科学技术与教育 2026年第4期
ISSN: 3079-4455

论智慧纪检监察中数据共享双轨制的构建

张珈畅*，海冰洋
郑州大学，河南郑州，中国
*通讯作者

【摘要】纪检监察数字化转型也进入关键阶段，数据共享作为智慧纪检监察的核心环节，其合法性、安全性与实效性的矛盾日益凸显。实践中，智慧纪检监察数据共享主要面临协同共享机制欠缺、涉密保护与数据利用失衡、合规治理模糊三大困境。针对这些困境，在数据共享方面可基于协同治理、数据分类分级等理论，构建常规共享轨道与受限共享轨道并行的双轨制体系，以一体化平台破解数据孤岛与互联鸿沟，通过差异化治理机制平衡涉密保护与数据利用，依据权责法定化与全流程风控保障合规运行。数据共享双轨制的创新既完善了纪检监察数据共享理论与数据法律体系，又提升了纪检监察数字化治理效能，保障个人信息安全与公共利益，为廉政治理现代化提供了系统性解决方案。

【关键词】智慧纪检监察；数据共享；涉密数据与非涉密数据；双轨制
【基金项目】郑州大学 2025 年大学生创新训练计划项目（编号：202510459086）

1.问题的提出

数字经济正在成为推动中国式现代化的重要力量[1]。进入新时代，廉政建设和国家治理现代化提出更高要求，纪检监察工作也迈入数字化转型关键阶段。数据共享作为数字纪检监察体系的核心环节，其制度构建与实践运行的矛盾日益凸显，成为亟待破解的时代课题。国家对此高度重视，从政策到法律层面构建了明确指引。二十届纪委二次全会提出“构建贯通全流程、全要素的数字纪检监察体系”，三次全会部署建设一体化工作平台实现数据集中管理，四次全会进一步强调以大数据赋能正风反腐，政策层层递进凸显数据共享的关键地位。与此同时，《监察法》确立隐私保密与技术调查审批规则，《数据安全法》构建分类分级保护制度，《个人信息保护法》明确敏感信息特殊要求，形成了数据共享的合法性边界，同时也提出了公共利益与个体权益平衡的迫切命题。

十八大以来，我国数字化进程推进成效显著。正如总书记所言，“数字技术作为世界科技革命和产业变革的先导力量，日益融入经济社会发展各领域全过程，深刻改变着生产方式、生活方式和社会治理方式[2]。”当今学界围绕智慧纪检监察中的数据共享问题，已经进行了许多研究，但仍未能破解当前数据共享领域中数据利用与个人信息保护的平衡等问题。针对纪检监察这一特殊公法领域的共享规则研究不足、缺乏适配监督实践的差异化保护方案、理论供给与实践需求存在明显落差。实践中各级纪检监察机关虽已进行了诸多探索，尝试以数字技术为引擎，驱动纪检监察工作迈向高质量发展新阶段[3]，但仍面临多重困境。第一是协同共享机制欠缺，上下级数据标准不统一、跨部门缺乏法定协同机制，导致数据孤岛与互联鸿沟并存；第二是涉密保护与数据利用失衡，静态授权模式存在安全隐患，人工审批流程冗长，形成保护过度与利用不足的双重矛盾；第三则是合规治理困境凸显，数据各方权责边界模糊，缺乏全流程风险防控机制，风险控制滞后于危害发生。这些问题本质上是技术应用与法律规范、制度设计与实践需求的协同失衡，这既削弱了数字技术的赋能效果，也制约了纪检监察工作的法治化、智能化转型。基于此，本文拟针对实践中亟待破解的现实难题，构建适配智慧纪检监察的数据共享制度，从而为落实全面国家战略、推动廉政治理现代化提供智识支撑。

2.智慧纪检监察中数据共享机制的实践困境

2.1 协同共享困境

在数字技术深度嵌入政务领域的背景下，跨部门协作成为提升政务效能的重要手段。然而，数据共享作为跨部门协作的核心环节，也引发了诸多法律冲突和实践困境[4]。智慧纪检监察数据共享的协同性不足，核心表现为数据流通中的结构性障碍，集中体现为“数据孤岛”

