

总体国家安全观下数据知识产权跨境治理的路径研究

李 尚

(西北大学 法学院, 陕西 西安 710127)

摘 要: 在总体国家安全观指引下, 有效开展数据知识产权的跨境治理, 对于维护国家主权、安全以及发展有着重要意义。数据知识产权既是企业参与全球竞争的核心资产, 也是国家必须严格把控的战略资源。这样的双重属性致使上市公司在履行境外信息披露义务时面临着多重风险, 包括核心数据资产失控、产业链信息泄露以及卷入地缘冲突等。因此, 应构建分类分级的数据确权体系, 筑牢数据跨境流动的全周期主权屏障, 提升系统性反制能力, 在保障国家安全的基础上实现数据知识产权的有序跨境流动, 从而为高水平开放与高质量发展提供坚实的制度保障。

关键词: 总体国家安全观; 数据知识产权; 跨境治理

中图分类号: D923.4

文献标志码: A

DOI: 10.19358/j.issn.2097-1788.2026.05.007

中文引用格式: 李尚. 总体国家安全观下数据知识产权跨境治理的路径研究[J]. 网络安全与数据治理, 2026, 45(5): 48-53.

英文引用格式: Li Shang. Research on the pathways for cross-border governance of data intellectual property under the overall national security concept[J]. Cyber Security and Data Governance, 2026, 45(5): 48-53.

Research on the pathways for cross-border governance of data intellectual property under the overall national security concept

Li Shang

(School of Law, Northwest University, Xi'an 710127, China)

Abstract: Under the guidance of the overall national security concept, effectively managing cross-border governance of data intellectual property is of great significance for safeguarding national sovereignty, security, and development. Data intellectual property is not only a core asset for enterprises competing globally, but also a strategic resource that the state must strictly control. This dual nature leads listed companies, when fulfilling overseas information disclosure obligations, to face multiple risks, including loss of control over core data assets, leakage of supply-chain information, and involvement in geopolitical conflicts. Therefore, by establishing a classified and hierarchical data rights confirmation system, building a comprehensive sovereign shield for the entire lifecycle of cross-border data flows, and enhancing systemic counter-measure capabilities, orderly cross-border flow of data intellectual property can be realized on the basis of national security, providing a solid institutional guarantee for high-level openness and high-quality development.

Key words: overall national security concept; data intellectual property; cross-border governance

0 引言

根据国家数据局对数据作出的官方解释, 数据是指任何以电子或以其他方式对信息的记录^[1]。2021年, 中共中央、国务院印发的《知识产权强国建设纲要(2021—2035年)》提出“研究构建数据知识产权保护规则”, 强调加强新领域知识产权制度研究^[2]。目前, 数据作为知识产权保护对象已经基本形成共识, 部分地方知识产权保护条例中已引入“数据知识产权”概念^[3]。然而, 在国内数据知识产权体系逐步发展的同

时, 数据要素的全球化配置需求与国家安全之间的结构性矛盾日益显现, 尤其在数据跨境流动的制度构建中, 数据知识产权的法律属性与国家安全诉求之间的张力愈发凸显。

2021年《中华人民共和国数据安全法》(以下简称《数据安全法》)与《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)的颁布, 标志着在总体国家安全观指导下, 我国数据安全规范体系初步形成。2021年《“十四五”国家知识产权保护和运

用规划》进一步提出“构建数据知识产权保护规则”，明确数据知识产权作为新型权利客体的战略地位。2022 年 12 月，中共中央、国务院印发的《关于构建数据基础制度更好发挥数据要素作用的意见》（以下简称《数据二十条》），在制度设计层面提出探索构建数据产权制度，并以数据资源持有权、数据加工使用权和数据产品经营权“三权分置”为基本框架。该文件作为数据产权制度的重要政策依据，并未对数据性质作出明确界定。围绕数据及相关数据产品的权利归属、权益内容及保护方式等问题仍存在一定争议。学界对此形成两种观点：一部分主张通过完善现有法律保护数据知识产权；另一部分认为现行制度存在不足，进而主张创设新型知识产权，并提出了衍生数据权、商业数据权、数据财产权等方案。然而，这些方案在权利客体、主体、内容及限制上尚存在分歧。国家知识产权局在实践中采纳后一种建议^[4]。同时，司法判例也认可数据相关权益，如“淘宝诉安徽美景案”“新浪微博诉脉脉案”中，法院均围绕数据权益或劳动投入保护进行审理。表 1 详细列出了我国数据知识产权概念的发展脉络。

