数据安全影响了企业的数字化转型吗？

——基于《数据安全法》的准自然实验

吴嘉祺[1]，徐 野[2]，温 倩[3]

（1. 江西财经大学应用经济学院，南昌 330013；2. 江西财经大学现代经济管理学院，南昌 330013；
3. 江西财经大学工商管理学院，南昌 330013）

摘要：以中国A股上市公司2021出台的数据安全法政策执行作为冲击事件，以2013—2022年度的面板资料为依据，采用双重差分（DID）模型，系统考察了数据安全规制对企业数字化转型的影响以及相应的作用机制。研究表明：《中华人民共和国数据安全法》显著推动企业数字化转型，且在非国有企业、数据泄露高风险行业、市场竞争力较强的企业中效果更显著；机制分析表明，政策通过合规成本压力倒逼企业开展技术创新，并吸引高技能人才加入，以双渠道驱动企业数字化转型进程；经过一系列稳健性检验后，结论依然可靠。揭示了数据安全政策与企业数字化转型的互动关系，为监管部门优化数字经济治理提供决策参考。

关键词：数据安全法；企业数字化转型；数据要素；合规成本

中图分类号：F272.3 **文献标志码：**A **文章编号：**1671－1807(2026)02－0271－11

在全球经济数字化转型的大背景下，数据已成为推动企业创新发展的核心生产要素，正深刻改变着企业的运营模式与市场竞争格局，企业借助数字化转型，不仅可以实现数据资源的高效整合，还能大幅提升运营效率、增强市场竞争力[1]。但随着企业数字化进程不断加快，数据安全问题愈发突出，逐渐成为制约数字化转型的关键瓶颈，数据滥用、篡改、泄露等安全事件的频繁发生，不但严重威胁着企业的可持续发展，更对国内经济的安全稳定构成重大挑战。为了应对日益严峻的数据安全挑战，中国积极推进数据安全立法工作，2018年9月，《中华人民共和国数据安全法》（以下简称《数据安全法》）被纳入第十三届全国人民代表大会常务委员会立法规划，由此，数据安全领域的法治建设正式步入了具有里程碑意义的重要发展阶段。经过多次开展深入调研，从全方位了解情况，到面向社会各界广泛征求意见，集思广益，再到进行严谨缜密的审议，在一系列工作完成后，2021年6月10日，十三届全国人民代表大会常务委员会第二十九次会议表决通过《数据安全法》，于2021年9月1日正式生效。作为全国数据安全领域的基本法律，《数据安全法》全面贯彻总体国家安全观，将数据安全上升到国家安全战略高度，它不仅清晰界定了数据安全保护的基本原则，更是从数据分类分级管理、安全风险评估、应急处置等环节，为企业开展数据安全管理工作搭建起一整套基本制度，为企业的数据安全管理提供了坚实的法律框架支撑。在政策体系构建上，该法与《中华人民共和国网络安全法》（以下简《网络安全法》）、《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》）等法律法规协同发力，强化了数据与信息的安全共享、流通与应用。此后，《关键信息基础设施安全保护条例》《网络安全审查办法》等一系列配套政策及专项行动相继出台，进一步细化了《数据安全法》的实施细则，有效提升了法律的可操作性与执行效能。

在此背景下，以《数据安全法》政策实施作为准自然实验场景，采用双重差分模型，深入研究《数据安全法》的政策实施对企业数字化转型的影响效应、传导机制和异质性效果，可更深入系统地反映

收稿日期：2025-07-28

基金项目：国家自然科学基金（72263011）；国家社会科学基金（23CJY006）

作者简介：吴嘉祺（1999—），江西赣州人，硕士研究生，研究方向为企业数字化转型；徐野（1992—），江西南昌人，博士，讲师，研究方向为数据要素与企业数字化转型；温倩（1992—），江西石城人，博士，讲师，研究方向为数据要素与企业数字化转型。

《数据安全法》的实施效应，为更好地贯彻执行《数据安全法》提供了理论与实践依据。

1 文献综述与理论分析

1.1 文献综述

在数字经济全球化发展进程中，数据安全治理已成为各国战略布局的核心议题，各国围绕数据要素的安全保护与合理利用等核心议题，陆续出台了一系列相关政策法规，学界对此也展开了多维度的研究，而数据安全政策与企业数字化转型的关联机制也逐渐成为学术界关注的热点。欧美等发达国家较早构建数据安全法律体系，为全球治理提供了制度参照。欧盟在2016年颁布的《通用数据保护条例》(General Data Protection Regulation，GDPR)，并非简单的区域性数据监管规则，而是全球数字治理领域首个以权利本位为核心逻辑的系统性制度框架，其影响力突破地理边界，形成对全球企业数据处理行为的普遍性约束。在数据跨境流动规制层面，GDPR并未采取一刀切的禁止性策略，而是基于充分性认定原则建立分级管控机制：对于数据保护水平与欧盟等效的国家和地区(如日本、加拿大)，允许数据自由流通；对于未达标的区域，则要求企业通过标准合同条款、绑定公司规则等合规工具，确保数据跨境传输全程可追溯、风险可管控。这种精细化的跨境治理逻辑，既避免了数据流动过度受限对数字经济效率的损害，又通过严格的合规门槛倒逼全球企业重构数据跨境管理体系。对于此，Aridor等[2]指出，GDPR虽提升了数据安全水平，但也增加了企业合规成本，部分中小企业因难以承担成本而放缓数字化投入。

美国采用行业差异化＋联邦与州协同的sector-specific规制模式，避免了一刀切对产业活力的抑制。在联邦层面，《健康保险流通与责任法案》(Health Insurance Portability and Accountability Act，HIPAA)针对医疗数据制定专属安全标准，要求医疗机构建立数据加密存储与访问权限分级体系；在州层面，《加州消费者隐私法案》(California Consumer Privacy Act，CCPA)赋予用户数据删除权与携带权，倒逼科技企业重构数据管理流程。Mulgund等[3]指出，这种差异化规制使高风险行业(如医疗)的企业更倾向于通过技术升级来满足合规要求，间接推动了行业数字化转型。但sector-specific规制模式也存在协调成本较高的问题，联邦与州层面的规则差异导致跨州经营企业需建立多套合规体系，增加了数字化转型的复杂性。亚太地区国家在借鉴欧美经验的基础上，更注重安全与发展的平衡，其政策设计既回应了个人信息保护的普遍需求，也体现了对数据要素价值释放的现实考量。日本2022年修订的《个人信息保护法》，在强化个人数据权利保护的同时，新增匿名加工信息灵活利用条款，允许企业在去除标识化处理后，将数据用于产品研发与服务优化，为数字化转型保留了数据利用空间。澳大利亚2020年更新的《隐私法》，引入数据信托制度，由第三方机构监督企业数据处理行为，既降低了企业自主合规的成本压力，又通过信托背书提升了用户对企业数字化服务的信任度。对于此，Daley等[4]认为，《个人信息保护法》和《隐私法》对数据全生命周期的管理要求促使企业重构数据流程，反而提升了数据利用效率。这些国际政策虽在立法理念与实施强度上存在差异，但均将数据安全提升至国家信息安全与国家经济安全的战略高度。