与“互联鸿沟”的双重阻滞，严重制约了数据资源的整合效能与协同监督合力的形成。从纵向维度来看，不同层级纪检监察机关在技术基础设施建设上存在显著差异，数据采集、存储、传输的技术规范缺乏统一性，导致数据格式不兼容、接口难以对接，使得上下级数据平台之间无法实现高效互联互通。传统工作模式下形成的“上级授权、下级执行”单向流程，进一步加剧了层级间的数据壁垒，下级机关的业务数据难以顺畅向上归集，上级机关的政策导向与数据需求也无法通过统一标准精准传递至基层，造成数据在纵向流转中的损耗与滞后。

从横向维度分析，纪检监察机关与财政、司法、审计、公安等相关职能部门之间缺乏法定化的协同共享机制，部门间“职能孤岛”现象突出。各部门往往基于自身业务需求制定数据管理规范，数据采集标准、存储格式存在差异，导致跨部门数据重复采集、资源浪费的问题普遍存在。同时，由于缺乏明确的权责划分与激励约束机制，部分部门因担忧数据共享可能引发的安全风险与责任纠纷，对数据共享持保守态度，共享意愿不足，即便在必要的协作场景中，也多采取碎片化的“点对点”对接模式，难以实现数据的全流程互通。更为关键的是，现行法律体系中尚未对数据跨领域流转、调取程序等作出统一规范，各地在实践中只能依赖自行制定的局部规则开展工作，导致不同地区、不同部门在数据共享流程上存在差异，出现“同案不同流程”的现象，既影响了程序的公正性，也降低了跨部门线索关联分析的效率，难以形成覆盖全域的协同监督网络。

2.2 涉密保护与数据利用平衡难题

数据融合共享是大数据信息化赋能正风反腐的客观要求[5]。涉密信息保护与数据高效利用之间的失衡，是智慧纪检监察数据共享实践中面临的突出矛盾，既存在数据安全防护不到位的风险，也存在数据利用效率低下的问题，形成了双重治理困境。在安全防护层面，传统涉密数据保护模式存在明显短板，难以适应数字化协作的需求。当前，涉密数据的访问控制多采用静态授权机制，授权决策一旦作出便长期有效，缺乏根据协作场景、任务进度动态调整的弹性，无法匹配跨部门、跨层级协作中复杂多变的授权需求，容易出现授权用户超范围使用数据、权限回收不及时等风险，违背了数据保护的“最小必要”原则。同时，涉密数据存储多依赖中心化服务器架构，这种集中式存储模式存在“单点故障”隐患，一旦服务器遭受攻击或出现漏洞，极易引发涉密数据大规模泄露，对纪检监察工作的保密性与权威性造成严重冲击。此外，部分地区在数据加密技术应用上较为滞后，涉密数据在跨系统流转过程中缺乏有效的加密保护措施，进一步放大了数据泄露的风险。

在数据利用层面，传统的数据调取与审核流程严重制约了工作效能。涉密数据的调取往往需要经过“申请—初审—复核—领导审批—跨部门协调”等多层级人工审核环节，流程繁琐、耗时漫长，单次审批往往需要数十小时甚至更长时间。在复杂案件办理中，关键证据因调取流程冗长而无法及时获取，不仅延误了案件查办进度，也可能导致部分重要线索流失。更为突出的是，部分基层纪检监察机关为规避数据安全责任，对涉密数据采取“保护性冻结”策略，即便部分数据经过脱敏处理后可安全共享，也因缺乏明确的分级分类标准而被纳入严格审批范畴，导致大量有价值的数据长期闲置，无法为监督执纪工作提供有效支撑。这种“重保护、轻利用”的倾向，使得数据资源的价值难以充分发挥，既浪费了数据治理的前期投入，也削弱了数字技术对纪检监察工作的赋能效果，形成了安全与效率双双受损的治理僵局。