总体国家安全观以人民安全为宗旨，以政治安全为根本，统筹经济、军事、文化、社会等领域安全，强调国家安全体系的整体性与系统性，是新时代国家安全工作的重要指导思想^[5]。党的二十大就国家安全工作作出专章部署，提出了“以新安全格局保障新发展格局”的核心要求，强调统筹传统与非传统安全、自身安全与共同安全的治理逻辑。在此背景下，跨国上市公司往往陷入两难境地：一方面，根据上市地的审计以及信息披露要求，企业需向上市地证券交易机

构或证券交易所披露供应链数据、核心技术参数等具有知识产权价值的信息；另一方面，跨国公司掌握或处理的重要数据跨境传输，将触发《数据出境安全评估办法》第 4 条规定的数据出境安全评估申报义务。实践中，已多次发生跨国上市企业核心数据泄露的事件，这类事件不仅可能引发资本市场的波动，还可能对国家主权安全和社会稳定构成潜在威胁。因此，如何在总体国家安全观框架下完善数据知识产权治理体系，成为破解跨境上市企业合规困局的重要命题。

1 数据知识产权的复合属性

当前立法尚未对数据知识产权作出明确规定，但国家层面相关政策文件已提出要研究构建数据知识产权保护规则。学界在具体规则构建上的分歧实则源于数据知识产权自身内在的法律属性冲突。数据知识产权并非单一性质的客体，其在法律上呈现出一种公、私法益交织的复合结构。

1.1 私权属性：作为企业核心资产的数据知识产权

数据知识产权作为一种私权，是民事权益的重要类型。《中华人民共和国民法典》（以下简称《民法典》）第 127 条虽为数据权益保护确立了原则性规范，却没有对数据来源者、处理者等主体的权利边界作出细化界定，导致企业在数据权属与流通过程中面临不确定性，市场主体难以形成稳定预期，从而制约数据要素市场化进程^[6]。数据知识产权的经济价值得以实现，依靠多元的法律保护路径以及数据本身的聚合效应。单个数据价值较为有限，只有通过数据集的形式在算法训练和预测分析中加以利用，才能释放出经济价值^[7]。数据权利主体对数据知识产权所享有的持有、使用、交易和收益的权利^[8]，更是其参与市场竞争的

表 1 数据知识产权概念的发展脉络

阶段	时间	关键事件/文件	核心内容与意义
概念萌芽	2017 年	习近平总书记提出完善数据产权保护制度	明确了数据产权制度建设的方向
	2020 年 4 月	《关于构建更加完善的要素市场化配置体制机制的意见》发布	将数据列为与土地、劳动力、资本、技术并列的第五大生产要素
顶层设计	2021 年 9 月	《知识产权强国建设纲要（2021—2035 年）》印发	明确提出“研究构建数据知识产权保护规则”
	2021 年 10 月	《“十四五”国家知识产权保护和运用规划》发布	再次强调研究构建数据知识产权保护规则，并部署了“数据知识产权保护工程”
	2022 年 12 月	《关于构建数据基础制度更好发挥数据要素作用的意见》（“数据二十条”）发布	提出“建立保障权益、合规使用的数据产权制度”和“研究数据产权登记新方式”
实践探索	2022 年底至今	国家知识产权局在北京、上海、浙江、湖南、山西等全国多地开展数据知识产权工作试点	各地开始探索制定具体的登记管理办法和搭建登记平台，推动数据知识产权从理论概念走向实务操作

核心权益基础,具体可通过数据产品交易、知识产权质押融资等模式,将数据资产转化为实际经济收益。另外,在行使数据知识产权私权时,需兼顾个人信息保护与市场公平竞争的法益,尤其是在数据跨境流动场景中,还需要应对私权保护与公法监管之间的价值平衡难题。