中国数据安全政策体系顺应数字经济发展进程不断迭代，在2017年《网络安全法》中首次在法律层面提出数据分类保护要求，为数据安全治理搭建起了坚实的制度根基。2021年，《数据安全法》以其基础性法律地位，逐渐构建起贯穿数据收集、数据报废、数据存储、数据使用等全生命周期的数据安全管理框架，并将数据安全提高至国家安全的战略高度，推动政策体系向系统化、战略化迈进[5]。同年开始实施的《个人信息保护法》对个人数据处理规则进行了进一步的细化，与《数据安全法》形成协同治理框架。随后，2024年颁布的《网络数据安全管理条例》以及《关键信息基础设施安全保护条例》等配套政策的陆续出台，更彰显了数据安全监管的立体化框架，标志着中国的数据安全治理已迈入了法治化、规范化的全新阶段[6]。这一制度演进既借鉴了国际经验，又立足本土实践，充分体现了“统筹发展与安全”的中国特色治理思路。

目前，国内学界对《数据安全法》的研究重点围绕法律文本解读方面逐步深入，但在实证研究的深度与广度方面仍显不足。学者们重点剖析了《数据安全法》的立法逻辑与制度创新，如苏桑妮[7]和蒋冬雪等[8]指出，《数据安全法》秉承“数据安全与发展并重”的数据安全观，构建起贯穿数据全生命周期的监管框架，通过确立数据分类分级管理制度、重要数据目录备案机制及跨境数据流动安全评估程序，为数据要素的合规流通构筑起立体化的法律屏障。蒋率兵[9]聚焦数据跨境流动，强调《数据安全法》确

立的“安全评估+分类管理”模式,既维护了数据主权,又为跨境数据合理利用保留了弹性空间,体现了立法的平衡艺术。《数据安全法》对企业数字化转型的影响方面,更多考虑的是会增加企业的合规成本,某种程度上可能会抑制企业的数字化转型[10]。企业在处理数据时需明确数据来源合法、数据处理合规,同时需要建立风险预警机制和违规处罚机制,短期内可能会影响企业的绩效,但是长期来看,平衡好个人隐私权益和企业对数据的创新利用,有助于企业可持续的数字化发展[11]。这些文献虽提及企业合规响应,但多基于案例描述或逻辑推断,缺乏微观数据支撑。

综上所述,国际数据规制政策实践的研究为中国制度建设提供了经验借鉴,而在国内,学界对数据安全的技术、法律、管理研究已形成丰富成果,但在数据安全政策与企业数字化转型的关联机制上仍存在理论争议与方法局限,基于中国《数据安全法》的本土化实证研究也有待深化。研究以2021年《数据安全法》的实施作为准自然实验,采用双重差分(difference-in-difference,DID)模型系统检验政策实施对企业数字化转型的影响,通过构建双渠道作用机制,揭示政策实施的作用机制,为中国数字经济治理提供基于本土实践的经验证据。

1.2 理论分析与研究假设

《数据安全法》作为数字经济治理的核心规制工具,其核心功能是通过法律强制力重构企业数据处理的成本收益结构。根据规制俘获理论,政策本质上是利益集团博弈的产物,但《数据安全法》的特殊性在于其目标兼具公共利益(数据安全保护)与市场效率(数字经济发展)的双重属性。这种双重属性决定了政策对企业行为的影响并非单向抑制,而是可能通过规制倒逼创新机制形成正向激励。从合规义务层面来看,《数据安全法》要求企业建立数据分类分级管理制度、部署数据安全技术措施、开展数据风险评估[5],企业为满足数据安全要求,进而提升数据安全技术,使原本分散的数据得以重新整合汇聚,以此来促进企业创新。在此过程中,数据安全政策成为企业数字化转型的“制度触发器”,推动其突破组织惯性,主动寻求技术范式变革。据此,提出以下研究假设。

H1:《数据安全法》的实施促进了企业数字化转型。

《数据安全法》的实施通过合规成本倒逼创新的形式来驱动企业数字化转型。一方面,数据安全合规成本(如技术升级、流程改造、人力投入等)本质是企业应对制度约束的预防性投资,其对转型的推动作用体现在,企业为满足数据分类分级管理、加密技术等合规要求,需增加数据中台架构升级、安全技术研发等投入,这类投入不仅是对政策的响应,更能通过技术溢出效应优化数据整合与分析能力[5]。另一方面,合规流程改造推动组织管理数字化,政策要求企业建立数据安全责任制,倒逼企业重构组织架构,如设立首席数据官岗位,这种调整促进了数据驱动的决策机制形成,从而提升了企业的效率。这种传导机制,打破了规制抑制创新的传统认知,证明合规成本可转化为企业数字化转型的核心动能。据此,提出以下研究假设。

H2:《数据安全法》的实施通过提高合规成本从而促进了企业数字化转型。

《数据安全法》催生了企业对高技能人才的需求,进而加速了企业数字化转型。高技能人才的引入不仅带来个体能力提升,更会通过组织内部的知识共享,形成群体性的数字化能力升级[12],人才之间的互动会促进隐性知识传播,这种传播效应在数据安全与数字化转型的交叉领域尤为显著,数据安全专家对加密技术的理解,能帮助业务部门更好地设计数字化产品的隐私保护方案;数据分析师对合规要求的掌握,能提升其挖掘数据价值时的风险控制能力。高技能人才作为知识、技术和经验的载体,其引入显著增强了企业的技术吸纳能力[13],高技能人才具备深厚的专业知识储备与关键技能,能够快速理解、消化并有效应用外部引进的技术(如外商投资的技术溢出),将其转化为实际生产力,人力资本存量越高,企业对先进技术的识别、获取和转化能力越强,从而为数据密集型的相关行业形成更强劲的转型动力。据此,提出以下研究假设。