2.3 合规治理困境

将数字技术深度融入国家监察体系，其核心在于构建系统化、标准化的数据体系[6]。智慧纪检监察数据共享在合规方面存在显著不足，核心问题是责任制度规范模糊且缺乏动态风险防控机制，两者交织形成的系统性治理漏洞阻碍数据共享的法治化推进。当前规范体系未明确划分数据提供使用管理三方的权利义务范围，缺乏法定权责分配准则及配套激励约束机制，跨部门跨层级数据交互多依赖行政指令或临时协调难以形成稳定可预期的协作关系。数据提供方面临“共享担责、不共享无责”的局面，因担忧数据真实性完整性引发法律责任而在共享中保持谨慎，仅提供少量核心数据导致共享全面性不足；数据使用方无明确使用边界准则常出现超范围使用数据的情况，责任追究机制缺失使得此类行为无法得到有效管控；数据管理方作为平台运营主体，其在数据安全保障和质量管控上的职责缺乏具体标准，出现问题后往往难以认定责任。权责划分模糊导致数据共享中推诿扯皮现象频发，还形成“数据沉睡”与“数据混乱”并存的治理乱象，部分民生领域因数据采集不全面出现监督盲区，削弱基层监督效能的发挥。

在风险防控层面，现行法律已确立数据分类分级保护、风险评估等原则性规定但缺乏具体配套细则和操作标准，导致这些原则无法在实践中落地执行。部分地区未结合纪检监察工作实际对数据风险等级进行科学分类，采用“一刀切”的粗放处置模式，既可能因过度保护限制正常数据流通，也可能因保护不足引发数据安全隐患。传统风险防控模式过度依赖事后审计追溯，未针对数据共享全流程建立动态监控和实时预警机制，越权访问、数据泄露等风险发生时只能在危害产生后追溯问责，无法在风险萌芽阶段及时发现并制止，导致风险控制滞后于危害发生，背离“预防为主”的风险治理原则。这种“重事后、轻事前”“重形式、轻实效”的风险防控模式难以有效防范数据共享中的各类合规风险，还可能因风险处置不及时引发连锁反应，增加智慧纪检监察数据共享的合规治理难度，延缓纪检监察工作向法治化规范化转型的进程。

3.智慧纪检监察中数据共享双轨制的理论基础

3.1 协同治理理论

整体性问题涉及组织的结构优化，而协同性关涉到主体间的协作行动[7]。协同治理理论是协同理论与治理理论深度融合的重要治理范式，核心要义在于整合多元主体资源与力量，优化系统互动关系，提升治理体系效率与稳定性，实现单一主体或局部力量难以达成的治理目标。该理论突破传统单一主体主导的治理局限，强调治理主体的多元性与协同性，主张公共事务的有效治理离不开各类相关主体共同参与，涵盖不同层级政府部门、社会组织、市场主体及社会公众，它们以公共利益为根本导向，在明确权责边界的基础上，通过资源共享、信息互通与流程协作，打破治理碎片化困境，形成上下联动、内外协同的治理格局。

在纪检监察工作领域，协同治理理论的应用具有极强的现实针对性与必要性。纪检监察工作的核心目标是维护廉政建设与国家治理的良性运行，其工作内容涉及对权力运行的全程监督、违纪违法线索的排查核实、案件的查办与问责等多个环节，从治理角度来看，这个过程不仅仅涉及纪检监察部门，多元主体也共同参与其中[8]。横向上，纪检监察工作需与财政、审计、公安、司法等多部门密切协作，这些部门的资金监管数据、专项审计报告、调查取证资源及法律适用支持，都是纪检监察机关开展工作的重要基础。但传统模式中，各部门多局限于自身职责边界，缺乏常态化沟通协作机制，导致信息传递不畅、资源难以互补，既增加治理成本，又易出现监督漏洞，使得跨部门、跨领域违纪违法问题难以及时发现查处。

纵向上，纪检监察工作涉及多个层级，上级机关政策部署需下级有效落实，下级在实践中遇到的新情况、新问题也需及时向上反馈，形成上下贯通的工作体系。但在缺乏协同治理理念指导的情况下，上下级机关易出现政策执行偏差、信息传递滞后等问题，上级监督指导难以精准对接基层实际需求，基层实践经验也难以有效上升为系统性制度规范，影响纪检监察工作整体效能。此外，纪检监察工作还需广泛社会参与，公众作为权力运行的直接影响者和监督者，其提供的举报线索、意见建议对发现隐性违纪违法问题、提升监督全面性至关重要，但传统模式中公众参与渠道不够畅通、机制不够完善，导致公众监督作用未能充分发挥，难以形成全社会共同参与反腐的良好氛围。