1.2 主权属性:作为国家战略资源的数据知识产权

数据知识产权的主权属性表明其法律定位已突破传统私权领域,成为数字时代具备战略价值的国家关键资源,更是网络空间国家主权在新型领域的重要载体^[9]。数据知识产权的主权属性,其法律根基主要来源于以《数据安全法》《中华人民共和国网络安全法》(以下简称《网络安全法》)等法律法规为核心构建的公共法律规范体系。在此框架下,国家对于关乎国家安全、国民经济命脉、重要民生以及重大公共利益等方面的“重要数据”与“核心数据”依法享有专门的监督管理与管控权力。

在数据治理实践中,我国已经建立数据分类分级保护体系,强制要求关键数据在境内存储,并为跨境传输设立了安全评估机制,明确划定国家数据主权的边界。面对部分国家借助“长臂管辖”手段开展的域外数据调取行为,我国依靠《中华人民共和国反外国制裁法》(以下简称《反外国制裁法》)等法律工具予以回应,坚决抵制美国《澄清域外合法使用数据法案》(Clarifying Lawful Overseas Use of Data Act,即知名的“云法案”)等相关举措,全力维护司法以及数字空间的国家自决权。当企业所掌握的关键基础设施运行数据、重点产业链核心数据被纳入国家数据主权监管范畴时,企业对外提供或披露这些数据已超出普通商业自主范畴,要依法接受国家安全审查。数据知识产权所内含的主权属性,要求国家在数字时代借助法治手段对关键数据实施必要管理与调控,以此保障国家安全。

1.3 交叉与冲突:双重属性在跨境披露中的张力

数据知识产权兼具双重属性:一方面,企业为进入全球资本市场、满足境外监管及投资者要求,往往追求数据要素的自由流动,这构成了其私权行使的核心表现;另一方面,国家基于整体安全考量,对涉及国家安全、关键基础设施和重大公共利益的数据实行严格的主权管控,以防止数据跨境流动带来的系统性风险。二者之间的张力在实践活动中不断显现。

在数据跨境流动中,企业常会陷入双重合规的两难局面:若仅仅是为了满足境外资本市场的披露要求,放宽数据本地化处理以及安全审查的要求,那么就有

可能因为违规向境外提供关键数据或者敏感个人信息,触及《数据安全法》《个人信息保护法》以及《网络安全法》的合规红线。2021年“滴滴事件”即暴露了企业数据资产权益主张与国家安全审查机制之间的冲突,平台掌握的交通地理信息既属于企业核心资产,又因涉及国家基础地理数据安全而需接受特别监管。更严重的是,若此类行为被认定为“执行或协助执行外国歧视性限制措施”,还可能因为违反《反外国制裁法》相关条款^[10],面临业务受限甚至直接责任人被追责的连锁法律后果。相反,若企业为了规避主权风险,过度地缩减信息披露范围,又会致使其在全球资本市场上透明度不足、信用受损,进而对融资效率以及市场竞争力产生影响。这种结构性矛盾表明,数据跨境场景下的市场逻辑与国家安全逻辑难以自发地进行调和,跨国上市企业正成为两种治理模式直接交锋的核心场域。

2 数据知识产权跨境安全风险解构

在数据知识产权跨境流动的实践中,其私权以及主权属性的内在张力呈现为多种安全风险。这些风险不仅会对企业的商业利益以及创新动力造成威胁,还会给国家产业安全以及战略自主带来系统性挑战。

2.1 权属模糊下的核心数据资产失控危机

在全球化资本市场环境下,跨国上市公司需要遵守上市地的相关法规规定披露公司的财务和审计数据。这种信息披露行为使得跨国上市企业常面临核心数据资产外流的风险。这种风险主要来源于向境外监管机构提交的审计底稿和备案文件,其中包括能够反映企业核心竞争力的非财务信息,例如关键算法参数、机器学习训练数据以及用户行为画像等内容^[11]。然而,企业核心数据面临失控风险的根本原因在于数据知识产权权属的模糊性。企业难以界定哪些是可以自由处分的“私产”,哪些是涉及国家安全的“核心数据”,导致其跨境决策缺乏稳定预期。这种不确定性进一步致使企业可能陷入“过度披露”而违法或“过度保守”而损害融资竞争力的两难局面。与此同时,由于缺乏清晰的权力边界作为判断依据,监管部门往往难以对数据出境形成准确的前瞻性预警和精准管控,这在一定程度上削弱了维护数据主权的效能。

