基于数据元件的领域数据治理工程化路径研究

陆志鹏
（中国电子数据产业集团，广东　深圳　518057）

摘　要：在数字化转型浪潮下，企业应用大语言模型挖掘数据价值的需求日益增长。然而，领域数据中普遍存在的隐私问题严重制约了模型的直接应用。为解决此难题，提出一条基于数据元件的领域数据治理工程化路径。数据元件是一种通过抽象化、特征化转换实现数据去隐私化的中间数据资产。围绕数据元件，提出了一条将原始数据加工为面向大语言模型应用的高质量数据集与知识库的数据治理路径。通过在财务领域的实例验证，证明了该路径在安全释放数据价值、赋能企业智能化转型方面的有效性与实用价值。

关键词：领域数据治理；数据元件；大语言模型；工程化路径
中图分类号：G203；TP391　　**文献标志码：**A　　**DOI：**10. 19358/j. issn. 2097 - 1788. 2026. 01. 007

中文引用格式：陆志鹏. 基于数据元件的领域数据治理工程化路径研究［J］. 网络安全与数据治理，2026，45(1)：42 - 47.
英文引用格式：Lu Zhipeng. Research on the engineering path of domain data governance based on data components［J］. Cyber Security and Data Governance，2026，45(1)：42 - 47.

Research on the engineering path of domain data governance based on data components

Lu Zhipeng
(China Electronics Data Corporation, Shenzhen 518057, China)

Abstract: The ongoing digital transformation is fueling enterprise demand to unlock data value with large language models. Yet, this ambition is significantly constrained by privacy issues inherent to domain-specific data, precluding their direct utilization. This research introduces a novel, engineered pathway for data governance built upon "Data Component" to resolve this impasse. Data components are defined as intermediate data assets that undergo abstraction and feature transformation for robust de-identification. Our proposed pathway systematically processes raw data, centered on these components, to construct high-quality datasets and knowledge bases for large language model applications. Through empirical validation in the financial sector, we demonstrate the pathway's efficacy and utility in securely releasing data value and accelerating enterprise intelligence transformation.

Key words: domain data governance; data element; large language model; engineering path

0　引言

在数字化浪潮的推动下，数据已成为驱动现代企业创新与增长的核心生产要素。随着数据积累的爆炸式增长，企业对数据价值的深度挖掘需求日益迫切，从传统的数据分析和可视化，正迈向更高级的预测、推理与自动化决策阶段。在此背景下，以大语言模型（Large Language Models，LLM）为代表的生成式人工智能技术展现出前所未有的潜力，其强大的自然语言理解与生成能力，有望革新企业内部信息交互模式，将数据洞察转化为更直观、更智能的业务赋能[1-2]。

然而，当企业尝试将 LLM 应用于领域场景以期释放数据深层价值时，数据隐私问题成为了模型应用的核心挑战之一[3]。企业内部最具价值的领域数据，往往蕴含着高度敏感的个人身份信息或商业机密。未经充分脱敏的原始数据，不仅难以直接用于大模型训练或推理，更可能引发严重的法律风险与声誉危机，使得数据资产在合规压力下处于“可用而不可见”的状态。

鉴于上述挑战，本研究的根本动机在于探寻一条在严格遵循数据隐私合规前提下，能够高效、规模化地释放企业领域数据深层价值的工程化路径。为弥合“数据可用不可见”所带来的鸿沟，本文创新性地提出基于数据元件的领域数据治理方案。数据元件是一种经过精心设计、从原始敏感数据中提取的、业务导

向且隐私安全的标准化信息单元。它作为一种新型的中间数据资产，旨在解决数据的“不可见”问题。作为隐私屏障，数据元件通过对原始数据进行抽象化、特征化转换，实现了数据的匿名化与去隐私化。这使得数据在不暴露个体隐私或商业机密的前提下，仍能保留核心的业务洞察，实现数据资产的“安全可见”。

本研究的重点在于构建一套以数据元件为核心的领域数据治理工程化体系，旨在通过标准化、自动化的方式，实现从原始数据到高质量、隐私安全的“数据元件”的转化、管理与应用，并特别关注其如何赋能大语言模型，构建新一代的企业智能应用。