H3:《数据安全法》的实施集聚更多数字、信息和网络人才,提高企业高技能人才占比从而加速了企业数字化转型。

2 研究设计

2.1 样本选择与数据来源

以A股上市公司的文本数据作为研究样本,选取2013—2022年作为样本区间。由于中国证监会在2012年发布了新一版的上市公司行业分类指引,因此以2013年为样本区间的起始点,选取该时间段可以保证行业分类上的连贯性。对样本数据进行如下处理:剔除*ST、PT和ST类企业;将金融行业剔除;剔除只有一年观测值的企业;剔除不受《数据

安全法》影响的行业内所有的企业，《数据安全法》作用范围非常广，深刻影响各行各业，但是对某些行业来说，影响较小，因此对企业进行分行业词频统计，剔除行业内实验组个数小于15个的行业内所有的企业，以此来进一步提高实验组与对照组之间的可比性；剔除变量缺失样本以及常见的异常值样本；选取的企业来自30个省份（因数据缺失，未包含西藏地区和港澳台地区）。企业基本信息、财务数据主要来源于国泰安数据库、马克数据网，在回归分析中对标准误进行公司层面的聚类调整。

2.2　变量构建与描述性统计

2.2.1　核心解释变量

以《数据安全法》的实施作为准自然实验，以treat和post两个虚拟变量的交互乘积项did表示核心解释变量，将《数据安全法》正式实施的2021年视为政策冲击事件的发生年份，因此2021年及以后的年份取为1，其余的年份取值为0，以此来构建时间虚拟变量（post）。再根据构建的《数据安全法》关键词组，若企业2021年报中出现了有关《数据安全法》关键词组内的词语，则虚拟变量treat取值为1；若未出现，则取值为0，由此得到核心解释变量treat×post的值。

虚拟变量treat的具体构建过程如下：第一步，收集2021年A股所有上市公司的相关年报信息。第二步，初步定义种子词库，通过人工阅读上市公司年报和《数据安全法》，得到初步定义种子词分别为合规收集、数据保护、数据安全、数据分级、数据处理、数据分类。借鉴马瑄忆和施新政[11]使用的Word2Vec词向量算法，依据词组与词组之间的距离关系，在上市公司的2021年报中查找种子词库的近义词，经过Word2Vec词向量算法获得的有关《数据安全法》关键词组内的词语一共19个。第三步，使用Python剔除年报里的停用词、数字、标点符号等，并且使用“jieba”中文分词模块对上市公司年报文本进行分词处理，但会出现“jieba”分词模块将一个完整的词语如数据安全切分为“数据”和“安全”两个词语的情况。为了解决这个问题，将生成的有关《数据安全法》关键词组作为预设专有名词词典加入“jieba”的分词模块，并统计上市公司年报中有关《数据安全法》关键词组的数量。为了确保使用Word2Vec词向量算法获得的有关《数据安全法》关键词组的准确性，进而进行人工筛选，剔除一些不符合实际情况的词语，如“数据库”这一词语在大多数企业年报中都会出现，并不适合作为关键词，因此将其进行剔除。人工验证后的关键词集合如表1所示。最后生成虚拟变量treat，若企业在2021年报中出现了相关词语，则treat取为1；否则为0。

2.2.2　被解释变量

被解释变量为企业数字化转型水平Digital，借鉴肖土盛等[14]所收集的企业数字化转型词典词汇，通过人工筛选的方式，以此去除一些重复的词语，一共得到191个与企业数字化转型相关的词语，通过Python统计相关词语的词频，对所获得的关键词词频采取词频总数加一取自然对数的方式，从而得到企业数字化转型水平Digital。

2.2.3　控制变量

参考马瑄忆和施新政[11]、吴武清等[15]、张正平和于新[16]的做法，选择公司规模（inAsset）、有形资产比率（Tangratio）、资产负债率（Lev）、无形资产比例（Intan）、董事会规模（BoardSize）、流动性比率（LR）作为控制变量。具体变量定义如表2所示。

表1　关键词集合

关键词	来源	词组
种子词	上市公司年报、《数据安全法》	合规收集、数据保护、数据安全、数据分级、数据处理、数据分类
扩充词	Word2Vec算法	软件开发、数据安全、数据泄露、数据处理、合规收集、数据服务、数据分类、数据分级、信息安全、隐私安全、数据保护、网络安全、信息系统、数据共享、隐私保护、数据库、数据管理、数据滥用、数据加密
	进一步人工验证	数据泄露、数据安全、数据处理、数据加密、数据共享、数据分类、数据分级、隐私保护、数据管理、隐私安全、数据保护

表2　主要变量定义

变量类型	变量名称	变量符号	变量定义
被解释变量	企业数字化转型水平	Digital	企业数字化转型相关词汇的总词频加1后取自然对数
解释变量	《数据安全法》实施	did	企业属于处理组且《数据安全法》实施当年及以后年度取1，否则取0
控制变量	公司规模	lnAsset	总资产对数
	董事会规模	BoardSize	用董事会人数来度量
	无形资产比例	Intan	期末无形资产数额与期末资产总额的比值
	有形资产比率	Tangratio	有形资产比率＝有形资产总额/总资产
	资产负债率	Lev	资产负债率＝负债合计/资产总计
	流动性比率	LR	流动资产/流动负债

2.2.4 描述性统计

表3是对相关变量进行的描述性统计报告,由此可知,数字化转型水平从统计结果看,Digital的均值为3.183,标准差为1.321,表明样本中企业的数字化转型水平整体上处于中等水平,且企业之间的差异显著。最小值为0.000,说明部分企业在样本期内未提及任何数字化相关内容,最大值达7.403,反映头部企业已深度进行数字化转型。数字化转型水平的显著差异,为政策冲击下的DID模型提供了有效样本基础。

表3 描述性统计

变量	观测值	平均值	标准差	最小值	最大值
Digital	24 402	3.183	1.321	0.000	7.403
InAsset	24 402	22.160	1.242	18.930	27.62
BoardSize	24 402	3.814	1.197	2.000	13.000
Intan	24 402	0.045	0.053	0.000	0.852
Tangratio	24 402	0.927	0.087	0.148	1.000
Lev	24 402	0.421	0.219	0.009	3.657
LR	24 402	2.808	3.430	0.079	144.000