协同治理理论恰好为解决上述问题提供了系统性思路。通过建立规范化协同机制，明确各参与主体权责清单，搭建信息共享与沟通协作平台，可使不同部门、不同层级及社会公众在纪检监察工作中形成合力。建立跨部门常态化沟通机制，能实现各部门监督数据实时共享与线索移送，让纪检监察机关整合各类资源，更高效开展案件查办；完善上下级机关协同联动机制，可确保政策部署精准落地与实践经验有效传导，提升纪检监察工作的整体性与针对性；搭建公众参与平台、畅通举报渠道，能充分调动社会公众监督积极性，形成全方位、无死角的监督网络。同时，该理论倡导的资源整合与流程优化，能有效降低各主体协作成本，减少治理内耗，推动纪检监察工作从分散化、碎片化探索转向系统化、一体化治理，最终提升廉政建设与反腐败工作整体效能，为国家治理现代化提供有力保障。

3.2 数据分类分级理论

数据分类分级理论是数据治理领域的基础性理论，核心要义在于依据数据固有属性与实际应用场景，通过科学划分标准与方法，对数据进行类别界定与等级划分，为数据安全保护、合规利用与高效流通提供系统性理论支撑。关于纪检监察机关大数据监督的规范化开展，最大的制度难题在于，如何对政务数据、网络信息企业数据、个人信息、政法机关和纪检监察机关的办案数据或管理数据等进行规范化地共享、处理与使用[9]。该理论的形成发展紧

扣数据治理现实需求，既以数据自身特征为逻辑起点，又衔接相关法律法规刚性要求，是平衡数据安全与利用价值、破解治理碎片化的关键工具，在智慧纪检监察等特殊公法领域数据共享实践中具有不可替代的指导意义。

数据分类是理论基础环节，核心是根据数据来源、内容属性、权属主体、应用场景等多元维度，划分具有共性特征的类别，为差异化管理奠定基础。从权属与内容属性来看，数据可分为公共数据、个人数据与企业数据，分别侧重公共利益、自然人隐私权益保护、商业秘密与经营利益；在纪检监察领域，可区分违纪违法线索数据、涉案人员信息数据、资金流向数据等。这种分类并非绝对割裂，需根据治理目标灵活调整，适配数据全生命周期管理需求，避免分类模糊引发治理混乱。数据分级是分类基础上的深化延伸，主要依据数据敏感程度、重要性水平，以及泄露、篡改或非法利用后的危害范围与程度，划定不同安全等级并匹配对应保护措施与利用规则。通常划分为核心数据、重要数据与一般数据三个层级：核心数据关乎国家安全、重大公共利益或关键权益，泄露可能引发严重后果；重要数据对特定领域正常运行与利益保障至关重要，风险影响范围集中；一般数据风险较低，合规前提下可灵活流通利用。分级需结合数据动态变化、政策调整与技术发展实时评估调整，既避免过度保护浪费数据价值，又防止保护不足引发安全隐患。

该理论的实践价值集中体现为提供“分类定界、分级施策”的精准化数据治理框架。在理论支撑层面，功能主义将法律视作政制机器的工具，用以实现与能动型国家的目标紧密相关的特定目的[10]。其与《数据安全法》确立的分类分级保护制度一脉相承，将法律原则性要求转化为可操作的治理路径；在实践应用层面，既能指导数据处理者建立规范化管理体系，明确不同类别、等级数据各环节操作标准，又能为跨部门数据协同提供统一沟通基础，消除数据定义不一导致的协作壁垒。

在智慧纪检监察数据共享场景中，该理论指导意义尤为突出：通过科学分类，清晰界定涉密数据与非涉密数据边界；通过精准分级，明确不同等级数据的共享范围与保护强度，为“常规共享轨道+受限共享轨道”双轨制构建提供直接理论依据，有效破解涉密保护与数据利用的失衡矛盾，确保数据共享在合法合规前提下实现效能最大化。同时，其倡导的动态调整机制，能适应纪检监察工作中数据类型丰富、风险场景变化的现实需求，为数据共享制度长效运行提供持续保障。

