审计学科发展

场景化弹性规制框架下的国家审计实践方法创新

——基于“法律-技术-审计”协同治理的视角

张荣刚[1],吴亚州[1,2]

(1. 西北政法大学 研究生院,陕西 西安 710063;2. 中国航空工业集团公司雷华电子技术研究所,江苏 无锡 214063)

[摘　要]针对数字时代数据主权博弈与算法治理异化对国家审计的挑战,需构建“法律-技术-审计”三元协同的治理框架。法律层明确主权层级与合规底线,技术层通过联邦学习与区块链实现穿透性验证,审计层依托动态授权与梯度豁免机制履行监督职能。研究创新性地提出“场景化识别—弹性化响应”的闭环治理逻辑,形成“规则代码化、证据可追溯、验证分布式”的智能审计模式,推动 ISAE 3000 标准本土化与跨境数据流动审计创新,为提升国家审计在数字治理中的适应性及制度型开放提供理论支撑与实践路径。

[关键词]场景化弹性规制;法律-技术-审计协同;主权分层理论;联邦学习审计;智能审计;国家审计

[中图分类号]F239　　[文献标志码]A　　[文章编号]2096-3114(2026)01-0009-13

一、引言

随着数字文明浪潮的演进,传统审计范式正面临前所未有的适应性挑战。数据主权的空间解构与算法权力的技术异化,使工业时代形成的刚性规制逻辑面临双重困境。其一,主权国家间的管辖权竞合,引发了审计穿透的合法性悖论;其二,算法黑箱的不可解释性,削弱了传统证据链的规范基础,带来证据难以认定的技术性风险。这种双重张力,在跨境数据流动等典型场景中演化为系统性风险。本文以其监管与审计作为核心案例,正是因为该场景所集中面临的管辖权竞合与算法黑箱难题,深刻体现了传统审计范式的适配性困境。其他场景(如公共卫生应急等)将作为辅助例证,阐释本框架的弹性适配能力。既往研究虽在主权分层理论、场景完整性原则等维度展开探索,却多囿于单一学科:具体而言,法学聚焦数据主权博弈的规范解构,审计学侧重合规性导向的流程优化,技术领域则聚焦算法可解释性的工具改良。这种分野导致未能形成跨学科协同的治理框架。

现有规制路径存在三重结构性不足。其一,传统审计范式存在静态合规导向与动态风险时序的不匹配,致使重大风险难以被有效纳入监管视野[1];其二,统一审计标准与场景异质性需求的空间失衡,造成中小企业面临“合规性挤出创新性”的生存困境[2];其三,组织边界消融引发的责任认定模糊,使得联邦学习等分布式技术应用陷入治理挑战。美欧通过《澄清域外合法使用数据法案》(CLOUD 法案)①、

[收稿日期]2025-06-16

[基金项目]国家社会科学基金项目(25FJYB050);审计署 2024 至 2025 年度重点科研课题(24SJ03003);西北政法大学国家级重大科研培育项目(2025ZD02)

[作者简介]张荣刚(1973—),男,陕西淳化人,西北政法大学教授,博士生导师,主要研究方向为数字治理、审计、财税法律制度;吴亚州(1983—),男,江苏沛县人,西北政法大学博士生,中国航空工业集团公司雷华电子技术研究所高级工程师、公司律师,主要研究方向为审计数字治理、纪检监察、国家安全法,通信作者,邮箱:13861742050@163.com。

①《澄清域外合法使用数据法案》(Clarifying Lawful Overseas Use of Data Act, CLOUD Act),2018 年由美国颁布。该法案的核心在于确立“数据控制者标准”,授权美国执法机构可调取受其管辖的企业(如微软、谷歌)在全球范围内掌控的数据,突破了传统的“数据存储地”管辖原则,是美国数据领域“长臂管辖”的典型体现。

②《通用数据保护条例》(General Data Protection Regulation, GDPR),由欧盟于 2016 年通过,2018 年 5 月 25 日正式生效。该条例以其广泛的域外适用效力、严格的数据主体权利保护(如被遗忘权、数据可携权)和最高可达全球年营业额 4% 的巨额罚款,成为全球数据保护立法的标杆。

《通用数据保护条例》（GDPR）②等制度输出，对全球审计治理的格局产生深远影响。

本文框架遵循“法律赋权—技术控权—审计监督”的递进逻辑。法律赋权聚焦于界定国家审计权与数据主权的边界，为框架提供法律根基；技术控权通过规则代码化、联邦学习等技术路径，将法律原则转化为可操作逻辑；审计监督承担验证与反馈职能，通过效果评估形成治理闭环，推动框架动态优化。

二、“法律－技术－审计”协同治理的研究述评

现有研究多在技术赋能或法律规制等路径下展开，对技术、法律与审计的协同需求整合尚不充分。本节对现有研究进行梳理与评述，旨在揭示二元分野的局限，论证法律、技术与审计三者协同的必然。

（一）技术赋能审计的研究进展：从工具理性到模式变革

随着信息技术的迅猛发展，技术赋能国家审计已成为学术研究的重要方向。

在技术作为审计效率提升工具的研究层面，早期学者重点关注了特定信息技术在审计业务流程中的应用效能，系统分析了大数据、云计算等技术在审计数据采集、处理与分析环节的应用，指出这些技术显著扩展了审计覆盖范围并提升了工作效率[3]。此类研究充分肯定了技术的方法论贡献，但多数研究将技术视为中立的效率工具，侧重于解决“如何做”的操作性问题，而对技术应用必须具备的法律授权基础、数据安全合规要求等“为何能做”及“如何合规地做”的根本性约束探讨不足，体现出明显的工具理性倾向。

在智慧审计与审计模式变革的研究层面，学者们开始关注技术对审计范式的系统性影响，剖析了智能审计的技术架构，论证了人工智能如何推动审计从传统抽样模式向全量数据分析模式转型[4]。近期研究更是聚焦于大模型技术在审计场景中的应用前景，探讨了基于自然语言处理的智能审单、风险自动预警等创新模式。这些研究敏锐地捕捉到审计从事后监督向事中、事前预警延伸的范式转变趋势。然而，这些研究多从技术内生逻辑出发，侧重于算法优化、模型构建与平台设计，对于如何将外部法律规则和合规要求内嵌于技术系统（即“Compliance-by-Design”①），以及智能审计技术应用所衍生的新型法律责任界定、算法伦理风险管控等关键问题，学术探讨尚不充分，未能形成技术与制度良性互动的完整理论框架。

综上所述，既有技术赋能研究虽丰富了审计工具，但多局限于“如何做”的技术控权层面，且常疏于考量“能不能做”的法律赋权根基，体现了与技术协同前的分野状态。

（二）审计与法律协同治理的研究视角：制度框架下的权力运行

审计与法律的协同治理研究主要围绕国家审计的法治基础及其与其他监督机制的互动关系展开，形成了从宏观制度建构到中观机制衔接的学术探讨。

既有研究从国家治理高度阐释了审计的法治基础，有学者系统论述了国家审计的功能和定位[5]，另有学者夯实了其服务于国家治理现代化的逻辑[6]。这类研究宏观上确立了审计的定位，却未能有效解决法律授权向技术化审计规程转译的核心困境。例如，在算法审计等新兴领域，如何将“数据主权”“算法透明”等抽象法律原则转化为可操作的审计程序与证据标准，现有研究缺乏系统方案。

