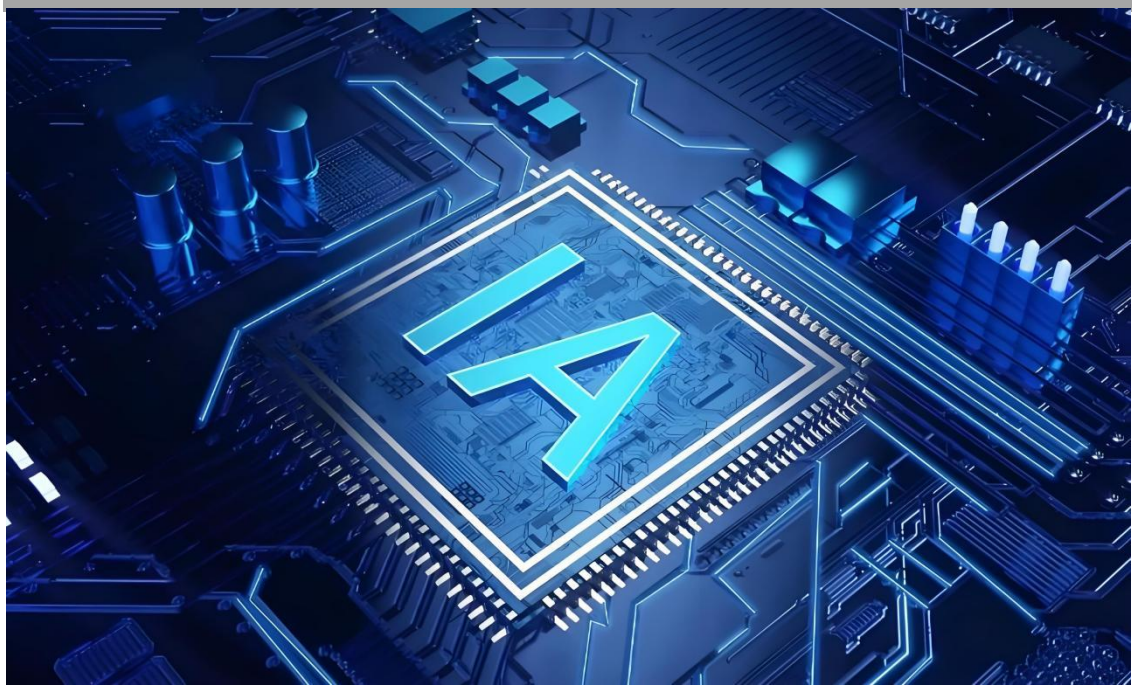
中国人民大学法学院
数字法学教研月报

2025 年第 7 期（总第 19 期） 2025 年 7 月 20 日



本期看点

【数字法治大事件】国家数据局等多部门联合印发数据流通交易合同示范文本，构建数据流通交易示范合同机制；《可信数据空间标准化研究报告》研讨会在京召开，聚焦可信数据空间标准化建设；地方层面，重庆推进 AI 赋能数字重庆建设，辽宁印发数字政府建设实施方案，多地动态助力数字发展；国家数据专家咨询委员会理论组、应用组分别召开内部交流研讨会，探讨数据要素市场化配置与跨境流动互信机制；多项法规政策出台，涉及数据出境安全评估、网信部门行政处罚裁量权、关键信息基础设施商用密码使用等，为数字领域提供规范指引。

【研究动态】本期研究动态涵盖数字法学多领域前沿。基础理论涉及数字时代合同合意、数字法律行为等；个人信息保护围绕信息主体同意撤回、合规审计等展开；数据确权流动研究数据授权管理权、数据财产权排除强制执行等；人工智能研究生成式 AI 服务提供者义务、法律定位等；平台治理、数字行政与司法、虚拟财产等领域亦有新成果，为数字法治提供理论支撑。

【教研活动】北京大学首届“数字法治的理论视野与实务前沿”暑期学校成功举办；清华大学计算法学课题组参加国际法律人工智能学术大会；国家市场监督管理总局竞争政策协调司党支部与中国政法大学数据法治研究院党支部开展共建活动；第四届“数字法学与数字司法”研讨会、“数字法治政府建设与治理现代化”学术研讨会等顺利召开，促进学术交流与实践探索。

