# 关于开展数据合规审计工作的探讨

晏维龙　童瑞连　钱　钢　叶　祥

数据资产，作为经济社会数字化转型进程中的新兴资产类型，正日益成为推动数字中国建设和加快数字经济发展的重要战略资源。近些年，我国先后出台了《中华人民共和国网络安全法》《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》，即“数据三法”，奠定了数据合规在法律层面的三大基石。其他中央层面的政策文件包括：2022年12月19日中共中央、国务院出台的《关于构建数据基础制度更好发挥数据要素作用的意见》（以下简称“数据二十条”）；2023年8月3日国家互联网信息办公室向社会公开征求意见的《个人信息保护合规审计管理办法（征求意见稿）》及配套的《个人信息保护合规审计参考要点》；2023年8月21日财政部对外发布的《企业数据资源相关会计处理暂行规定》，从推动规范企业执行会计准则、准确反映数据相关业务和经济实质方面做出了顶层设计；为规范和加强数据资产管理，更好推动数字经济发展，财政部近期还制定印发了《关于加强数据资产管理的指导意见》，要求企业应当按照企业会计准则相关规定，根据数据资源的持有目的、形成方式、业务模式，以及与数据资源有关的经济利益的预期消耗方式等，对数据资源相关交易和事项进行会计确认、计量和报告。

一系列数据相关法律法规和政策文件的出台，客观要求数据合规成为政府、企事业单位的法定义务和社会责任，而数据合规审计作为捍卫国家数据主权、保障发展数据生产力、保护个人信息的一道重要防线，成为监督履行这一责任与义务、规避法律风险的关键工具。

## 数据合规审计的现实价值

修订后的审计法在审计机关权限方面有了较大拓展。主要体现在审计机关有权要求被审计单位提供并检查被审计单位财政收支、财务收支电子数据及其管理系统，查询被审计单位在金融机构的账户、以个人名义在金融机构的存款，封存有关资料以及违反国家规定取得的资产。开展数据合规审计是审计机构依法维护国家利益、保护国家核心数据、捍卫国家数据主权的需要。

数据正成为国家之间竞争的战略工具，所谓数据主权是指网络空间中的国家主权，体现了国家控制数据权的主体地位。维护数据安全就是维护国家安全，捍卫数据主权就是捍卫国家主权。我国颁布实施的“数据三法”明确要求政府、企事业单位加强数据管理、数据治理、建立健全数据合规体系，对监管部门履行职责、开展数据监管，为政府、企事业单位合法处理数据，规范数据跨境传输和保障个人数据隐私等，提供了充分的法律依据。但目前“数据三法”落地施行面临诸多挑战，审计机关要在全新的数据要素领域持续推进国家治理体系和治理能力现代化，建议需要以数据合规为抓手，将“关系国家安全、国民经济命脉”的数据治理情况和算法责任纳入审计范围，通过数据合规审计检查国家相关政策落实执行的效果，评价重点领域和行业的数据安全管理制度是否健全和执行到位；依法履行监督职责实现审计监督全覆盖，对于审计发现的问题可以及时反馈相关决策部门，推动政策落实和改革创新。

数据合规作为数字治理生态的基础，是数字化发展的前提。以数据合规为主题开展“经济体检”工作，发挥审计监督作用是数字经济时代下维护国家经济秩序、保障经济社会健康发展、加快建设数字中国的重要手段。建设数字中国是推进中国式现代化的重要引擎，是构筑国家竞争新优势的有力支撑。中共中央、国务院发布的《数字中国建设整体布局规划》确定了到2025年“数字治理体系更加完善”的建设目标，并明确要求“建设公平规范的数字治理生态”。在建设网络强国和数字中国进程中，伴随大量关键数据的汇集、传输和存储，针对数据的合规风险控制融合了多主体多方面的需求，数据合规审计可以维护市场秩序、维护数据产品的流通交易，从而保障市场各主体的权益，推动构建新发展格局、服务数字经济的健康发展、加快建设数字中国。

个人信息直接关系到人民群众的隐私、财产和生命安全，个人信息保护对维护广大人民群众网络空间合法权益具有重要意义，因此数据合规审计变得尤为重要，是保护个人隐私安全、强化道德责任、推动法治中国建设的必要举措。数据合规审计确保组织在处理和存储个人数据时应遵循相关法律法规和标准，以防范数据泄露、滥用、盗窃等风险；数据合规审计强调组织特别是互联网企业、数据服务提供商，应当依法管理和运用数据，确保数据处理过程的合法、透明。通过合规审计，强化法治观念，促进政府、企事业单位更好地遵守法律，维护社会公平和正义，从而达到保护个人隐私信息的目的。

