将合规组织的有效运行纳入董事等高级管理人员法定勤勉义务的范畴。在已经或者极可能发生数据违法的情形下，及时采取补救

措施或预防措施，尤其是人事措施，以避免美国监管部门采取更加严格的外部（行为或组织性）监控措施等风险。

（二）积极利用美国宪法框架下的司法救济机制

与外国对手 ICTS 交易审查作为一种行政权力对于经营活动的干预措施，美国行政部门监管权的扩张在个案中受到司法制约。TikTok 案与微信案均表明，针对监管部门基于外交政策等政治动因而对个体企业采取的限制性措施面临着美国宪法所保障之（实体性或程序性）基本权利的制约。然而，这种制约的边界需要司法机关基于个案涉及的基本权利的类型和其他事实来具体界定。例如，在 TikTok 案中，司法机关在 IEEPA 所规定限制条件的框架下，通过将 TikTok 用户交换的“信息”解释为“构成或者类似于”“出版物、电影、摄影、艺术作品以及新闻推送”，而通过 TikTok 发布构成“传播途径”，从而排除总统直接或间接的规制权。与此不同，微信案中，审理法院在宪法第一修正案所保障之言论自由框架下审查监管部门的禁止性措施是否构成对言论自由的不当限制。“微信”被解释为华裔美国人以及汉语社区的“公共广场”，而微信禁令“等同于”对言论的事前约束，从而必须满足美国宪法司法审查中严格审查的要求。在涉及内容中性的“时间地点或方式”限制时，应当满足司法审查的中级审查标准要求，尤其是应当存在充分的替代性选项。

此外，尽管美国历史上的立法与判例均确认行政机关对于“国家安全”问题的认定不受司法审查，但是不仅从“罗尔斯案”的判例到 FIRRMA 在规范层面上认可司法机关基于公民基本权利对行政权的程序性审查权，而且美国学界更有观点基于行政机关监管权的过度扩张而主张推翻“罗尔斯案”先例。原因在于，该先例通过确认行政机关对于国家安全事项的决定权而对外国投资者通过司法诉讼挑战行政机关国家安全决定产生“阻却效应”或“寒蝉效应”。这反过来导致行政机关的恣意和滥权并进而损害了其合法性，因此主张司法机关应当有权对行政部门的国家安全决定进行司法审查，以维护美国宪法所保障的个体权利。〔55〕

概言之，中资企业在美投资或者在美经营中遭遇外资安全审查或者与外国对手 ICTS 交易审查工具干预的情况下，应当积极利用美国宪法框架下的司法救济机制，以诉讼途径寻求司法机关对行政部门监管权的边界予以理清，从而维护自身合法权益。

（三）对等原则下完善我国反干涉、反制裁涉外法治体系

IEEPA 框架下的与外国对手 ICTS 交易审查机制本质上是美国数字保护主义政策的法律化，不仅规范层面具有强烈的政治针对性和歧视性，而且行政执法更加具有选择性和针对性。〔56〕在 IEEPA 框架下，从特朗普政府《第 13873 号行政令》开始，美国将保护主义政策的针对性和歧视性展现得更加直白。在将中国明确列为“外国对手”的基础上，美国通过颁布一系列总统行政令和商务部实施细则直接针对中资企业参与的 ICTS 交易，甚至直接干预已经完成数年的交易（如

〔55〕 Isaac Lederman, *The Right Rights for the Right People? The Need for Judicial Protection of Foreign Investors*, 61 Boston College Law Review 703, 703 – 748 (2020).

〔56〕 张怀岭、邵和平：《对等视阈下外资安全审查的建构逻辑与制度实现》，载《社会科学》2021 年第 3 期，第 52 页。

TikTok 案）。鉴于此，在对等原则下强化我国以《反外国制裁法》为中心的涉外法治体系是应对美国歧视性保护主义立法的必要措施。诚如学者所言，中美贸易摩擦的“暗线”是“中美之间就制裁与反制裁、遏制与反遏制展开的法律战”。〔57〕目前，我国已经颁布了包括《阻断外国法律与措施不当域外适用办法》《不可靠实体清单规定》以及《反外国制裁法》等法律法规，初步建成了我国的涉外法治体系。然而，总体上我国当前涉外立法处于被动地弥补立法空白阶段，尚待向主动性、系统性立法转型。针对美国数字经济领域与外国对手 ICTS 交易立法，亟须在对等原则指导下完善我国涉外法治体系。

第一，《外商投资法》框架下的外资国家安全审查制度应当遵循对等原则，引入“投资者国别条款”，反制 IEEPA 框架下的“外国对手”条款（以及 FIRRMA 框架下的“特别关注国家”制度）。为了保障中国投资者的合法权益，在判断特定外商投资是否对国家安全构成潜在威胁时将外国投资者的国别，尤其是外国投资者与来源国特定政党或者政府的关系纳入考虑因素之中。通过二元划分，即将外国投资者区分为源自美国与源自其他国家和地区的投资者，将美欧所采取的歧视性审查立法和执法措施对等地应用于我国的外资监管机制中，为实现我国与美欧实质性对等的投资法律环境创造必要的前提条件。