【数字法评】

《论人工智能法律规制的内部路径》，《河北法学》2025 年第 8 期，作者：邓矜婷。

《数据财产权排除强制执行的权益结构》，《中国法学》2025 年第 3 期，作者：陈爱飞。

本期目录

数字法治大事件

导言：当下数字法治已然成为时代发展的关键议题，深刻影响着社会的方方面面。随着数据作为新型生产要素，深度融入经济社会各领域全过程，数据市场规模如春笋拔节般加快增长。然而，发展之路并非一帆风顺，诸多挑战横亘在前。例如，数据流通交易情况新颖复杂，经营主体在前行时缺少可参照的合同范本，导致实践中问题频发。有的事前未明确数据质量等要求，事后极易引发纠纷，无形之中抬高了流通交易成本，阻碍了数据市场的高效运行。在此背景下，一系列数字法治大事件相继登场，成为推动行业发展的关键力量。国家数据局、市场监管总局联合印发数据流通交易合同示范文本，为数据市场经营主体参与流通交易提供了重要的范本与参考，有望降低交易成本，维护公平竞争环境，推动数据市场健康有序发展。《可信数据空间标准化研究报告》研讨会的成功召开，聚焦可信数据空间的技术架构、标准化建设及示范应用等重点内容，为可信数据空间标准化工作绘制了蓝图。而在地方层面，重庆借助 AI 赋能数字重庆建设，全面提升超大城市发展服务治理能力，通过九大应用场景深度影响市民生活，让人们切实感受到数字法治带来的便捷与高效。这些事件，无一不在彰显着数字法治领域的积极探索与创新实践，为我们展现了一幅充满希望与挑战的发展画卷，也为后续的深入探讨奠定了坚实基础。

专家解读|构建数据流通交易示范合同机制，促进数据市场有序健康繁荣发展

原载：“国家数据局”微信公众号

文|清华大学法学院教授　申卫星

高效的数据流通交易是数据市场繁荣发展的重要目标之一，数据流通交易示范合同旗帜鲜明地将“数据”作为交易标的物，鼓励各方积极参与数据流通，以释放数据要素价值、实现数据要素市场化配置。2022 年 12 月，中共中央、国务院印发《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》）指出要“建立健全基于法律规定或合同约定流转数据相关财产性权益的机制”。2025 年 7 月，国家数据局和市场监管总局联合发布数据流通交易合同示范文本，推进数据产权等数据基础制度的落地实施，为数据市场有序、健康、高效发展提供有力支撑。

一、发挥示范效应，引导数据供得出、流得动、用得好、保安全

在现代市场经济中，合同是实现专业化合作的纽带，也是维护社会经济秩序的凭据，是包括数据在内的生产要素市场化的重要法律工具。数据示范合同可以降低数据流通交易成本，规范数据流通交易行为，引导当事人公平、合理分配数据产权和相关利益。市场监管总局、住建部、交通部等部门将示范合同建设作为其构建规范有序市场的主要抓手之一，在过往经济改革发展中发挥了重要作用。当前我国正值数据市场蓬勃发展之际，国家数据局和市场监管总局联合发布数据流通交易合同示范文本，引导数据供得出、流得动、用得好、保安全，为构建透明、公平、公正的数据市场环境奠定坚实基础。

一是释放出“数据可以安全交易”的明确信号，激活市场信心，为数据要素的市场化配置提供实用范式文本。当前数据持有方与亟需数据赋能的传统行业企业之间，存在着数据价值转化断层。数据持有方拥有激活传统产业升级的宝贵数据资源，而传统企业则迫切希望借助数据要素的乘数效应，提升产品竞争力、优化服务体验、驱动经营模式创新，但双方因对数据流通交易的合法性与安全性，以及数据权责边界、使用限制、安全保障等条款缺乏共识而只能“望数兴叹”，不敢达成数据流通交易合作。通过示范合同的推行，可以缓解数据供需双方对于数据可交易的担忧，打破“供需两旺但交易不畅”的僵局，提振市场信心，引导场内外交易有序繁荣，促进数据长效“供得出”，使其真正成为可用的“生产要素”。