2.3 模型构建

采用双重差分模型(DID)评估《数据安全法》对企业数字化转型的影响,构建如下回归模型:

$$Digital_{it} = \alpha_0 + \alpha_1 Treat_i \times post_t + \alpha_2 Control_{it} + \mu_i + \gamma_t + \delta_j + \varepsilon_{it} \quad (1)$$

式中:i为上市公司;j为行业;t为年份;$Digital_{it}$为企业i在t年的数字化转型水平;$Treat_i$为实验组的虚拟变量;$post_t$为政策实施后虚拟变量;$Control_{it}$为控制变量;μ_i、γ_t、分别为企业、年份固定效应。由于受《数据安全法》影响的企业呈现明显的行业聚集特征,故添加δ_j为行业固定效应,ε_{it}为随机误差。

3 实证结果及分析

3.1 基准回归结果

对模型(1)进行基准回归,表示《数据安全法》政策对企业数字化转型水平的影响。表4列(1)显示,在未加入任何控制变量与固定效应时,did的系数显著为正,说明《数据安全法》的实施对企业的数字化转型具有显著的促进作用,而不是抑制企业的数字化转型。列(2)表示在加入了三种固定效应以后,did系数出现大幅的减小,但其显著性不变,说明固定效应有效剥离了个体特征和宏观趋势的干扰,此时系数反映的是政策净效应,即排除企业、年份、行业差异后,政策推动数字化转型的净影响。列(3)的结果显示,在同时加入全部的控制变量以及三种固定效应以后,did的相关系数仍显著为正,且与列(2)的结果相近,表明在控制了企业的基本特征和宏观经济因素之后,数据规制政策对企业数字化转型的促进作用是稳健的,H1得到验证。

表4 基准回归结果

变量	(1)	(2)	(3)
	Digital	Digital	Digital
did	1.634***	0.130***	0.126***
	(0.037)	(0.026)	(0.025)
InAsset			0.205***
			(0.026)
BoardSize			0.006*
			(0.003)
Intan			−0.422
			(0.346)
Tangratio			−0.961***
			(0.161)
Lev			−0.205***
			(0.067)
LR			−0.007**
			(0.004)
常数项	3.058***	3.173***	−0.381
	(0.021)	(0.002)	(0.634)
个体固定效应	否	是	是
年份固定效应	否	是	是
行业固定效应	否	是	是
观测值	24 402	24 402	24 402
R^2	0.108	0.848	0.851

注:***、**、*分别表示1%、5%、10%的显著性水平;括号内为稳健标准误。

3.2 稳健性检验

3.2.1 平行趋势检验

为检验《数据安全法》的实施对企业数字化转型的促进效应,实验组与对照组在政策实施前应该具有平行趋势,构建动态效应模型。

$$Digital_{it} = \beta_0 + \sum_{t=2014}^{2022} \beta_t Treat_i \times post_t + \beta_2 Control_{it} + \mu_i + \gamma_t + \delta_j + \varepsilon_{it} \quad (2)$$

式中:β_0为截距项;β_t、β_2为相关系数。

为避免共线性干扰,参考龚勤林等[17]的做法,将《数据安全法》实施前第8年(2013年)作为基准年,其他各变量与模型(1)定义相同。参考Beck等[18]的相关做法,首先计算政策前各个年份的平均值,然后再对2014—2022年的置信区间和回归系数采取减去平均值的方法,尽可能地处理存在的事前趋势。图1是以横轴为政策实施前后的时间,纵轴为数字化转型水平的估计系数,刻画90%置信区间平行趋势检验的估计结果。结果表明,在政策实施前回归系数与0无显著差异,说明样本企业在政策

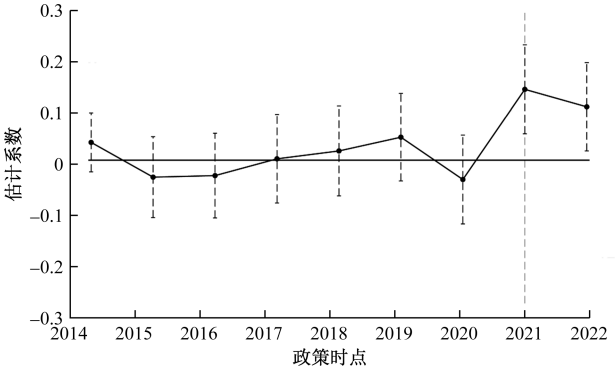


图 1　平行趋势检验

实施前具有平行趋势；在政策实施后，回归系数显著大于 0，说明政策实施后样本企业的数字化转型水平具有显著增长。平行趋势检验结果支持了 DID 模型的核心假设，为基准回归结果的可靠性提供了关键支撑，同样也证明了《数据安全法》实施后实验组企业数字化转型水平的显著提升，确实是由政策冲击而非样本选择偏差或其他时间趋势导致，平行趋势假设得以验证。

3.2.2　调整样本期间

由于《数据安全法》是在 2021 年才颁布实施的，而样本期间为 2013—2022 年，使得平行趋势检验存在政策实施前时间周期过长的问题。为了缓解政策实施前时间周期过长可能会对平行趋势检验造成影响，参照马瑄忆和施新政[11]的做法，通过缩短政策实施前的时间周期来缓解这类问题。将样本期间调整为 2016—2022 年后，结果如图 2 所示，平行趋势假设仍然成立。

3.2.3　安慰剂检验

参考葛世龙和涂振宇[19]的做法，通过对实验组进行随机性抽取，从而将其他不可观测因素对企业数字化转型水平的影响进行进一步的排除，保证基准回归的稳健性。针对自变量的分布情况，随机抽样 1 000 次构建为实验组，并使用模型(1)重新进行回归估计，结果如图 3 所示。根据图 3 显示的结果，抽样回归的系数分布 0 的附近，基准回归的真实系数值与安慰剂检验系数的平均值不存在明显的差异，这表明基准回归结果是相对稳健的。

3.2.4　重新定义解释变量

从立法进程看，《数据安全法》于 2018 年列入规划后，历经 2020 年 6 月初稿初审，至 2021 年 6 月 10 日由中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议通过并于 9 月 1 日正式施行，三年时间内快速推进，凸显国家对数据安全

