doi. 10. 3724/1005-0566. 20251019

中国企业境外上市网络安全审查制度优化研究

鄢浩宇
（武汉大学法学院，湖北　武汉　430072）

摘　要：境外上市网络安全审查制度是国际证券监管局势不断紧张和数据跨境活动日益频繁的背景下，由滴滴事件推动形成的应急性立法。随着制度环境和立法背景的不断变化，其暴露的缺陷日益明显，概念解释模糊不清、风险规制存在漏洞、制度设计叠床架屋等问题不仅产生较重的市场合规负担，也造成较大的监管资源消耗。提出应当对境外上市网络安全审查制度进行体系性的调整与革新，参考相关的域外制度经验，厘清制度的核心定位，统筹其与数据安全审查等其他国家安全审查的制度关系，强化其与境外上市证券监管法律制度的衔接，减少监管重叠，提升监管能效，降低合规成本，实现国家安全与市场效率的协调统一。

关键词：境外上市；网络安全审查；网络安全；数据安全；数据跨境
中图分类号：D922. 28；F832；F49　　**文献标识码**：A　　**文章编号**：1005－0566（2025）10－0205－09

Optimizing the cybersecurity review system for Chinese enterprises' overseas listings

YAN Haoyu
（*School of Law*, *Wuhan University*, *Wuhan* 430072, *China*）

Abstract: The cybersecurity review regime for overseas listing is a piece of emergency legislation promoted by the DIDI Incident against the background of increasing tension of international securities regulation and increasingly frequent data transborder flow activities. With the constant change of the institutional environment and legislative background, the defects it exposed are increasingly obvious. Vague concept interpretations, loopholes in risk regulations, superfluous system designs and other problems not only give rise to a heavy burden of market compliance, but also cause a high consumption of regulatory resources. The cybersecurity review regime for overseas listings requires systematic restructuring and innovation. It is necessary to take into account relevant extraterritorial institutional experiences, clarify the core positioning of the system, coordinate the relationship between the system and other national security review systems such as data security review, strengthen the connection between the system and the securities regulation system in overseas listing, reduce regulatory overlaps, improve regulatory efficiency, reduce compliance costs, and finally foster the coordinated integration of national security and market efficiency.

Key words: overseas listing; cybersecurity review; cyber security; data security; cross-border data flow

数字经济时代，全球经济治理体系深度重构与数字技术革命交织，共同推动国际经济秩序的结构性变革[1]。我国在制度型开放的战略部署下，由“要素型开放”向“制度型开放”转型[2]，努力把握国际规则制定的话语权。境外上市网络安全审查制度是一项涉及国家安全、网络数据治理、

收稿日期：2025-05-30　　**修回日期**：2025-09-30
基金项目：国家社会科学基金重大项目“我国资本市场制度型开放的法律体系构建研究”（22&ZD204）；浙江省法学会重点资助课题项目“规范金融数据跨境流动问题研究”（2025NA30）；武汉大学社会科学数智创新研究团队项目“数智治理现代化研究”（WDSZTD2024A01）。
作者简介：鄢浩宇（1997—），男，江西赣州人，武汉大学经济法研究所助理研究员，研究方向为金融法、数字法学。

境外上市活动秩序的综合性制度,在规范企业出海活动中具有重要作用,但该制度作为国家互联网信息办公室对滴滴出行启动网络安全审查这一重大突发网络安全事件(以下简称“滴滴事件”)后产生的应急性立法,随着制度环境和立法背景的不断变化,在实践运行中逐渐暴露出诸多问题,不仅给市场主体增加了过多的合规负担,也给相关主管机构带来了繁重的监管压力,亟须结合现实境况进行制度调整和革新。本文以境外上市网络安全审查的制度源流为切入点,系统梳理其在实践运行中所暴露的制度缺陷,并结合制度运作的现实考察,对制度异化与偏离的成因展开分析与反思,进而提出相应的制度优化与完善路径,最终实现境外上市网络安全审查制度的系统性重塑。

一、境外上市网络安全审查的制度源流

我国的网络安全审查制度以滴滴事件为划分标志。滴滴事件前,我国网络安全审查制度处于初始阶段,仅包含对网络产品和服务的审查,聚焦于网络环境安全和信息系统稳定;滴滴事件后,我国网络安全审查制度进入发展阶段,制度范畴得到较大拓展,纳入了对数据处理活动以及境外上市过程中网络数据安全的审查,并逐步统筹网络环境、信息系统和数据内容的整体安全。但随着制度环境和立法背景的不断变化,境外上市网络安全审查制度开始陷入制度边界模糊与制度定位不清的尴尬处境,亟须进行制度革新。