进一步看，研究多聚焦于审计与纪检监察、司法等外部监督的机制协同[7]，这固然重要，但尚未触及提升审计效能的底层逻辑，即审计活动自身如何实现从法律赋权到技术控权的闭环。现有探讨在“法律-技术-审计”三者关系上呈现分野，对借助技术手段将法律规则代码化、操作化的转译机制研究不足，制约了治理效能。

（三）研究述评：走向“法律-技术-审计”的三元协同

既有研究在“法律－技术－审计”三者关系的探讨上呈现分野，尚未能形成系统协同视角。其一，法律赋权研究疏于向技术控权的操作化转译；其二，技术控权探索弱于同审计监督的闭环化衔接。这种

①Compliance-by-Design 指的是将法律法规等合规要求，在技术系统或业务流程的最初设计阶段就作为核心原则嵌入其中，而不是在系统建成或业务开展后作为附加功能进行弥补。

链条断裂导致治理在“合法性奠基—合规化执行—效能反馈”环节出现脱节。因此,构建一个三者递进协同的理论框架,为系统化解当前治理挑战提供了关键路径,亦是本研究的核心方向。

三、问题缘起与研究进路

数字技术革命重构审计治理底层逻辑,传统审计范式在数据主权分层与算法权力异化的双重张力下面临系统性困境。数据跨境流动突破物理边界管辖,算法黑箱冲击传统证据链规范基础,CLOUD 法案与 GDPR 等制度工具正将审计场域异化为数字霸权博弈场。

(一) 规制范式转型的现实诉求

1. 传统审计范式的场景适配困境

传统审计范式植根于标准化、线性化的工业经济逻辑,其刚性规制模式在应对数字经济场景时面临适配性挑战,尤其体现在统一审计标准与差异化治理需求之间的动态平衡上。其一,统一审计标准与差异化治理需求的结构性失衡。在跨境数据流动、算法决策、平台经济等新兴场景中,审计对象的异质性显著增强。例如,金融征信场景需验证算法公平性,医疗健康场景需追踪基因数据全生命周期,而传统审计准则(如 ISAE 3000)仍沿用“全行业通用指标 + 抽样检查”模式,导致风险敏感性与技术可靠性评估失准。其二,静态合规导向下的监管滞后性表征。在现代审计实践中,虽然信息技术应用已显著提升了数据处理能力,但传统审计范式以周期性复核和历史数据验证为核心的特性,使其在应对高度动态、实时的数据流风险时仍面临时效性挑战。以中概股审计为例,在 2020 年瑞幸咖啡财务造假事件中,SEC① 要求调取实时交易数据以核查关联方舞弊行为,但传统审计底稿仅依赖周期性复核的历史财务数据,导致监管滞后性显著。瑞幸通过虚构订单量及收入的历史数据,累计虚增交易额达 22 亿元人民币,而静态底稿审计未能实时追踪其实际现金流与订单系统的动态差异,致使舞弊行为持续近一年才被揭露(源自 SEC 2020 年行政处罚决定书 File No. 3 – 19770)。其三,组织边界消融引发的责任认定困境。联邦学习、分布式账本等技术的广泛应用,使得数据处理链条中的参与主体更加多元、权责关系更为复杂,对传统审计所依赖的“委托 – 代理”责任框架提出了新的治理挑战[8]。在跨境云服务场景中,数据存储、计算与传输环节由多国主体协同完成,导致《中华人民共和国数据安全法》(以下简《数据安全法》,本文提及的其他中华人民共和国法律均用简称)第三十六条②与 GDPR 第四十八条③出现管辖权竞合,审计证据链的完整性与法律效力遭受严峻挑战。

2. 数字时代的双向规制张力

数字技术的指数级发展催生了技术赋能与风险溢出并存的治理悖论,形成双重规制张力。一方面,数据主权重构引发审计管辖权冲突。数字主权已突破传统领土边界,向算法层、协议层与价值层延伸。美国 CLOUD 法案依托技术霸权实施“长臂管辖”;欧盟通过 GDPR 第四十五条④中的“充分性认定”输出规则标准,形成事实上的审计治外法权。这种主权博弈在跨境审计中具象化为“数据本地化存储”与

①SEC 是美国证券交易委员会的英文缩写,全称为 Securities and Exchange Commission。它是根据美国 1934 年《证券交易法》成立的、负责监管美国证券市场的独立联邦政府机构。其核心使命是保护投资者,维护公平、有序和高效的市场,并促进资本形成。

②《数据安全法》第三十六条:中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定,或者按照平等互惠原则,处理外国司法或者执法机构关于提供数据的请求。非经中华人民共和国主管机关批准,境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

③《通用数据保护条例》(GDPR)第 48 条:第三国法院或法庭的任何判决以及行政机关的任何决定,若要求数据控制者或处理者传输或披露个人数据,只有在基于请求的第三国与欧盟或成员国之间生效的国际协议(如司法协助条约)的情况下,才可以任何方式得到承认或执行,但不妨碍本章规定的其他传输理由。

④《通用数据保护条例》(GDPR)第 45 条:当欧盟委员会作出认定,认为相关的第三国、第三国中的某区域或一个或多个特定部门、或国际组织具有充足保护,可以将个人数据转移到第三国或国际组织。此类转移不需要特定的授权。

“监管穿透需求”的对冲。例如，PCAOB① 要求即时访问中概股审计底稿，而《网络安全法》第三十九条②要求重要数据境内存储，二者冲突使审计管辖权的协调陷入困境。另一方面，算法黑箱穿透挑战审计证据链。深度学习算法的不可解释性导致传统审计证据规则失效。在电商平台个性化推荐场景中，算法决策依赖数万亿级参数的非线性交互，审计人员无法通过逆向工程还原决策逻辑。穿透式审计虽能通过 API 接口抓取实时数据流[9]，但面临两大困境：一是算法偏见检测需依赖监督学习标注，而标注规则本身可能嵌入文化偏见（如 Sch rems II 判决③）；二是隐私计算技术的“数据可用不可见”特性与审计证据可验证性存在内生冲突。司法实践要求通过严格的哈希值校验机制确保数据完整性，其校验结果需达到高度一致性方可获得司法采信。

传统审计范式面临场景适配困境，同时在数字时代承受着双向规制的张力。其深层根源在于现行治理模式未能系统构建一个递进式的协同链条。该链条应贯穿权力授予（法律赋权）、权力运行控制（技术控权）与权力效果验证（审计监督）三大环节。当前，这一链条的断裂导致审计行为在“合法性奠基—合规化执行—效能反馈”各环节出现脱节。

（二）理论突破的递进路径

为系统回应上述由数字技术重构所带来的审计范式困境，本文尝试超越局部应对的策略，致力于构建一个层次分明、环环相扣的理论突破路径。该路径旨在实现从价值调适到技术实现的贯通。