此外，数据合规审计还有助于提高数据伦理意识、强化社会道德责任，“数据三法”鼓励政府、企事业单位审慎考虑数据的收集、使用和共享方式，确保数据用于公共利益和社会责任，而不是滥用或损害个人权益。鉴于道德与法治双重约束，数据合规审计不仅有助于保护个人隐私、避免数据泄露，增强公众对数字世界的信任感，还有助于强化法治观念、促进数据伦理、降低法律风险、提升组织声誉，从而推动数字时代的可持续发展。

## 数据合规审计的实施框架

### （一）数据合规审计的特殊性

1. 审计目标

个人信息保护法将合规审计分为自主审计和强制审计两种情形，前者主要是规定个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。后者则是指履行个人信息保护职责的监管部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。两者的合规审计目标存在较大差异。

国家互联网信息办公室于2021年11月14日发布《网络数据安全管理条例（征求意见稿）》。与个人信息保护法一脉相承，该管理条例第五十三条规定大型互联网平台运营者应当通过委托第三方审计方式，每年对平台数据安全情况、平台规则和自身承诺的执行情况、个人信息保护情况、数据开发利用情况等进行年度审计，并披露审计结果。第五十八条规定国家建立数据安全审计制度。数据处理者应当委托数据安全审计专业机构定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。主管、监管部门组织开展对重要数据处理活动的审计，重点审计数据处理者履行法律、行政法规规定的义务等情况。相较于个人信息保护法中的自主审计，此处的“自主审计”明确为外部审计；强制审计则是主管、监管部门组织开展的对重要数据处理活动的审计，主要聚焦于重要数据处理活动的安全。从法条也可以看出，管理条例将数据合规审计的对象从“个人信息”扩大到“数据”，尤其“重要数据”更是主管、监管部门的审计重点。

2. 审计对象

与其他审计类型的最大不同在于：数据合规审计的对象是广义上的数据，既有数据本身，也有数据环境（算法模型、信息系统和网络空间），是数据产品、数据技术与数据服务的融合。同时，数据合规审计超越了法律领域传统的“合法、合规”义务范畴，是数据要素下的传统审计、信息技术与法律融合的时代产物。除了与数据相关法律规定的数据合规各主体的法定义务外，政府、企事业单位还有道德义务来维护数据的合规性和隐私权，因此数据合规审计作为保障发展数据生产力、保护个人信息的关键工具，其要素的构成具有特殊性。

3. 审计要素框架

数据合规审计的三方关系人以数据要素为核心，涉及国家核心数据时还关系到国家安全、国民经济命脉、重要民生和重大公共利益。鉴于数据合规审计对象的特殊性，结合大数据审计方法论，构建数据合规审计的要素框架（见下页图1）。

数据合规审计计划阶段的主要任务包括：在委托人确定审计项目的审计模式即自主审计或强制审计的前提下，审计主体明确被审计单位应承担的数据合规与义务，制定审计计划、审计工作方案，主要包括审计目标、范围、内容和重点，以及主要依据的法律法规（包括国内法和国际法）、行业监管、社会道德等。

数据合规审计准备阶段的主要任务包括：根据审计计划明确审计任务，组成审计组；开展必要业务培训；进行审前调查，收集相关数据资料；针对以下几个方面开展分析，一是数据本身即数据的采集、传输、存储，二是数据环境即信息系统、网络环境（主机/基础设施/网络边界），三是数据应用即算法分析与处理、数据服务、个人信息保护，四是数据跨境与交易；在此基础上编制审计实施方案。

数据合规审计实施阶段的主要任务包括：审计主体发出审计通知书或持书直接实施审计；根据被审计单位提供的数据资料和采集的必要外部数据资料，运用大数据审计方法交叉验证开展审计，分散核实发现的审计疑点，编制审计取证单进行审计取证，编制审计工作底稿；开展证据处理等其他程序性工作。在此阶段特定的审计技术与工具的运用，体现了数据合规审计与其他审计类型的区别，如针对数据生命周期内数据相关操作的审计可以使用日志挖掘技术，鉴证数据资产可以使用元数据技术等。

