

doi:10.11920/xnmdzk.2025.01.015

# 数字时代数据安全研究现状可视化分析

胡尔贵, 沈阳阳

(西南政法大学总体国家安全观研究院, 重庆 401120)

**摘要:** 总体国家安全观视域下, 安全应是系统的、联系的。数据安全突破传统与非传统安全领域界限, 与各领域安全深刻融合, 是国家安全的重要内容。通过数据分析工具 CiteSpace 和 VOSviewer 软件对中国知网 2003-2023 年数据安全研究样本文献进行可视化分析, 以期揭示数据安全研究概况与趋势。分析发现, 数据安全研究从侧重业务与技术应用转向理论探索, 研究地位从“附属”走向独立, 主要形成了两大类热点: 一类是以数据安全、网络安全、信息安全和隐私保护等关键词为代表的研究; 另一类是以大数据、数据治理、数据共享和数据挖掘等关键词为代表的研究。未来数据安全研究应针对当前存在的理论基础薄弱、已有理论系统性不显著、研究成果延伸性和应用性不足等问题, 加强总体国家安全观理论指导以及多学科交叉融合, 推动数据安全研究体系纵深发展。

**关键词:** 数据安全; 国家安全; 知识图谱; 文献研究

中图分类号: TP309; TP393.08

文献标志码: A

文章编号: 2095-4271(2025)01-0109-10

## Visualized analysis of current research status in data security in the digital age

HU Ergui, SHEN Yangyang

(National Security School, Southwest University of Political Science and Law, Chongqing 401120, China)

**Abstract:** From the perspective of the holistic approach to national security, security should be systematic and interconnected. Data security breaks through the boundaries of traditional and non-traditional security fields and is deeply integrated with security in various fields, making it an important part of national security. The article used data analysis tools such as CiteSpace and VOSviewer software to conduct a visual analysis of sample literature on data security research from 2003 to 2023 on CNKI, aiming to reveal the general situation and trends of data security research. The analysis found that data security research had shifted from focusing on business and technical applications to theoretical exploration, and its research status had changed from being "subsidiary" to being independent. Two major categories of hotspots mainly emerged: one was the research on the value of data content represented by keywords such as data security, network security, information security, and privacy protection; the other was the research on data management and application represented by keywords such as big data, data governance, data sharing, and data mining. In the future, data security research should address the existing problems such as a weak basic theoretical system, insignificant systematicness of existing theories, and insufficient extensibility and applicability of research results. It should strengthen the theoretical guidance of the holistic view of national security and the cross-disciplinary integration to promote the in-depth development of the data security research system.

**Keywords:** data security; national security; knowledge graph; literature research

收稿日期: 2024-11-19

作者简介: 胡尔贵 (1972-), 男, 西南政法大学总体国家安全观研究院执行院长, 教授, 博士生导师, 研究方向: 国家安全学。沈阳阳 (1998-), 女, 西南政法大学总体国家安全观研究院研究员, 研究方向: 国家安全学

基金项目: 重庆市教育委员会人文社会科学规划重点项目: 国家数据安全保障体系研究 (项目编号: 23SKGH002)

数字经济时代,数据安全打破传统与非传统领域界限,与多领域安全融会贯通、密切交织,各领域数字化转型战略逐步铺开,成为总体国家安全观中的重要方面以及各安全领域的重要内容<sup>[1]</sup>。习近平总书记提出的总体国家安全观强调统筹安全与发展,既重视安全问题又重视发展问题。这就意味着新时代国家安全必须重新审视数据安全之地位,数据安全亦需立足总体国家安全观的要求谋发展。纵观我国的数据立法始终坚持统筹安全与发展主旨,网络安全法中安全与发展贯穿于数据要素治理整体架构,数据安全法设专章“数据安全与发展”,明确数字时代的数据安全治理必须统筹发展和安全。2020年,国务院明确将数据与土地、技术等生产要素并列,数据基本完成了向“要素”的转变<sup>[2]</sup>。在此背景下,加快加强数据安全研究是促进国家经济发展、增强国家国际竞争力、国家安全的必然和迫切需要。

从样本文献关键词来看,现有数据安全研究主要形成了两大类热点:一类是以数据安全、网络安全、信息安全和隐私保护等关键词为代表的数字内容价值的研究;另一类是以大数据、数据治理、数据共享和数据挖掘等关键词为代表的数字管理与应用的研究。从样本文献数量及分布来看,2021年以来数据安全研究发文进入爆发期,研究成果丰富,在国家安全相关期刊中也开始形成了一定聚焦。虽然研究趋势向好,但相较于数据“新石油”的时代地位而言仍有诸多问题亟待研讨。一方面,当前研究虽强化了总体国家安全观科学理论的指导,但仍存在研究学者及机构之间缺乏合作,研究领域广泛但各领域发展不平衡及纵深不足等问题。另一方面,就样本数据来看,已有文献研究视角多从已知安全风险出发,对其展开规制路径、制度构建、应对措施等较高维度研究,问题导向性与政策导向性显著,相较而言则缺少了对数据领域基础概念及理论体系构成要素的解构分析,对国内外数据政策、标准的底层制定原则、逻辑分析适应性不足,从而造成目前数据安全研究缺乏完整的基础理论体系,以支撑各类标准的制定及相关规范体系的构建,进而难以避免研究成果欠缺可操作性等弊端。为此,本文拟从文献计量学视角,基于知识图谱对该领域研究作总体回顾,并揭示其研究热点和趋势,以期为我国数据安全研究发展提供借鉴和参考。