(一)制度起源:以网络安全审查制度为基础

境外上市网络安全审查是网络安全审查制度的一部分,以网络安全审查制度的总体规则框架为基础。2014—2020 年为我国网络安全审查制度的初始阶段,这一阶段构建了网络安全审查的制度雏形。2014 年,国家互联网信息办公室首次在部门工作规划中提出要建立网络安全审查制度,此后通过法律层面的原则性规定、中央纲领性文件的引导推动、部门规章的规则细化初步形成了网络安全审查制度的规则体系。网络安全审查制度的产生,与互联网技术的快速发展和数字经济的蓬勃兴起密切相关,在总体国家安全观的框架下,将网络安全纳入国家安全审查,是对既有国家安全审查体系的重要补充与应然延伸,是保障国家数字主权的必然要求[3]。但在这一阶段,网络安全审查制度局限于网络产品和服务采购活动的审查[4],聚焦于网络环境安全和信息系统稳定,重静态审查而轻动态审查,重“引进来”的审查而轻“走出去”的审查。

(二)制度发端:滴滴事件产生的应急性立法

境外上市网络安全审查制度具有明显的应急性立法特征,中外证券监管法律制度的紧张对立是制度产生的根本原因,滴滴事件的爆发是制度产生的直接原因。2021—2022 年是我国网络安全审查制度的发展阶段,这一阶段网络安全审查的制度范畴进行了较大的拓展,境外上市网络安全审查制度在这一阶段产生。2020 年 12 月,美国《外国公司问责法案》(HFCAA)签署生效,其对外国企业的审计底稿跨境要求与我国对中资企业的审计底稿本地化要求形成抵触,造成数据跨境风险及在美上市中资企业的退市危机[5],为后续滴滴事件的爆发埋下伏笔。2021 年 7 月 2 日,滴滴事件爆发,中国企业境外上市活动一度陷入停滞状态,中央部门开始推动相关的制度改革,仅半年时间内,针对企业跨境上市的网络数据安全和证券监管问题颁布了一系列规范。根据 2021 年修订的《网络安全审查办法》(若无特别说明,本文后续使用的《网络安全审查办法》均指 2021 年修订后的版本),网络安全审查制度由原来的局限于对网络产品和服务采购活动的审查,开始拓展到对数据处理活动、企业境外上市活动的审查,逐渐统合静态审查和动态审查,兼顾“引进来”和“走出去”的双向审查。

但这一阶段的网络安全审查制度具有明显的应急性立法特征,在当时的立法背景下,中外证券监管法律制度紧张对立,企业境外上市活动风险激增,为了维护国家金融和网络数据安全,亟须相关的制度规则填补该领域的立法空白。某种程度上,此时应运而生的境外上市网络安全审查制度即发挥了这一作用,其不仅承担了网络安全审查制度应有的职能,还承担了企业境外上市证券监管、数据出境流动安全保障等相关法律制度的职能,导致其在制度产生之初即带有制度目的上的混合和杂糅,为后续立法背景变化后制度规则的边界不清和叠床架屋等诸多问题埋下了隐患。

（三）制度现状：立法背景变化后的尴尬处境

随着制度环境和立法背景的不断变化，网络安全审查制度陷入尴尬处境，面临制度定位模糊和制度边界不清的问题，亟须反思和革新。2022年至今，《数据出境安全评估办法（2022）》等数据跨境流动相关规范陆续出台，《境内企业境外发行证券和上市管理试行办法（2023）》等企业境外上市相关规范陆续出台，数据跨境流动和境外上市监管法律制度逐渐完善和成熟，为企业境外上市活动提供了多元的安全保障，此时不再需要依靠网络安全审查制度对相关领域的立法空白进行应急性的填补，网络安全审查制度理应进入反思和革新阶段。境外上市网络安全审查制度与逐渐成型的数据跨境流动法律制度、企业境外上市监管法律制度之间出现规则交叉和重叠，造成合规负担与监管冗余，已经形成对现有数据跨境流动和境外上市监管法律制度发展的阻碍。因此，需要重新厘清境外上市网络安全审查的制度定位与制度边界，明确制度存续的合法性基础，对制度本身进行系统性的审视与重塑。

二、境外上市网络安全审查的制度缺陷

实践中，境外上市网络安全审查制度对于相关核心概念的界定尚不清晰，对于部分潜在的安全风险未纳入规制范围。加之制度环境和立法背景变化后造成的规则交叉重叠和制度叠床架屋，导致其暴露出越来越明显的制度缺陷，亟须作出系统性的调整和完善。

（一）概念解释模糊不清

概念定义的准确性是制度有效运行的基础[6]，境外上市网络安全审查制度最核心的条文依据为《网络安全审查办法》第7条，“掌握超过100万名用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查”。但该条文中的相关概念存在定义模糊的问题，导致规则解释不清，产生制度执行过程中的争议和矛盾。