数据合规审计报告阶段的主要任务包括：汇集审计底稿，经系统研究，依据有关法律法规和标准作出审计评价，形成审计报告并征求被审计单位意见，围绕数据本身、数据环境、数据应用等方面向委托人提出改革与管理建议，对被审计单位提出审计整改要求，如通过持续整改提升数据治理水平；针对个人信息保护法中要求的，大型互联网平台运营者应定期发布个人信息保护社会责任报告，等等。

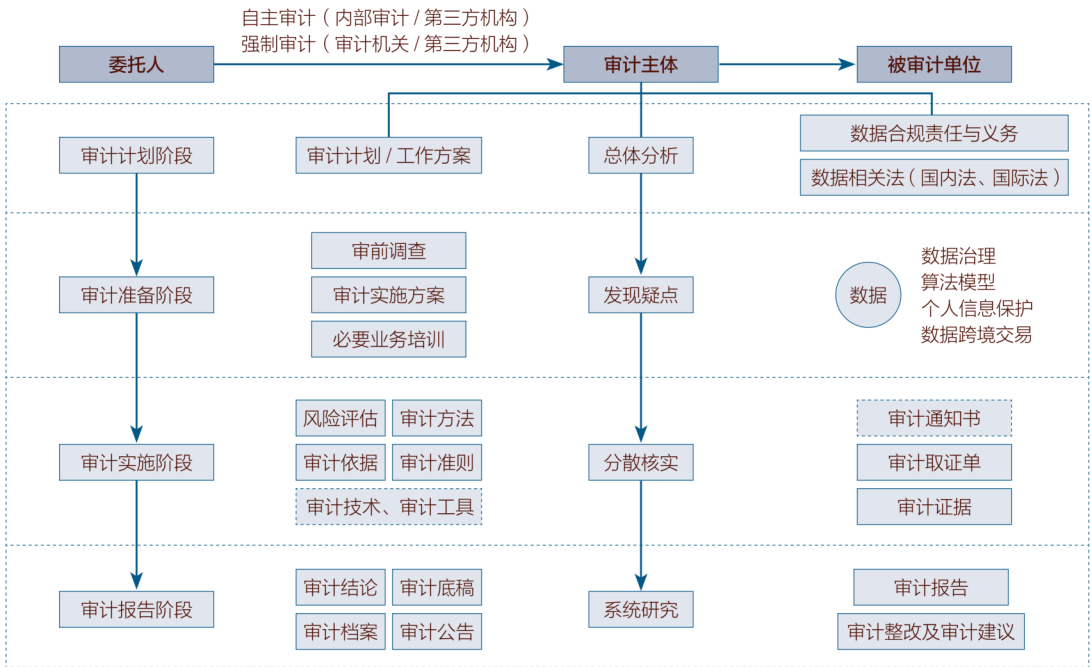


**图1　数据合规审计要素框架**

（二）数据合规审计的重点内容

1. 数据治理审计

数据安全法规定从中央和地方两个层面规范建设数据分类分级制度，要求各地区、各部门建立重要数据具体目录，将需要重点保护的数据列入目录中。这为健全数据治理奠定了基础。从审计视角看，数据治理审计是数据合规审计中的一个关键领域，涵盖了对组织内部数据治理流程、政策和实践的审计，也是摸查组织数据资产情况的重要途径。

数据治理审计以数据本身和数据环境为核心，主要关注四个方面。一是数据治理框架审计。审计人员将评估组织是否拥有明确的数据治理框架，包括数据所有权、数据质量标准、数据分类、数据访问控制、数据备份和恢复策略等，通过审计确定组织是否遵循相关法律法规，以及适当的数据治理技术标准和最佳实践。二是数据访问和权限审计。审计人员将审查组织的数据访问和权限控制机制，以确定是否只有授权人员能够访问敏感数据，包括审查用户权限、身份验证措施和访问日志，其中访问日志中要明确记录数据的采集和传输过程。三是数据质量审计。包括对数据质量的评估，审计人员主要检查数据采集、存储和处理过程，审查数据目录建立情况，以确定数据是否准确、完整和可靠，是否符合相关法律的合法性要求，并审查纠错措施和数据质量改进计划。四是数据环境审计。审计人员要从数据的物理环境（主机和基础设施）开始，针对信息系统可从一般控制审计和应用控制审计入手，针对安全防护边界和安全计算环境，重点审查数据是否存在未经授权流出或超出授权另作他用的情况。

