doi:10.3772/j.issn.2095-915x.2024.06.008

科技管理数据安全治理实践路径研究

徐晨阳 寇亚东 李子伦 王飘 王东

中国科学技术信息研究所 北京 100038

开放科学（资源服务）标识码（OSID）

摘要：[目的 / 意义] 科技管理数据作为国家科技创新与经济社会发展的关键资源，在大数据时代，其安全治理显得尤为重要。[方法 / 过程] 随着科技投入增加和创新能力提升，科技管理数据量激增，质量提高，但同时也面临着数据安全的新挑战，包括合规性不足、数据孤岛、数据质量参差不齐、数据流转复杂化以及安全风险加剧等问题。为应对这些挑战和问题，结合科技安全战略背景，规划了科技管理数据安全治理体系，并对摸清现状、安全建设规划、分级分类、全生命周期管理、运营监管等安全治理实践路径做了详细介绍。[结果 / 结论] 科技管理数据安全治理是一个系统工程，需要从战略高度出发，综合运用管理与技术手段，构建动态适应、全面覆盖的安全防护体系，以保障数据安全，促进科技管理工作的高效、健康发展，支撑国家科技创新战略的顺利实施。

关键词：科技安全；科技管理；数据治理；数据安全

中图分类号：G35; TP391

Research on the Practice Path of Data Security Governance in Science and Technology Management

XU Chenyang KOU Yadong LI Zilun WANG Piao WANG Dong

Institute of Scientific and Technical Information of China, Beijing 100038, China

Abstract: [Objective/Significance] Science and technology management data is a key resource for national science and technology innovation and economic and social development. In the big data era, its security governance is particularly important. [Methods/Processes] With the increase of science and technology investment and the improvement of innovation capacity, the volume and quality of science and technology management data have soared, but at the same time, they are faced with new challenges of data security, including insufficient compliance, data silos, uneven data quality, complicated data flow, and increased security risks. In order to cope with these challenges and problems, this paper, combined with the background of science and

作者简介 徐晨阳（1992-），硕士，助理研究员，主要研究方向为科技安全、数据治理、安全管理；寇亚东（1992-），硕士，助理研究员，主要研究方向为信息安全、信息系统运维，E-mail: kouyd@istic.ac.cn；李子伦（1994-），硕士，助理研究员，主要研究方向为计算机应用、信息系统建设；王飘（1992-），硕士，助理研究员，主要研究方向为计算机应用、信息系统建设；王东（1987-），博士，副研究员，主要研究方向为系统建设、自然语言处理、知识图谱。

引用格式 徐晨阳 , 寇亚东 , 李子伦 , 等 . 科技管理数据安全治理实践路径研究 [J]. 情报工程 , 2024, 10(6): 82-92.

technology security strategy, plans the science and technology management data security governance system, and makes a detailed introduction to the security governance practice paths such as finding out the current situation, security construction planning, classification, whole life cycle management, and operation supervision. [Results/Conclusions] Science and technology management data security governance is a systematic project, which needs to start from a strategic height, comprehensively apply management and technology means, and build a dynamic adaptive and comprehensive security protection system to ensure data security, promote the efficient and healthy development of science and technology management, and support the smooth implementation of national science and technology innovation strategy.

Keywords: Scientific and Technological Security; Science and Technology Management; Data Governance; Data Security

引言

科技管理数据是国家科技创新发展的重要资源[1]，是信息时代影响面最宽、开发利用潜力最大的科技资源。在大数据时代，科技创新、科技战略决策越来越依赖于大量、系统、高可信度的科技管理数据。近年来，我国高度重视科技创新工作，科技投入和创新能力不断提升，科技管理数据也大幅增长。随着信息化技术的快速发展，科技管理业务数字化转型迎来新机遇，数据成为科技管理业务发展的重要资源要素，但新技术、新需求、新场景也给数据安全带来新的压力与挑战，泄漏、窃取、滥用风险与日俱增。当前我国正处于实施创新驱动发展战略和建设科技强国的关键时期[2]，开展科技管理数据安全治理是加强我国科技创新能力建设和保障国家安全、科技安全的重要方式和手段。

1 数据安全治理研究现状

科技管理数据质量和应用效果是各国开展科技统筹[3]、科技竞争的内容，其在全球范围内关注度与重要性的日益提高引发了各界对如何高效进行数据治理，最大限度地发掘其内在价值的考虑。加快科技管理数据开发、共享与保护的步伐成为世界各国竞相提升数据治理水平、实现科技强国的重要战略目标[4]。