1 领域数据治理现状与挑战

领域数据治理是指针对特定行业或业务领域的数据资产实施的一套定制化的管理策略、流程和技术框架[4]。其核心目标在于确保领域数据的可用性、完整性、安全性、合规性及价值释放，以支撑该领域的业务决策、运营优化和创新应用。当前，针对领域数据治理的研究与实践已在学术界取得显著进展。众多学者围绕石油化工[5]、航空航天[6]、医疗健康[7]等不同领域的数据特性，构建了适配的治理框架，提出了针对性的实施路径，为各行业数据治理的落地提供了重要参考，推动了数据资源在实际场景中的有效应用。例如，张照龙等人[8]针对电信企业数据安全合规治理，围绕“人员、流程、技术”核心，从多维度构建了数据可知、风险可视、体系防护、持续有效且不断优化的电信领域数据安全合规治理体系。张培等人[9]提出了以信息流动为导向、以多元耦合为内核、以数据驱动为理念、以系统集成为支撑的教育领域数据治理核心思路。

然而，近年来领域大语言模型的兴起对领域数据治理提出了新的挑战。领域大语言模型的构建依赖于高质量、大规模的领域专业数据，而通用场景的训练数据难以支撑其形成精准的领域认知体系和知识表征[10]。为应对这一现实需求，各领域已开始探索针对性的数据集构建路径。例如，医学领域数据集 MedReason[11]的构建依赖于知识图谱来生成结构化的推理路径。然而，在此过程中，领域大模型的训练依赖海量数据，其中往往包含大量敏感信息，这些信息在数据流转与模型应用环节面临着泄露、滥用或被篡改的风险，不仅可能侵犯个人权益与企业利益，还可能引发一系列法律与社会问题[12-13]。

在此背景下，数据元件作为一种创新的数据治理模式，展现出解决隐私困境的潜力。数据元件通过对原始数据资源进行系统化重组与专业化建模，能够有效过滤其中的敏感信息，形成兼具可用性与安全性的数据“中间态”[14]。这种“中间态”实现了数据资源与数据应用的解耦，在保障数据价值得以正常发挥的同时，从源头上隔离了数据被滥用和篡改的风险，为 LLM 在领域场景中的安全应用提供了重要保障，也为破解数据隐私保护与价值释放之间的矛盾开辟了新路径。

综上所述，通过定义标准化的数据处理流程、开发自动化工具链、建立严格的质量与安全管控机制，构建一套以数据元件为核心的领域数据治理工程化体系，能够为 LLM 在特定领域的深度应用提供安全、合规、高质量的数据元件供给，从而驱动企业智能应用的构建与升级。

2 数据元件：数据要素化治理的关键支点

数据作为我国基础性与战略性资源，已上升为新型生产要素，其价值的充分、有序释放是数字经济高质量发展的关键。而数据要素化，正是将数据资源加工为数据初级产品，再通过市场化机制推动这些初级产品参与社会生产经营活动，进而释放数据要素价值的过程[15]。本节将以数据元件这一核心概念为切入点展开数据要素化治理的研究，解析其核心内涵与典型特征，辨析其与传统数据处理方法的本质区别，系统阐述数据元件的设计原则及分类体系，同时揭示数据元件在企业数据治理与应用体系中所承载的战略作用。

2.1 数据元件的定义与特性

数据元件是对数据资源进行清洗治理、加工生产形成的信息密度大、安全属性强、形态稳定、产权清晰、价值释放效率高的数据表征结果[16]。数据元件并非原始数据的简单复制或聚合，而是业务导向的特征抽取后承载特定分析目的高度提炼的信息单元。数据元件旨在成为企业内部数据流通与应用的基础，在保留核心业务洞察的同时，彻底切断与个体可识别信息或敏感商业秘密的直接关联。