## 1 数据与方法

### 1.1 数据来源

遵循理论与实践、社会科学与自然科学相结合的原则,结合国家安全学学科研究的重点方向,文章选取中国知网 CNKI 数据库,以“数据安全”“数据安全理论”“数据安全战略”“数据安全治理”“数据安全技术”等为主题词进行“精确”检索。另外,2003年曾被称为是中国网络安全事故最多、波及面最广的一年<sup>[3]</sup>,并在之后制定了大量应急预案<sup>[4]</sup>。因而文章以2003年作为检索起点,将2003年至2023年作为研究区间。同时,为保证数据的权威性,将样本文献期刊来源类别限定为SCI、EI、北大核心、CSSCI、CSCD、AMI等期刊。共检索到6318篇文献,检索时间为2024年6月23日。利用Cooc(CO-occurrence)软件对文献进行合并、检验、去重等,最终共筛选出5241篇样本文献。

### 1.2 研究方法

文章采用文献计量法与文献阅读法开展研究。首先运用Cooc和VOSviewer文献计量软件,对CNKI核心合集所收录的国内中文(2003-2023年)数据安全研究的5241篇文献进行频次统计、共现与聚类、突变词检测等可视化分析并分别绘制相关知识图谱。其次,鉴于智能分析工具缺乏研究主题知识背景及其认知理解,仅靠算法进行术语提取与统计的方式难以反映文章写作类型和背景。故而本文在利用统计分析工具的基础上,对样本文献标题与摘要内容进行逐条阅读,并抽样精读部分样本文献,综合分析研究阶段与研究主题,判断研究演化动态与发展趋势。

## 2 研究基本特征

### 2.1 发文量分析

通过对样本文献年发文量变化的观察,可以分析该研究领域的发展态势。据2003-2023年发文量柱状图(图1)显示,数据安全研究整体呈上升趋势。结合历年发文数量年度增长率(本年度对比上年度)得出,2016年与2021年的发文增长率分别为40.56%、51.54%,是增幅最大的两年,结合当时的国家宏观形势及重大决策,可将数据安全研究发文活跃度大致分为探索期(2003-2015年)、发展期(2016-2020年)和爆发期(2021-2023年)3个阶段。

### 2.2 发文期刊分析

对样本文献的发文期刊分布进行统计,累计载文超 40 篇的期刊共计 20 个(图 2). 其中 13 个为计算机科学期刊. 刊文最多的是《信息网络安全》,共 113 篇,占总发文量的 2.16%,该期刊是由中国计算机学会主办的电信期刊,具有较强的技术应用性. 可见,现行数据安全研究发文长期以计算机科学领域期刊为主要

阵地,没有在国家安全相关期刊形成明显聚集,更没有数据安全研究的专门期刊. 然而,当前数据安全具备国际国内独立战略地位,是各国综合国力竞争关键要素,在国家安全中具有重要地位,无论从国家安全还是国家发展层面,当前学术期刊分布、数量及类别都难以与数据在新时代的重要地位相匹配.



图 1 2003-2023 年发文量柱状图

Fig. 1 Bar chart of the number of published papers from 2003 to 2023

### 2.3 作者及学科分析

利用 Vosviewer 对作者及其发文关键词绘制共现图谱(图 3),5 241 篇样本文献共有 10 320 名作者(未考虑作者重名). 发文 10 篇及以上有 16 人,仅占作者总人数的 0.16%,黑龙江大学马海群教授的发文章最多,为 38 篇. 作者间合作率为 0.673 3,合作度为 1.969 3. 共现频次最高的三个团体分别为:马海群与张涛合作发文 11 篇,主要聚焦政府数据治理问题,两

人均来自黑龙江大学;陆康、任贝贝、刘慧三人合作发文 10 篇,主要关注智慧图书馆相关制度建设与用户隐私保护问题,三人分别来自南京晓庄学院、上海市网络技术综合应用研究所、中国科学院大学;王秉、吴超合作发文 9 篇,主要涉及大数据环境下的情报学研究,两均来自中南大学资源与安全工程学院. 相关结论直接地反映出当前数据安全研究学术群体缺乏跨学科跨机构交流与合作的问题.

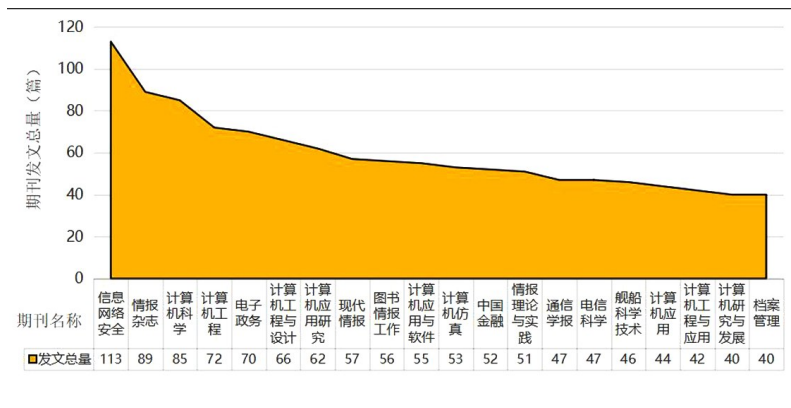


图 2 发文期刊统计图(前 20)