面对数字化浪潮下数据的井喷式增长引发的乱象，许多国家都从国家安全、社会稳定、企业和个人信息安全层面出台相应的法律法规和管理要求，加强对信息安全，特别是数据安全的风险防范。梅傲等[5]从顶层设计、监管机制、国际合作3个方面出发，梳理日本数据安全治理制度，并阐释日本数据安全治理制度现状。陈毅等[6]探讨了国家安全体系和能力现代化视域下数据安全治理的困境及突围路径。吕明元等[7]从政策、法律、制度、行业等方面分析我国数据安全治理进展，剖析目前在数字基础设施建设、数据保护法律体系、数据安全监管、国家数据主权方面存在的问题，分析了美国、德国、日本、韩国的数据安全治理措施。李雪莹等[8]和王庆德等[9]分别从数据安全治理实践和数据安全治理的行业实践等方面开展研究，提出数据安全治理理念，并从民航、企业、金融、能源和零售5个行业实践展开分析，提出数据安全治理的政策建议。

doi:10.3772/j.issn.2095-915x.2024.06.008

在不同行业的数据安全治理研究中，王玉等[10]对政务数据安全治理体系开展研究探索，提出了适用于我国政务数据安全治理的体系框架，并介绍了相关技术以及项目实践案例。朱洪斌等[11]研究了电力大数据安全治理体系，提出了电力大数据安全治理要求。杨超等[12]对工业互联网数据安全治理实践进行了研究，论述了工业互联网数据安全治理所采取的各种策略、技术和活动，从组织建设、业务流程、规章制度、技术工具等方面介绍了提升数据安全风险应对能力的过程。侯鹏等[13]对金融数据安全治理智能化技术与实践开展了研究。原磊[14]研究了平台企业数据安全治理。在数据治理相关技术工具上，朱佳妮等[15]、程伟等[16]、许杰等[17]和胡剑等[18]，分别研究了区块链、大数据等技术在数据安全治理体系中的应用和创新。

在国家层面发布加强和规范数据安全保护的政策制度，推动数据开放共享[19]，对于服务科技创新、支撑科技决策等方面具有重要意义。盛小平等[20]研究了科学数据开放共享中的数据安全治理，运用规范分析法，梳理与界定科学数据开放共享中的数据安全问题，并从多个维度探究科学数据安全治理措施。面对当前科技创新对科技管理数据的应用和服务需求，尤其是与欧美发达国家相比，我国科技管理数据的治理、管理与应用仍然存在明显不足，对科技管理数据的安全治理研究也较少。随着科技管理业务的发展，在利用数据资产创造价值、辅助决策的同时，对数据质量和稳定性、安全性要求也有所提升。因此在科技安全视角下，为了有效应对严峻的国际信息安全和数据泄漏风险等巨大挑战，需开展数据安全治理体系[21]的探索研究、建设。

2 科技管理数据安全治理的痛点和问题

结合数据安全治理研究现状，以往数据安全建设中沿用自下而上的“堆产品”思维、烟囱式建设，导致数据安全普遍存在管理制度体系不健全、数据资产权责不清晰、数据业务流程不明确等问题挑战。科技管理数据安全治理是科技安全的重要组成部分也是难点之一，对于科技管理数据的利用与安全的平衡，仍然存在“对数据识别不完整”“数据流转无法溯源”“安全与业务难以兼顾”等一系列现实问题。

数据梳理与分类分级实施难度大。数据资产量级不清，在科技管理业务过程中，因其内部业务模块多、数据类别多、分布广的特点，所引发出的数据标准不统一、数据质量有差别等一系列问题亟须解决。在数据分类分级方面[22]，一旦数据梳理不清，很难依据规范开展落地实践的分类分级。

数据安全实施细则尚不完善。科技管理数据会在不同载体和场景环境下流转，数据价值、量级、周期性都会发生动态变化。数据安全建设要求、数据安全风险评估等[23]是基于某个标准，进行相对静态、固化的评估，无法适应数据在不同科技业务场景、不同数据应用目标下的安全要求。

数据流转场景下的高安全需求。随着科技管理业务的发展和科技管理信息系统的不断完善，数据量大、数据调用常态化、数据处理活

动复杂。国产化建设背景下，数据流转在终端、应用、组件等场景发生巨大改变，数据安全性要求也随之增多。数据流转频繁下的数据安全需求[24]已打破传统的网络安全区域划分，传统的边界、主机、系统、终端、数据库的单点防护已无法满足数据安全防护的需求。

数据安全风险态势持续加剧。近年来，数据安全风险事件频发，常规状态下管理、技术层面的安全防护属于静态防护，难以及时根据科技管理业务和合规性的变化动态调整，导致数据安全策略滞后，无法有效应[25]。