第二，坚持统筹推进国内法治和涉外法治，丰富“国家安全”内涵，完善我国网络安全审查机制。数字经济下，个人敏感信息安全、数据安全以及网络安全构成“国家安全”重要组成部分，而美国、欧盟战略上将我国定位为“对手”和实践中推行“脱钩”“去风险化”使得我国的信息与通讯基础设施供应链的安全（如不当断供）、数据和个人信息的安全（如不当数据收集与出境）形势非常严峻。鉴于此，有必要对标美国 ICTS 交易监管规则，完善我国《网络安全法》《数据安全法》《网络安全审查办法》框架下的“网络安全审查机制”。具体包括：一是将适用范围限缩在美国等对我国采取针对性立法的国家直接或间接所有、控制的信息与通讯技术与服务；二是基于法治原则要求完善网络安全审查中“国家安全”的判断要素，尤其是特定群体（青少年）或行业部门（政府部门、科研院所）个人敏感信息、重要数据与国家安全威胁之间的关联；三是完善现行法框架下的“初步审查—特别审查”二阶程序，依法保障当事人程序性权利，明晰当事人“举报”的程序以及其他救济程序。

第三，对等原则下，实现《反外国制裁法》框架下反制工具的精准化。相较于美国复杂而精准的针对性立法，目前我国反制裁、反长臂管辖的法律工具过于原则性，缺乏明确的程序性规定和实体性判断标准，数字领域中对于国家安全至关重要的 ICTS 交易也缺乏直接的干预手段，而是依赖于外资安全审查、反垄断审查等法律工具，缺乏针对性。相比之下，美国与外国对手交易的管制更加精准：从 IEEPA 作为一般性授权立法，到总统颁布针对特定行业领域的一般性行政令和针对具体交易的行政令，再到商务部的实施细则。三个不同效力层次的法律规范相互结合，既

〔57〕沈伟：《中美贸易摩擦中的法律战——从不可靠实体清单制度到阻断办法》，载《比较法研究》2021 年第 1 期，第 180 页。

能够实现政策目的，同时也将对经济自由的干预降低到最低，从而有利于最大限度地实现经济开放与国家安全之间的平衡。美国的立法与执法实践表明，外资安全审查和与外国对手 ICTS 交易的适用范围虽然有重合，但却各有侧重，不能相互取代。

鉴于此，应当以《反外国制裁法》第 3 条第 2 款的规定为依据，即“外国国家违反国际法和国际关系基本准则，以各种借口或者依据其本国法律对我国进行遏制、打压，对我国公民、组织采取歧视性限制措施，干涉我国内政的，我国有权采取相应反制措施”，在数字经济领域引入针对美国、欧盟等将我国界定为“外国对手”“体制性对手”的 ICTS 交易干预工具。从法律效力和修订的便捷性考虑，适宜由我国商务部、国家发展和改革委员会等部门制定部门规章。内容上，在对标美国与外国对手 ICTS 交易立法的总体目标下，结合我国数字经济发展的实际情况制定明确的审查程序和审查标准。基于比例原则的考量，审查程序中应当纳入特殊的救济程序，从而有助于维护外国投资者的合法权益，防止保护主义。

六、结语

在中美科技竞争日益激烈以及美国单方面推行“中美脱钩”的背景下，美国外资监管的政治化并未随着政府领导人的更迭而弱化，相反，充满政治针对性的法律工具被延续和强化。对我国而言，这些多元的新型法律工具导致中国科技企业赴美投资、开展正常经营面临新的法律风险与不确定性，不仅直接冲击数字经济领域中资企业的投资和经营，而且也威胁数字经济领域全球供应链的安全。作为因应措施，首先应当准确地掌握外资安全审查和与外国对手 ICTS 交易审查工具的制度内容，并将之作为企业完善公司治理，尤其是构建企业数据合规机制的基础。同时，也需要在统筹推进国内法治和涉外法治的视野下，基于个案事实对行政部门滥用监管权的非法干预启动宪法框架下的司法救济，以维护自身合法权益。此外，作为对美国“歧视性限制措施”的反制，应当在对等原则指导下完善我国的涉外法治体系，从而形成必要的制度威慑。

Regulation and Legal Limits of U.S. ICTS Transactions with Foreign Adversaries in the Digital Economy

—Analysis Based on the TikTok and WeChat Ban

ZHANG Huailing

Abstract: Along with geopolitical changes and the U.S. policy of “decoupling” with China, the U.S. legal tools for regulating foreign investment in the digital economy have become increasingly diverse. Normatively, the U.S. government has abused the emergency national security safeguards

authorization under the IEEPA to strengthen the regulatory tools for ICTS transactions with foreign adversaries, which in practice has led to huge legal risks for the operations of Chinese technology companies. At the same time, there are legal limits to that regulatory power, but the boundaries of its authority need to be defined by the judiciary based on the facts of individual cases. As a response strategy for China, at the micro level, the corporate data compliance mechanism in the digital economy should be improved, and the judicial remedy mechanism under the U.S. constitutional framework should be actively utilised against illegal discriminatory measures; At the macro level, China shall adheres to the overall national security concept and strengthens anti-sanctions and anti-interference system based on the *Anti-foreign Sanctions Law* and with the FDI Screening and cyber security review systems as important elements under the principle of reciprocity.

Keywords: Transaction with Foreign Adversaries; Digital Economy; IEEPA; Foreign-Related Rule of Law System

（责任编辑：王乐兵　汪友年）