二是降低流通交易成本，实现数据流通交易的规范化和标准化，促进交易达成。数据市场的高

效运行依赖于透明、规范、高效的交易环境。当前数据市场中衍生出多样化的合同文本，显著推高了交易各方的识别成本、协商成本与合规审查成本，更可能因为条款设计存在合法性、合规性、严谨性等方面瑕疵而潜藏交易失败、履约争议及法律风险，影响数据流通交易的规范化与交易效率。为此，数据流通交易合同示范文本为市场提供一套规范、科学的合同模板，统一“度量衡”，从而有效破解市场中合同类型繁杂、规则模糊、难以归类的困局，为数据市场各参与方提供标准化的合同模板。在场外交易、供需方双边交易等场景中， 合同示范文本得以为交易双方提供清晰的合同条款基准，简化谈判流程，降低因条款歧义或缺陷引发的后期风险。在数据交易机构、数据服务平台等要素汇聚平台场景中，合同示范文本可作为基础交易规则或通用模板嵌入平台流程，提升场内撮合及高频交易的效率与可操作性，支撑数据要素的大规模、高效率市场配置。通过提高交易达成的可预测性与可执行性，推动数据供得出、流得动、用得好、保安全。

三是落实《数据二十条》有关数据产权结构性分置安排的任务。《数据二十条》创新性地提出了数据产权“结构性分置”安排，但经营主体对其如何与实践场景结合仍存疑虑。为此，数据流通交易合同示范文本提供了可操作的合同实践方案，推动这一关键制度落地。合同示范文本不仅包含基础交易条款，更系统嵌入了数据产权流转规则、产权登记指引等内容。在数据提供、委托处理、融合开发、中介服务等多种交易模式下，通过预设的标准条款，清晰界定了持有权、使用权、经营权的边界、流转方式、行权范围与期限，实现了数据产权在不同场景下的结构性分置与流转，从而促进数据要素的高效流通与价值释放，助力数据用起来、用得好。

四是坚持安全底线，实现法定安全义务的合同化转化。对数据上所承载的个人信息、商业秘密、知识产权、国家社会安全等在先权益，《数据安全法》《网络安全法》《个人信息保护法》等的法定义务是数据流通安全交易的红线，其不因合同约定而减损，而是通过合同示范文本将法定安全义务转化为合同义务。通过细化安全责任分配，明确数据安全报告义务和数据安全技术保障要求、嵌入对数据知识产权与商业秘密保护的专门条款，引致与衔接国家发布的《数据出境标准合同》及配套规范标准等方式，确保境内数据流通规则与跨境数据流通要求形成闭环，落实“将安全贯穿数据供给、流通、使用全过程”的思路要求。

二、问题牵引动态演进，提供稳定灵活合同规则供给

近期发布的首批四类数据流通交易合同示范文本，为四类数据流通交易场景提供参考。合同示范文本的选择需聚焦行业高发、典型交易法律关系，符合数据市场动态演进的客观规律，以问题为导向，循序渐进，不断迭代，为数据市场治理提供兼具灵活性与稳定性的合同规则供给。

一是以问题为导向，文本类型不求全面但求典型。商业交易模式日新月异，合同示范文本不可能也不需要涵盖所有交易类型。应聚焦高发、典型场景形成示范文本库。在总结归纳典型场景的标准化条款基础上，保留持续迭代更新的空间，实现基础范式与个性需求的衔接。**二是文本适用遵循“实践认同——惯例形成”的渐进路径。**合同示范文本的制度生命力源自经营主体的自发采纳与重复适用，通过交易实践的承认规则逐步演化为行业惯常做法和交易惯例，为各行业、各主体提供可参照的治理工具。**三是详略得当，构建数据流通交易中的条款协商框架。**合同示范文本既明晰主要的交易内容和权利义务，又预留了多种方案和留白填空，供当事人协商选择，能够灵活地设计出各类数据流通交易商业模式。