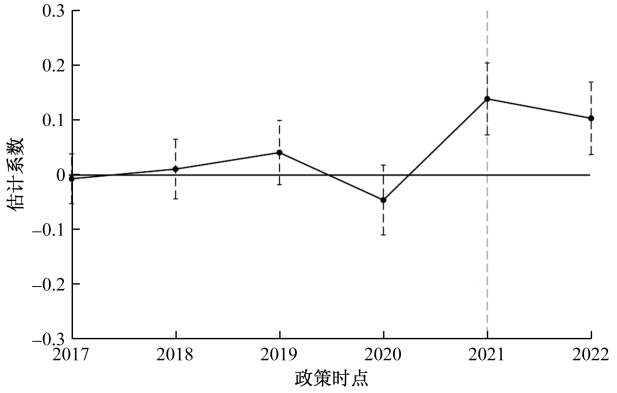


图 2　调整样本期间

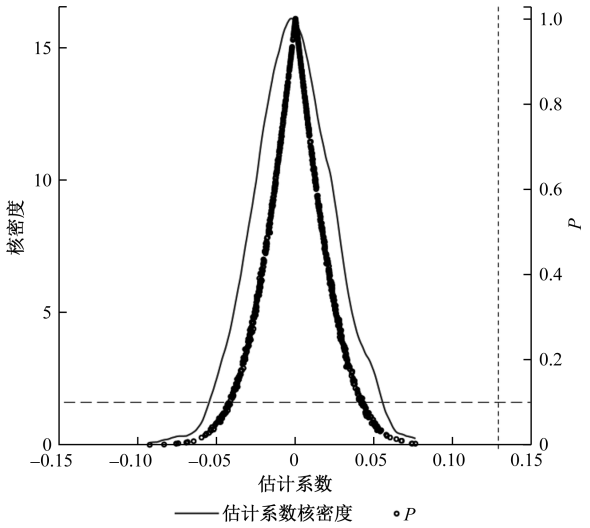


图 2　安慰剂检验

治理的高度重视。《数据安全法》的立法动态引发各行各业的广泛关注，在数字经济背景下，数据已成为各行业的基础性战略资源，无论是传统制造业、服务业，还是新兴的科技产业，数据的采集、存储、使用等环节均与业务运营深度绑定。为了避免不必要的影响，参考马瑄忆和施新政[11]的做法，假定《数据安全法》在 2018 年就已经开始造成影响，当观测期处在 2018 年以后时，post 取值为 1，否则取值为 0，得到新的核心解释变量 did1。表 5 列(1)和列(2)的相关结果表明，无论是否加入控制变量，新的解释变量的系数仍然显著为正，证明了基准回归结果的稳健性。

3.2.5　替换被解释变量

参考吴非等[20]、赵宸宇等[21]、甄红线等[22]的做法，重新计算被解释变量，进一步验证基准回归结果的稳健性。重新选取企业数字化转型水平的关键词，一共筛选出 313 个相关的关键词，并将其导入 Python 中，从而对上市公司年报中“管理层讨论与分

表 5　稳健性检验结果

变量	(1)	(2)	(3)
	Digital	Digital	Digital2
did1	0.073***	0.060**	
	(0.027)	(0.027)	
did			0.112***
			(0.014)
常数项	3.173***	−0.388	−0.409*
	(0.004)	(0.634)	(0.246)
控制变量	否	是	是
个体固定效应	是	是	是
年份固定效应	是	是	是
行业固定效应	是	是	是
观测值	24 402	24 402	24 402
R^2	0.847	0.851	0.838

注:***、**、* 分别表示 1%、5%、10%的显著性水平;括号内为稳健标准误。

析”(MD&A)部分的中英双语文本进行分词处理。在剔除一系列无关内容后,计算数字化关键词的总词频,除以 MD&A 中英部分的文本语段长度,最终将结果乘以 100,得到新的被解释变量 Digital2。相关回归结果如表 5 列(3)所示,解释变量 did 的系数仍显著为正。这一结果表明,即使采用不同的数字化转型测度方法,《数据安全法》的实施仍显地促进企业数字化转型水平的提升,再一次验证了 H1 的稳健性。

3.3　异质性

3.3.1　产权性质

参考杜群阳等[23]的做法,国有企业作为政府政策执行的重要载体,在数据安全领域往往承担更多前置性合规责任,国有企业与数字化转型有关的决策会受到政治目标与市场目标的双重影响,与之相比,非国有企业更依赖于激烈的市场竞争维系生存,数据安全政策可通过合规倒逼效应转化为战略调整的内生动力。根据企业实际控制人的性质来划分,分为国有和非国有两组,回归结果如表 6 列(1)列(2)所示。国有企业回归系数不显著,而非国有企业回归系数显著为正。这表明《数据安全法》政策对非国有企业数字化转型的促进作用更强,而对国有企业的影响却并不明显。可能原因是,国有企业在政策实施前已普遍建立数据安全管理体系,政策带来的边际规制压力有限,以及国有企业虽具备资源优势,但科层制管理可能延缓转型决策,从而使其不显著。非国有企业则因市场竞争压力,数据安全事件可能直接威胁客户信任,倒逼其加速数字化转型以提升安全能力,并且非国有企业组织架构扁平化,能更快将数据安全需求嵌入数字化战略,迫使其加快数字化转型进程。

3.3.2　数据泄露风险

行业数据泄露风险的异质性分析基于违规成本-数据依赖双重作用逻辑。从违规成本看,数据泄露高风险行业的数据资产具有高敏感性与高价值密度,一旦发生相关的数据安全事件,将会面临相关法律的处罚、相关业务的中断以及企业声誉损失等复合成本,这种高风险-高代价机制促使企业对政策产生更强的响应动机。从数据依赖度看,高风险行业的核心业务高度依赖数据流转,数据安全与业务连续性深度绑定,政策实施后企业为满足合规要求,必须同步升级全链条数字化系统,从而形成合规需求促使技术升级的倒逼效应。而低风险行业的数据资产价值密度较低,业务运营对数据的依赖程度有限,政策带来的合规投入易被视为额外的成本,难以转化为低风险行业的企业进行数字化转型的主要动力。因此,参考吴武清等[15]的做法,将科学研究和技术服务业,交通运输、仓储和邮政业,批发和零售业界定为容易发生数据泄露的行业。同时,甄红线等[22]指出,随着制造业数字化水平持续提升,防范数据泄露、抵御非法访问等仍是制造业数字化发展的核心挑战,并且,根据《2024 年数据泄露调查报告》的统计,制造业发生 2 305 起攻击事件,849 起确认数据泄露。系统入侵、社会工程和基本 Web 应用攻击是常见事件模式,25%的数据泄露事件中,不法分子通过窃取凭证安装恶意软件、勒索软件。其漏洞利用在数据泄露中的比例达 20%,较 2024 年增长 34%,勒索软件在数据泄露中的比例为 44%,较 2024 年增长 37%,种种数据表明,制造业面临的内外部数据安全威胁严峻,数据泄露风险极高,据此,将其定义为容易发生数据泄漏的行业。最后,根据奇安信发布的《2024 中国政企机构数据安全风险研究报告》显示,互联网行业是数据泄露风险事件的高发行业之一,互联网行业企业可泄露的数据占所有可泄露数据的 60.5%,信息传输、软件与信息技术服务业与互联网行业紧密相关,大量的数据处理、存储和传输使其面临极高的数据泄露风险,因此也将其定义为容易发生数据泄漏的行业。将上述行业定义为数据泄露行业,其他则为非数据泄露行业。回归结果如表 6 列(3)和列(4)所示,数据泄漏高风险组的回归系数显著为正,低风险组的回归系数不显著。表明政策对数据泄漏高风险行业的企业数字化转型的促进效应更为显著,而对数据泄漏低风险行业无显著影响。可