1. 基石：法律与技术的价值协同

面对数据主权分层与算法权力异化带来的核心张力，首要的理论突破在于化解国家审计监督权与个人信息自决权之间的价值冲突[10]。具体而言：前者以财政法治为价值导向，强调审计权的独立性与公开性；后者以人格尊严为伦理根基，主张个人对信息处理活动的控制权。在实践中，这种张力在数据审计实践中表现为双重矛盾。其一，审计证据链的透明度要求与数据主权分层之间的冲突；其二，审计公开的公共利益属性与隐私泄露风险的平衡困境。因此，要实现法律赋权与技术控权的深层协同，关键在于构建一个以法理原则为引领、伦理准则为约束的价值调适框架，而非具体技术方案的堆砌。

首先，在规范层面，应确立“合法性优先”原则，即以比例原则为基准，推动《个人信息保护法》与《审计法》等规范的衔接，明确审计调取数据的法定边界与程序正义要件，确保任何技术手段的应用都根植于明确的法律授权，避免技术超越法律边界。例如，对于敏感信息需设定更严格的合规义务，而在公共利益场景下则需审慎适用豁免规则，这本质上是法律价值权衡的体现[11]。

其次，在协同机制上，必须确立“伦理嵌入”原则。这意味着技术路径的选择与应用，必须内嵌公平、透明、可解释、可控等伦理要求，以确保技术赋能不会异化为技术专断，从而在价值层面实现“科技向善”的治理目标。此价值协同框架为后续技术工具的选择与运用划定了根本遵循。

2. 进阶：审计学理论的动态化赋能

在奠定法律与技术的协同基石后，理论突破需进一步嵌入审计学的内生演进脉络，使其获得动态执行力。场景化弹性规制的核心在于构建一个由“风险敏感性－技术可靠性－法律约束力”构成的三维动态均衡框架。该框架旨在通过三者的协同互动，实现国家审计在复杂场景下的精准、高效与合规。

该框架包含三个维度。（1）风险敏感性维度要求审计参数配置与场景特征动态适配。具体而言：在金融征信场景中，需重点验证信用评估算法的公平性（如模型偏差系数阈值设定）；在跨境传输场景中，则需

①PCAOB（Public Company Accounting Oversight Board），即美国公众公司会计监督委员会，是根据《2002 年萨班斯－奥克斯利法案》设立的、受美国证券交易委员会监督的审计行业自律监管机构。

②《网络安全法》第三十九条：关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

③Sch rems II 判决，指 2020 年欧盟法院（CJEU）作出的判决，该判决以美国法律无法提供与欧盟实质同等的保护水平为由，宣布用于规制欧美数据跨境传输的《隐私盾协议》无效，并强化了使用其他传输工具（如标准合同条款 SCCs）时数据出口方的尽职调查义务。

关注数据出境的动态合规认证(如欧盟的充分性认定与中国的等效性评估)。此维度确保了审计强度与场景风险等级的精准匹配。(2)技术可靠性维度强调技术工具与法律规制的功能耦合。例如,隐私计算技术通过算法黑箱的可验证性设计(如基于 Paillier 加密①的梯度隔离传输协议),在保障数据主权的前提下实现跨域审计协同;区块链存证技术则通过时间戳固化与节点共识机制,为审计证据的司法认定提供技术背书。(3)法律约束力维度聚焦规范效力的场景化落地。为此,可通过《审计法实施条例》的修订,确立"应急场景触发—临时数据脱敏—事后合规审查"三阶段程序,并在跨境审计中构建"白名单管理与认证结果互认"的协调机制。

在技术实现上,该框架可依托联邦学习架构落地。其"数据不动模型动"机制将审计分解为本地计算与全局聚合,从而将主权分层理论技术化:物理层主权通过数据地理边界控制实现,算法层主权则借助梯度更新策略达成弹性授权。实践中,可依据企业信用评级动态配置节点权限,例如高信用企业参与全局训练,低信用企业接受穿透审计,可有效平衡合规成本与规则适配性。

该框架在操作上可具体映射至"法律赋权—技术控权—审计监督"的协同闭环:法律约束力为"法律赋权"提供刚性边界,技术可靠性是"技术控权"实现合规化执行的基础,风险敏感性则依托"审计监督"的持续验证与反馈来动态调适。三者共同构成了从规则设定到执行再到优化的完整治理回路。

四、实践方法创新的理论溯源和逻辑基础

本文通过法学、审计学与数字治理理论的跨学科协同构建理论支撑。法学以数据主权分层理论为核心,审计学提供风险分级响应和证据链穿透路径,数字治理依托情境完整性原则构建信息流动动态适配范式。三者协同形成"法律赋权—技术控权—审计监督"的机制,支撑场景化弹性规制的构建。

(一) 场景化弹性规制框架的理论渊源

1. 法学理论的演进在数据主权分层、个人信息权益保护与场景化治理范式等领域展开,为规制框架提供核心法理支撑。王利明的研究阐释了隐私权与个人信息权益的二元保护逻辑:隐私权以人格尊严为价值内核,通过《民法典》第一千零三十二条②确立的生活安宁权实现消极防御功能;而个人信息权益需平衡利用与保护的双重目标,则依托《个人信息保护法》第四条③知情同意规则构建积极控制机制[12]。这种界分为公私法益的协同保护奠定了规范基础,为调适审计监督权与个人信息自决权的张力提供了法解释学路径。程啸的权能结构化理论,进一步拓展了场景化治理的规范内涵[13]。其主张个人信息权益应解构为基础性权能与工具性权能,前者包含知情权、决定权等核心权项,构成信息主体对数据处理活动的根本控制,后者涵盖查阅、复制、删除等程序性权利,为动态场景中的权益救济提供技术性保障。针对敏感信息处理,程啸强调,生物识别、医疗数据等高风险信息需遵循"单独同意 + 事前评估"的双重合规义务[14],这为审计程序中的风险分级机制提供了法教义学依据。数据主权理论的发展为场景化规制奠定了空间治理逻辑。冉从敬、刘妍解构了数据主权的三维架构,其中,物理层主权体现为《数据安全法》第三十六条确立的数据存储地理边界控制,协议层主权依托技术标准制定权实现算法规则的域内管辖,应用层主权则通过数据价值链治理维护国家数字竞争优势,后又进一步阐述了数据主权的分类、基本特性及其谱系构造,为实施梯度化豁免策略提供支撑[15]。

---

①Paillier 加密是一种基于复合剩余类困难问题的概率公钥加密系统,其核心特性包括加法同态与数乘同态运算能力。该系统通过引入随机数参数实现概率性加密,相同明文经加密后生成不同密文,有效防止信息分布泄露。

②《民法典》第一千零三十二条:自然人享有隐私权。任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权。隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。

③《个人信息保护法》第四条:个人信息是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息,不包括匿名化处理后的信息。