3.3 比例原则与最小必要原则

值得特别注意的是，在数字纪检监察监督全流程需要特别加强对数据安全维护与个人隐私保护的专门研究[11]。比例原则与最小必要原则作为公法领域与数据治理的核心准则，共同构成智慧纪检监察数据共享“双轨制”的合法性基础与操作指引，二者理论衔接、实践互补，是平衡公权力与个体权利、数据安全与利用价值的关键工具，为破解安全与效率失衡、权力边界模糊等难题提供系统性方案。

比例原则源于公法，核心包含合目的性、必要性与均衡性：合目的性要求数据处理措施需直接服务于线索排查、案件查办等纪检监察合法目的，不得有无关行为；必要性强调在多种实现路径中，选择对个人权益、数据安全影响最小的方式；均衡性要求数据共享的公共利益增益，需与可能的权益损害、安全风险保持合理比例，不得忽视个体权益保护。在数据共享场景中，该原则为“双轨制”的轨道划分、机制设计提供价值判断标准，确保数据共享符合廉政建设需求且不突破合规边界。

最小必要原则聚焦数据处理的范围与限度，核心是数据的收集、存储、传输、使用等环节，均限定在实现特定目的必需的最小范围，不得过度收集或超范围处理，这一原则在《个人信息保护法》《数据安全法》中均有明确体现。在纪检监察数据共享中，其为“双轨制”划定刚性边界：常规共享轨道的非涉密数据，以满足基础监督需求为限，避免冗余收集；受限共享轨道的涉密数据，严格限定共享对象、场景与留存时间，仅为特定办案需求提供支持。同时，该原则并非静态标准，需结合数据类型、敏感程度动态调整，兼顾数据利用精准性与源头风险防控。

两者的内在关联构成“双轨制”运行核心逻辑：比例原则为最小必要原则提供价值指引，确保数据“最小化”处理不偏离公共利益目标；最小必要原则为比例原则提供具体操作路径，将“最小侵害”要求转化为可量化标准。在实践中，二者共同作用于“双轨制”全流程：轨道划分阶段，依比例原则判断目的正当性，结合最小必要原则界定共享范围；机制运行阶段，通过比例原则校验措施均衡性，借最小必要原则规范数据流转；风险防控阶段，以比例原则权衡安全措施强度，避免过度防控损耗效率。

两项原则的实践价值尤为突出，共同破解

了传统数据共享“重效能轻安全”“重保护轻利用”的双重困境，既为常规共享轨道高效流通提供合规依据，也为受限共享轨道安全可控筑牢制度防线。通过二者协同适用，“双轨制”既能保障纪检监察机关依法履行监督执纪问责职责、提升治理效能，又能严格约束权力行使、保护个人信息权益与数据安全，实现公共利益与个体权益、治理效率与合法合规的动态平衡，为智慧纪检监察的规范化、法治化发展提供坚实保障。