能原因是，数据泄露行业间的政策效应差异本质上由违规成本与数据依赖度的行业分化所致，数据泄露高风险行业面临的违规成本具有灾难性，一旦发生数据泄露事件，企业将遭受巨大的声誉和财产损失，这就迫使企业将数据安全政策转化为数字化转型的直接动力。此外，数据泄露高风险行业的业务模式高度依赖数据要素运转，政策实施后，企业为满足数据分类分级保护、跨境传输评估等要求，必须同步推进数据中台、区块链加密等数字化基础设施建设，客观上推动了数字化转型进程。反观数据泄露低风险行业，其生产经营对数据的依赖程度较低，数据泄露对业务的直接冲击有限，政策要求的合规投入常被视为非必要成本，加之数据资产价值密度低，企业缺乏将合规需求转化为数字化升级的经济激励，导致政策效应未能有效释放。

3.3.3　企业市场竞争力

为探究《数据安全法》对不同市场竞争力企业数字化转型的差异化影响，采用个股勒纳指数（PCM）来衡量企业市场竞争力，参考张伯伟和马凡慧[24]的做法，计算公式为：PCM＝（营业收入-营业成本-销售费用-管理费用）/营业收入。具体而言，按照PCM的中值将样本企业划分为两组，分别为市场竞争较强组和市场竞争较弱组两组，以此来分析政策效应在不同市场地位企业中的异质性特征。回归结果如表6列（5）和列（6）所示。在市场竞争较弱组中，did的系数不显著；市场竞争较强组中，did的系数显著为正。这表明《数据安全法》对市场竞争力较强企业的数字化转型促进效应更为显著，而对市场竞争力较弱企业的影响不显著。可能原因是，市场竞争力较强的企业通常具备更充足的资金储备与技术积累，能够将数据安全合规成本转化为长期竞争优势，而且市场竞争力较强的企业往往更依赖数据要素维持竞争优势，其数据资产价值密度更高，导致数据泄露的潜在损失更为严重，因此，这类企业更倾向于将《数据安全法》视为优化数据管理体系的契机，通过数字化转型强化数据安全防护。反观市场竞争力较弱的企业，由于面临激烈的价格竞争，难以通过涨价转嫁成本，且合规投入可能挤压研发预算，导致转型动力不足，并且市场竞争力较弱的企业数据依赖度较低，政策对其核心业务的影响有限。

4　进一步分析

《数据安全法》对企业数字化转型除具有直接的推动作用外，还可能通过其他变量对企业数字化转型具有间接的推动作用。为研究《数据安全法》对企业数字化转型的间接推动作用，参考江艇[25]提出的二步法构建中介效应模型，构建如下回归模型。

$$DC_{it} = \alpha_0 + \alpha_1 Treat_i \times post_t + \alpha_2 Control_{it} + \mu_i + \gamma_t + \delta_j + \varepsilon_{it} \quad (3)$$

式中：DC_{it}为中介变量；回归时分别用数据保护重视程度（Data Protection）、高技能人员占比（rc）作为中介变量。

4.1　数据保护重视程度

《数据安全法》作为一项重要的制度规范，为企业的数据管理划定了合规边界，当该政策实施后，企业面临数据安全合规的外在约束与数据资产保护的内在需求，数据保护重视程度（以合规成本衡量）成为连接政策冲击与企业数字化转型的关键传导纽带。企业为契合法律要求，必然要在数据安全体系构建上进行资源投入，这一投入过程不仅是对制度压力的响应，更是对企业所依赖的数据资产价

表6　异质性分析结果

变量	（1）	（2）	（3）	（4）	（5）	（6）
	国有企业	非国有企业	数据泄露行业	非数据泄露行业	企业市场竞争较弱	企业市场竞争较强
	Digital	Digital	Digital	Digital	Digital	Digital
did	0.069	0.140***	0.125***	0.051	0.028	0.177***
	（0.052）	（0.029）	（0.026）	（0.104）	（0.039）	（0.033）
常数项	1.778	−0.428	−0.207	−1.241	−2.461***	2.601***
	（1.304）	（0.760）	（0.649）	（2.368）	（0.834）	（0.870）
控制变量	是	是	是	是	是	是
个体固定效应	是	是	是	是	是	是
年份固定效应	是	是	是	是	是	是
行业固定效应	是	是	是	是	是	是
观测值	7 085	17 269	22 631	1 769	11 837	11 846
R^2	0.826	0.861	0.857	0.803	0.842	0.884

注：***、**、*分别表示1%、5%、10%的显著性水平；括号内为标准误。

值进行的保护与深度探索。参照吴武清等[15]的做法,采用构建核心解释变量时筛选得到的企业2021年报中出现的有关《数据安全法》的关键词,然后计算出年报相关词的词频并除以年报总词频,再乘100,得到中介变量数据保护重视程度(Data Protection)。回归结果如表7列(1)所示,回归系数显著为正,意味着政策实施后,企业在数据保护重视程度(合规成本)方面的投入显著增加。