数据知识产权权属不明确是企业数据跨境流动面临多重风险的根本原因。由于权属不清,企业难以有效控制自身的核心数据资产。从技术上看,境外竞争者可以通过数据挖掘、反向工程等技术手段深入研究企业的技术架构和创新路径;从商业上看,若数据画

像等关键数据发生泄露，企业的市场策略和商业模式将会直接暴露出来，企业极易遭受竞争对手的精准打击；从产业上看，若行业内众多企业的核心数据失控，将对整个数字产业的技术安全与创新环境造成系统性冲击。最为根本的在于，数据知识产权权属不清会从源头抑制企业创新发展的内生动力。企业如果对自己的数据产品没有稳定的权属预期，其投入数据资产化和参与市场交易的意愿将大幅降低。因此，核心数据资产失控不仅是企业面临的商业风险，更是关乎国家长期竞争力的战略风险。

2.2 产业链信息的系统性暴露

在全球资本深度融合的背景下，企业为满足境外市场的强制信息披露要求，往往需要公开供应链结构、主要客户与供应商、产能分布以及库存周转率等核心经营数据^[12]。这些看似比较常规的商业信息，经过专业机构整合梳理及深度挖掘后，可清晰地呈现出我国重点产业的整体格局以及运行逻辑。单个企业所披露的供应链信息，可能仅仅体现其自身的运营状况，但如果同行业多家企业的数据被集中汇总比对，就能系统地还原出整个行业的发展态势，甚至还可以精准地识别出行业当中的薄弱环节。

这些信息被泄露的安全隐患主要体现在两个方面。一是产业安全，一些国外研究机构利用先进的数据分析技术，精确锁定相关产业链的关键环节和“卡脖子”环节。比如针对半导体行业的相关企业，通过比较他们各自的供应商名单、采购数据等来判定我国对于尖端光刻设备和特殊化工原料等的依赖程度。二是经济安全，这些经过系统梳理的信息，有可能成为他国制定针对性限制举措的依据，从而约束我国的战略性新兴产业。实际情况表明，基于数据的打压具有较强的战略性，且传导性强。当产业链核心企业受到冲击时，影响会沿着供应链网络向上下游企业扩散，引发连锁负面反应。这种系统性风险的积累与传播，不仅会威胁单个企业的长期发展，还可能引发产业生态的整体震荡，对国家经济安全以及产业体系韧性构成持续性挑战。

2.3 监管规则的政治化转向

当下全球监管格局正在经历系统性重塑，美国通过《外国公司问责法》等立法举措，将数据披露要求转变为新型战略工具^[13]。这些政策表面上是以市场透明和投资者保护为名义，然而在实践中，却把审计监管和数据访问权转变成国际博弈的战略筹码。这种监管政治化的趋势，致使进行跨境融资的中国企业面临

前所未有的复合型挑战。

这些监管政策的风险在于其本身的复杂性。法律条文往往会留有一定的弹性空间，加之执法过程中存在动态裁量的情况，导致企业很难形成稳定的合规预期。例如，美国《外国公司问责法》虽然对“被认定发行人”的认定设置了相对明确的客观标准，但实质上将证券监管工具化，使中概股企业面临极高的强制退市风险。在执行时，监管力度与国际政治环境之间存在着密切的关系，使得企业的合规问题不再仅仅是单纯的法律技术层面的问题，而是融入更为宏大的国际关系叙事之中。这种制度环境的变化改变了企业的战略选择，使得企业被迫建立风险预警与应对体系，合规成本呈现出几何级增长态势，长期布局以及技术投入决策也因为政策的不确定性而受到影响。政治层面的监管审查、制裁机制以及市场准入管控，已然成为企业国际化进程中不可忽视的制度性风险，持续对其全球运营构成威胁。因此，跨国企业既是市场中的经济主体，也是深度参与到地缘政治博弈中的参与者，面临着日益复杂的系统性环境。