4.智慧纪检监察中数据共享双轨制的构建路径

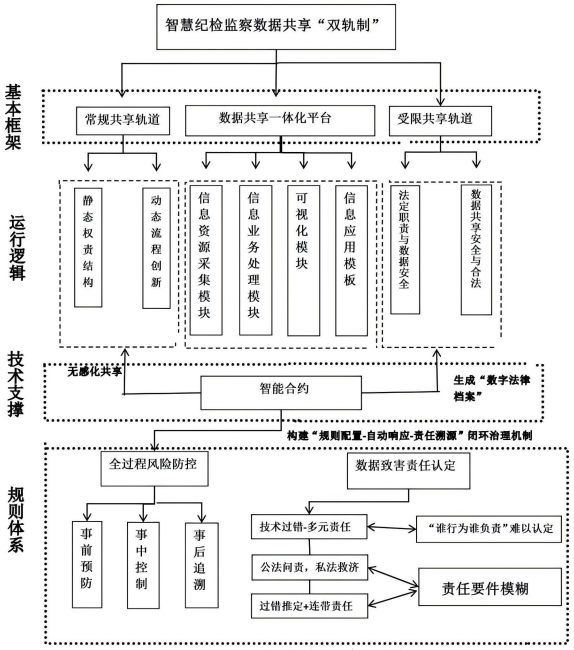

图 1.“双轨制”机制图

在数字信息技术的加持下，智慧纪检监察体系正从信息化、数字化迈向智能化发展[12]。针对智慧纪检监察数据共享实践中存在的协同共享困境、涉密保护与数据利用平衡难题、合规治理困境三大核心问题，基于法学与纪检监察专业理论，以数据分类分级为基础，以法律规范为边界，以技术工具为支撑，构建常规共享轨道与受限共享轨道并行的“双轨制”治理体系（见图 1:“双轨制”机制图）有助于实现数据共享的安全、高效与合规统一，推动智慧纪检监察数据共享从碎片化探索向体系化治理转型。具体而言，智慧纪检监察数据共享双轨制是以一体化平台为核心支撑，依托常规共享轨道与受限共享轨道，通过明确静态权责结构、优化动态流程，结合相应技术构建规则配置、自动响应、责任溯源的治理机制，同时以全过程风险防控与数据致害责任认定制度为保障，确保数据共享在合法安全的前提下，有效适配纪检监察工作的实践需求。

4.1 构建双轨协同治理架构，破解协同共享困境

协同共享困境的核心症结在于数据孤岛与互联鸿沟并存，本质是数据标准缺乏统一性、协同机制法定化不足、跨部门权责划分模糊。只有打破数据壁垒，实现各类数据要素汇聚融合，才能更好释放监督效能[13]。各级纪检监察机关特别是纪委国家监委和省级纪委监委开发了若干核心业务平台，但各个业务系统平台相对独立，数据互联互通不顺畅，难以实现集成高效的目标。对此，二十届纪委三次全会作出了“建设一体化工作平台”的部署。本研究所提出的“双轨制”通过技术适配、制度衔接与权责界定的三维发力，构建系统性解决方案，重塑数据协同共享的法治生态。

数据共享一体化平台作为“双轨制”运行的核心枢纽，为跨部门、跨层级数据协同提供坚实技术支撑。平台依托区块链、大数据与人工智能等数字技术的深度融合，整合信息资源采集、业务处理、可视化分析、场景应用四大功能模块，严格遵循相关法律对数据采集、存储、使用的法定要求，建立统一的数据标准体系与接口规范。在常规共享轨道中，非涉密数据被纳入标准化流通范畴，通过跨部门数据接口的统一化建设，打破不同地区、层级、部门间的技术壁垒，实现相关部门数据的实时归集与动态更新，从技术层面消解数据孤岛现象。

“双轨制”通过静态权责架构与动态流程创新的有机协同，构建法定化的协同机制。在静态层面，依据相关法律明确数据提供方、使用方、管理方的平等法律地位与权责边界，三方形成权利有清单、行为有依据、责任可追溯的法律关系结构。在动态层面，数据决策可以辅助监察决策的作出，但是需要对数据信息的质量进行控制，并非“量多”的类案信息就能够为纪检监察人员提供足够的决策支持[14]。通过协同决策机制签订跨部门数据共享协议，将抽象法律原则转化为具体操作规范；借助数据回流机制，以智能合约技术自动触发基层监察机关所需非涉密数据的流转，破解资源配置失衡问题。同时，将全流程贯通机制嵌入平台运行，实现各类业务数据的跨轨道协同，消除互联鸿沟导致的治理碎片化，形成协同治理格局。