3 科技管理数据安全治理框架

结合上述痛点和问题，科技管理数据安全治理亟需与时俱进、体系化开展，以数据为中心、数据安全合规为底线，驱动科技管理数据开展分级分类，落实全生命周期安全防护。通过数据安全运营，持续开展治理效果评估与优化。保障数据在安全可控的情况下应用并发挥价值，实现安全与业务发展兼顾、从管理到技术全方位体系融合，持续提升数据安全保障能力。框架如图 1 所示。

科技管理数据安全治理以数据为中心，一方面是站在数据的视角看数据，当科技管理数据被访问时，从内外层次去区分，分别是数据载体、数据逻辑、数据访问拓扑和数据身份等。另一方面是从流动的视角来看，科技管理数据本身是为科技管理业务服务的，基于业务的需求需要看到数据、互相调用数据，最终数据流动至各个科技管理业务系统，因此相比较网络安全，数据安全风险的暴露面无限大，任何数据会从有序、无序最终到失控，因此数据流动到任何位置，安全防护就应该覆盖到该位置。

在科技管理数据安全治理过程中，需以安全合规为前提。在满足合规性要求的同时，兼顾业务实际发展状况，开展科技管理数据分级分类，并结合数据级别和类型，制定数据全生命周期安全防护策略，一方面动态支撑数据治理安全运营，另一方面结合运营效果，反向监管、动态更新防护策略和技术手段。该框架突出环形治理思路，是互相支撑、互相驱动、互相补充完善的过程。

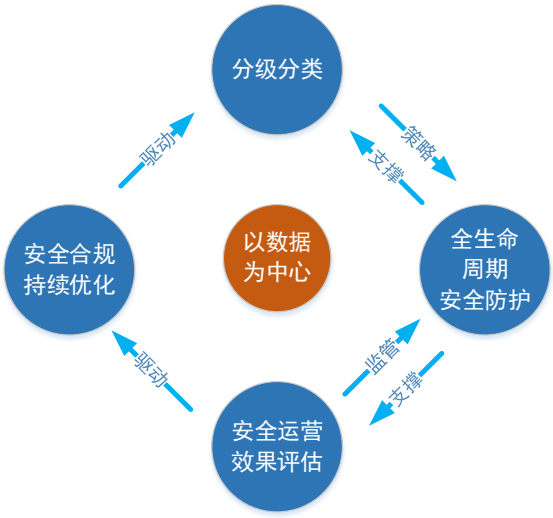

图 1　科技管理数据安全治理框架

4 科技管理数据安全治理实践路径

科技管理数据安全治理的目标是开展治理工作的前进方向，根据上述框架和思路，本文重点开展科技管理数据安全治理实践路径研究，通过厘清数据现状、摸清安全风险现状、开展数据分级分类、规划数据安全建设，进行常态化数据安全防护以及持续有效的监管，逐步实现数据安全全域可管、风险全局可视，以及数据安全可信的目标。实践路径如图 2 所示。

doi:10.3772/j.issn.2095-915x.2024.06.008

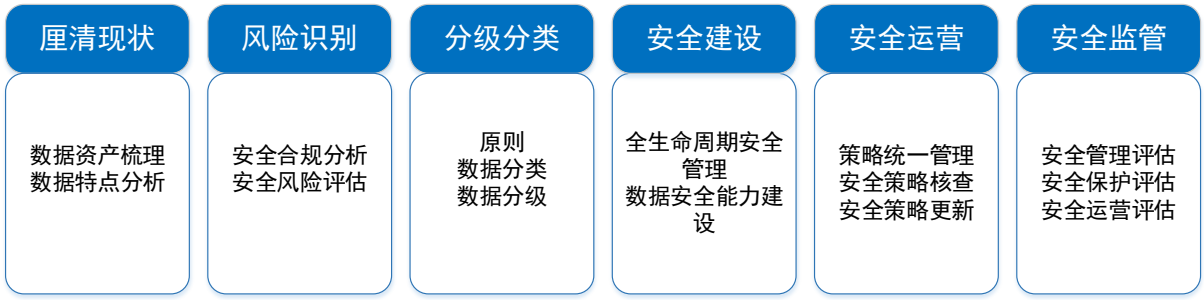

图 2　科技管理数据安全治理实践路径

4.1　厘清现状

4.1.1　数据资产梳理

数据资产梳理是数据安全治理的基础，通过对数据资产的梳理，可以确定数据的类型和量级、数据范围、数据业务场景、数据流转形式、敏感性数据的分布等。通过开展科技管理数据资产梳理，可以进一步明确防护重点，改善决策制定，保证数据准确性，加强数据安全和合规性，提高数据管理效率，以便能最大程度地利用这些数据，提升科技管理服务水平。