数据元件的定义蕴含其三大核心特性，这些特性共同构成了其在现代数据治理体系中的独特价值。

（1）隐私安全性：数据元件在设计之初就将隐私保护内嵌于其生命周期。它通过有损的特征转换、聚合、匿名化等手段，使得从数据元件无法逆向推导出原始敏感数据，从而从根本上避免了敏感信息的泄露风险。

（2）业务价值导向：与传统的通用脱敏方法不同，数据元件的生成是基于明确的业务分析目标。它

聚焦于提取原始数据中对特定业务场景有用的“信号”，而非追求原始数据的完整复刻。例如，在信贷风控中，客户的“收入稳定性等级”可能比其精确收入数字更能有效支持决策，且更加隐私友好。这种导向性确保了数据元件在满足隐私需求的同时，能够切实支撑业务决策和应用。

（3）标准化与可复用性：数据元件通常以统一的格式、标准化的命名和清晰的语义被定义和存储。一旦一个数据元件被生产出来，它就可以作为一种共享的数据资产，被企业内多个不同的分析团队、应用系统或 AI 模型重复调用，避免了重复的数据处理工作，提高了数据资产的利用效率和一致性。

2.2 数据元件的设计原则

数据元件的有效性与价值，决定性地依赖于其设计质量。为确保所生成的数据元件既能有效支撑业务应用，又能严格遵守数据隐私规范，以下三项核心原则至关重要：

（1）业务目标对齐原则：此原则强调数据元件的设计必须紧密围绕特定的业务目标或分析场景。高质量的数据元件并非对原始数据的随机抽象，而是对核心业务问题的精准回应。这意味着在元件设计之初，需明确其预期解决的业务痛点、支持的决策类型或需揭示的业务洞察。例如，若业务目标是评估员工的职业发展潜力，则应设计如“高潜人才标签”“晋升速度分级”等元件，而非仅关注其基础学历。这种以终为始的设计方法，确保了数据元件具备实际的业务价值，避免了“为脱敏而脱敏”的无用功。

（2）信息熵平衡原则：数据元件的生成过程本质上是一种有损的信息转换，它旨在去除原始数据中不必要的细节与敏感信息，同时保留对业务分析至关重要的“信号”[17]。信息熵平衡原则要求设计者在隐私保护的严格要求与信息效用的最大化之间寻求最佳平衡点。过度的抽象可能导致信息损失过多，使元件丧失业务价值；而信息保留过多则可能引入隐私风险。因此，设计者需精准识别业务所需的最小信息集，并通过诸如区间化、概括化、统计特征提取等手段，确保在满足隐私合规的前提下，尽可能地保持数据元件的决策支撑能力。

（3）可解释性原则：尽管数据元件是对原始数据的抽象与聚合，但其含义和生成逻辑应尽可能保持清晰与透明。可解释性有助于业务分析师、决策者乃至合规审计人员理解数据元件所代表的业务意义及其背后的计算逻辑。这不仅能增强用户对分析结果的信任度，还能便于对元件进行验证、调试和迭代优化。对于通过复杂机器学习模型生成的指数型或模式型元件，应辅以如特征重要性分析、决策路径可视化等解释机制，确保其“黑箱”特性得以最大程度地被穿透与理解。

3 基于数据元件的领域数据治理

本节将详细阐述基于数据元件的数据治理工程化路径。该路径旨在系统地将异构的原始敏感数据转化为安全可见的高质量数据集和知识库，以支撑大模型的训练与应用。

基于数据元件的领域数据治理工程化路径是一个多阶段、系统化的过程，其核心在于将原始、异构的敏感数据转化为模型可用的数据集和知识库。如图 1 所示的技术路径流程图涵盖了四个核心阶段：数据归集与预处理、数据元件的自动化加工、面向 LLM 的适配、数据集与知识库构建。

3.1 数据归集与预处理

数据归集处理是数据治理的起点，其核心功能在于收集私有领域数据和数学、代码、法律等领域的公开数据。除了收集数据，此阶段还包括对数据的初步清洗，以剔除明显的冗余、错误或不一致信息。然后根据数据是否涉及隐私问题进行分级，根据企业业务场景进行初步分类。