Fig. 2 Statistical chart of the journals where papers were published (Top 20)

### 2.4 发文机构分析

样本文献分别来自 5 219 个机构,发文总量大于 30 篇的研究机构共有 4 个(图 4),包括武汉大学信息管理学院(69 篇)、国家计算机网络应急技术处理协调中心(43 篇)、黑龙江大学信息资源管理研究中心(37 篇)、武汉大学信息资源研究中心(33 篇). 机构合作率为 0.371 8,合作度为 1.006 9. 从机构最高共现的三个团体看,武汉大学信息管理学院、武汉大学

信息资源研究中心共现 23 次,黑龙江大学信息管理学院、黑龙江大学信息资源管理研究中心共现 22 次,中南大学资源与安全工程学院、中南大学安全理论创新与促进研究中心共现 15 次. 不难看出,上述共现关系实际为机构内部的协作. 这于数据安全较强的交叉学科属性而言是难以满足其发展需求的,加之数据安全问题已与国家安全各领域交叉融合,要形成成熟的研究体系,跨界交流势在必行.

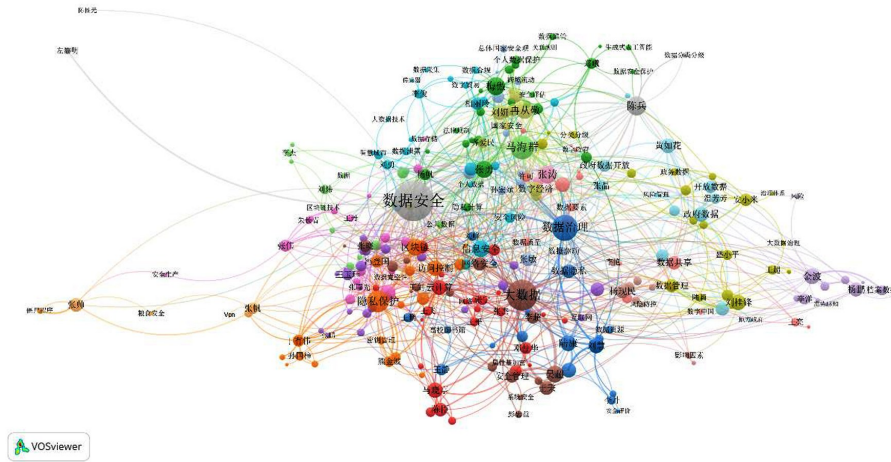


图 3 作者关键词共现图

Fig. 3 Co-occurrence graph of authors' keywords

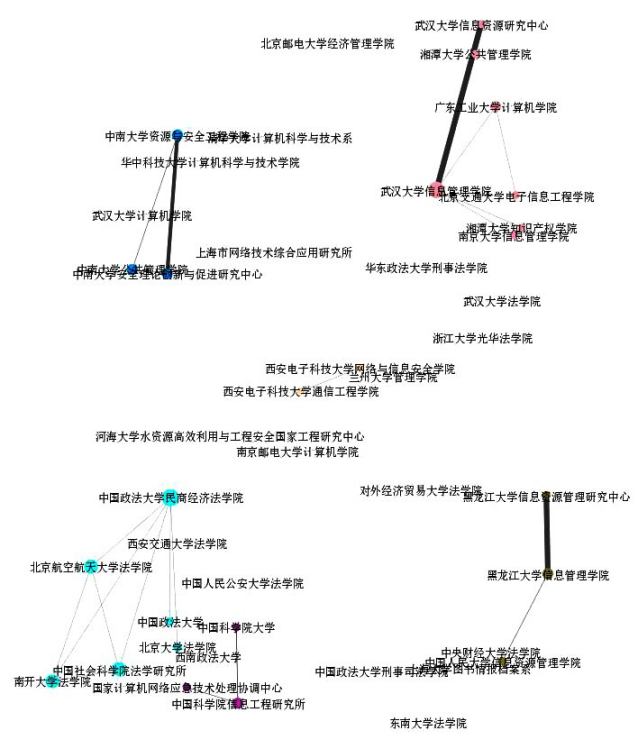


图 4 机构共现图

Fig. 4 Co-occurrence graph of institutions

综上,近 20 年来数据安全研究整体呈上升趋势,在 2021 年进入研究爆发阶段,研究独立性不断增强。在一定程度上反映了数据社会变革趋势与数据安全地位转变的现实映照,数据安全研究愈加受到重视。但是,数据安全研究尚没有在国家安全相关期刊形成聚集,更没有数据安全研究的专门期刊,学术群体、学术机构间跨学科、跨领域合作极少。以上反映出这个领域研究模式成熟度还不够,不足以支撑形成系统完善的理论体系。在数据资源“石油化”的今天,数据安全尚具有很大的研究空间。