首先，对“网络平台运营者”的概念解释不清。根据立法资料，2021年7月发布的《网络安全审查办法（修订草案征求意见稿）》中曾采取“运营者”的表述，但在2021年12月发布的《网络安全审查办法》正式稿中改为采用“网络平台运营者”的表述，这一概念表述的转变从立法意图上解释，是为了明确境外上市网络安全审查制度的审查重点，集中聚焦于网络平台企业等掌握数据规模较大、影响范围较广的企业，减少不必要的审查负担。但由于《网络安全审查办法》未对“网络平台运营者”这一概念作出清晰的解释，导致制度实践中产生一系列问题。部分企业不确定自身是否属于网络平台运营者，但出于合规风险的考量仍然花费较大成本进行解释说明、咨询确认或申报审查，增加了不必要的企业合规负担和监管资源消耗，拖延了企业的上市节奏。例如，星辉印刷（NASDAQ. SFHG）、昊鑫控股（NASDAQ. HXHX）等企业均表示对“网络平台运营者”这一概念的疑惑，并在上市过程中花费较大成本进行解释说明；优博控股（08529. HK）、宜搜科技（02550. HK）等企业出于对“网络平台运营者”这一概念的困惑，以实名方式向国家网信部门进行咨询确认；小I机器人（NASDAQ. AIXI）等企业明显不属于典型的网络平台运营者，但仍然主动向网信部门申报网络安全审查，直到收到无需网络安全审查的确认后才继续开展上市工作流程。

其次，对“赴国外上市”的概念解释不清。根据立法资料，2021年7月发布的《网络安全审查办法（修订草案征求意见稿）》中采取的是“赴国外上市”的表述，使得市场实践对于赴香港上市是否属于赴国外上市、是否需要申报网络安全审查产生疑义，2021年11月发布的《网络数据安全管理条例（征求意见稿）》中增加“赴香港上市，影响或者可能影响国家安全的，应当申报网络安全审查”，似乎对这一问题作出了回应，但在2021年12月发布的《网络安全审查办法》正式稿中仍然采取了“赴国外上市”的表述，且没有再对该表述作出其他解释。从立法意图看，采取赴国外上市的表述一方面是为了将赴香港上市和赴美国、新加坡、英国等国外上市区分开来，明确制度审查的重点，集中聚焦于对国家安全可能产生实质影响的国外上市活动，另一方面是考虑到赴香港上市在我国企业境外上市中占据了较大比重，在没有明显安全威胁的情况下将赴香港上市纳入审查范围可能造成较大的企业合规负担和行政监管压力。但这一制度立法意图并未得到良好的传达和落实，导致

实践中仍有大量赴港上市的企业出于合规风险的考虑主动解释说明、咨询确认甚至申报审查,违背了制度初衷。例如,嘀嗒出行(02559. HK)、健康之路(02587. HK)、沪上阿姨(02589. HK)等企业均表示对“赴国外上市”这一概念的疑惑,并在上市过程中花费较大成本进行解释说明;顺丰控股(06936. HK)、蜜雪冰城(02097. HK)、绿茶集团(06831. HK)等企业出于对“赴国外上市”这一概念的困惑,实名向国家网信部门进行咨询确认,收到无需申报审查的确认后才继续开展上市工作流程。

上述概念解释不清的问题将严重降低境外上市网络安全审查的制度可预期性。一方面,可能导致市场主体应申报而未申报审查,产生风险隐患,若后续由国家网信部门依职权启动审查将对市场主体造成较大的负面影响;另一方面,可能导致市场主体无需申报而进行申报,徒增企业合规负担和行政监管压力,不利于促进境外上市活动的健康发展。

(二)风险规制存在缺漏

首先,现有制度仅规定掌握大规模个人信息的企业应当纳入申报审查范畴,忽略了掌握重要数据的企业也应当纳入申报审查范畴。从制度目的上看,境外上市网络安全审查是为了保障企业在境外上市过程中的网络主体安全,包括网络环境安全、信息系统稳定和数据内容安全,以避免国家安全遭受威胁,重要数据是一旦遭到篡改、破坏、泄露或者非法获取、非法利用,可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据,其相比于大规模个人信息,更加直接地关乎国家安全[7]。按照举轻以明重的原则,如果掌握大规模个人信息的企业需要纳入申报审查范畴,则掌握重要数据的企业更应当纳入申报审查范畴。从规范体系上看,《网络安全审查办法》第 7 条仅规定掌握 100 万条以上个人信息的企业应当纳入申报审查范畴,但在第 10 条的重点评估风险因素中却包含了重要数据被非法利用、非法出境以及被外国政府影响控制的风险,如果在前期申报过程中未将重要数据纳入申报审查范畴,则在后续安全评估过程中就无法对重要数据出境的安全风险进行审查,为了弥补规范设计上的矛盾,应当将重要数据纳入申报审查范畴。