数据格式转换的主要任务是将非结构化数据转换为结构化数据。结构化的格式能够提供丰富的语义标签，便于大模型基于语义分割文档内容，服务数据集和知识库的构建。统一的数据格式是实现自动化数据处理和提高数据可读性的基础。

3.2 数据元件的自动化加工

数据元件加工是本文提出的数据治理流程的核心。数据元件的生成可以根据数据特性和业务需求，采用以下多种自动化技术。

（1）基于规则引擎的生成：通过预先定义的业务规则集，将原始数据转换为标准化的元件。这些规则通常是显式的、逻辑清晰的，如区间划分、阈值判断、布尔值判断等。

（2）元数据驱动的生成：结合数据治理平台中的元数据信息，如数据类型、隐私等级、业务分类，自动匹配并应用预设的元件化策略。当新数据流入时，系统根据其元数据标签自动触发相应的元件加工流程。

（3）基于机器学习的生成：利用机器学习算法从原始数据中自动发现复杂的模式和关系，并将其转化为结构化的特征或标签作为数据元件。该过程包括聚类、降维、异常检测、预测模型输出等。

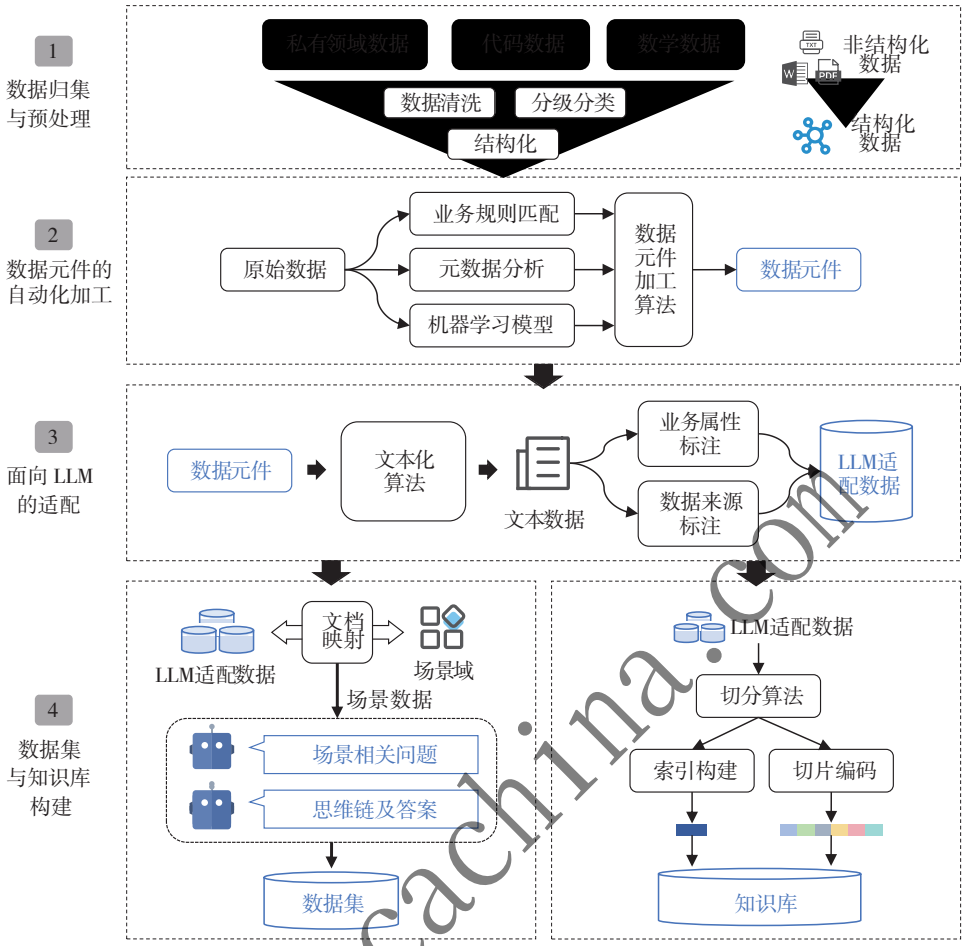

图 1　基于数据元件的领域数据治理体系

3.3　面向 LLM 的适配

为了弥合结构化数据元件与 LLM 自然语言理解能力之间的鸿沟，需要将抽象的数据元件转换为连贯的自然语言文本。这一过程通常采用模板化填充技术，通过预设的句式结构，将元件名称和元件值作为变量填入，自动生成描述性的事实陈述。这种转换不仅使数据对模型可读，更重要的是保留了元件中蕴含的核心逻辑与信息。生成的自然语言文本是后续进行数据标注、构建问答对和思维链数据集的直接输入，是适配大模型的关键一环。

数据标注是根据数据业务属性和数据来源等对数据进行分类和打标签。数据标注直接服务于知识库构建过程中的文档分类和数据集构建过程中的文档映射，即明确特定场景需要的文档。

3.4　数据集与知识库构建

数据集与知识库的构建是数据治理工程化路径的最终目标，旨在构建两大核心输出：支撑模型微调的数据集以及用于模型推理的知识库。高质量的问答对和思维链（Chain of Thought，CoT）[18]数据集用于大模型的微调训练，结构化的领域知识库用于检索增强生成（Retrieval Augmented Generation，RAG）[19]和事实性校验。