### 3 研究热点主题及脉络

#### 3.1 数据安全研究热点主题

学界围绕数据安全研究形成了大量研究成果。本文利用聚类共现方法,对于主题研究关键词进行聚类

分析,设置  $g\text{-index}(k = 25)$ ,  $LRF = 3.0$ ,  $L/N = 10$ ,  $LB\gamma = 5$ ,  $e = 1.0$ ,得到关键词聚类图谱,共包含 885 个关键词,1 643 条联系,网络密度为 0.004 2。在此基础上进行聚类分析, $S$  值 = 0.839 3, ( $S$  值:聚类平均轮廓值,一般认为  $S > 0.5$  聚类就是合理的, $S > 0.7$  意味着聚类是令人信服的,图谱的聚类结果是合理的,即此次聚类符合科学标准。)得到 10 个聚类标签(图 5)。主要包括#0 数据主权、#1 数据治理、#2 网络安全、#3 大数据、#4 数据安全、#5 区块链、#6 数据挖掘、#7 金融科技、#8 信息安全和#9 云计算。其中最大的研究聚类是#0 数据主权,聚类中的热点词包括数据主权、国家安全、个人数据、跨境流动、数据犯罪等。其次是#1 数据治理,其热点词包括数字经济、政府数据、数据开发、数据要素等。

CiteSpace, v. 6.3.R1 (64-bit) Advanced  
 May 1, 2024, 6:16:04PM CST  
 CNK1: /Users/xqwine/Desktop/Citespace\_data/data  
 Timespan: 2003-2023 (Slice Length=1)  
 Selection Criteria: g-index (k=25), LRF=3.0, L/N=10, LB $\gamma$ =5, e=1.0  
 Network: N=885, E=1643 (Density=0.0042)  
 Nodes Labeled: 1.0%  
 Pruning: Pathfinder  
 Modularity Q=0.5981  
 Weighted Mean Silhouette S=0.8393  
 Harmonic Mean(Q, S)=0.6985



图 5 关键词聚类图谱

Fig. 5 Keyword clustering map

#### 3.2 数据安全研究发展脉络

在关键词聚类的基础上,利用 CiteSpace 的 TimelineView 功能得到关键词聚类时区图(图 6)。该图谱

不仅能展示每一聚类包含的关键词有哪些,而且能清晰地看到每一聚类主题的开始和结束的时间节点,从而可以总结出相关研究的演化路径。它主要侧重于勾

画聚类之间的关系和某个聚类的历史跨度. 如#0 数据主权从 2012 年左右开始持续有研究出现, 其中国家安全、跨境流动、数据犯罪是热点话题, 说明该聚类涉及的领域是新兴领域且发展趋势较好, 一直受到学者的关注. #1 数据治理的相关研究聚焦于 2016 年左

右, 其中数字经济与数据要素作为热点话题分别在 2020 年前后受到广泛关注. 同时, #3 大数据、#7 金融科技研究趋势也较好, 此四大聚类可能是未来研究热点, 可持续关注.