其次,目前境外上市网络安全审查的大量制度规则均围绕事前审查评估展开,对于事中事后持续的风险控制则少有涉及。其一,未规定重新申报审查的情形,难以将企业境外上市后因环境或业务变化而产生的风险纳入申报审查范围。例如,当企业在境外上市初期不满足审查条件,但在持续运营过程中掌握的个人信息规模达到审查条件时,落入规制的空白,由于未规定重新申报审查的情形,只能根据《网络安全审查办法》第 16 条第 1 款以“影响或可能影响国家安全”为由依职权启动审查,如此将极大地破坏市场主体的行为预期,并可能给市场主体的正常经营造成较大负面影响。其二,对于风险消减措施的规定过于片面,不利于境外上市过程中对风险的及时处置。《网络安全审查办法》第 16 条第 2 款对风险消减措施的适用情形进行了规定,但从体系解释的角度看,该款仅适用于依职权启动网络安全审查的情形,而无法适用于依申请启动网络安全审查的情形,适用条件过于片面,不利于境外上市过程中风险的消减和控制。与之相对的是,《境内企业境外发行证券和上市管理试行办法》第 9 条则规定了“及时整改、作出承诺、剥离业务资产”等风险消减措施可以适用于依申请开展的境外上市相关安全审查中。为了更好地消减和控制境外上市过程中的风险,与其他相关部门规则形成衔接,风险消减措施的适用条件应当进行拓展。

(三)制度设计叠床架屋

根据实践调研,境外上市网络安全审查的申报内容主要包括企业上市情况、企业控制权情况、企业掌握数据情况、企业对外提供数据情况等方面,中国网络安全审查认证和市场监管大数据中心(原名为中国网络安全审查技术与认证中心,以下简称 CCRC)将根据申报内容判断是否需要进入实质审查程序,以《网络安全审查办法》第 10 条中的重点评估内容为依据开展审查。

基于制度产生的历史背景,境外上市网络安全审查在设计之初即具有制度目的上的混合和杂糅,随着数据跨境流动、境外上市证券监管等制度规则的不断完善和成熟,境外上市网络安全审查制度中的相关内容越来越暴露出规则交叉、重复

评估、边界不清的问题,导致制度规则间的叠床架屋。

一方面,境外上市网络安全审查可能与数据出境安全评估制度产生重叠。在审查内容上,境外上市网络安全审查内容包括企业对外提供数据及其是否可能危害国家安全的情况,涵盖“数据被窃取、泄露、损毁、非法利用、非法出境以及被外国政府影响控制的风险”,数据出境安全评估的审查内容也包括“数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险”,两者在数据出境安全风险的审查内容上高度相似[8]。但在审查程序和审查机构上却不尽相同,若不区分制度重心和协调制度衔接,可能造成重复审查、前后矛盾的问题[9]。

另一方面,境外上市网络安全审查可能与境外上市证券监管法律制度产生重叠。其一,境外上市网络安全审查中 CCRC 对于数据出境安全风险的审查可能与中国证监会对审计底稿等相关文件资料数据跨境的监管产生重叠,CCRC 和中国证监会不同的审查程序和审查要求可能造成制度规则上的矛盾和监管机构间的权力掣肘。其二,境外上市网络安全审查中 CCRC 对于企业控制权架构的审查与境外上市备案过程中国证监会对股权结构和控制架构的核查形成重复[10],增加了企业合规成本和监管资源消耗。其三,境外上市网络安全审查可能过度拖延企业的境外上市进程,根据《境内企业境外发行证券和上市管理试行办法》第 9 条规定,境外上市网络安全审查需要在境外上市备案前完成,由于网络安全审查的周期较长、结果不确定、审查内容又与境外上市备案程序存在大量交叉,如果缺乏制度的衔接协调,将极大地延误甚至破坏境外上市进程。

三、境外上市网络安全审查的制度反思

通过对境外上市网络安全审查制度的运行进行实证考察,可以发现其在实践中所面临的突出矛盾与挑战;结合域外相关制度模式的比较研究,则能够揭示我国制度在国际语境下的独特性与局限性;在理论层面对制度定位进行逻辑厘清,有助于揭开制度设计背后的底层逻辑。由此,不仅能够全面反思现行制度存在的问题,也为其未来的优化与完善奠定基础。

(一)制度运行的实证考察

实践中,境外上市网络安全审查的开展情况可以分为 6 种情形,分别为未申报审查且未在招股书中说明原因、未申报审查但在招股书中说明原因、咨询后确认无需申报审查、申报审查后被确认无需审查、申报审查后通过审查、申报审查后未通过审查。这 6 种情形的审查程度逐渐递进,对企业境外上市活动的影响依次增强,合规成本和监管强度也随之增大。通过统计 2024 年 5 月—2025 年 5 月近一年境内企业赴香港、美国上市的网络安全审查情况(见表 1、表 2),可以得出以上 6 种审查情形在实践中的分布情况,进而分析制度运行的实际效果与潜在问题。

表 1　2024 年 5 月至 2025 年 5 月赴港上市企业网络安全审查情况

审查类型	数量	占比/%	代表企业
未申报审查且未在招股书中说明	30	42.3	老铺黄金、美的集团、宁德时代等
未申报审查但在招股书中说明	12	16.9	泰晶科技、宜宾银行、沪上阿姨等
咨询后确认无需申报审查	29	40.8	嘀嗒出行、顺丰控股、蜜雪冰城等
申报审查后被确认无需审查	0	0	无
申报审查后通过审查	0	0	无
申报审查后未通过审查	0	0	无
总计	71	100	