2. 算法模型审计

算法模型是数据应用与服务的基础，算法在数据处理转化过程中扮演的角色是如此重要，从一定程度而言，数据经济的实质即“算法定义经济”。虽然大数据、算法和算力的紧密结合给经济社会发展带来了颠覆性的影响，使得人类社会逐渐步入数字经济时代，但也带来了诸多风险，主要有：一是算法模型的滥用。一些互联网平台和技术公司利用算法模型进行不公平定价、价格歧视等“杀熟”行为侵犯消费者权益，还有通过算法进行舆论引导、信息过滤侵犯公民知情权。二是算法垄断。大型互联网平台通过收集海量数据，利用算法获得更准确的分析，形成“富者越富”的算法垄断，加剧社会财富的分配不公。三是算法资本化。算法本应作为工具服务于社会公平，但有时被资本利益所左右，导致算法存在偏见、缺乏包容性等问题。四是损害公共利益。上述问题综合起来都可能导致公共利益受到损害。

数字经济时代催生针对算法进行监管审计的需求。我国关于算法模型的要求分散在“数据三法”、《新

一代人工智能伦理规范》《互联网信息服务算法推荐管理规定》等法律规范中。不同于传统的范式与手段，针对算法模型进行监管审计存在诸多问题与挑战。在审计算法模型时，不仅要关注算法模型的合规性、安全性、风险管理和透明度，还应考虑算法模型的效益评估，包括其对社会的影响、可维护性以及成本效益分析。算法模型对社会的影响包括是否存在歧视性、不平等待遇等问题，是否满足社会道德和价值观，特别是互联网平台规则的合法合规与公平公正性；算法模型的可维护性包括是否存在依赖特定个人或团队、是否容易维护和更新等问题，特别是能否自主可控而不受境外先进技术“卡脖子”，从而确保算法模型的合法合规、安全可信、风险可控、透明可解释，有助于维护国家和社会的利益，促进算法模型的健康发展。

3. 个人信息保护合规审计

个人信息保护合规审计，是指对个人信息处理者的个人信息处理活动是否遵守法律、行政法规的情况进行审查和评价的监督活动。为指导、规范个人信息保护合规审计活动，根据个人信息保护法，国家互联网信息办公室起草了《个人信息保护合规审计管理办法（征求意见稿）》，以个人信息保护为抓手开展数据合规性审查和评价，将政府、企业、个人关联起来，在“个人信息处理者”这一概念下归拢并制定了相关审计准则：如规定处理超过100万人个人信息的个人信息处理者至少1年开展1次合规审计、其他未达100万人的个人信息处理者至少每二年开展1次合规审计；个人信息处理者处理个人信息应当履行告知义务；个人信息处理者利用自动化决策处理个人信息的，审计时应当重点评价自动化决策的透明度和结果的公平性、公正性。数据合规审计由此分为两类：一类是定期自主审计，即个人信息处理者定期对其处理个人信息遵守法律、行政法规的情况进行合规审计；另一类是专项强制审计，即履行个人信息保护职责的监管部门在一定情形下，可要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。此外，该征求意见稿涉及事前对算法模型进行科技伦理审查，采取必要措施对算法和参数模型进行保护，对个人信息处理、标签管理、模型训练等自动化决策过程中的人工操作进行记录，防范人为恶意操纵自动化决策信息和结果。在个人信息保护合规审计中，审计以独立的第三方视角，依据法律、行政法规等对个人信息处理者的相关活动进行监督和评价。

## 数据合规审计的实现路径

### （一）完善数据合规责任与义务模型

数据安全法规定国家建立数据分类分级保护制度，该法落实的首要问题就是数据分类分级管理。网络安全法第三十四条指出，除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；定期对从业人员进行网络安全教育、技术培训和技能考核；对重要系统和数据库进行容灾备份；制定网络安全事件应急预案，并定期进行演练；法律、行政法规规定的其他义务。因此，不同类型的数据应明确其合规义务的责任主体，如个人信息保护法中个人信息的合规义务主体是个人信息处理者，关键信息基础设施运营者要承担前述的数据合规义务等。基于此，从合规管理体系、合规风险、数据治理、算法模型、个人信息保护和保障与应急六个方面，区分义务与道德维度，给出数据合规责任与义务矩阵架构（见表1）。