4.1.2　科技管理数据特点分析

科技管理数据是实施国家科技创新战略的重要基础性资源。大数据时代，科技创新越来越依赖于科技管理数据的治理与应用。科技管理数据不同于其他数据，具有体量大、影响面广等特点，在进行数据治理过程中，需结合特点针对性开展。科技管理数据是支撑科技发展的基础，因此对科技管理数据进行有效安全治理，本身就是辅助科技创新发展的一种方式。

4.2　风险识别

4.2.1　数据安全合规性分析

科技管理数据安全合规是开展科技管理业务工作的底线要求。近年来，陆续出台的法律持续健全我国数据安全法律法规矩阵[26]，构建了我国网络空间治理和数据保护的基本法。因此对照国家法律法规、政策文件、标准规范，通过数据安全合规性分析，尽可能发现数据安全方面存在的问题，能够更有针对性建设全方位的数据安全治理体系。

4.2.2　数据安全风险评估

科技管理数据安全风险评估，主要围绕数据和数据处理活动，聚焦可能影响数据的保密性、完整性、可用性和数据处理合理性的安全风险，掌握数据安全总体状况，发现数据安全隐患，为后续数据安全治理建设规划提出数据安全管理和技术防护措施建议，提升数据安全防攻击、防破坏、防窃取、防泄露、防滥用能力。

4.3　数据分级分类

4.3.1　原则

结合科技管理数据特点，科技管理数据在开展数据分级分类时，需遵循相关原则。

合法合规原则，遵循有关法律法规和标准规范规定，满足数据安全管理要求[27]。

科学系统化原则，综合考虑科技管理数据敏感性高、关联性强、涉及主体多等特点进行科学系统化的分类。

就高从严原则，数据分级时采用就高不就低的原则进行统一定级，例如某一数据类别包含多个级别的数据项，按照数据项的最高级别对数据进行定级。

适用客观性原则，确保分级结果能够为数据安全管理提供可落地的管控措施，避免过于复杂的分级规划，保证执行的可行性。

自主灵活性原则，根据科技管理业务特性和数据安全管理需要，依据相关分类分级实施指南，确立数据的审核机制，落实数据逐级报批流程。

动态调整原则，数据的类别级别可能因时间变化、管理要求变化而发生改变，因此需要对数据分类分级进行定期审核并及时调整。

4.3.2 数据分类

结合业务场景，科技管理数据按照数据特性可分为科研项目、科研主体、过程管理、科技监督及基础运行五个类别。如表 1 所示。

表 1 数据分类表

数据类型	数据描述
科研项目类数据	各类科技计划（专项、基金等）项目（课题）基本信息、各阶段的申报材料，以及科研成果等。
科研主体类数据	开展科技计划、科技专项项目申报的科研单位、申报人员及科技专家数据，以及开展科技管理的专业机构、管理部门等单位及人员数据。
过程管理类数据	各类科技计划从需求征集、实施方案、管理通知、评审结果、预算安排、监督检查、结题验收结论等过程中产生的管理数据。
科技监督类数据	科技管理工作中科研诚信数据。
基础运行类数据	支撑科技管理工作的系统运行维护及安全保障过程中所产生的数据，包括日志、流量等。

4.3.3 数据分级

结合科技管理数据类别，根据数据在遭受泄露、破坏或非法利用后，对国家安全、科技安全、社会利益、个人及组织的合法权益带来的危害程度和影响，将数据从低到高分成公开、一般、重要、 核心四个级别。如表 2 所示。

表 2 数据分级表

数据级别	数据描述
公开级别	数据完全公开，可被公众获知、使用。数据被泄露、破坏或非法利用后，对国家安全、科技安全、社会利益、个人及组织的合法权益带来轻微影响。
一般级别	数据有条件公开，可被认证后的对象获知、使用。数据被泄露、破坏或非法利用后，对国家安全、科技安全、社会利益、个人及组织的合法权益带来轻微危害。
重要级别	数据不对外公开，可被科技管理单位获知、使用。数据被泄露、破坏或非法利用后，对个人及组织的合法权益带来严重危害，对国家安全、科技安全、社会利益带来一定危害。
核心级别	数据不对外公开，可被科技管理政府机构获知、使用。数据被泄露、破坏或非法利用后，对个人及组织的合法权益带来特别严重危害，对国家安全、科技安全、社会利益带来严重危害。