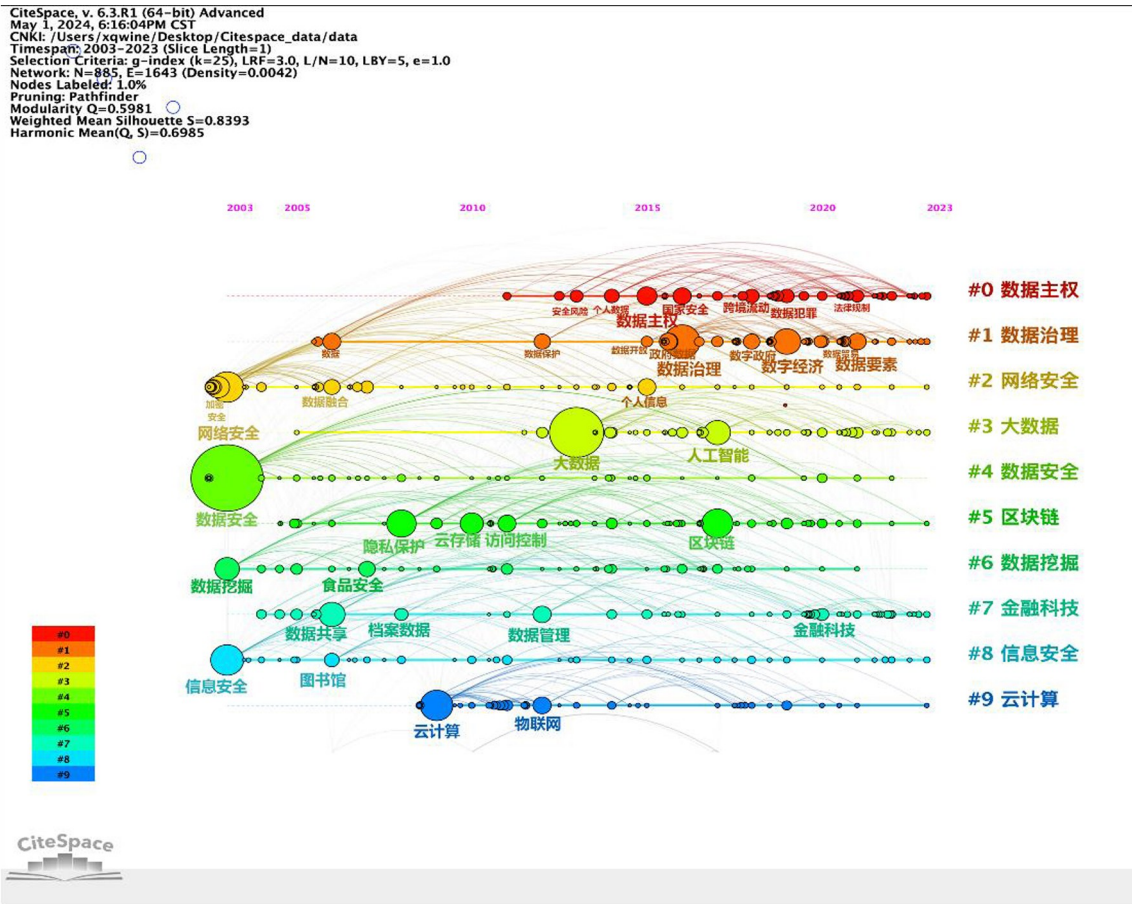


图 6 关键词聚类时区图

Fig. 6 Keyword clustering time zone map

## 4 研究发展趋势分析

### 4.1 数据安全研究地位逐步趋于独立

从前文发文量及关键词图谱分析发现, 近 20 年来数据安全研究大致经历了三个阶段. (1) 探索期 (2003 - 2015 年), 数据安全研究总体置于网络安全框架之下. 这一时期的数据安全样本文献关键词无“国家安全”, 研究将数据作为计算机系统构成元素, 以计算机领域及企业相关人员为主体, 基于网络系统视角, 从技术角度针对网络数据的物理安全进行访问控制、加密技术等策略分析, 包括安全技术、系统管理、整体解决方案以及立体化整体信息防泄漏体系几个过程<sup>[5]</sup>. 以防火墙、终端防护、流量清洗系统等安

全产品为主要输出. (2) 发展期 (2016 - 2020 年), 数据安全研究逐渐超越网络安全研究的范畴. 这一时期我国发布实施《国家网络空间安全战略》等重要文件, 颁布一系列数据规范、标准, 确认数据独立生产要素地位, 与大数据相关的政策、法规、技术、应用等发展因素初步完善. 数据安全研究从信息内容开始转向数据本身, 以数据为中心的关注快速增长, 数字经济、数据确权、数据泄露、数据处理权益、数据泄露通知等议题兴起. 数据安全内涵不断延伸, 逐渐超越对网络安全的“依附”, 研究主题广泛涵盖经济、政治、文化、教育、医疗交通等领域<sup>[6]</sup>. (3) 爆发期 (2021 - 2023 年), 数据安全研究成为具有独立属性的研究议题. 在该阶段, 无论是研究主体、研究领域、研究视野都前所未有

的广泛。建设数字中国、培育数据要素市场、赋能数字经济、颁布实施数据安全法等众多战略举措的推进落实是这一时期数据安全研究背景。以数据为中心的安全价值已超越单纯的生产要素层面,而是延伸并融合于微观个人安全与宏观国家安全领域。数据成为深刻改变国际竞争格局的关键因素之一,数据主权、数据跨境流动、数据全球治理等成为各国共同关注<sup>[7]</sup>。

#### 4.2 开始注重数据安全理论体系构建

大数据时代,以人工智能为代表的颠覆性数字技术迅猛发展,持续嵌入与赋能社会各领域发展<sup>[8]</sup>。诸多传统法益以数据为媒介、载体来储存、分享、利用。与此同时,基于网络的发展及数字经济背景,一系列以数据为对象的侵犯数据安全性的网络犯罪日渐增多。从数据安全研究的发展脉络来看,研究学者同样意识到了数据安全之复杂性、重要性,必须健全相关理论体系用以引导与规范数据资源在各领域的安全发展。(1)数字经济理论体系。数字经济是新型社会经济发展形态,其发展情况是国家综合国力的重要体现,是近几年数据安全研究领域快速增长的研究话题。当前数字经济发展需应对与实体经济融合过程中产生的一系列数据安全与挑战<sup>[9]</sup>。数据要素市场培育是首要目标,但我国数据要素市场流动机制尚未建立起来<sup>[10]</sup>,数据内涵价值没有得到充分释放<sup>[11]</sup>。因而较多学者围绕数据定价、数据确权等主题形成理论构架,旨在为统一数据要素市场的顶层设计和相关法律法规政策方面提供借鉴。具体来说包括数据权属界定、数据评估标准、数据开放、数据共享、市场交易规则、数据市场监管等方面的规则构建与理论论证。(2)数据治理理论体系。数字技术引发的问题以及数字社会背景下的社会治理挑战,已经成为治理能力与治理现代化的最大考验。从数据安全治理参与者出发,包括国家治理、社会治理、基层治理到个人治理多个维度。从数据安全治理的目标出发,其最终目标是实现数据安全和数字经济发展之间的平衡<sup>[12]</sup>。从数据安全治理对象出发,建设以数据为中心的安全体系,认为包括“数据安全治理评估、数据安全组织建设、数据安全管理体系建设、数据安全技术建设、数据安全运营建设和数据安全监管建设<sup>[13]</sup>。”就数据安全国内治理来看,当前研究在主题上得到拓展,理论体系亦有所深化。研究从已暴露的安全风险及其规制、应对策略等