2. 审计学理论的突破聚焦动态流程模型与系统韧性机制的创新，为规制框架提供了技术实现路径。DeFond 与 Zhang 开创性地构建“审计投入→过程→结果”的全流程动态模型，揭示了审计服务生命周期管理的时序动态性[16]，为场景化框架的弹性调适机制提供了方法论基础。该理论强调审计策略需随业务环境变化实时迭代，与 Knechel 等提出的情境嵌入理论形成学理共振，后者主张将内部审计师能力与外部市场结构、监管环境等要素耦合，构建环境、治理、业务交互反馈机制[17]。这直接启发了风险敏感性梯度豁免机制的设计，使审计重心能够依据行业特征与技术变革实现自适应迁移。钱钢等提出的智能审计理论，通过自然语言处理与机器学习技术重构多模态数据治理路径，其核心价值在于将联邦学习算法嵌入反洗钱监控等动态模型中，实现风险预警的实时化与证据链穿透的自动化[4]。秦荣生依托物联网与区块链构建审计轨迹分布式存证系统，为理论框架的规则代码化验证提供了技术锚点[18]。值得关注的是，陈汉文等构建的模块化治理体系突破了传统审计范式桎梏，通过业务层数据模型、治理层迭代机制、环境层变量整合的弹性架构[19]，实现了审计系统在动态环境中的韧性存续。该理论通过敏捷开发机制响应了张庆龙等的风险场景理论的核心诉求[20]，即从碎片化审计对象向系统性风险识别的范式跃迁。以上中外理论对话为构建场景化弹性规制框架提供了审计学理支撑。

3. 数字治理理论的演进在情境完整性原则与信息流动动态适配等维度深化，为场景化弹性规制框架奠定了治理范式基础。Nissenbaum 提出的情境完整性（Contextual Integrity）理论为场景化治理提供了核心范式，其强调隐私保护的本质在于信息流动与社会情境规范的适配性，主张通过信息主体、信息类型、传播原则三要素的动态平衡实现风险控制[21]。这一理论突破传统公私二分法的局限，将治理焦点从静态数据保护转向动态信息流动规制，为弹性治理框架奠定了方法论基础。马长山提出的数字法治规范秩序理论拓展了场景化理论的内涵指出，数字社会的治理需构建技术规则、市场规范、法律制度协同的框架，强调不同场景中技术逻辑与法律价值的耦合机制[22]。这与情境完整性形成呼应，揭示了数字治理必须回应技术嵌入社会关系过程中产生的规范重构需求。

场景化治理的理论支撑还体现在规制工具的创新层面。曾雄等提出的基于风险的协同治理框架强调，应当通过场景特征识别建立风险分级响应机制，实现治理成本与保护效能的均衡[23]。

综上，“经济体检”论奠定了审计监督作为国家治理体系中风险预警、问题诊断与治理优化反馈环节的功能定位，协同治理理论为多元主体的分工协作提供了组织范式，而法律的不完备性理论则揭示了通过技术手段实现规则精准执行（技术控权），以弥补法律抽象性（法律赋权）的内在需求。三大理论分别从功能、组织与规则层面，共同论证了构建“法律赋权-技术控权-审计监督”协同框架的理论根基与现实需求。

（二）运用场景化弹性规制理论分析“法律－审计－技术”协同问题的基础逻辑

场景化弹性规制的本质，是依托“法律－技术－审计”三元协同机制实现的动态治理能力。场景化治理通过识别不同行业或制度背景的差异，界定治理问题的具体前提；弹性规制则以此为基础，进行动态调整与灵活应对，形成针对差异的响应机制。二者通过“识别差异—动态响应”的链条初步衔接，并通过审计监督等反馈路径实现修正闭环（见图 1）。

1. 核心要素的规范内涵

场景化弹性规制理论的核心在于构建“法律-技术-审计”三元协同治理范式，并围绕三个层面运作：（1）协同识别机制，基于场景异质性，法律提供差异化授权，技术实现风险动态感知，审计则据此制定监督策略。（2）风险分级逻辑，具体表现为法律设定标准，技术精准识别，审计进而实施从穿透式审查到简易程序的梯度化监督，以平衡安全与效能。（3）技术赋能路径，通过主权分层将法律规则代码化，使技术系统自动适配审计要求，同时，利用区块链与智能合约构建可验证的动态证据链，最终形成闭环运行体系。

2. 应用场域的范式创新

在应用场域层面，本理论的创新性主要体现在推动治理范式从静态合规转向动态均衡。例如，在个

人信息保护领域，它构建了动态治理路径。法律上依托《个人信息保护法》等确立基于场景的差异化授权；技术上借助风险感知工具，动态适配医疗高敏感与公共事务低风险等不同场景的保护强度；审计上则通过梯度化监督，验证规则执行与技术效能，最终平衡数据保护与流通效用。又如，在人工智能法律治理领域，该理论形成了风险规制闭环。在闭环中，法律负责设定算法透明度、反歧视等底线与沙盒监管等弹性空间，技术通过可解释性算法等工具度量与管控“算法黑箱”风险，审计则对法律遵守情况与技术措施有效性进行穿透式审查。

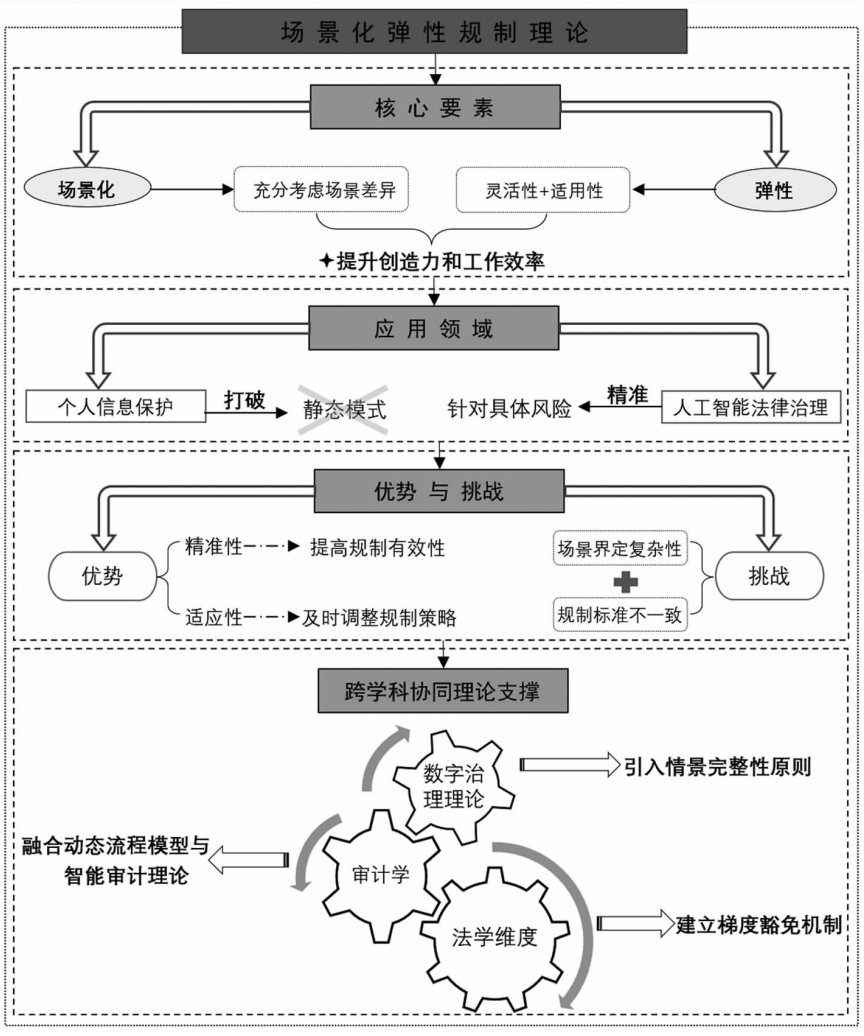

图1　场景化弹性规制理论框架图

3. 制度效能与实施挑战

在制度效能层面，本理论的优势在于其动态调适性。精准性体现为能基于场景风险谱系，弹性配置法律规则强度、技术验证深度与审计监督频度。适应性则表现为对技术迭代的敏捷响应，例如，当联邦学习、区块链重构业务逻辑时，其主权分层架构可通过更新协议层参数，实现规制策略的同步优化。然而，框架实施也面临固有挑战。首要挑战在于，场景融合导致界定困难。以跨境云审计为例，多国协同的数据处理使《数据安全法》与 GDPR 等法规出现管辖权竞合，传统基于地理边界的风险参数难以适用。另一项挑战是，规制梯度差异引发协同困境。不同场景下对数据主权与算法透明度的优先考量不同（如跨境流动与国内审计），这种治理强度的差异化配置可能削弱法律一致性，影响市场预期的稳定性。