4.4 数据安全建设

数据作为资产，具备完整生命周期，在科技管理数据全生命周期各个环节均存在数据安全风险。为了更好地应对数据安全风险，需从管理和技术两方面入手，实现对数据安全使用和全生命周期管理 [28]，数据安全将一方面服务科技管理业务，保障数据的安全使用与共享，另一方面满足数据安全合规性要求，达成“进

doi:10.3772/j.issn.2095-915x.2024.06.008

不来、拿不来、看不懂、改不了、走不脱”的安全管理目标。科技管理业务涵盖项目申报、立项、过程管理、验收管理等多个阶段，每个阶段都有其独有的业务服务场景，科技管理数据就是这些不同的业务服务过程中产生的全部数据，既包括科技管理和服务业务数据，也包括系统运行维护数据。科技管理数据安全建设技术框架如图 3 所示。

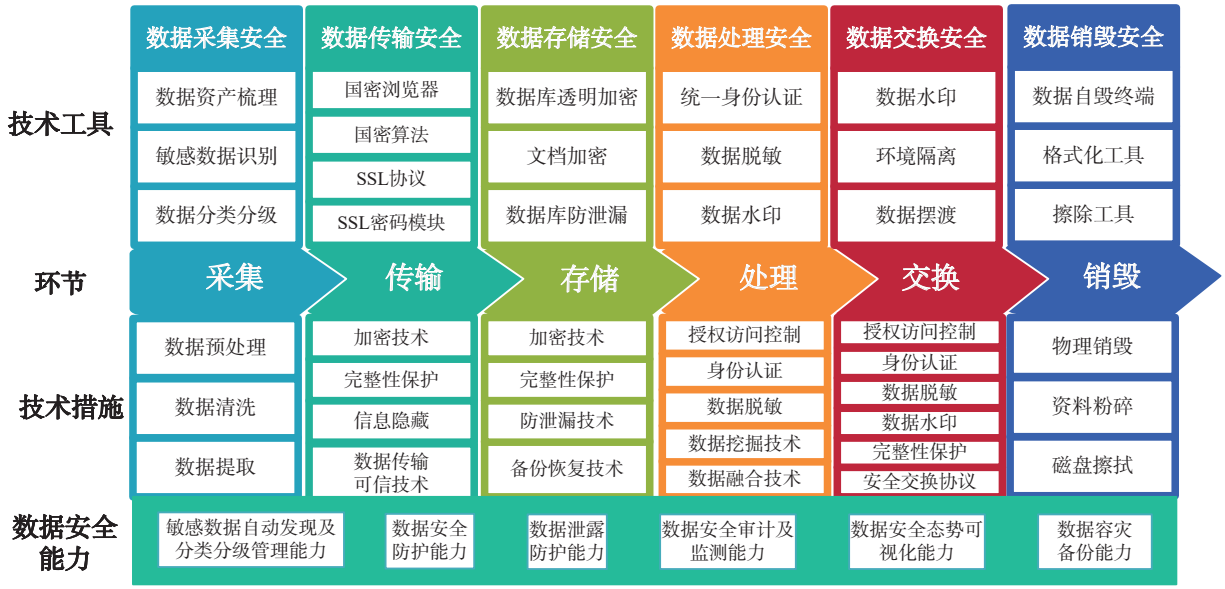

图 3　科技管理数据安全技术建设框架

4.4.1　数据全生命周期管理

按照数据产生的环节，科技管理数据全生命周期包括收集、传输、存储、处理、交换、销毁六个阶段，以数据保密性、完整性、可用性为核心目标，秉持用户授权、最小够用、专事专用、全程防护原则，结合科技管理数据分级分类结果，对各个环节落实相关的安全管理措施和技术防护措施。

（1）采集阶段。采集指获取数据的过程，包括但不限于科研单位在线填报、外部应用对接共享、公开数据获取等方式。针对科技管理数据采集阶段可能面临的非授权采集、数据分类分级不清、敏感数据识别不清和缺乏细粒度的访问控制等风险，技术上应采取传统的数据安全防护措施，包括数据传输加密、文档加密技术、数据访问控制、安全认证等。在管理层面，应遵循合法合规、正当必要的原则，在规定的职责和范围内开展数据的采集活动，不收集与科技管理业务无关的信息。

（2）传输阶段。传输指按照一定的规程，实现点对点之间数据的安全传输和交换的通信过程。科技管理数据传输阶段主要指数据在科研用户和科技管理部门之间，或科技管理业务平台系统间传输的过程。数据传输阶段需采用符合国密算法的密码技术构建安全的传输通道，确保传输过程中的保密性和完整性。通过身份认证、权限限制等技术措施实现传输过程中的访问控制，保证传输的节点安全；使用成熟的安全传输协议，保证传输的通道安全。