维度着手,问题导向性与政策导向性显著,但也暴露出目前仍缺乏完整的数据安全基础理论体系以支撑各类标准的制定及相关安全规范体系的构建。(3)数据权益理论体系。学者指出,数据权益体系多元繁复。从权利角度,可区分为个人数据主体的数据人格权益、数据财产权益以及公共数据之上社会大众的公共利益。从权力角度,数据权力具有对海量数据的控制和处理优势,是促进经济发展、社会管理、科技创新的重要因素,具有的扩张性、广泛性、不透明性、排他性和软权力性等特征。针对较为滞后的现有保护体系,有学者提出要建立以数据安全法为中心,以行政法、刑法、民法、行业规范为辅助的多层次法律体系,在政府、社会不同主体的共同参与下,实现数据安全的多元“共治”<sup>[14]</sup>。因此,有必要结合数据时代特征,从基础概念、利益主体、保护对象、保护框架、行为类型等层面对数据可携带权、数据隐私权、个人信息权、数据限制处理权、数据调取权、公平利用权等进行理论构建,从而以公私法保障数据权益、健全程序机制,实现数据价值应用与数据权益保护的平衡<sup>[15]</sup>。

#### 4.3 数据安全研究国际化趋势显著

伴随全球数字贸易的纵深发展及各国数据战略博弈,数据主权、全球数据安全治理等议题热度较高。同时,总体国家安全观科学理论趋于成熟,学界对数据安全研究愈发重视与国家安全的结合,从制度、规则、价值等角度予以深化。(1)数据主权。由于数据主权并非一个既定的法律概念,因此学界对它的理解有很大差异,映射到实践中,理解偏差演变成了对数据主权的误解与滥用<sup>[16]</sup>。在国际环境中与数据主权密不可分的话题是数据的跨境流动,因而一些国家将数据主权与数据本地化画上等号,我国学者围绕各国制度、政权、意识形态等方面进行分析对比,认为当前国际主体之间主要形成了以欧盟为代表的“数据保护主义”与以美国为代表的“数据自由主义”<sup>[17]</sup>。我国则基于维护数据主权的核心诉求,致力于实现数据安全与数据跨境高效流动的双重价值平衡,以总体国家安全观等科学理论指导,积极构建数据跨境流动国际规则和网络空间命运共同体,维护我国的数据主权与国家安全<sup>[18]</sup>。(2)全球治理。根据国家数据局发布的《数字中国发展报告(2023年)》显示,当前我国数字基础设施算力总规模居全球第二位,关键核心技术不断取得

突破,高性能计算持续处于全球第一梯队,数字经济保持稳健增长,连续 11 年成为全球第一大网络零售市场。因此,积极拓展数字领域国际合作,推动建成公正合理的全球数据安全治理框架显得尤为重要。但现有的治理模式由单边、双边和多边框架以及贸易规则拼凑而成,存在标准差异化、规则碎片化、治理乏力等问题<sup>[19]</sup>。对此,学者从社会制度、经济模式、数据资源等方面分析造成治理主体利益诉求差异的原因,并指出部分国家的“长臂管辖”“数据霸权”等问题。同时也意识到,与“欧洲数据保护主义”“美国数据自由主义”相比,我国致力于构建网络空间命运共同体的方案竞争优势及国际话语权优势并不突出,因而需积极参与相关国际规则制定,加快推进国际新秩序的构建。

## 5 数据安全研究展望

数据安全作为国家安全的重要领域,尽管目前已经迎来研究热潮,但从样本分析的整体来看,数据安全研究基础理论体系薄弱,已有理论系统性不显著,研究成果延伸性、应用性不足等问题,离总体国家安全观的要求还有较大差距。随着数字社会的数据“要素”地位确立,数据安全将面临更多的理论与实践难题。数据安全研究领域尚有较大的拓展空间。

### 5.1 进一步突出总体国家安全观理论指导,强化国家安全站位

总体国家安全观是我国在新时代应对国际国内复杂形势的重要指导思想,其包含一系列有关国家安全的新理念、新思想、新战略,对各领域安全进行科学统筹,是新时代我国国家安全工作的指导思想。随着总体国家安全观的不断成熟发展,数据安全的内涵外延亦随之丰富,加之数字经济大力建设,数据安全研究迈入新的阶段<sup>[20]</sup>。但是,我国大数据发展相较于西方发达国家整体进程较为落后,在西方开始将数据作为重要竞争要素并出台一系列数据保护法律法规的早期阶段,我国数据安全研究尚处于依附网络安全回应各领域业务需求的阶段。这种发展上的差距令我国数字经济发展在全球数字贸易中遇到诸多不公与阻碍,如美国以数据安全为借口对我国设置贸易壁垒,并试图在全球形成数据霸权。当前研究阶段确有强化总体国家安全观科学理论的指导,但是,从整体分析结果来看仍显示出研究领域宽泛但零散,研究的基础