4. 理论框架的多维协同逻辑

场景化治理作为识别差异与界定问题的起点，驱动弹性规制进行动态响应，弹性规制的实施效果又通过审计监督等反馈机制修正场景化认知，形成“识别差异—动态响应—反馈修正”的闭环。这一闭环逻辑使框架具备自我运行与迭代的内在动力，增强了整体适应性和方法论意义。

五、理论内核的层次解构与法理证成

场景化弹性规制的理论内核遵循“输入层（场景化识别差异）→输出层（弹性动态响应）”的逻辑（见图2）。

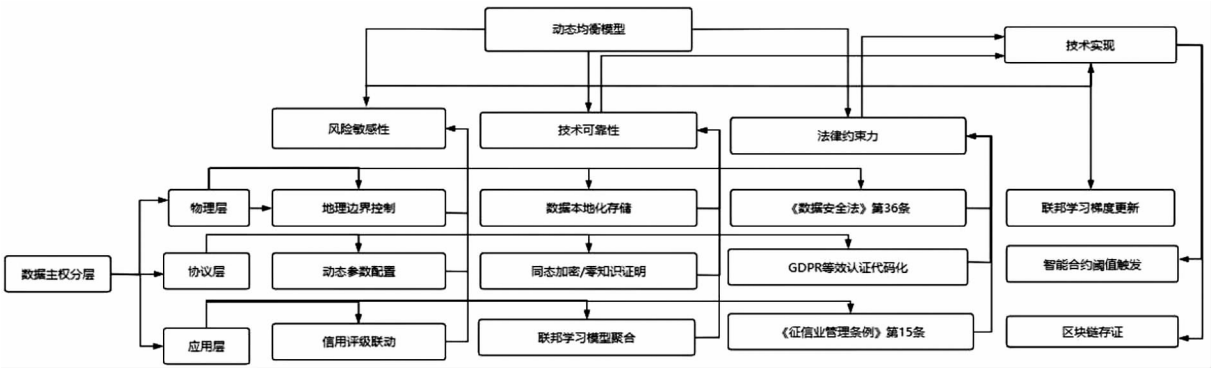

图 2　主权分层→动态均衡→技术实现逻辑映射图

动态均衡模型在操作层面实现了“法律赋权—技术控权—审计监督”的递进协同闭环:“法律约束力”为法律赋权提供合法性根基,“技术可靠性”保障技术控权的合规与自动化执行,“风险敏感性”依托审计监督实现动态监测与反馈。三者相互作用,形成从规则设定、执行到评估优化的完整治理回路。

(一)弹性规制的双重维度调适机制

1. 空间维度:主权分层理论下的梯度豁免

场景化弹性规制理论建构于风险敏感性、技术可靠性与法律约束力的动态均衡框架。其规范逻辑遵循数字时代治理范式转型的内在要求,并通过主权分层理论实现法律规则与技术架构的耦合。首先,风险敏感性的法理调适机制。基于情境完整性原则与比例原则,构建动态适配的场景化治理范式。数据主权分层理论包含三重规范内涵:其一,物理层主权彰显刚性,依据《数据安全法》第三十六条确立数据本地化存储义务,形成地理边界的绝对管辖权屏障[24];其二,协议层主权相对弹性,通过算法规则的技术赋权实现跨境审计合规传输,平衡技术标准与法律规制;其三,应用层主权达成衡平,依托公共利益豁免与紧急响应机制,在国家安全与数据效用间实施梯度化裁量。其次,风险敏感性与算法规则的动态适配。风险敏感性维度要求依据场景特征动态配置审计强度,其技术实现依托主权分层架构中的协议层算法规则。具体实现路径可分为三步:第一步,规则代码化,将风险敏感性参数编译为智能合约可识别的逻辑条件,嵌入联邦学习梯度更新协议;第二步,动态响应,当实时监测数据突破预设风险阈值,协议层自动触发主权弹性授权;第三步,“法律—技术”耦合,即通过《数据安全法》第三十六条与 Paillier 加密算法的协同,实现物理层数据本地化存储与协议层跨境验证的合规衔接。再次,在技术可靠性层面,其规范转化路径主要依赖于协同机制。规则代码化,即将法律原则转化为智能合约参数,并利用区块链存证保障审计证据穿透性验证;验证分布式架构,基于联邦学习框架构建“数据不动模型动”协作范式,从而确保物理层主权下的跨域审计协同;效力分层认定,即通过业务链与监管链分离,实现技术真实性与司法真实性的双重确认,进而确保证据链的司法可归责性。最后,在法律约束力层面,其动态实现模式主要体现在三个方面。一是豁免程序阶梯设计,通过构建紧急触发、临时脱敏、事后审查三阶段应急响应规则,落实合规缓冲机制;二是跨境治理双轨协调,即通过“白名单管理 + 等效认证”制度,协调 GDPR 与《数据安全法》的规范衔接;三是责任分配重构,依据数据处理者风险等级实施穿透式审计与梯度豁免,以此破解“合规性挤出创新性”困境。

2. 时间维度:风险响应的动态均衡

风险响应动态均衡机制的法理证成体系基于主权分层理论与动态法治原则的深度融合。首先,动态均衡的法理基础。风险响应机制以比例原则与动态平衡原则为价值内核,通过时序分层设计实现治理韧性转化[25]。参照模化治理体系构建业务层、治理层与环境层三级弹性架构,有助于突破传统静态监管范式,形成常规监管、风险预警、危机处置的全周期治理闭环[26]。此外,区块链存证技术可固化审计轨迹的时空节点,使《数据安全法》确立的动态监管义务与风险识别得以同步响应。其次,分层治理的规范逻辑。应急状态阈值触发规则遵循风险敏感性梯度原则,其法理正当性源于数据主权分层理论的拓展。具体实

践中,可参考四级风险预警体系,在数据生命周期维度构建风险识别、分级响应、动态调适框架[27]。通过主权动态授权调节模型实现法律约束力与技术可靠性的动态适配。例如,金融征信场景中,算法偏差系数阈值与《征信业管理条例》第十五条①合规要求深度耦合,形成司法审查与智能合约协同治理路径,进而确保风险分级与监管强度精准匹配。最后,过渡机制的衡平原则。合规缓冲设计体现法律"父爱主义"与市场理性的动态平衡。具体而言,场景完整性理论为过渡性豁免规则提供规范指引,其核心在于构建必要性、适当性、均衡性三阶审查标准。例如,《数据出境安全评估办法》第二十条②设置的6个月技术整改期,正是比例原则在数字治理中的具体实践[28]。该机制通过梯度化合规义务设置,既保障《网络安全法》第三十七条的数据主权要求,又落实《优化营商环境条例》第二十八条③对市场主体的保护目标,从而实现安全与发展的动态均衡。