（3）存储阶段。存储是指通过一定的计算

机技术将数据存储在服务器、存储等特定的介质中，包括结构化、非结构化存储形式。科技管理数据存储面临数据分类分级不清、重要敏感数据的安全管理不足、缺乏细颗粒度访问控制等问题。主要技术措施包括对数据进行识别和分类分级、对重要数据存储提供加密手段、对存储在平台中的敏感数据提供更强细粒度的访问控制能力。结合数据分级分类结果，对不同类别和级别的数据采取相应的安全存储措施。必要情况下，建立科技管理数据异地备份和容灾管理机制，同时采用必要的冗余策略和管理措施，确保数据备份与恢复操作过程规范，保障备份数据的有效性、可用性。

（4）处理阶段。处理指对科技管理数据进行清洗、转换、整合、服务的过程。在处理过程中，严格遵循最小必要原则，对于进行数据处理的操作人员，应当授予且仅授予必须的数据访问和操作权限，降低数据泄露的风险。数据处理时面临的安全风险包括数据缺乏访问控制、数据结果的访问接口缺乏控制、数据处理结果缺乏敏感数据保护措施、缺乏安全审计和数据溯源的能力，应加强数据细粒度访问控制、敏感数据标记访问控制、数据脱敏、处理过程日志记录以及数据追踪溯源技术的应用。在开展敏感数据处理时，建立安全隔离的数据加工处理环境，确保在数据安全可控的基础上配合特殊科技管理业务的顺利开展。同时，针对数据展示场景或需求，应建立敏感数据去标识化规范，使用数据脱敏、数据加密等技术对数据进行去标识化处理，降低数据泄露安全风险。

（5）交换阶段。数据交换主要是指数据在系统平台中各节点之间、各组件之间以及从数据平台和其他外部系统之间交换的过程。针对可能存在泄露问题，应提供数据加密能力，保证数据交换时的安全，并提供相关的安全审计能力。当进行线下交换时，应使用符合数据安全管理要求的介质对数据进行保存，并做好介质管理，确保专事专用、及时回收。

（6）销毁阶段。销毁指删除科技管理数据及其相关备份副本的过程。当进行销毁时，应通过有效技术手段，保证数据被完整、有效删除，且不可恢复。如涉及存储介质，应采用不可恢复的方式（如消磁、焚烧、粉碎等）对介质进行销毁处理。销毁过程应进行全程监督与控制，对销毁介质的登记、审批、交接、销毁执行等过程进行监督，并保留销毁过程有关记录。

4.4.2 数据安全能力建设

考虑到不同数据安全技术可能复用于科技管理数据全生命周期各阶段，依照整体规划，统一部署的原则，科技管理数据全生命周期安全管理将从安全措施可实现的角度，规划五大数据安全能力建设。

（1）敏感数据自动发现及分类分级管理能力建设。规划建立科技管理业务敏感数据特征库，依据法律法规及组织规范，建立敏感特征与级别类别的关联，形成敏感数据自动识别能力，并对接数据自动分类分级。

（2）数据泄露防护能力建设。规划建设敏感数据泄露防护能力，实现对科技管理业务网络、终端敏感数据的监测、识别、分析、审计和阻断控制，通过在重要网络节点处（如内网与外网节点、上联区域中心节点）部署数据泄露防护工具，通过预制策略与外发的敏感数据匹配，实现敏感数据外发监测。

doi:10.3772/j.issn.2095-915x.2024.06.008

（3）数据安全审计及监测能力建设。维护敏感数据全生命周期各环节日志，并实现数据操作审计，规划建立全周期化的数据流动审计能力，监督监测用户行为，防范敏感数据的违规使用，该能力将覆盖数据的采集、使用、共享、使用等阶段 [29]。

（4）数据安全态势可视化能力建设。从科技管理业务、平台、用户和数据资源等角度，规划建设科技管理数据可视化能力，呈现数据全生命周期的安全风险态势。通过敏感数据日志信息审计能力，综合记录用户行为的情况，形成数据安全感知全景，评估数据安全风险。

（5）数据容灾备份能力建设。科技管理数据应具备数据备份容灾功能 [30]，在本地备份的基础上，需具备跨数据中心、建立异地容灾机制。

4.5 科技管理数据安全运营

开展科技管理数据安全运营 [31]，全局管控数据资产、身份、权限等，结合数据分类分级结果，实现安全策略的统一管理及下发、安全风险监测、安全威胁分析、安全事件处置，达到对科技管理数据全生命周期的统一、全局的管理和掌握、数据可视化、数据风险可控的目标。例如在数据安全策略统一管理层面，统一管理数据安全策略，集中展示各个数据安全组件状态，对各个数据安全组件涉及的识别类及防护类安全策略进行统一配置，实现安全策略集中管理。在数据安全策略核查方面，制定核查策略模板，基于模板，检验、核查数据安全策略设定的完备性及执行效果。此外，基于对策略、事件、数据综合分析，全局化分析安全态势，提升科技管理数据安全运营能力。