经过适配模型的数据首先通过文档映射明确构建数据集所需要的数源。文档映射是指依据特定场景需求，建立场景域与相关文档之间的逻辑链路。这通常依赖领域专家的经验，以确保生成的数据集与实际业务场景高度相关。数据集生成则基于大模型的训练数据自动生成。大模型利用映射的文档和精心设计的提示词作为上文，首先生成业务场景相关的问题。随后，利用这些问题和专家设计的提示词，使用 DeepSeek 的推理型模型生成 COT 数据。

知识库是大模型实现精确检索增强生成和减少幻觉的关键。知识库的构建包括文档切分、索引构建、文档编码以及知识存储。文档切分根据特定的场景需求将大型文档切分为更小、更易于管理的片段。索引构建对切分后的文档片段，利用大模型或其他自然语言处理模型

生成关键词或摘要。这些关键词和摘要将作为知识库的索引，用于快速定位相关信息。文档编码针对切分后的文档片段，利用大模型进行语义编码，生成高维度的文档片段向量。这些向量捕获了文档片段的深层语义信息，是实现语义搜索和相似性匹配的基础。知识存储根据知识的类型和访问模式选择最合适的存储方案，能够确保知识库的高效存储、管理和检索[20]。

4 应用实践：财务领域的场景验证

本节旨在通过具体的应用场景，演示前述以数据元件为核心的领域数据治理工程化方案的实际运行机制与价值。本节以一家金融服务平台为例，阐述如何利用数据元件构建一套智能评估助手，用于对大量非上市企业进行高效、隐私安全的价值评估、信贷风险分析或投资潜力识别。

4.1 场景概述

投资机构需对潜在被投或授信的非上市企业进行全面、深入的尽职调查和风险评估，以支持投资决策、信贷审批或并购考量。然而非上市企业的具体财务数据，如营收、利润、负债、客户明细等属于高度敏感的商业机密，该类企业通常不愿直接提供原始报表供第三方进行集中分析，甚至连审计报告也可能存在披露限制，导致机构难以获取全面且可比的数据视图。与此同时，传统评估方式依赖大量人工分析，效率低下且易受主观判断影响。

4.2 领域数据治理方案在财务场景的实践

本文按照第 3 节概述的工程化方案，分步阐述在该场景下，如何从上市公司数据出发，构建训练集和知识库，并最终赋能对非上市企业的评估。

4.2.1 数据归集与预处理

本文从沪深交易所、上市公司官方网站等公开渠道，批量获取中国 A 股上市公司历年的年度报告。在通过网络爬虫或 API 接口自动化下载后，本文利用 PDF 解析和自然语言处理技术，将非结构化或半结构化的年报内容抽取为结构化数据。最后，针对结构化数据，进行包括统一报表科目、处理缺失值与异常值等处理操作。