在既有研究中,由政府政策引发的合规成本,常常被视为企业数字化转型的阻碍,例如,屠西伟和张平淡[26]认为,当企业需将资源投向治污设备等合规领域,企业在数字化转型方面的投入容易被削减,从而抑制企业数字化转型;李剑培等[27]认为,数字政府建设可以通过降低合规成本的方式来促进企业数字化转型。但《数据安全法》带来的合规成本,却呈现截然不同的作用逻辑,这源于数据要素特性与数字化转型技术架构的深度关联。在企业数字化转型过程中,数据是核心生产要素,《数据安全法》实施后,企业提升数据保护重视程度(合规成本),表面是应对制度约束的资源消耗,实则是构建数据要素安全生态的必要投资。当企业强化数据加密技术研发、搭建安全存储体系、优化访问控制流程时,这些数据安全基础建设,与云计算平台的数据分层存储、大数据分析的全链路溯源需求高度互补,反而成为企业数字化转型的助推力,最终推动企业进行数字化转型。由此验证了H2,《数据安全法》的实施通过提高合规成本从而促进企业数字化转型。

4.2 高技能人员占比

在数字化转型与数据安全的双重需求下,高技能人员占比成为连接政策与转型的另一关键中介。《数据安全法》重塑了企业人才需求体系,既需要精通数据安全合规的专业人才,也需要适配数字化技术创新的复合型人力,推动企业优化人力资源配置。参考赵宸宇和李烦钰[28]的做法,采用企业技术人员占比以及本科及以上学历人员占比作为中介变量,得到了中介变量高技能人员占比(rc),回归结果如表7列(2)所示。解释变量对高技能人员占比的回归系数(0.016 5)显著为正,说明数据规制政策的实施促使企业高技能人员占比提升。

高技能人员既是数据安全合规的执行者,更是数字化技术融合创新的推动者。高技能人员占比的提升,一方面直接强化了企业的数据安全防护能力,这类人才能够运用专业知识设计先进的数据安全方案,保障企业数据资产在数字化流程中的安全性;另一方面,高技能人员的知识溢出效应极为关键,他们在参与数据安全建设与数字化项目时,会将先进技术理念、创新思维传递到企业组织内部,带动整体技术能力提升。这种人才驱动的技术创新与管理优化,为企业数字化转型提供了人力与知识的双重支撑,将政策对人才结构的影响,转化为企业数字化转型的内在动力,实现从人才储备到数字化能力跃升的传导。孙伟增等[29]认为,政府发放的专项补贴能推动企业培养和引进数字人才,从而产生数字人才集聚的"雁阵效应",进而提升企业数字化转型能力,破解企业在数字化转型中能力不足等难题。由此H3得到验证。

表7 中介变量回归结果

变量	(1)	(2)
	Data Protection	rc
did	0.004***	0.017***
	(0.001)	(0.006)
常数项	−0.001	0.294*
	(0.008)	(0.169)
控制变量	是	是
个体固定效应	是	是
年份固定效应	是	是
行业固定效应	是	是
观测值	24 402	24 402
R^2	0.871	0.890

注:***、**、*分别表示1%、5%、10%的显著性水平;括号内为标准误。

5 结论与启示

5.1 结论

在高速发展的数字经济浪潮中,数据作为新的生产要素的战略价值愈发凸显,而《数据安全法》的正式实施,为规范各类数据处理行为、筑牢数据安全防线提供了坚实的法律基石。本文以2021年实施的《数据安全法》为准自然实验,以2013—2022年A股上市公司数据为基础,对《数据安全法》政策的实施对企业数字化转型的影响进行了检验。研究表明,数据规制政策实施以后,实验组企业数字化转型水平较对照组企业得到了显著的提升(提升12.6%),且经过多重稳健性检验后,结论依然稳健。这一发现改变了以往将数据安全政策单纯视为企业合规成本负担的认知,证明了数据安全规制对企业数字化转型水平是具有正向的推动作用。异质性分析表明,《数据安全法》政策的作用在非国有企业、数据泄露高风险行业、市场竞争力较强的企业中效果更显著;机制分析表明,政策通过合规

成本压力倒逼企业开展技术创新，并吸引高技能人才加入，以双渠道驱动企业数字化转型进程，最终提升企业数字化转型水平和能力。

从长期看，《数据安全法》对企业数字化转型的影响可能并非静态的短期推动，而是随技术迭代、行业生态演变呈动态变化的过程。短期内企业的合规投入多聚焦于满足基础安全要求，而长期中这些投入形成的技术基础与数据治理能力，可能转化为企业核心竞争力。但长期影响也面临多重不确定性。一方面，若政策未能与技术发展保持同步，可能出现规制滞后问题。随着AI生成式数据、边缘计算等新兴技术的普及，现有数据安全标准可能难以覆盖新型数据处理场景，导致企业陷入合规与创新的两难，如果严格遵循旧标准可能限制技术应用，而突破标准又面临合规风险，这种矛盾可能在长期中抑制数字化转型的创新活力。另一方面，行业内企业的数字化能力分化可能加剧。市场竞争力较强的企业，可通过长期持续的合规投入形成技术壁垒，进一步扩大与中小微企业的差距，而非国有企业虽短期转型动力强，但长期若缺乏政策对研发资源、人才培养的持续支持，可能因合规成本累积陷入转型瓶颈，反而拉大与国有企业在数字化深度上的差距。

5.2 启示

首先，完善差异化政策实施机制。监管部门应根据企业产权性质和行业数据泄露风险差异，完善数据安全政策的差异化实施机制。对于数据泄露高风险行业，可加强政策引导与监管力度，推动其将数据安全合规要求转化为数字化转型的动力。其次，对于民营企业，因其在数据安全政策响应中表现更强的转型动力，但可能面临资源有限等问题，监管部门可提供更多的支持与指导，同时，加强数据安全政策与其他数字经济政策的协同配合，形成全方位的政策支持体系，为企业创造一个有利于数字化发展的环境。最后，建立跨区域数据安全执法协调机制，避免因地方保护主义导致政策执行差异，同时通过“监管沙盒”试点探索新兴技术场景下的合规路径。

本文虽取得了一定的成果，但仍存在一些局限。一方面，仅考察了《数据安全法》实施的短期效应，未来可进一步追踪政策的长期影响，分析其对企业数字化转型的持续作用机制；另一方面，未涉及地区数据安全执法力度差异的分析，不同地区执法力度的不同可能会对企业数字化转型产生不同的影响，这也是未来值得拓展的研究方向。此外，随着数字经济的不断发展，数据安全问题可能会呈现新的特点和挑战，后续研究可结合新的政策环境和技术发展，深入探讨数据安全与企业数字化转型的动态关系，为数字经济治理提供更全面、更深入的理论支持和决策参考。

参考文献

[1] 张一林，郁芸君，陈珠明. 人工智能、中小企业融资与银行数字化转型[J]. 中国工业经济，2021(12)：69-87.