4.6 科技管理数据安全治理监管

数据安全治理监管 [32] 主要是对科技管理数据安全保障状况定期开展合规性评估，从而对数据安全保护的管理制度、安全防护措施、数据运营等方面进行有效监管。数据安全治理监管主要从安全管理、数据安全保护、数据安全运营三个方面开展评估工作。在安全管理评估层面，包括组织架构评估和管理制度评估两个方面，其中组织架构评估是对组织架构的设定完备性、岗位工作职责与分工的明确性方面进行评估；管理制度评估是指从技术管理、人员管理、流程管理多个维度对管理制度进行评估。在数据安全保护评估层面，包括数据分类分级管理与数据全生命周期管理评估两个方面，其中数据分类分级管理评估是对数据分类分级目标和原则、涉及的数据内容、分级方法和具体要求、分级结果等内容进行评估；数据全生命周期管理评估是围绕数据处理活动涉及的采集、传输、存储、处理、交换、销毁等环节的数据安全保护措施的合规性、完备性进行评估。在数据安全运营评估层面，包括从事前的安全访问控制，事中的安全监测、应急响应与事件处置，事后的安全审计等维度对数据安全运营的效果进行评估。

5 总结与展望

在科技竞争背景下，科技管理数据治理是数据价值发挥、支撑科技决策、维护科技安全的基础性工作。在数据要素时代，随着科技管理数据价值的不断提升，科技管理数据治理就是以释放数据价值为核心目标，旨在提升数据

质量，保障数据安全，进一步维护科技安全。科技管理数据安全治理作为保障国家科技创新能力和科技安全的重要组成部分，面临着前所未有的机遇与挑战。随着大数据时代的到来，科技管理数据不仅成为推动科技进步的关键资源，同时也伴随着潜在的安全隐患。当前，虽然我国已出台多项法律法规强化数据安全保护，不少学者也在研究、实践中探索了一系列治理措施，但数据安全治理依然存在诸多瓶颈，如管理制度不完善、数据安全建设不到位、数据资产权责不明晰、数据流转缺乏有效监管等。新形势下，科技管理数据治理应充分认识科技管理改革新形势和科技管理数据安全合规治理的新变化新需求，坚持规范引领，从多维度、多角度、多层次作出科技管理数据安全战略规划，坚持数据安全保障与业务服务并重的基本立场，秉承合规优先、逐层推进原则，构建科学、合理、有效的数据安全治理体系，从而积极应对数据安全治理面临的困难挑战，实现平稳、有序推进科技管理数据安全治理与业务发展。

展望未来，在科技管理数据安全治理实践路径下，结合框架各部分内容，需进一步提高智能化与自动化水平，借助人工智能和机器学习等先进技术，实现数据的自动发现、分类分级及异常检测，从而提升治理效能。同时，建立统一的标准与规范，促进不同组织间的数据互信，减少安全风险。在数据隐私保护方面，平衡数据利用和个人隐私的重要性将日益凸显，促使研发更多专注于隐私保护的技术方案。此外，数据安全治理不仅是技术层面的问题，更是管理层面的任务。因此，需制定科技管理数据安全保障的战略规划和顶层设计，不断完善相关法律法规体系；加强科技管理数据安全治理宣传教育，培养专业的人才队伍，不断提升全民的数据安全意识。只有通过政府、企业及社会各界的共同努力，才能构建起一个既安全又高效的科技管理数据安全生态系统，为我国的科技创新提供坚实的数据保障。