(二)场景完整性的规范建构路径

1. 行业特征的类型化识别标准

不同行业场景的治理需遵循风险敏感性、技术可靠性与法律约束力的动态均衡逻辑。首先,在教育、社交、医疗等涉及社会民生与个人权益的场景中,治理框架分别聚焦于基于数字年龄分层的梯度授权、抑制信息茧房的风险分级响应以及对生物识别数据的特殊保护,这体现了场景化弹性规制在差异化治理中的基础应用。其次,金融征信治理模型凸显技术赋能下的动态风控。技术可靠性层面,依托区块链固化审计轨迹,基于零知识证明实现穿透验证;通过智能合约预设偏差阈值,指标异常时自动触发联邦学习参数重校准,形成整改闭环。法律约束力维度嵌入《征信业管理条例》反歧视条款,建立偏差系数动态监测与自动修正系统。风险敏感性维度采用主权动态授权模型,依据信用评级实施穿透式审计与梯度豁免的差异化监管。最后,相较于前述特定行业场景,跨境数据流动审计因其涉及主权博弈、规则冲突与技术穿透的复杂性,成为检验本场景化弹性规制框架效能的关键核心场域。在此场景下,基于情境完整性原则构建GDPR等效认证动态清单,在技术可靠性层面部署零知识证明协议与多方安全计算节点,实现隐私保护与数据效用的制度性均衡。在法律约束力维度,则通过主权分层架构协调物理层数据本地化要求与协议层跨境验证规则,建立"白名单管理+等效互认"的双轨制协调框架[29]。

2. 权益冲突的衡平性调适

权益冲突的衡平性调适维度,应构建价值位阶分层、动态平衡机制、技术赋能路径调适框架。首先,构建价值位阶分层机制。该机制基于情境完整性理论确立权益保护优先级序列。第一,核心权益的刚性保障,即隐私权优先于一般个人信息权益[29],敏感信息处理需遵循《个人信息保护法》第二十八条特殊合规义务,并可通过主权分层理论解构数据价值链,在物理层实施绝对保护。第二,衍生权益的弹性适配,即数据主权与人格权冲突通过主权动态授权调节模型实现动态平衡,具体可依据《数据安全法》第三十六条建立梯度豁免规则,在协议层部署Paillier加密实现跨境审计合规。第三,公共利益的合理让渡,这要求融合《网络安全法》的安全保障理念与《个人信息保护法》第六条的"最小必要"原则,并引入比例原则进行校准,共同构建"安全底线+最小必要"的双重约束框架。其次,完善动态平衡实现机制。一方面,可通过风险分级响应模型,融合情境完整性理论与动态法治原则,构建风险预警体系,将算法偏差系数阈值与《征信业管理条例》第十五条深度耦合,形成司法审查与智能合约协同治理路径。另一方面,可设置过渡性豁免规则,依据《数据出境安全评估办法》第九条设置技术整改期,通过主权分层

①《征信业管理条例》第十五条:信息提供者向征信机构提供个人不良信息,应当事先告知信息主体本人。但是,依照法律、行政法规规定公开的不良信息除外。

②《数据出境安全评估办法》第二十条:本办法自2022年9月1日起施行。本办法施行前已经开展的数据出境活动,不符合本办法规定的,应当自本办法施行之日起6个月内完成整改。

③《优化营商环境条例》第二十八条:供水、供电、供气、供热等公用企事业单位应当向社会公开服务标准、资费标准等信息,为市场主体提供安全、便捷、稳定和价格合理的服务,不得强迫市场主体接受不合理的服务条件,不得以任何名义收取不合理费用。各地区应当优化报装流程,在国家规定的报装办理时限内确定并公开具体办理时间。

架构协调数据本地化要求与跨境验证需求,实现安全与效能的制度性均衡。最后,强化技术赋能调适路径。在技术层面,可借助穿透式验证技术,采用零知识证明协议实现“数据可用不可见”的审计穿透,同时通过区块链存证固化证据链[30],从而既满足《审计法》第三十八条监督要求,又保障《民法典》第一千零三十二条隐私权。智能合约转化机制,将法律规则转化为 Solidity 编辑语言,在跨境场景中构建“权限授予—数据脱敏—轨迹存证”自动化控制模块,最终实现 ISAE3000 标准与主权管辖规则的动态适配。该理论内核以“主权分层”界定治理场域,依托“动态均衡模型”实现法律、技术、审计的协同运作。审计监督不仅是治理效果的验证环节,更是驱动法律规则与技术策略动态优化、实现弹性规制的反馈核心,从而确保了整个框架的自我演进与持续优化能力。

六、跨境数据流动审计中的框架效能验证

跨境数据流动作为数字治理中的典型复杂场景,为检验场景化弹性规制框架的实践效能提供了关键场域。本部分旨在验证该框架在应对跨境数据审计时的应用路径与效果。

(一)跨境数据流动审计的典型性与验证逻辑

1. 案例的典型性特征

跨境数据流动审计并非一个普通的审计场景,而是集中体现了数字时代国家审计所面临的合法性、技术性与均衡性三重维度的挑战。在合法性层面,其深刻触及不同法域间的管辖权竞合与法律冲突。在技术性层面,审计对象扩展到联邦学习、同态加密等隐私计算技术所构成的“算法黑箱”。在均衡性层面,则需调节数据安全主权与数据要素价值高效释放之间的动态平衡。这种高度复杂性,使该场景成为检验场景化弹性规制框架解释力、适应性与效能性的理想场域。

2. 验证的逻辑进路与目标

基于上述典型性,本部分的验证遵循场景压力测试的逻辑进路,即通过考察理论框架在最富挑战性的情境下的应用,反证其潜在的普适性效能。具体的验证目标聚焦于框架的核心理论构件:其一,考察主权分层理论在化解跨境审计中管辖权冲突的指导作用,为审计实践提供清晰的合法性边界;其二,分析规则代码化路径在实现对复杂算法与数据流进行穿透式核查方面的技术可行性;其三,评估动态均衡模型如何依据风险敏感性,在差异化场景中实现审计策略的梯度化适配与动态调节效果。

(二)审计方案设计的理论映射与操作化

跨境数据流动审计方案设计需以主权分层理论界定审计范围,以规则代码化路径创新审计程序,以动态均衡模型调整审计策略,具体呈现“法律赋权—技术控权—审计监督”的递进协同运行逻辑。