理论体系薄弱,已有理论系统性不显著、可操作性欠佳,研究成果延伸性、应用性不足等问题。具体来说,从研究领域来看,数字技术应用已日常化、普及化,但研究主要关注船舶、电力、水利、教育、医疗、金融等关键基础行业领域的场景应用,对群众生活化场景关注较少,且多聚焦于隐私价值而忽视了其蕴含的经济价值、文化价值等内容。从文章数量和各领域内部及彼此之间联系来看,对内,各领域内部没有形成体系性研究成果,多围绕显性热议话题论述;对外,研究人员、研究机构等合作情况暴露出各研究主体之间各自为政,互动互促与借鉴不足。要应对上述困境,数据安全必须进一步突出总体国家安全观理论指导作用<sup>[21]</sup>,强化系统思维,将数据安全状态、能力及其过程理解为一个有机系统的观念体系,从全局的高度看待数据安全各领域、各层面、各阶段、各应用场景安全问题,统筹运用各方面资源和手段予以综合解决,实现数据安全多方面内容和要求的有机统一<sup>[22]</sup>。

### 5.2 完善数据安全基础理论,健全数据安全标准规范体系

构建科学的理论体系框架是表述复杂和抽象概念、开展数据治理实践工作的首要任务。强化数据安全理论研究可以为相关制度与标准体系制定提供坚实理论支撑与价值参考。具体来说,数据安全理论体系涵盖广泛,包括基础理论、数据权属理论、数据治理体系、数据技术应用等内容。其中数据基础理论则是整个理论体系的根基,包含数据及数据安全相关概念的基本定义、内涵外延、相邻概念关系厘清、发展沿革等,是数据安全研究与国家政策制定的起点。虽说数字技术的发展日新月异,其变化发展不断推新,但当前数据安全独立属性已然显现,数字经济蓬勃发展,数据相关法律法规与制度体系日渐完善,因而形成普遍认同的基础理论成为研究基础和现实需求,也是进一步推动数字经济与制度体系健全的题中之义。另一方面,数据标准是保障数据各业务系统对数据统一理解、使用和交换的一致性、准确性和完整性的规范性约束<sup>[23]</sup>。也是解决当前诸多制度与规则构建和落实的重要因素。近年来我国虽先后发布了《大数据服务安全能力要求》《数据安全能力成熟度模型》《个人信息安全规范》等重要标准,包括基础共性安全技术、安全管理、安全测评和典型应用五大类,并包含 50 多项

标准,数据安全国家标准体系初步形成<sup>[24]</sup>。但深入来看,数据分类标准、数据生命周期不同阶段中的安全标准、应用与服务标准、网络标准、管理标准、数据交易中的格式标准、质量标准等基础内容均未达成技术与法律的广泛统一,所构建的相关标准在结合国情与国际标准对标之间亦需进一步平衡。因而必须持续把握数据安全研究的前沿,形成理论成体系,把控研究话语权。

### 5.3 坚持创新应用,致力实现科技自立自强

党的二十大报告强调,坚持创新在我国现代化建设全局中的核心地位,加快实施创新驱动发展战略。数字技术是引领第四次工业革命的主要推动力,我国数字技术创新力量不断增强<sup>[25]</sup>。数字技术的发展为经济社会带来发展福利的同时,风险相伴而生。针对当前网络安全事件高发、攻击手段不断升级、攻击范围持续扩大、攻击对象日常化等态势,学术研究须秉承“以技术对技术,以技术管技术”理念,通过安全技术的创新与应用为数据安全问题提供解决方案,防御技术风险,以技术创新生长新安全能力<sup>[26]</sup>。一方面要继续突破数据应用系统的安全技术。包括从底层硬件、操作系统到上层应用软件等环节分析设备和程序安全、流程安全和防攻击处理等,对网络入侵防御技术、访问控制技术、数据加密技术、认证技术、防火墙技术、网络防毒及防蠕虫技术、安全防护系统等技术展开设计路径、原理及实施进行讨论,从而对数据的物理完整性、逻辑完整性、数据保密性等进行维护。另一方面,随着数字化进程推进,数据应用面及与生活融合程度深化,人们对数据的认知及利益相关度改变,国家间数据竞争加剧。数字技术的开发与应用更强调合规与安全价值属性,体现为以总体国家安全观为指导,转变数字技术纯粹中立的技术工具定位。具体来说,需从算法设计、需求设定等环节将法律法规与社会伦理的规则纳入考量,并对安全技术的测试和问题发掘予以突出,加强对数据隐私、数据授权加密、数据赋能等内容的理论凝练和对策分析<sup>[27]</sup>。从数据技术的创新应用看,以区块链技术和人工智能为代表是当前数字技术广泛应用与讨论的具体指向。在学者研究中主要对技术赋能的价值及存在的应用风险进行了总结,指出人工智能发展面临的信任危机、科技伦理、侵权归责、算法操控等多方面风险正对公共伦理、社

会秩序甚至总体国家安全带来挑战。因而持续以创新为动力推动数字技术发展,实现关键核心技术的自立自强将是数字时代国家发展和国家安全的重要力量。研究视角虽从技术本身延伸到国家整体,但数据作为技术的产物,其核心仍需要回归技术的创新与约束。