参 考 文 献

[1] 糟玉庆 , 赵捧未 , 尹丽英 , 等 . 面向政府宏观科技决策的科技管理数据服务模式构建 [J]. 科技管理研究 , 2023, 43(2): 167-176.
[2] 李品 . 统筹科技发展与科技安全的情报体系框架研究 [J]. 情报学报 , 2024, 43(3): 357-368.
[3] 孙婕 , 沈恒超 . 美日宏观科技统筹协调机制及启示 [J]. 世界科技研究与发展 , 2022, 44(4): 504-517.
[4] CHAOHUI M A, RUIHUA N, HAOXIANG T, et al. Research on data schema and security in data governance[J]. Big Data Research, 2016(3): 89-101.
[5] 梅傲 , 李坤佳 . 日本数据安全治理制度述评及其启示 [J]. 情报理论与实践 , 2023, 46(7): 195-200.
[6] 陈毅 , 华蕊 . 国家安全体系和能力现代化视域下数据安全治理的困境及突围路径 [J]. 学习与探索 , 2023(12): 41-47.
[7] 吕明元 , 弓亚男 . 我国数据安全治理发展趋势、问题与国外数据安全治理经验借鉴 [J]. 科技管理研究 , 2023, 43(2): 21-27.
[8] 李雪莹 , 张锐卿 , 杨波 , 等 . 数据安全治理实践 [J]. 信息安全研究 , 2022, 8(11): 1069-1078.
[9] 王庆德 , 吕欣 , 王慧钧 , 等 . 数据安全治理的行业实践研究 [J]. 信息安全研究 , 2022, 8(4): 333-339.
[10] 王玉 , 安鹏 , 栗文科 , 等 . 政务数据安全治理体系研究与实践 [J]. 信息安全研究 , 2023, 9(9): 900-907.
[11] 朱洪斌 , 安龙 , 杨铭辰 . 电力大数据安全治理体系研究 [J]. 电信科学 , 2019, 35(11): 140-145.
[12] 杨超 , 郭刚 , 叶林佶 , 等 . 工业互联网数据安全治理实践 [J]. 信息安全与通信保密 , 2022(9): 18-27.
[13] 侯鹏 , 李智鑫 , 张飞 , 等 . 金融数据安全治理智能化技术与实践 [J]. 网络与信息安全学报 , 2023, 9(3): 174-187.

doi:10.3772/j.issn.2095-915x.2024.06.008

[14] 原磊 . 平台企业数据安全治理研究 [J]. 世界社会科学 , 2024(1): 103-118.
[15] 朱佳妮 , 赵丽梅 . 基于主权区块链的科学数据安全治理研究 [J]. 科技管理研究 , 2023, 43(9): 171-176.
[16] 程伟 , 马成 , 凌捷 . 大数据技术在数据安全治理中的应用 [J]. 大数据 , 2023, 9(6): 3-14.
[17] 许杰 , 张锋军 , 陈捷 , 等 . 面向大数据环境下的数据安全治理技术 [J]. 通信技术 , 2021, 54(12): 2659-2665.
[18] 胡剑 , 戚湧 . 基于区块链跨链机制的政务数据安全治理体系研究 [J]. 现代情报 , 2023, 43(9): 85-97.
[19] 陈媛媛 , 赵晴 . 数据利他 : 全球治理观下基于公共利益的数据共享机制 [J]. 图书馆论坛 , 2023, 43(5): 71-80.
[20] 盛小平 , 郭道胜 . 科学数据开放共享中的数据安全治理研究 [J]. 图书情报工作 , 2020, 64(22): 25-36.
[21] 李晓东 , 董少平 , 吴菁 . 总体国家安全观视域下数据安全治理的路径选择 [J]. 中国科技论坛 , 2024(2): 147-157, 167.
[22] 徐婧欣 , 郭丰 , 苏鹏 . 数据分类分级政策演化研究 [J]. 图书馆 , 2023(2): 48-55.
[23] 陈永刚 , 赵增振 , 陈岚 . 政务数据安全合规评估要点及实践 [J]. 信息安全研究 , 2022, 8(11): 1050-1054.
[24] ZHOU F, HUANG J. Cybersecurity data breaches and internal control[J]. International Review of Financial Analysis, 2024(93): 67-75.
[25] 程啸 . 论个人信息权益 [J]. 华东政法大学学报 , 2023, 26(1): 6-21.
[26] 徐玉梅 , 王欣宇 . 我国重要数据安全法律规制的现实路径 —— 基于国家安全视角 [J]. 学术交流 , 2022(5): 37-48.
[27] 马费成 , 熊思玥 , 孙玉姣 , 等 . 数据分类分级确权对数据要素价值实现的影响 [J]. 信息资源管理学报 , 2024, 14(1): 4-12.
[28] 段尧清 , 姜慧 , 汤弘昊 . 政府开放数据全生命周期 : 概念、模型与结构 —— 系统论视角 [J]. 情报理论与实践 , 2019, 42(5): 35-40.
[29] 戴荣峰 , 陶晓英 , 于萌 , 等 . 大数据驱动下的数据全生命周期安全监测方法 [J]. 信息安全研究 , 2023, 9(12): 1226-1232.
[30] CHAUDHARY J, VYAS V, SAXENA M. Backup and Restore Strategies for Medical Image Database Using NoSQL[J]. Communication, Software and Networks, 2023(10): 161-171.
[31] 刘志勇 , 何忠江 , 阮宜龙 , 等 . 大数据安全特征与运营实践 [J]. 电信科学 , 2021, 37(5): 160-169.
[32] 梅傲 , 陈子文 . 总体国家安全观视域下我国数据安全监管的制度构建 [J]. 电子政务 , 2023(11): 104-115.