表 2　2024 年 5 月至 2025 年 5 月赴美上市企业网络安全审查情况

审查类型	数量	占比/%	代表企业
未申报审查且未在招股书中说明	4	9.8	朴荷生物、山友暖通、柏雅国际等
未申报审查但在招股书中说明	28	68.3	荣业食品、网班科技、亚盛医药等
咨询后确认无需申报审查	3	7.3	星竞威武、云学堂、中驰车福
申报审查后被确认无需审查	1	2.4	软云科技
申报审查后通过审查	5	12.2	进馨科技、一品成客、霸王茶姬等
申报审查后未通过审查	0	0	无
总计	41	100	

在赴港上市的网络安全审查中,完全没有实质审查的情形,大量关于审查的解释说明和咨询确认增加了不必要的合规监管负担。其中,有 12 家企业(16.9%)在招股书中对境外上市网络安全审查的相关问题作出了详细的解释和说明。有 29 家企业(40.8%)通过电话实名咨询或现场实名咨询的方式向 CCRC 确认无需申报境外上市网络安全审查,并在招股书中进行了详细的记录和阐述。

上述解释说明和咨询确认普遍围绕“企业是否属于网络平台运营者”“赴香港上市是否属于赴国外上市”等概念定义问题展开,表明相关制度概念解释不清的问题已经给市场实践带来了负面影响。

在赴美上市的网络安全审查中,实质审查的占比显著提升,网络安全审查对企业境外上市活动的影响程度显著提高,但仍然存在风险规制的漏洞。其中,有 4 家企业(9.8%)未申报境外上市网络安全审查且未在招股书中作出任何解释说明,有 28 家企业(68.3%)未申报境外上市网络安全审查但在招股书中作出了一定的解释说明,对未申报审查原因的解释说明集中于“企业不属于网络平台运营者”“企业未掌握超过 100 万名用户个人信息”等,但上述做法存在两方面的问题,可能导致风险规制的漏洞。一方面,现行《网络安全审查办法》并未对网络平台运营者这一定义作出明确解释,企业的自评估可能存在偏误,造成应当申报审查而未申报的情形。另一方面,企业可能存在上市过程中不满足申报审查条件,但在后续的经营过程中由于业务范围和经营模式的重大变化达到申报审查条件,仅判断过去一段时间内的数据存量和增量不足以实现准确评估,若未规定重新申报审查的情形,将导致风险规制的漏洞。

境外上市网络安全审查制度的实证考察进一步印证了现有制度规则存在的缺陷,一方面是赴香港上市中存在制度解释不清导致的不必要的合规监管负担,另一方面是赴美国上市中存在制度解释不清和规则设计缺陷导致的风险漏洞问题,合规负担过重与风险规制不足同时存在,表明现有制度规则的不周延。

(二)制度模式的域外经验

在全球制度比较的视角下,中国的境外上市网络安全审查制度具有较强的制度独特性,无法在域外找到完全对应的制度安排。相较之下,域外国家和地区虽然同样注重资本流动、数据出境与国家安全的耦合,但往往是以外国投资安全审查和数据出境管控制度为基础,尚未发展出与我国境外上市网络安全审查制度直接对应的制度模式。

美国通过外国投资安全审查和数据出境的针对性管控实现与我国网络安全审查相似的制度安排。在外国投资安全审查方面,美国《外国投资风险审查现代化法案》(FIRRMA)授予外国投资委员会(CFIUS)审查权力,评估外国投资是否可能对美国国家安全构成威胁,尤其是在涉及敏感技术、关键基础设施和大规模个人数据的交易中,CFIUS 具有阻止或附条件批准的权力。这与我国网络安全审查制度中对关键信息基础设施运营者采购产品和服务的审查具有相似性,二者均强调防范外部资本或交易对国家关键网络和数据信息资源的潜在控制[11]。在数据出境管控方面,2024 年拜登政府发布第 14117 号行政令,强调防止中国、俄罗斯等“受关注国家”获取美国人敏感个人数据及美国政府相关数据,并要求建立严格的数据安全审查机制。同年,美国国会通过《防止外国对手获取美国人数据法案》(PADFA),禁止中国、俄罗斯等“外国对手”获取美国个人数据,并设置了严格的审查和限制。这些规定与中国境外上市网络安全审查中对数据跨境流动安全风险的审查高度相似。由此可见,虽然美国没有直接针对本国企业境外上市设置网络安全审查制度,但其通过相关的立法和行政命令,在本质上实现了相似的防控目标。