4.2.2 数据元件的自动化加工

这一阶段旨在从上市公司的年报中，针对其所投资的非上市实体，提炼出业务导向且隐私安全的财务数据元件，以及相关的非敏感背景信息。表 1 列举了一部分关键数据元件。

针对每一家上市公司年报中提及的非上市被投资实体，该步骤都将获得一份由数据元件和其他非敏感数据组成的描述被投企业的结构化数据。

4.2.3 面向 LLM 的适配

此阶段是连接结构化数据元件与 LLM 理解能力的关键，也是构建模型训练数据和知识库的核心。基于每条被投企业画像集，结合其非敏感背景数据，本方法通过模板化填充自动生成一份描述该实体财务状况和经营特征的自然语言事实陈述。经过填充后的自然语言事实示例如下：“根据上市公司 A 的年报披露，其重要被投资企业 B 是一家位于华东的新能源行业公司。该公司投资影响类型为重大影响，对母公司的利润贡献趋势表现为显著增长。其资产规模属于中型被投企业，关联风险因子低。”

在生成自然语言事实陈述之后，每条数据会被赋予明确的业务场景标签（如“价值评估”“信贷风控”）和来源标签（如“上市公司 A_2023 年报”）。这些标注为后续数据集构建提供了精确的筛选和映射依据，例如，当需要构建一个专注于信贷风险分析的微调数据集时，系统可以快速筛选出所有标记为“信贷风控”的数据源，确保了生成数据集的场景相关性。采用高性能的文本嵌入模型将上述切分后的每一个知识块转化为高维稠密的向量。这些向量能够捕捉文本

表 1 财务数据元件概览

序号	元件名称	元件解释
1	投资影响类型元件	根据附注中对投资类型的描述，如对联营企业和合营企业的投资为元件赋值“重大影响”或“共同控制”。
2	投资收益贡献趋势元件	通过分析上市公司披露的历年“投资收益”或“按权益法确认的投资损益”的变化趋势生成投资收益贡献趋势，该元件可被赋值为显著增长、稳定、下降等值。
3	被投企业规模元件	根据上市公司披露的对被投企业的投资额或股权比例，结合上市公司自身规模，估算并生成被投企业规模：小型、中型、大型。
4	关联风险因子元件	从年报附注中识别与被投企业相关的潜在风险描述，如“商誉减值准备”“诉讼风险”，并对该元件赋值高、中、低或具体的风险标签。
…	…	…

块的语义信息，使得在向量空间中，语义相似的知识块彼此距离更近。将生成的向量及其对应的原始知识块文本存储到专门的向量数据库中，并构建高效的索引结构，以支持后续查询时的快速相似性搜索。

4.2.4 数据集构建

该步骤通过利用 DeepSeek671B 模型作为教师模型，以上一步生成的自然语言事实作为输入，结合精心设计的提示词，自动化生成高质量的问答对和 CoT 数据。自动化生成的问答对和 CoT 数据在经过去重与质量筛选后将形成财务评估领域微调数据集用于微调基础的 LLM，使其内化投资机构或银行在非上市企业评估方面的专业知识、推理逻辑和问答风格，从而培养出一个具备非上市企业评估专家思维的语言模型。

4.2.5 知识库构建

为优化检索效率和 LLM 的上下文利用，需对整合后的知识源进行合理的颗粒度切分。每一个由数据元件和非敏感数据形成的“企业评估摘要”通常被视为一个独立的原子知识单元。对于非敏感背景数据，可根据其主题或段落逻辑进行切分。例如，将“新能源行业发展趋势报告”按照“市场规模”“技术创新”“政策影响”等子主题进行分块。