3 数据知识产权跨境治理的路径构建

要破解数据知识产权跨境治理所面临的诸多问题，亟需构建系统化的治理路径。通过建立分类分级确权体系筑牢权属根基，依靠全周期主权屏障防御产业链风险，并运用系统性反制框架应对国际规则博弈，以此在开放与安全之间达成动态平衡。

3.1 构建分类分级数据确权体系

数据知识产权的复合属性致使其确权机制要突破传统产权制度的线性逻辑，构建与国家安全战略紧密耦合的分类分级体系。目前，中共中央、国务院发布了《关于构建更加完善的要素市场化配置体制机制的意见》《“十四五”数字经济发展规划》等规范性文件，为数据确权制度建设提供方向性指引^[14]。《数据安全法》所提出的“数据分类分级”原则为这一体系提供了顶层设计的架构，然而在实践中仍需进一步细化操作规则^[15]。数据确权的关键问题在于如何界定数据权属的边界，既要保障企业对数据资产拥有合法的控制权，又要防范数据跨境流动过程中的主权风险。对此，需要从法律赋权、技术确证、场景适配这三个层面协同推进，凭借主权控制来应对权属侵蚀风险。

在法律层面，关键是通过立法与司法解释，厘清数据从产生到加工各环节的权利归属以及跨境流转的相关规则^[16]。其首要任务是构建“源起-衍生”二元权利框架：于“源起”端，强化对个人作为数据来源

者的人格权益保护,明确其知情同意权是数据处理的合法性基石;于“衍生”端,通过立法确认企业对经过“实质性投入”形成的数据产品享有新型财产权,保护其创新收益。最后,国家则基于“主权”对经过识别定级的“重要数据”与“核心数据”行使最终的监管与安全审查权。《民法典》第127条虽涉及数据权益保护,但缺乏具体的实施细则,这使得企业在实际操作时面临困境。可参考欧盟《数据治理法案》中的“数据利他主义”制度,建立用于公益目的的数据自愿分享与自愿注册机制^[17]。同时,要加快推进数据知识产权登记制度,针对核心数据资产展开法定登记工作。《上海市数据产品知识产权登记存证暂行办法》自2024年12月8日开始实施以来,截至2025年4月21日,上海已受理登记申请409件,发证289件。其中,有243个数据产品实现许可收益20.66亿元,161个数据产品在各交易机构挂牌交易,交易总额达33.53亿元^[18],10余家企业通过质押融资获银行贷款超2亿元^[19]。这些数据充分说明,登记程序可将数据资产转变为受到法律保护的客体,为其跨境流动提供坚实的权属凭证。

在技术层面,区块链以及隐私计算为确权提供了全新的工具,区块链利用时间戳、哈希存证等技术手段实现了全链条的可追溯性,如深圳微众银行的“WeIdentity”分布式身份协议已经实现了企业数据资产的可信授权与身份认证;而隐私计算则是在保障数据主权的基础上实现跨域价值交换,如蚂蚁集团的“摩斯”安全计算平台已经在医疗、金融等多个领域完成了数据确权与价值流转的协同工作。

在场景适配层面,数据确权应当依据不同的应用场景动态调整保护强度等级,对于涉及国家安全的核心数据要严格管控,坚决禁止其跨境流动;对于专利池共享、供应链等产业竞争数据,可以通过数据信托或者跨境许可的方式实现有条件的流动;对于一般商业数据,在经过脱敏处理之后可以纳入自由流通的范畴。

3.2 完善数据跨境流动的全周期主权屏障

数据知识产权的跨境治理应以风险防控和主权维护作为核心导向,针对供应链的价值链穿透风险,构建一套从前期预防到后期追踪的一体化治理体系^[20],借助制度设计把国家安全诉求转化为数据流动规则,在保障数据要素可在全球范围内合理配置的同时,筑牢安全防线,抵御外部势力与“长臂管辖”。