欧盟同样通过外资安全审查和数据出境管控实现相似的制度安排。一方面,《欧盟外资审查条例》确立了针对外国直接投资的安全审查机制,要求在涉及关键基础设施、核心技术和敏感数据的情况下进行严格审查,从而确保外国资本进入不会损害欧盟的公共秩序和安全[12]。另一方面,欧盟《通用数据保护条例》(GDPR)通过对个人数据跨境流动设置“充分性认定”或标准合同条款等合规机制,对企业跨境经营和境外交易构成了实质性约束。因此,虽然欧盟并未建立直接针对境外上市的网络安全审查制度,但其通过制度组合同样体现出对外资引进和企业出海过程中网络数据安全的审查。

综上所述,虽然中国的境外上市网络安全审查制度无法在域外找到完全对应的制度范式,但各国存在功能相似和目的共通的制度安排,即围绕国家数字主权,对于外资引进和企业出海过程中的网络数据安全进行审查,以确保数据与资本的跨境流动不会侵蚀本国的安全边界。因此,中国境外上市网络安全审查在制度优化过程中,应

当在保持安全底线的同时,注重与国际主流规则的衔接,以实现国家安全与市场发展的动态平衡。

(三)制度定位的逻辑厘清

应当明确境外上市网络安全审查的核心制度目的,即网络主体安全。境外上市网络安全审查的制度目的在于通过构建系统性风险防控机制,聚焦网络主体安全这一核心维度[13],针对境外上市过程中网络环境安全、信息系统稳定及数据内容安全三大要素进行保障,强化对网络主体的可信性、可控性与安全性审查,确保跨境上市活动不会对相关网络设施的完整性、网络服务的连续性及网络数据主权的安全性造成威胁。在容易产生交叉重叠的几项制度当中,数据出境安全评估制度侧重数据跨境流动的合规性,企业境外上市证券监管制度聚焦境外上市活动可能给资本市场带来的安全影响,境外上市网络安全审查制度则以网络主体安全为锚点,通过穿透审查境外上市主体的控制权架构、技术规制水平、数据治理能力及供应链依赖性,防范境外资本通过股权控制、技术依赖或数据聚合等方式干预网络主体的运营进而威胁我国的国家安全,保障境外上市企业网络主体的可信性、可控性和安全性,具有鲜明的制度宗旨。

四、境外上市网络安全审查的制度优化

制度环境和立法背景的变化以及制度本身存在的规则设计缺陷导致境外上市网络安全审查难以发挥应有的制度效果,零敲碎打式的规则调整不足以推动制度的有效革新,需要对境外上市网络安全审查制度进行体系性的重塑。

(一)统筹制度协调以减少监管重叠

一方面,需要统筹协调境外上市网络安全审查与数据出境安全评估之间的关系。数据出境安全评估是数据安全审查制度的一部分,与网络安全审查同属于国家安全审查体系[14],两者既存在制度联系也存在制度区别。境外上市网络安全审查主要关注主体性内容,包括企业主体的控制权架构、技术规制水平、数据治理能力,数据安全审查主要关注客体性内容,包括数据跨境过程中和跨境后的保密性、完整性和可用性[15],境外上市网络安全审查应当着重于数据内容的审查以及对数据控制能力、数据治理能力的审查,数据安全审查应当注重于数据在跨境中和跨境后可能产生的风险以及相关应对措施安全性的审查[16],从而使两者在审查内容上明确不同的侧重点。此外,境外上市网络安全审查是基于未来数据跨境流动场景的预设进行的风险审查,数据安全审查是基于已有数据跨境流动场景的现实进行的风险审查,可以通过两者在审查考量上的不同区分制度的实施,进而避免监管的重叠。

另一方面,需要统筹协调境外上市网络安全审查与境外上市证券监管法律制度之间的关系。一是可以建立境外上市网络安全审查的申报预审制度。CCRC 应当开放沟通咨询渠道,企业在准备境外上市的早期阶段,可以通过自评估判断是否可能涉及网络安全审查并提前联系 CCRC,为进入实质审查程序和筹备相关材料预留充足时间,避免延误后续的上市进程。二是可以建立申报材料的复用机制。在申报材料上,企业境外上市需要向证监会提交的招股书、说明书、法律意见书等材料足以覆盖境外上市网络安全审查中大部分申报审查内容,可以协调 CCRC 和中国证监会的申报材料要求,促进企业前期准备的境外上市备案申报材料在网络安全审查中的复用,降低企业的合规压力。三是应当强化国家网信部门与中国证监会之间的沟通协调。应当发挥网络安全审查工作机制成员组的统筹协调作用,建立网信部门与证监会之间的沟通协调和信息共享机制[17],CCRC 可以将相关的网络安全审查意见向证监会反馈,证监会发现可能的网络数据安全风险时也应当及时向网信部门反馈,两者应当根据各自职责明确在不同审查或备案阶段的主导或协助关系,共同推进企业境外上市活动的有序高效开展。

(二)强化风险规制以提升监管能效

首先,应当将重要数据纳入境外上市网络安全审查的申报审查范畴。如前所述,无论从制度目的还是规范体系上解释,均应将重要数据纳入申报审查范畴,《网络安全审查办法》在制定之初并未将重要数据纳入申报审查范畴的立法考量在于,当时的重要数据认定和识别标准尚不清晰,相关的国家标准、行业指南尚处于征求意见的状态,相关的行业重要数据目录制定也尚处于起步阶段,贸然将重要数据纳入申报审查范畴,可能引发