1. 基于主权分层的审计范围界定

基于主权分层理论,审计范围界定为三个维度。在物理层,审计范围严格限定于中国内地(即除港澳台以外的中国主权管辖地域,以下简称境内)。核心操作原则是确保审计行为本身不触发受管辖数据的非授权出境。这意味着审计数据的采集、预处理、分析及存储等全流程必须在境内的数据中心或经认证的安全环境中完成。具体审计活动包括:核查被审计对象的数据资产地图,确认其重要数据与核心数据是否依法实现本地化存储;验证其数据访问控制机制能否有效防止境外对境内原始数据的直接调取;评估其数据中心物理安全及网络安全防护水平是否符合国家等级保护要求。此层面的审计是维护数据主权的根基,其范围界定直接依据强制性本地化存储条款。在协议层,审计焦点从数据实体转向规制数据流动的逻辑规则与算法模型。此层面的审计范围涵盖两大核心要素:一是数据跨境传输的法律合规性协议,例如企业自评估报告、个人信息出境标准合同(SCC)的条款完备性与签署有效性、跨境传输安全评估的审批文件等。审计需穿透文本形式,实质性审查这些协议是否真实反映了业务场景,其条款设置是否足以保障数据出境后的安全与权益。二是驱动数据处理与价值挖掘的算法模型,特别是涉及用户画像、个性化推荐、信用评估等关键业务的模型。审计需评估其训练数据的代表性、决策逻辑的

公平性与透明度，以及是否存在潜在的歧视或偏见，确保算法活动符合我国法律法规和社会主义核心价值观的要求[31]。在应用层，审计视野扩展至数据出境后的全生命周期价值实现与风险衍生过程。审计范围在此聚焦于数据在境外被访问、使用、共享乃至销毁的实际场景与效果。具体而言，需评估数据出境后是否严格用于申报的既定目的，其产生的经济效益（如跨境贸易便利化）与社会效益（如科研合作）是否达到预期；同时，需动态监测和评估数据使用过程中可能引发的次级风险，如国家安全风险、关键技术泄露风险、个人隐私大规模侵权风险以及因境外司法长臂管辖导致的数据控制权丧失风险。

2. 遵循规则代码化的审计程序创新

审计程序创新遵循规则代码化路径。将法律规范（如《数据安全法》条款）编译为智能合约逻辑，实现自动化合规扫描；融合联邦学习等隐私计算技术，构建“数据不动模型动”的穿透式验证机制。程序创新的核心在于法律规则的形式化转译与嵌入式审计。首先，需对《个人信息保护法》《数据安全法》等关键条文进行解构，将其核心义务要求转化为结构化的数据参数与逻辑判断规则。例如，将“告知—同意”原则分解为对数据主体授权状态、授权时间、授权范围等字段的自动校验逻辑；将数据分类分级标准编码为对不同级别数据实施差异化访问控制、加密强度与脱敏策略的触发条件与执行标准。这些经过转译的规则可被封装为审计智能合约或嵌入审计系统的规则引擎，实现对数据流转策略、访问日志、权限设置等的大规模自动化合规扫描与异常检测[32]。在技术赋能层面，审计程序需深度融合隐私增强技术（PETs）①与分布式账本技术，以实现“数据不动”前提下的可信核查。针对数据内容本身的审计，可采用联邦学习（Federated Learning）②架构，将统一的审计分析模型下发至被审计单位的本地环境，数据在本地完成模型推理与特征提取，仅将加密后的模型参数更新或聚合统计结果返回给审计方。这种方式实现了“数据不动模型动”，在保护数据隐私的同时，完成了对数据处理行为的有效性验证。针对审计过程的可信性与可追溯性，区块链技术不可或缺。所有关键的审计操作指令、数据访问请求、合规校验结果、异常交易记录等，均生成哈希值并记录于经过许可的分布式账本上，形成一条时间序列完整、不可篡改的审计证据链。这不仅为后续的责任认定提供了铁证，也实现了对审计行为自身的透明化监督，防止审计权力滥用。

3. 嵌入动态均衡模型的审计策略制定

审计策略调整嵌入动态均衡模型，通过风险矩阵实现梯度化响应。高风险触发实时穿透审计，中低风险采用周期抽查。策略随审计反馈动态优化，形成“评估—响应—修正”闭环。策略制定的起点是建立一个多维度的风险分级矩阵。该矩阵应综合考虑以下关键因素：一是数据本身的敏感性，依据国家数据分类分级指南，区分一般数据、重要数据、核心数据及敏感个人信息；二是数据接收方所在国家或地区的法治环境、数据保护水平及其与我国的政治互信与合作关系；三是数据出境的具体业务场景及其关键程度；四是数据规模与出境频率；五是被审计对象的历史合规记录与内部治理成熟度。通过定量打分与定性研判相结合的方式，将审计对象划分为高、中、低等不同的风险等级。基于风险分级结果，审计策略呈现显著的梯度化特征。对于高风险等级的数据流动（如核心数据出境至高风险地区），审计策略应体现“全面从严”的原则，采取持续性实时监控、定期的全面穿透式检查、要求引入第三方权威机构进行独立验证等措施。对于中风险等级，可采取“周期性审计 + 关键控制点抽查”的组合策略，侧重于对合规协议执行情况、访问控制有效性、安全事件响应能力等进行验证。对于低风险等级（如匿名化数据出境至可信区域），则可以简化审计程序，更多地依赖被审计单位的内部控制自评估报告与承诺声明，审计

①隐私增强技术（PETs）是一类通过密码学或数据扰动等手段，在保证数据可用性的前提下，防止敏感信息泄露的技术集合，其核心目标是实现“数据可用不可见”，在数据流转与协同分析过程中保护个人隐私与商业机密。典型技术包括差分隐私、同态加密、安全多方计算、零知识证明等，广泛应用于跨境数据审计、联邦学习等场景。

②联邦学习（Federated Learning）是一种分布式机器学习范式。其核心机制为“数据不动模型”，即多个参与方在本地数据不移动、不共享的前提下，通过协作训练一个全局共享的机器学习模型。这种方式旨在从技术上解决“数据孤岛”问题，并成为实现“数据可用不可见”、满足数据隐私保护合规要求的重要技术路径。

机关进行不定期的抽样验证与事后稽查。这种梯度化策略确保了宝贵的审计资源被优先配置于风险最高、影响最大的领域,实现了监管效能的最大化。尤为关键的是,该模型可内置动态反馈与调整机制。审计实施过程中获取的新证据(如安全漏洞发现、违规事件)、外部环境的变化(如新的国际条约签署、地缘政治风险升级、技术突破)都会触发对审计对象风险等级的重新评估。审计系统应能依据预设规则或经人工审核后,自动或半自动地调整后续的审计频率、深度与资源投入,从而实现从静态、被动的合规检查向动态、主动的风险适配型审计的根本性转变[33]。

(三)框架应用的过程考察与效能检验

在具体应用过程中,该框架的三元协同机制呈现清晰的运行逻辑。以跨境数据流动审计为例:首先,在法律赋权层面,《数据安全法》《个人信息保护法》等法律法规为审计活动奠定了合法性基础,不仅明确了数据出境的安全评估要求,也划定了审计机关的监督权限。其次,在技术控权层面,核心在于通过规则代码化路径,将法律条文中的具体规范(如数据分类分级标准、出境安全评估条件)转化为可执行的智能合约与校验规则。在此基础上,融合零知识证明、区块链存证等技术,可实现"数据可用不可见"式的穿透验证,从而确保审计过程在满足合规要求的同时,不触及原始数据内容。最后,在审计监督层面,则需依据法律授权与技术验证结果,对数据出境的合规状况、风险等级及控制效果进行专业判断,最终形成有效的监督闭环。通过上述三个层面的递进协同,该框架使审计活动在复杂的跨境场景中,既能坚守安全底线,又能动态适应具体情境的需求。