[2] ARIDOR G，CHE Y K，SALZ T. The economic consequences of data privacy regulation：empirical evidence from GDPR [R]. Cambridge，MA，USA：National Bureau of Economic Research，2020.

[3] MULGUND P，MULGUND B P，SHARMAN R，et al. The implications of the california consumer privacy act (CCPA) on healthcare organizations：lessons learned from early compliance experiences[J]. Health Policy and Technology，2021，10(3)：100543.

[4] DALEY M J，PRIEBE J，ZELLER P. Theimpact of emerging Asia-Pacific data protection and data residency requirements on transnational information governance and cross-border discovery[J]. Journal of Sendon a Conference，2015，16：201.

[5] 高磊，赵章界，林野丽，等. 基于《数据安全法》的数据分类分级方法研究[J]. 信息安全研究，2021，7(10)：933-940.

[6] 戴双兴. 数据要素：主要特征、推动效应及发展路径[J]. 马克思主义与现实，2020(6)：171-177.

[7] 苏桑妮. 爬取公开信息行为入罪的逻辑解构与标准重构——从“反爬行为”的性质切入[J]. 浙江社会科学，2024(4)：55-67.

[8] 蒋冬雪，李芳芳，李三希. 数据要素加速流通形势下我国个人信息保护态势分析与评估[J]. 工信财经科技，2025(3)：1-11.

[9] 蒋率兵. 深化大湾区数字贸易协同推动区际法治与国际法治有效衔接[J]. 中国外资，2025(8)：56-58.

[10] 丁晓东. 数据交易如何破局——数据要素市场中的阿罗信息悖论与法律应对[J]. 东方法学，2022(2)：144-158.

[11] 马瑄忆，施新政. 隐私保护与企业业绩表现——基于《个人信息保护法》的实证研究[J]. 经济科学，2024(6)：122-147.

[12] 申宇冰. 智能化转型影响商贸流通企业服务创新效率的机理[J]. 商业经济研究，2025(15)：154-159.

[13] 李秋斌. 创新生态系统视角下高职院校科技成果转化的构建路径与实践[J]. 中国职业技术教育，2025(9)：58-65.

[14] 肖土盛，孙瑞琦，袁淳，等. 企业数字化转型、人力资本结构调整与劳动收入份额[J]. 管理世界，2022，38(12)：220-237.

[15] 吴武清,田雅婧,叶康涛,等. 企业数据资源的价值——基于《通用数据保护条例》实施的准自然实验[J]. 会计研究,2024(9):76-90.
[16] 张正平,于新.《数据安全法》对商业银行金融科技投入的影响研究[J]. 现代金融研究,2025,30(3):56-67.
[17] 龚勤林,乔涛,冷玉婷. 数字经济与农业全要素生产率:技术进步和要素流动的视角[J]. 华中农业大学学报(社会科学版),2025(2):15-27.
[18] BECK T, LEVINE R, LEVKOV A. Big bad banks? the winners and losers from bank deregulation in the United States[J]. The Journal of Finance, 2010, 65(5): 1637-1667.
[19] 葛世龙,涂振宇. 政府数据治理、数字生态与企业新质生产力[J]. 工业技术经济,2025,44(6):57-67.
[20] 吴非,胡慧芷,林慧妍,等. 企业数字化转型与资本市场表现——来自股票流动性的经验证据[J]. 管理世界,2021,37(7):130-144.
[21] 赵宸宇,王文春,李雪松. 数字化转型如何影响企业全要素生产率[J]. 财贸经济,2021,42(7):114-129.
[22] 甄红线,王玺,方红星. 知识产权行政保护与企业数字化转型[J]. 经济研究,2023,58(11):62-79.
[23] 杜群阳,刘登鳌,洪晨翔,等. ESG表现与企业劳动力就业——数字化转型的调节作用[J]. 软科学,2025,39(4):69-76.
[24] 张伯伟,马凡慧. 智能制造如何提升产业链供应链韧性:理论机制与实证检验[J]. 经济学动态,2024(11):20-37.
[25] 江艇. 因果推断经验研究中的中介效应与调节效应[J]. 中国工业经济,2022(5):100-120.
[26] 屠西伟,张平淡. 企业数字化转型、碳排放与供应链溢出[J]. 中国工业经济,2024(4):133-151.
[27] 李剑培,时洁,顾乃华. 数字政府建设对企业数字化转型的溢出效应研究——来自政府采购合同大数据的证据[J]. 南方经济,2025(2):1-25.
[28] 赵宸宇,李炳钰. 劳动力成本与企业数字化转型:机制讨论与经验证据[J]. 当代经济科学,2024,46(6):103-115.
[29] 孙伟增,毛宁,兰峰,等. 政策赋能、数字生态与企业数字化转型——基于国家大数据综合试验区的准自然实验[J]. 中国工业经济,2023(9):117-135.

Does Data Security affect the Digital Transformation of Enterprises? A Quasi-natural Experiment Based on the *Data Security Law*

WU Jiaqi[1], XU Ye[2], WEN Qian[3]

(1. School of Applied Economics, Jiangxi University of Finance and Economics, Nanchang 330013, China;
2. School of Modern Economics and Management, Jiangxi University of Finance and Economics, Nanchang 330013, China;
3. School of Business Administration, Jiangxi University of Finance and Economics, Nanchang 330013, China)

Abstract: Taking the implementation of the Data Security Law introduced in 2021 for A-share listed companies in China as an exogenous shock and employing the difference-in-differences (DID) model, the impact of data security regulations on enterprises' digital transformation and the corresponding mechanism was examined based on panel data from 2013 to 2022. The results indicate that the Data Security Law of the People's Republic of China significantly promotes enterprises' digital transformation. More significant effects are observed in non-state-owned enterprises, industries with high risk of data leakage and enterprises with strong market competitiveness. Mechanism analysis shows that the policy forces enterprises to carry out technological innovation through the pressure of compliance costs and attracts high-skilled talents to join, driving the process of enterprises' digital transformation through dual channels. After a series of robustness tests, the conclusions remain reliable. This study reveals the interaction between data security policies and enterprises' digital transformation, and decision-making references are provided for regulatory authorities to optimize digital economy governance.

Keywords: data security law; enterprise digital transformation; data elements; compliance costs