在数据出境前的风险防控阶段,应构建依据数据知识产权分类的审查体系,以《数据安全法》确定的

“重要数据”标准为依据,监管部门对企业拟披露的供应链数据进行多维评估,并重点核查数据是否属于产业链某一环节的关键点。对于那些可能会暴露产业布局薄弱点的数据,应当纳入重点数据清单,开展出境前的强制性安全评估。对于评估合格的非涉密数据,可以实行分级备案,要求企业提交数据流转路径、使用场景以及境外接收方资质证明,以此形成跨境流动的前置保障。在数据出境之后,应当构建以主权为导向的监测响应体系,借助技术手段对跨境数据流动的全链条进行存证,实时追踪数据在境外的使用场景以及衍生加工行为。在分布式账本中实时记录其各项数据的调取,并及时向相应司法部门发出预警,以便于提供司法举证支持。一旦检测到相关信息出现异常流动,立即启动“熔断机制”,停止相关接口操作并展开溯源调查。

此外,治理框架要形成闭环,需要兼顾激励与约束。一方面,借助法律明确违规红线,针对故意泄露产业链关键数据的企业,实施市场准入限制以及高额罚款等惩戒举措;另一方面,构建数据合规贡献度评价体系,将企业的数据治理能力纳入信用评级以及政策扶持的考量范围,通过降低合规企业的融资成本与监管负担,切实调动企业主动构建数据保护体系的积极性。

3.3 强化数据主权的系统性反制框架

在大国博弈的复杂格局下,数据知识产权跨境治理必须直面深层次的结构性矛盾。美国等国家依托其技术主导地位与规则制定优势,实施具有针对性的管制措施。面对这一态势,我国数据主权战略应加强治理体系的顶层设计,并细化数据跨境流动的管辖要求^[21]。这一系统性反制框架的核心在于从被动防御转变为主动塑造。这要求我国在国际层面积极参与规则制定,提升话语权;在国内层面不断夯实法律体系,巩固主权根基。最终构建起国际规则、国内法律与技术实力三位一体、协同发挥效用的立体反制体系。

数据知识产权跨境治理需要构建多层次的应对体系。在国际层面,可以借助多边机制质疑美国数据管制的合法性,依据《与贸易有关的知识产权协定》第73条关于国家安全例外的规定,通过争端解决机制主张美国的相关措施是变相的贸易壁垒^[22];并利用外交和国际平台抵制这种损害全球化自由贸易体系的行为。在国内层面,要完善数据主权法律体系,打造多层次反制能力。实体法层面将《反外国制裁法》应用于数据领域,制定核心数据知识产权负面清单以及相应的制裁措施;程序法层面要探索跨境数据争议域外管辖

规则，赋予司法机关对于境外侵害我国数据主权行为的管辖权，以及加强出口管制清单与数据分类分级体系对接，实施人工智能、量子计算等重点领域跨境数据流出口许可等。技术上打破对西方技术路径的过度依赖，加快隐私计算、区块链等关键技术的自主研发，建立符合我国数据主权的技术标准，推动国产加密算法、认证协议等在跨境数据流动场景中的应用，搭建属于中国的相对独立于西方技术生态的数据交互通道。

4 结论

在数字经济时代，数据知识产权的治理不再局限于传统知识产权保护的范畴，而是演变成国家核心竞争力以及战略安全领域的全新战场。这一治理进程不仅直接影响到企业全球市场中的竞争地位，也对国家主权安全以及数字时代的发展主动权产生了深刻的影响。数据知识产权兼具私权与主权的双重属性，这使其在跨境流动中必须同时应对商业层面的风险与国家安全的考量。将数据知识产权融入国家安全治理体系是实现发展与安全动态平衡的必经之路。通过构建分类分级的确权体系、完善跨境流动的全周期监管、强化主权导向的反制能力，于开放与安全间找到最佳平衡点。最终形成以数据知识产权激励创新、以安全治理保障发展的良性格局。在制度方面，要突破传统治理框架，创新契合数字时代特征的法律规则与监管模式；在技术方面，要持续推进区块链、隐私计算等核心技术的研发及应用，为数据治理筑牢技术基础；在国际方面，要积极参与全球数字治理规则的制定，通过对话协商推动构建公平合理的国际数据治理秩序。在总体国家安全观的指导下，应以更加全面、系统、长远的眼光审视数据知识产权治理这一时代课题。通过构建具有中国特色的数据治理体系来化解跨境企业在合规经营过程中遭遇的现实难题，以此为数字经济的健康发展提供保障，为全球数字治理贡献中国智慧以及中国方案。