### 5.4 加强多学科交叉融合研究,培养复合型人才

数据安全与国家安全各领域已是深度融合状态,关乎国家安全、公共利益、经济发展、个人权益,兼具经济学、法学、理学、工学等多学科门类特征,需要政策、法律、技术多方参与<sup>[28]</sup>。在数字经济发展的的大趋势和背景下,多学科交叉融合是数据安全研究发展的重要策略。在未来的研究中学者应当立足所在机构特色与专长,探索最大限度发挥自身特色与优势的基础上丰富相关课程设置,从课程形式与知识来源等方面进行拓展和发掘。同时,在强化跨机构,尤其是高校间的跨校合作方面,不仅要寻求同类院校的合作,对教学模式、教学内容、师资力量等进行轮岗试课等合作模式尝试,而且要积极探索与不同类别院校的合作,强化技术与理论的互相融汇理解和问题思维的转换能力。另一方面,理论学者与技术学者之间可尝试校企联合模式,技术学者从行业内部、用户需求、数据应用成效等层面发现问题,从专业角度对问题进行归纳总结,以此作为学术研究机构或立法机构对于相关问题的考量因素之一,强化法技结合,为数据安全研究提供更多的研究思路与研究方法,推动学术繁荣、科技进步和数字经济发展。

### 参考文献

- [1] 左晓栋. 当前我国数据安全工作的形势与任务[J]. 国家治理, 2023(10): 63-67.
- [2] 今天的数据安全和过去有何不同? 专家畅谈“数据安全”[EB/OL]. [2021-05-28] (2023-10-27). <https://finance.eastmoney.com/a2/202105281940529827.html>.
- [3] 蠕虫作祟 2003 年是中国网络安全事故最多的一年[EB/OL]. (2004-01-03) [2023-10-27]. <https://news.sohu.com/2004/01/03/79/news217817958.shtml>.
- [4] 杜跃进. 陌生的危机: 我国的网络安全形势[J]. 中国金融电脑, 2014(1): 32-35.
- [5] 孟鑫东. 数据防泄密发展趋势[J]. 保密科学技术, 2012(5): 54-57+68.
- [6] 鄢世萍. 论大数据时代数据安全法律综合保护的完善——以《网络安全法》为视角[J]. 数码世界, 2019(3): 257.

- [7] 陈志鹏,陈媛媛. 政府数字治理路径探索中的模糊集定性比较分析[J]. 图书情报工作,2023,67(15):118-128.
- [8] 黎四奇. 数据科技伦理法律化问题探究[J]. 中国法学,2022(4):114-134.
- [9] 中国信息通信研究院. 中国数字经济发展白皮书(2020年)[R]. 2020:7-12.
- [10] 张嵩,李雪岩,汪诚,等. 数字经济时代数据安全治理的探索和研究[C]//第38次全国计算机安全学术交流会论文集. 长沙,2023:134-137.
- [11] 范文仲. 完善数据要素基本制度 加快数据要素市场建设[J]. 中国金融,2022(S1):14-17.
- [12] 杜跃进. 数据安全治理的几个基本问题[J]. 大数据,2018,4(6):85-91.
- [13] 数据安全治理的“前世今生”[EB/OL]. [2021-11-12](2023-10-27) [https://m.163.com/dy/article/GOIV5V6V0511ALHJ.html?spss=adap\\_pc](https://m.163.com/dy/article/GOIV5V6V0511ALHJ.html?spss=adap_pc).
- [14] 韩伟. 安全与自由的平衡——数据安全立法宗旨探析[J]. 科技与法律,2019(6):41-48+67.
- [15] 尹华容,王惠民. 数据权力的兴起、异化及规制[J]. 湖南大学学报(社会科学版),2022,36(03):124-132.
- [16] 漆晨曦. 当我们谈论数据时,我们在谈论什么[J]. 通信企业管理,2020(11):59-61.
- [17] 徐拥军,王兴广. 总体国家安全观下的跨境数据流动安全治理研究[J]. 图书情报知识,2023,40(06):20-30.
- [18] 邱璇. 系统综述——一种更科学和客观的综述方法[J]. 图书情报知识,2010,27(1):15-19.
- [19] 阙天舒,王子玥. 数字经济时代的全球数据安全治理与中国策略[J]. 国际安全研究,2022,40(01):130-154+158.
- [20] 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.
- [21] 王秉,徐方廷. 多学科交叉视角下国家安全情报体系构建研究[J]. 情报学报,2023,42(12):1448-1457.
- [22] 杨楠. 大国“数据战”与全球数据治理的前景[J]. 社会科学,2021(7):44-58.
- [23] 朱艳华,高瑜蔚,胡良霖,等. 我国科学数据标准规范实践与思考[J]. 中国科学数据,2023,8(1):165-174.
- [24] 李建彬,李智勇,李诗珂. 2022年度国内数据安全的现状与发展[J]. 中国信息安全,2023(1):43-48.
- [25] 陈睿,刘大椿. “双循环”新发展格局下政府数字化转型的创新路径研究[J]. 经济体制改革,2022(1):28-34.
- [26] 网络安全迎发展新拐点奇安信总裁吴云坤谈四点应对新机遇\_数字化[EB/OL]. (2021-08-27)[2023-11-08]. [https://www.sohu.com/a/486072316\\_118622](https://www.sohu.com/a/486072316_118622).
- [27] 刘润平,万佩真. 企业网络安全问题与对策[J]. 企业经济,2010,29(7):53-55.
- [28] 杜跃进,叶晓虎,赵伟. 《数字经济》对话头条—数据安全 深耕数据安全保障数字经济健康发展[J]. 数字经济,2021(S1):38-45.

(责任编辑:肖丽,殷锋,付强,张阳,和力新;英文编辑:周序林,郑玉才)