较大争议,增加制度运行的不确定性,给制度的有效实施造成障碍。但随着相关规则制定和立法改革的不断推进,制度环境和立法背景已经发生很大变化,国家标准《数据安全技术 数据分类分级规则》(GB/T 43697 - 2024)的出台为重要数据的认定和识别提供了重要的指导,众多行业领域都已制定相关的重要数据识别指南,各行业领域对于重要数据目录的编制也已经较为成熟,此时应当将重要数据纳入申报审查范畴,强化风险规制的系统性和有效性。

其次,应当优化重新审查和风险消减的制度规则。一方面,应当明确境外上市网络安全审查中重新审查的规则情形。企业境外上市过程中的网络数据安全风险是动态变化的[18],原有审查是在特定时间节点、特定业务模式和技术架构基础上作出的评估,一旦市场主体的控制权架构、业务范围、数据处理方式、技术应用或合作对象等发生重大变化,原有的风险识别与防控机制不再适用,应当要求市场主体在风险状况变化时重新申报审查。同属于国家安全审查体系的相关制度中,《外商投资安全审查办法》《数据出境安全评估办法》当中均规定监管机构对市场主体作出无需审查或审查通过的决定后,当事人的运营情况或行为活动发生重大变化,影响或者可能影响国家安全的,应当重新向监管机构申报审查,网络安全审查制度也应当明确重新审查的规定。另一方面,应当拓展风险消减措施的适用范围。滴滴事件中,国家网信部门对滴滴出行采取的暂停新用户注册、下架相关 App 的处置行为属于典型的风险消减措施,但目前该类风险消减措施仅适用于依职权启动审查的情形,适用范围过于局限。应当明确的是,风险消减措施的目的在于控制网络数据安全风险的蔓延,不应以审查程序是否依职权启动而限制了该措施功能的发挥,一旦发现企业境外上市过程中的网络数据安全风险可能扩散和加重,无论由监管机构依职权启动审查的情形,还是由市场主体自主申报审查的情形,均应当适用风险消减措施。

(三)优化制度规则以降低合规成本

概念解释的模糊将加剧制度运行的不确定性,削弱制度的可预期性,使市场主体在合规过程中陷入过度防御与资源浪费的困境[19],审查结果的过于刚性,将限制企业正常的境外上市需求,削弱市场活力。因此,需要从明晰制度概念解释和优化制度审查结果两个方面对制度规则进行革新,以降低企业的合规成本,在国家安全与市场效率之间实现协调统一[20]。

1. 明晰制度概念解释

首先,应当明确“网络平台运营者”的概念。现行《网络安全审查办法》中并未对网络平台运营者这一概念作出明确的解释,相关的法律法规中也并无对这一概念的直接解释,通过对相近概念的提炼归纳,可以将概念定义方式划分为两种模式:一是基于功能主义的概念定义[21],其聚焦于网络平台在提供经营场所、交易撮合、信息发布等服务中的作用,强调其作为组织架构为双边或多边主体开展交互活动所提供的功能支撑;二是基于业务场景的概念定义,其将网络平台定义为向用户提供信息发布、社交、交易、支付、视听等互联网平台服务的数据处理者。网络安全审查制度的目的在于评估网络平台运营者的平台功能所带来的安全风险,基于业务场景的概念定义有循环定义之嫌,基于功能主义的概念定义更具备实际价值。因此,应当基于功能主义对网络平台运营者的概念定义作出解释,并着重考虑 3 点因素:一是业务内容是否涉及交易撮合、信息发布、社交通信等典型的网络平台服务类型;二是业务内容是否包含双方或多方的交互和连接关系;三是业务内容是否具有累积或汇聚大量数据的可能性。

其次,应当明确“赴国外上市”的概念。《网络数据安全管理条例(征求意见稿)》中曾规定“赴香港上市,影响或可能影响国家安全的应当申报网络安全审查”,这种解释方式存在不当之处。一方面,赴香港上市影响或可能影响国家安全的可能性较小,即使出现相关情形也可以通过《网络安全审查办法》第 16 条依职权启动审查,无需特别规定;另一方面,采用上述解释方式反而会强化赴港上市可能需要网络安全审查的暗示,诱导市场主体进行合规加码。科学的方式应当是在附则或条文末尾对赴国外上市进行概念上的解释,明确赴国外上市不包含赴香港上市等情形,以厘清境外上市网络安全审查的制度边界。