5 结论

本研究旨在弥合企业在数字化转型过程中，利用大语言模型（LLM）深度挖掘领域数据价值时所面临的“数据可用而不可见”这一核心挑战。为解决上述挑战，本文创新性地提出了基于数据元件的领域数据治理工程化路径，涵盖了数据归集与预处理、数据元件的自动化加工、面向 LLM 的适配以及数据集与知识库构建等关键阶段。其中，数据元件的自动化加工是核心，它结合规则引擎、元数据驱动和机器学习技术，实现了从原始数据到高质量、隐私安全的业务导向型数据元件的转化。这些数据元件随后被转化为自然语言事实陈述，用于自动化生成大模型微调所需的高质量 CoT 数据集，以及构建支持 RAG 的领域知识库。通过这种机制，基础 LLM 得以被赋予企业领域的专业知识、推理逻辑和问答风格，并能基于隐私安全的数据元件进行精准推理，加速企业在数字化转型中的落地实践。

参考文献

[1] 张熙，杨小汕，徐常胜. ChatGPT 及生成式人工智能现状及未来发展方向［J］. 中国科学基金，2023，37（5）：743－750.
[2] 刘学博，户保田，陈科海，等. 大模型关键技术与未来发展方向——从 ChatGPT 谈起［J］. 中国科学基金，2023，37（5）：758－766.
[3] 刘志红. 人工智能大模型的隐私保护与数据安全技术研究［J］. 软件，2024，45（2）：143－145，151.
[4] 李继峰，张成龙，刘鑫，等. 面向人工智能的数据治理框架［J］. 大数据，2025，11（1）：3－20.
[5] 雷克，王伟，任胜利，等. 数据治理在石油企业中的应用实践［J］. 石化技术，2021，28（6）：180－182，16.
[6] 赵鹏，张青，胡刚，等. 面向航天设计领域数据治理方法研究［J］. 软件，2024，45（7）：128－130.
[7] 常朝娣，陈敏. 大数据时代医疗健康数据治理方法研究［J］. 中国数字医学，2016，11（9）：2－5.
[8] 张照龙，谢江，包宏宇. 电信领域数据安全合规治理思考［J］. 信息通信技术与政策，2023，49（2）：14－19.
[9] 张培，夏海鹰. 教育领域数据治理的基本思路与实践路径［J］. 现代教育技术，2020，30（5）：19－25.
[10] JI Z W，LEE N，FRIESKE R，et al. Survey of hallucination in natural language generation［J］. ACM Computing Surveys，2023，55（12）：1－38.
[11] WU J C，DENG W L，LI X X，et al. MedReason：eliciting factual medical reasoningsteps in LLMs via knowledge graphs［J］. arXiv preprint arXiv：2504.00993，2025.
[12] 赵月，何锦雯，朱申辰，等. 大语言模型安全现状与挑战［J］. 计算机科学，2024，51（1）：68－71.
[13] 纪守领，杜天宇，李进锋，等. 机器学习模型安全与隐私研究综述［J］. 软件学报，2021，32（1）：41－67.
[14] 陆志鹏. 数据元件对数据资源价值释放的“杠杆原理”［J］. 信息通信技术，2024，18（5）：62－70.
[15] 陆志鹏，孟庆国，王钺. 数据要素化治理［M］. 北京：清华大学出版社，2024.
[16] TAO X M，WANG Y，PENG J Y，et al. Data component：an innovative framework for information value metrics in the digital economy［J］. China Communications，2024，21（5）：17－35.
[17] 陶晓明，彭勃扬，王钺，等. 基于信息熵的数据元件信息计量——以数据定价及其电能统计应用分析为例［J］. 中国科学：信息科学，2025，55（3）：654－680.
[18] WEI J，WANG X Z，SCHUURMANS D，et al. Chain-of-thought prompting elicits reasoning in large language models［J］. Advances in Neural Information Processing Systems，2022，35：24824－24837.
[19] LEWIS P，PEREZ E，PIKTUS A，et al. Retrieval-augmented generation for knowledge-intensive NLP tasks［J］. Advances in Neural Information Processing Systems，2020，33：9459－9474.
[20] TOPALOGLOU T. Storage management for knowledge bases［C］// Proceedings of the Second International Conference on Information and Knowledge Management，1993：95－104.

（收稿日期：2025－08－18）

作者简介：

陆志鹏（1964－），男，博士，正高级工程师，主要研究方向：数据安全与数据要素治理、经济管理、数字经济等。

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