本案例验证了理论框架的协同运行。主权分层赋予审计范围合法性,规则代码化确保程序执行精准性,动态均衡驱动策略适配性。三者闭环联动,使框架在复杂场景中具备自我迭代能力。

七、结论

数字时代要求审计范式系统性重构。本文构建的"法律赋权—技术控权—审计监督"三元递进协同场景化弹性规制框架,核心贡献在于实现了理论、技术与治理的三重创新整合。理论层面,框架通过解构数据主权,创立了"主权分层→动态均衡→技术实现"的逻辑映射模型,为破解跨境数据审计中的管辖权竞合与算法黑箱难题提供了系统性的分析工具。技术路径上,将联邦学习、区块链智能合约与审计流程深度融合,形成了"规则代码化—证据穿透性—验证分布式"的可操作方案,实现了从法律条文到技术逻辑的闭环转译。治理价值上,框架推动 ISAE 3000 标准本土化与跨境数据流动审计创新,为构建中国自主的国家审计知识体系、贡献全球数据治理的"中国方案"提供了路径参考。未来研究可深化主权动态授权模型在多元场景下的适配性,以拓展理论边界。

参考文献:

[1]贺勇,李佳蔚,刘筱祎. 数字平台算法审计:现实理据、客观挑战与关键进路[J]. 南京审计大学学报,2025(2):10-20.

[2]黎桦,吴庆洁. 企业数据合规的法律构建[J]. 武汉理工大学学报(社会科学版),2025(1):62-71.

[3]秦荣生. 大数据、云计算技术对审计的影响研究[J]. 审计研究,2014(6):23-28.

[4]钱钢,叶祥,龙利民. 智能审计场景、核心技术与实现路径研究[J]. 会计之友,2024(20):14-21.

[5]彭华彰,戚振东,刘军,等. 审计发挥经济体检作用研究[J]. 审计研究,2020(5):3-9.

[6]刘家义. 国家治理现代化进程中的国家审计:制度保障与实践逻辑[J]. 中国社会科学,2015(9):64-83.

[7]周泽将,修宗峰. 国家审计与腐败治理体系协同研究[J]. 中国行政管理,2017(7):24-27.

[8]郑石桥. 算法审计客体论[J]. 财会月刊,2024(17):81-85.

[9]李谦. 美国场景化司法规制数据爬取的经验与启示[J]. 电子政务,2020(11):86-98.

[10]张淇. 论数字时代我国个人信息算法审计制度的构建 兼评《个人信息保护合规审计管理办法(征求意见稿)》[J]. 实事求是,2024(4):74-83.

[11]陈耿,潘香,周诗琪. 基于区块链技术的审计证据数字存证探究[J]. 财会月刊,2022(22):105-109.

[12]王利明. 和而不同:隐私权与个人信息的规则界分和适用[J]. 法学评论,2021(2):15-24.
[13]程啸. 论个人信息权益[J]. 华东政法大学学报,2023(1):6-21.
[14]程啸. 论个人信息权益与隐私权的关系[J]. 当代法学,2022(4):59-71.
[15]冉从敬,刘妍. 数据主权的理论谱系[J]. 武汉大学学报(哲学社会科学版),2022(1):19-29.
[16]DeFond M L, Zhang J. A review of archival auditing research[J]. Journal of Accounting and Economics, 2014, 58(2-3): 275-326.
[17]Knechel W R, Krishnan G V, Pevzner M, et al. Audit quality: Insights from the academic literature[J]. Auditing: A Journal of Practice & Theory, 2012, 32(Supplement 1): 385-421.
[18]秦荣生. 大数据、云计算技术对审计的影响研究[J]. 审计研究,2014(6):23-28.
[19]陈汉文,杨道广,韩洪灵. 构建中国自主实证审计理论体系[J]. 财会月刊,2024(17):20-25.
[20]张庆龙,何佳楠,顾青青,等. 场景审计:数字化时代商业银行内部审计工作模式[J]. 审计研究,2021(4):119-128.
[21]Nissenbaum H. Privacy as contextual integrity[J]. Washington Law Review, 2004,79(1): 119-157.
[22]马长山. 数字法学的理论表达[J]. 中国法学,2022(3):119-144.
[23]曾雄,梁正,张辉. 中国人工智能风险治理体系构建与基于风险规制模式的理论阐述——以生成式人工智能为例[J]. 国际经济评论,2025(4):131-152.
[24]姚天,王宇. 数据主权视阈下的数据跨境流动及中国因应[J]. 国际商务(对外经济贸易大学学报),2025(2):141-156.
[25]赵精武,周瑞珏. 论数字法学研究范式的转向:风险体系化治理[J]. 求是学刊,2024(4):136-147.
[26]黄海瑛,何梦婷,冉从敬. 数据主权安全风险的国际治理体系与我国路径研究[J]. 图书与情报,2021(4):15-28.
[27]汪庆华. 新技术新应用风险规制的结构性反思与法律理念的重塑[J]. 法律科学(西北政法大学学报),2025(3):45-55.
[28]王敏,曹放. GDPR 时代数据保护的欧美标准与中国策略[J]. 新闻大学,2022(7):53-66.
[29]王利明. 和而不同:隐私权与个人信息的规则界分和适用[J]. 法学评论,2021(2):15-24.
[30]范伟,李海波,张珠君. 区块链数字取证:技术及架构研究[J]. 通信学报,2024(12):124-141.
[31]张永忠,张宝山. 算法规制的路径创新:论我国算法审计制度的构建[J]. 电子政务,2022(10):48-61.
[32]廖丽环. 个人信息处理中同意规则弱化适用的路径优化——基于情境脉络完整性理论的场景细分[J]. 法制与社会发展,2022(6):156-180.
[33]张鹏. 持续审计的发展历程与研究展望[J]. 西安财经大学学报,2021(3):62-68.

[责任编辑:苗竹青]

Innovation in National Audit Practice under the Scenario-based Elastic Regulation Framework: A Law-Technology-Audit Collaborative Governance Perspective

ZHANG Ronggang[1], WU Yazhou[1,2]

(1. Graduate School, Northwest University of Political Science and Law, Xi'an 710063, China;
2. China Aviation Industry Group Radar Institute, Wuxi 214063, China)

Abstract: The interplay of data sovereignty and the alienation of algorithmic governance present new challenges for national audit. Based on the governance function of national audit, this study constructs a tripartite collaborative framework of "law-technology-audit": the law clarifies the sovereignty hierarchy and compliance bottom line, technology enables penetrating verification through federated learning and blockchain, and audit performs supervision functions relying on dynamic authorization and gradient exemption mechanisms. This study innovatively proposes a closed-loop governance logic of "scenario-based identification-elastic response" to adapt to diverse governance needs. In practice, it integrates federated learning with blockchain to form an intelligent audit model characterized by "codified rules, traceable evidence, and distributed verification." This model promotes the localization of the ISAE 3000 standard and innovates cross-border data flow audits, providing theoretical support and practical pathways for enhancing the adaptability of national audit in digital governance and advancing institutional openness.

Key Words: scenario-based elastic regulation; law-technology-audit collaboration; sovereign layer theory; federated learning audit; intelligent audit; national audit