2. 优化制度审查结果

应当增加附条件通过审查作为一种新的审查结果,以平衡境外上市网络安全审查中国家安全与市场效率的平衡需求。当前境外上市网络安全审查的结果仅包括审查通过和审查不通过两种情形,全有或全无的二元裁量导致审查结果过于刚性,不利于企业的境外融资与国际市场拓展。在外商投资安全审查、经营者集中审查等安全审查制度中,均设置了附条件通过审查的规则,通过设置股权结构限制、经营行为约束、持续监督机制等相关要求允许企业附条件通过审查,以平衡国家安全和市场效率。应当探索设置境外上市网络安全审查的"附条件通过审查"机制,为企业提供整改优化的路径选择,通过业务剥离、资产拆分、数据活动调整等整改措施降低企业赴国外上市的网络数据安全风险,企业可以在作出承诺进行整改的条件下保留继续推进上市计划的可能性。为保障安全性,对于附条件通过审查的情形,应当对相关承诺的执行情况进行持续性的监督,以避免在获得审查通过后重新引发安全风险。

五、结语

在数字经济深刻重塑国家治理边界与全球市场秩序的时代背景下,境外上市网络安全审查制度不仅是对资本全球流动的制度回应,更是国家实现金融安全与数字主权的战略部署。正如Zuboff[22]所言,数字时代,数据不再仅仅是一种资源,它成为权力、控制和操纵的焦点,网络数据空间的治理,因其跨域特性和高技术属性,已突破传统金融监管范畴,进入法、技、权交织的新领域[23]。境外上市网络安全审查制度不应停留在一项应急性立法,而应当发挥其对境外上市过程中网络安全、数据安全、金融安全的综合性治理功能,应避免制度设计的叠床架屋,厘清制度功能的核心定位,统筹制度规则的协调,完善制度规则的设计与解释,通过建立前置性、可控性与包容性的审查机制,重塑数字时代下制度型开放和全球化路径中的安全逻辑。

参考文献:

[1]陈颖. 制度主义视角的全球数据监管扩散:基于跨国面板数据的事件史分析[J]. 中国软科学, 2025(7): 180-189.

[2]冯果. 资本市场制度型开放的内在机理与法治因应[J]. 北京大学学报(哲学社会科学版), 2023(5): 164-174.

[3] FRATINI S, HINE E, NOVELLI C, et al. Digital sovereignty: a descriptive analysis and a critical evaluation of existing models[J]. Digital society, 2024, 59(3): 1-27.

[4]李青. 美国网络安全审查制度研究及对中国的启示[J]. 国际安全研究, 2017(2): 47-65.

[5]姜立文,姜欢. 数据安全对跨国证券监管的法律挑战与对策[J]. 南方金融, 2021(11): 83-92.

[6]雷磊. 法教义学的基本立场[J]. 中外法学, 2015(1): 198-223.

[7]刘金瑞. 数据安全范式革新及其立法展开[J]. 环球法律评论, 2021(1): 5-21.

[8]曹泮天,袁瑞璟. 企业境外上市数据安全风险的预防性治理[J]. 河北学刊, 2023(3): 203-210.

[9]鄢浩宇. 金融数据协同治理的制度困境与路径突破[J]. 财经科学, 2025(3): 45-57.

[10]刘向东. 企业境外上市监管与中概股回归[J]. 中国金融, 2022(4): 49-51.

[11]包柠榛. 美国外资国家安全审查制度中的数据审查与应对[J]. 国际商务研究, 2025(3): 103-114.

[12]姚若楠. 数字权力竞争下美欧外资安全审查的规则演进与中国应对[J]. 国际经贸探索, 2025(8): 104-118.

[13]马宁. 国家网络安全审查制度的保障功能及其实现路径[J]. 环球法律评论, 2016(5): 134-150.

[14]王东光. 国家安全审查:政治法律化与法律政治化[J]. 中外法学, 2016(5): 1289-1313.

[15]BOSWORTH S, KABAY M E, WHYNE E. Computer security handbook[M]. New York: John Wiley & Sons Press, 2014.

[16]丁晓东. 数据跨境流动的法理反思与制度重构:兼评《数据出境安全评估办法》[J]. 行政法学研究, 2023(1): 62-77.

[17]周志忍,蒋敏娟. 中国政府跨部门协同机制探析:一个叙事与诊断框架[J]. 公共行政评论, 2013(1): 91-117.

[18]吕乃基. 大数据与认识论[J]. 中国软科学, 2014(9): 34-45.

[19] FRACASSI C, MAGNUSON W. Data autonomy[J]. Vanderbilt law review, 2021, 74(2): 327-384.

[20]鄢浩宇. 企业数据合规的困境纾解与体系构建[J]. 华中科技大学学报(社会科学版), 2024(4): 36-45.

[21]刘权. 网络平台的公共性及其实现:以电商平台的法律规制为视角[J]. 法学研究, 2020(2): 42-56.

[22]ZUBOFF S. The age of surveillance capitalism: the fight for a human future at the new frontier of power[M]. New York: Public Affairs Press, 2018.

[23]鄢浩宇,袁康. 金融法制定背景下数字金融的立法路径[J]. 西南政法大学学报, 2025(4): 59-73.

(本文责编:默　黎)