参考文献

- [1] 国家数据局. 数据领域常用名词解释 (第一批) [EB/OL]. (2024-12-30) [2025-11-30]. https://www.nda.gov.cn/sjj/zwgk/zcfb/1230/20241230160715745237413_pc.html.
- [2] 中国政府网. 中共中央、国务院印发《知识产权强国建设纲要(2021—2035年)》[EB/OL]. [2025-11-30]. https://www.gov.cn/gongbao/content/2021/content_5643253.htm.
- [3] 汤贞友. 数据知识产权登记的制度逻辑及完善[J]. 知识产权, 2024(3): 34-53.
- [4] 胡开忠. 数据知识产权赋权理论之质疑[J]. 法学, 2025(10): 114-131.
- [5] 刘自雄, 雷跃捷. 总体国家安全观的思想内涵与传播实践[J]. 传媒观察, 2022(10): 25-32.
- [6] 张素华. 数据资产入表的法律配置[J]. 中国法学, 2024(4): 229-249.
- [7] 赵军. 知识产权视域下的数据财产权建构[J]. 知识产权, 2025(6): 77-90.
- [8] 叶雅珍, 朱扬勇. 数据知识产权: 一种可流通交易的数据权[J]. 大数据, 2024, 10(2): 192-195.
- [9] 李爱君. 数据权利属性与法律特征[J]. 东方法学, 2018(3): 64-74.
- [10] 胡晓凡, 姜芳. 习惯国际法下反措施与第三方关系探析——以《反外国制裁法》第12条为例[J]. 语言与法律研究, 2021, 2(2): 123-136.
- [11] 韩洪灵, 陈帅弟, 刘杰, 等. 数据伦理、国家安全与海外上市: 基于滴滴的案例研究[J]. 财会月刊, 2021(15): 13-23.
- [12] 汪宓. 中概股审计底稿数据出境规则反思与完善——以“多边型数据合作主义”为导向[J]. 金融法苑, 2025(1): 86-100.
- [13] 朱江. 中国证券法域外适用法律制度: 现状、问题与完善[J]. 武大国际法评论, 2025, 9(2): 52-69.
- [14] 张新宝. 论作为新型财产权的数据财产权[J]. 中国社会科学, 2023(4): 144-163, 207.
- [15] 张继红. 国家安全视域下我国数据安全法的制度构造[J]. 西北工业大学学报(社会科学版), 2021(3): 96-103.
- [16] 王璿, 底亚星. 数据确权: 必要性、复杂性与实现路径[N]. 光明日报, 2024-03-15(011).
- [17] 杨瑜娟. 数据交易平台治理: 欧盟制度经验与借鉴[J]. 世界社会科学, 2024(4): 65-79, 243-244.
- [18] 澎湃新闻. 上海开展数据产品知识产权登记存证试点 243个产品许可收益超20亿元[EB/OL]. (2025-04-22) [2025-11-30]. https://www.thepaper.cn/newsDetail_forward_30698449.
- [19] 上海市知识产权局. 上海: 数据产品知识产权登记人工智能领域占比超60%[EB/OL]. (2025-04-01) [2025-11-30]. https://sipa.sh.gov.cn/2020_mtjd/20250401/17eb42bb1f174f318a06919524ea3fcc.html.
- [20] 包柠榛. 中概股赴美上市的数据安全审视: 风险来源、中美监管与应对[J]. 东北师大学报(哲学社会科学版), 2023(4): 145-155.
- [21] 郑琳, 李妍, 王延飞. 新时代国家数据主权战略研究[J]. 情报理论与实践, 2022, 45(6): 55-60.
- [22] 何华. 知识产权保护的安全例外研究由《TRIPs协定》第73条展开[J]. 中外法学, 2019, 31(3): 817-839.

(收稿日期: 2025-12-02)

作者简介:

李尚(2000-), 男, 硕士研究生, 主要研究方向: 知识产权。

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