4.2 建立差异化治理机制，破解保护与利用平衡难题

涉密信息保护与数据利用的平衡难题，根

源在于传统单一治理模式无法适配数据敏感性差异，导致保护过度与利用不足的双重困境。数字技术在为纪检监察工作注入效能的同时，也使其实践中制度边界与法治保障的适配陷入复杂张力[15]。“双轨制”基于数据分类分级理论，针对非涉密数据与涉密数据设计差异化治理路径，建立差异化管理机制，既保障数据安全，又避免数据垄断导致的信息流动受阻[16]，兼具落实相关法律刚性要求与保障监督执纪工作高效开展的意义于一体。这种中立的数字化技术作为规范纪检监察行为的“监督人”，通过规范化，公开化，透明化的方式，保障在纪检监察行为全过程中对于个人数据的合理、规范、有序的流通使用，既不影响数字化对于纪检监察行为的效率帮助，也不会导致不规范操作中可能产生的数据隐私泄露风险[17]。常规共享轨道聚焦非涉密数据的高效合规流通，通过无感化共享机制提升数据利用效率。该轨道严格遵循相关法规，对高频、低敏感的基础业务数据实行无条件共享原则。依托一体化平台的智能合约技术，将协作配合程序转化为自动化流程，实现非涉密数据的实时碰撞与智能预警，自动识别异常线索。同时，平台建立数据质量分级评估制度，对数据的完整性、准确性、时效性进行动态监测，确保数据利用的可靠性，既避免非涉密数据因流程冗余导致的利用不足，又通过合规校验保障数据共享的合法性。

受限共享轨道针对涉密数据，构建安全可控、精准授权的融合访问控制机制。在技术层面综合运用属性基加密技术与非对称加密技术，将涉密数据以密文形式存储与传输，严格遵循相关法律对加密技术的要求，构建三重防护体系，确保数据访问主体与法定职责严格对应，实现最小必要范围内的精准共享。在流程层面，通过智能合约构建自动化审批机制，将技术调查措施审批程序代码化，实现涉密数据调取全流程自动化，大幅缩短审批周期。这种数据驱动的监督范式革新，本质是通过数字技术将现实世界的复杂联系转化为可计算、可追溯的监督路径，使得权力运行的每个数字痕迹都成为反腐利剑的磨刀石，这正是数字化纪检监察体系超越传统监督效能的深层逻辑。这种数据驱动的监督范式革新，本质是通过数字技术将现实世界的复杂联系转化为可计算、可追溯的监督路径，使得权力运行的每个数字痕迹都成为反腐利剑的磨刀石，这正是数字化纪检监察体系超越传统监督效能的深层逻辑[18]。同时，区块链技术对涉密数据的使用轨迹进行全程存证，确保操作可追溯、责任可追究，既防范泄露风险，又满足案件查办对涉密数据的紧急需求，实现保护与利用的动态平衡。

4.3 完善权责与风控体系，破解合规治理困境

在智慧纪检监察领域，完备的组织体系能够通过明确职责与分工，提高工作效率、减少冲突，促进沟通与协作。合规治理困境的核心是责任界定模糊与动态风险防控缺位，本质是法律规范与技术实践的协同失衡。“双轨制”通过构建责任法定化加风控全流程化的制度体系，将相关法律的原则性要求转化为可操作的具体规则，实现数据共享的合规治理。

纪检监察监督技术研究是对数智技术在新时代中国纪检监察“智慧监督”中的应用创新和丰富实践的理论化总结，能够为数智技术驱动引领纪检监察工作高质量发展提供理论指导，具有重大理论和现实意义[19]。构建过错推定与连带责任相结合的责任认定规则，明确多元主体的法律责任。依据相关法律，结合纪检监察数据共享的特殊性，确立数据致害责任专项规则：数据提供方若不能证明已履行相关义务，推定其存在过错；数据使用方超权限、超范围使用数据导致损害的，承担主要责任；技术服务方因系统漏洞、代码缺陷引发数据泄露的，承担产品责任。同时，明确数据管理方的安全保障义务，区分不同过错程度承担相应责任，实现权责一致原则在数字时代的具象化。此外，打通公法问责与私法救济的双重渠道，保障权利救济的全面性。

根据系统论中的冗余机制原理，任何组织和制度均存在固有局限性，均具有一定的风险根源，风险始终是根植于社会组织的社会现象[20]。建立事前预防、事中控制、事后追溯的全过程风险防控规则，实现风险的动态治理。纪检监察信息化建设从顶层设计到具体运行都需要法律制度体系的引导、规范，并提供合法性基础和稳定的预期。事前预防阶段，依据相关法律的风险评估义务，构建法律风险量化模型，将法定要件转化为可计算的风险参数，对双轨运行中的潜在风险进行分级预警。事中控制阶段，依托一体化平台的实时监测功能，对数据共享行为进行合规校验，一旦检测到违规情形，智能合约自动触发阻断程序，并同步推送预警信息。事后追溯阶段，区块链存证的操作日志可直接作为电子证据，为责任认定与纠纷解决提供技术支撑。这种全流程风控机制既落实了全过程监督管理的要求，又弥补了传