从数据收集、存储、使用、传输、共享、销毁全生命周期出发，审计机构应建立全过程的数据合规审计模型，将不同环节对应不同的合规审计重点，不断完善数据合规责任与义务矩阵架构，包括以下方向：针对数据处理者开展数据安全和合规风险评估，强化风险评估和预警机制，发现问题主动报告监管部门，对重大风险制定改进措施；根据数据的敏感性和重要性，明确数据跨境合规要求，区分本地化数据和可跨境传输数据，并对后者制定严格的跨境合规规范；利用数据进行自动化决策的，应加强对自动化决策的管控，建立算法审查机制，保证决策的公平性、透明度和可解释性；建立并公开数据合规验收标准，完善数据合规考核和问责机制并将其纳入对数据合规工作的考核体系，对责任人进行问责；建立第三方评估认证机制、推行企业数据合规公示制度，引入独立第三方对数据合规状况进行评估认证，提升合规水平，要求企业定期公布合规报告接受社会监督。

### （二）提高审计领域的大数据治理水平

审计领域大数据的来源包括外部的公共资源数据、审计基础数据、审计业务数据、审计知识和审计共享数据。在应对监管要求与满足经济发展的双重挑战下，审计可以以独立、客观的视角对组织的数据治理范畴内各项工作进行检查和评价，促进对组织数据资产的重视与积累，促进组织数据治理体系的完善。同时，通过创新审计技术，实现审计数据资产应用的系统化、多元化、全面化、智慧化的价值提升。审计大数据治理既是顶层策略和管理体系，也是技术体系，涵盖战略、组织机构、文化、方法、制度、流程、技术和工具等多个层面的内容，还涉及元数据管理、主数据管理、数据标准管理、数据质量

**表1 数据合规责任与义务矩阵架构**

| 大类 | 小类 | 应做类义务 | 禁止类义务 | 契约类义务 | 社会与道德责任 |
|---|---|---|---|---|---|
| 合规管理体系的建立、运行 | 制度建立 | | | | |
| | 合规管理 | | | | |
| | 合规运营 | | | | |
| 合规风险的识别、评估 | 技术风险 | | | | |
| | 业务风险 | | | | |
| | 管理风险 | | | | |
| | 工具风险 | | | | |
| 数据治理合规 | 数据全生命周期 | | | | |
| | 数据资产建设 | | | | |
| | 数据质量 | | | | |
| | 数据安全 | | | | |
| 算法模型合规 | 事前安全评估 | | | | |
| | 自动化决策存在的缺陷 | | | | |
| | 事前科技伦理审查 | | | | |
| | 对算法和参数模型必要保护措施 | | | | |
| 个人信息保护合规 | 合法性基础条件 | | | | |
| | 个人信息处理规则 | | | | |
| | 内部管理制度和操作规程 | | | | |
| | 大型互联网平台规则 | | | | |
| | 向境外提供 | | | | |
| | 个人信息安全事件处理 | | | | |
| 保障与应急 | 合规保障 | | | | |
| | 技术措施 | | | | |
| | 风险应对措施 | | | | |
| | 补救措施 | | | | |

管理、数据生命周期管理、数据组织、数据安全治理和数据服务、数据集成与共享等。审计领域大数据治理不是对所有数据的无偏差治理，而是注重数据之间的勾稽关系、注重数据服务持续支撑审计目标的实现、严守审计质量“生命线”。数据只有在看得见、找得到、管得住、用得好的情况下，才能发挥其真正的价值。在操作层面，上述审计大数据治理常用的技术手段对于推动审计的组织方式、工作方式、审计方法和创新理念起到行之有效的作用，特别要通过完善审计大数据治理破解物理性和逻辑性“数据孤岛”、提升数据管理水平、加强数据资源的分析利用，多维度保证数据的安全和合规常态化。

（三）培养兼备审计、信息技术和法律专业素质的复合型人才

守护好国家数据资源，要建设一支高素质专业化审计干部队伍，需要培养具有审计、信息技术和相关法律知识的数据合规审计专业复合型人才。数据作为新型的关键生产要素，交织着个体权利、商业价值、产业发展及战略部署、公共利益、国家安全等诸多因素。数字化时代数据的采集、处理和存储依赖于信息系统和算法模型，审计人员需要了解信息系统的运作方式、算法的底层逻辑，以便检查其安全性和数据合规性，只有具备信息技术专业素质的人员才可能更好地理解和审计信息技术系统。同时，数据合规审计牵涉“数据三法”以及其他事关国家安全的法律规范，审计人员需要理解相关法律法规的要求，并能够评估组织的数据处理活动是否符合法定的合规要求。审计的数字化转型必然带来审计人才选拔使用条件的改变，应更加重视审计人员的专业技术特征，要以数字化为突破点，通过不断培养和对人才结构的战略性调整，造就一支与数字经济发展相适应的审计人才队伍。

**作者单位：**南京审计大学

原载《审计观察》（京），2024.2.4~11