统事后审计追溯的滞后性缺陷，确保“双轨制”运行的合规性与安全性。

5.结语

智慧纪检监察数据共享双轨制，是法学、纪检监察业务与数字技术融合的系统性制度创新，契合纪委政策导向，也严守相关法律边界。实践中，它打破了数据壁垒，平衡了涉密保护与数据利用，完善了合规治理体系；理论上，丰富了纪检监察数据共享理论，为相关公法原则应用提供了实践样本。双轨制基层实践仍面临技术、人员等现实问题，需动态优化完善。其不仅为纪检监察数据共享提供方案，也为其他公权力机关数据治理提供借鉴，对推进国家治理体系和治理能力现代化意义深远。

参考文献

[1]吴学品，李雨澄，李东敖.数字经济推动中国式现代化的机制分析和实证检验[J].成都理工大学学报（社会科学版），2024，32（3）：66-82.
[2]总书记向 2022 年世界互联网大会乌镇峰会致贺信[EB/OL].(2021-09-26)[2023-03-29].http://www.qstheory.cn/yaowen/2022-11/09/c_1129113635.htm.
[3]赵雪.构建数字纪检监察体系的现状、难点及对策[J].内蒙古社会科学，2025，46（03）：39-46.
[4]伍荼，易茗.数字政务中纪检监察与行政法个人信息协同保护路径研究[J].北京政法职业学院学报，2025，（03）：58-64.
[5]陈超凡，杰.以大数据信息化赋能正风反腐的现实梗阻与调适进路[J].中国纪检监察研究，2025，（05）：77-86.
[6]赵永红，子宁.数字技术赋能纪检监察工作的现状、制约因素与法治路径[J].成都理工大学学报(社会科学版):，2025，33（03）：12-23.
[7]舒绍福，苏江涛.数字赋能国家监察：特征、问题与推进[J].电子政务:，2022，（10）：99-109.
[8]舒绍福，苏江涛.数字纪检监察 20 年：实践及启示[J].行政管理改革，2025，（01）：42-51.
[9]杨建军.纪检监察机关大数据监督的规范化与制度构建[J].法学研究，2022，44（02）：19-35.
[10][英]马丁·洛克林.公法与政治理论[M].郑戈译.北京:商务印书馆，2002：188.
[11]白秀银,徐亮.构建数字纪检监察监督实验室的理论基础与实践路径[J].成都理工大学学报(社会科学版)，2025，33（02）：1-11.
[12]喻少如，鲜翰林.智慧纪检监察：内涵要义、逻辑理路与规范进路[J].广州大学学报(社会科学版)，2025，24（04）：102-117.
[13]李张光.加快完善数字纪检监察体系[N].中国纪检监察报，2025-10-28（007）.
[14]吴建雄，宋阳.人工智能辅助纪检监察办案的法律风险及其控制[J].广州大学学报(社会科学版)，2025，24（04）：118-131.
[15]孙同泽.论数字纪检监察制度边界与法治保障间的三重张力[N].农业科技报，2025-11-12（007）.
[16]张撒宇.论数字纪检监察中的信息对称与不对称[J].无锡职业技术学院学报，2025，4（06）：58-65.
[17]肖云祥.以数字技术赋能纪检监察工作高质量发展[J].中国纪检监察研究，2024（2）：71-78.
[18]邱思宇.数字化纪检监察的价值、挑战与因应[J].时代法学，2025，23（04）：45-53.
[19]纪检监察监督技术研究的基础理论与实践路径[J].中国纪检监察研究，2025，（01）：43-51.
[20]沙夫里茨，海德.公共行政学经典[M].7 版.刘俊生译.北京:中国人民大学出版社，2019：302.