三、多域多主体体系协同，示范合同与实践经验良性互动

数据领域合同示范文本是一项长期推进、跨领域规范协同工程。下一步，建议调动数据企业、研究机构共同参与合同示范文本的制定与推广。

一是跨部门合作，统筹管理、分工负责。构建定期评估与协同监督机制，确保数据流通交易合同示范文本的有效实施和监督，促进数据市场的规

范化和健康发展。**二是推动示范文本应用落地，在市场检验中不断优化。**定期发布合同示范文本应用的典型案例，分析成功经验和存在的问题，为企业提供实际操作的参考。建立合同示范文本使用的反馈机制，收集使用过程中的意见和建议，提炼交易实践中条款适用的创新范式，通过实践共识助推文本优化，促进合同示范文本始终与市场创新的同步进化。**三是培育发展数据流通交易各参与方对数据合同示范文本的理解与应用能力。**鼓励行业龙头企业和数据交易机构应用示范文本，提炼归纳示范文本应用的经验模式并加以推广，发挥示范引领作用。探索通过指南、解读、合同工具包等形式，提升其对示范文本条款的理解水平和应用能力，促进经营主体间、经营主体与交易机构间的经验流动，及时回应合同示范文本使用中的疑问困惑与新型挑战。

《可信数据空间标准化研究报告》研讨会在京成功召开

原载：“国家数据局”微信公众号

6 月 25 日，《可信数据空间标准化研究报告》研讨会在北京召开。会议由全国数标委秘书处组织，中国电子技术标准化研究院、北京大数据先进技术研究院、中国信息通信研究院、华为技术有限公司、北京大学、浙江大学、中电数据产业集团有限公司、中国电信集团有限公司、中国联合网络通信集团有限公司、中国移动通信集团有限公司、上海芯超数据科技有限公司、云基华海信息技术股份有限公司、百度在线网络技术（北京）有限公司、中国南方电网有限责任公司、浪潮云信息技术股份公司等百余位编制组专家、学者及企业代表参加会议。

会上，《可信数据空间标准化研究报告》编制组围绕国内外可信数据空间发展现状、趋势、标准化实践等方面进行了交流研讨，进一步明确了可信数据空间技术架构、业务架构、功能技术、业务运营、能力评价、安全保障等重点方向的标准化工作思路。

下一步，编制组将进一步完善《可信数据空间标准化研究报告》，有序推进各章节编制工作，按照《国家数据基础设施建设指引》，加快形成结构严谨、衔接密切、切实可行的可信数据空间标准体系，为可信数据空间标准化工作提供系统性指引。

地方动态|袁家军：AI 赋能数字重庆建设 全面提升超大城市发展服务治理能力

原载：“国家数据局”微信公众号

袁家军在市数字化城市运行和治理中心调研并召开座谈会

AI 赋能数字重庆建设

全面提升超大城市发展服务治理能力

7 月 7 日上午，市委书记袁家军前往市数字化城市运行和治理中心，调研人工智能赋能数字重庆建设工作并召开座谈会。袁家军强调，要全面贯彻习近平总书记关于人工智能的重要论述精神，全面落实党中央决策部署，强化 AI 赋能加速形成数字重庆基本能力，加快打造人工智能应用高地，全面提升超大城市发展、服务、治理能力。

市委副书记、市人大常委会副主任李明清，市领导刘尚进、郑向东、江敦涛参加。

在市数字化城市运行和治理中心指挥大厅，袁家军主持召开座谈会，听取人工智能赋能超大城市治理和“33618”现代制造业集群体系建设、全市人工智能科技创新工作情况汇报，来自重庆邮电大学、阿里云和长安科技公司的专家代表作了发言。

在认真听取大家发言后，袁家军作了讲话。他指出，习近平总书记高度重视人工智能发展，提出了一系列新思想新观点新论断。要深入学习贯彻习近平总书记关于人工智能的重要论述精神，聚焦综合应用场景开发、AI 应用高质量数据归集和培育壮大新质生产力、提高群众生活服务现代化水平等重点工作，积极构建人工智能发展知识体系、工作体系和能力体系，不断提升超大城市现代化治理能力。

袁家军强调，数字重庆体系构架与人工智能相互赋能、相互支撑，为人工智能发展提供了广阔空间。要围绕打造综合应用场景强化 AI 赋能，聚焦

一二三产业发展、公共安全、政务服务、民生改善、科技创新等重点领域，加快打造一批多跨协同示范性标志性应用场景。要构建满足 AI 应用的高质量数据集，发挥龙头企业作用，强化算力基础设施建设和人工智能人才培养，提升数据安全治理水平，夯实人工智能发展基础。要聚焦城市数据、行业可信数据、企业可信数据等构建人工智能开源生态，大力促进多元主体资源共享、价值共创、互利共赢。要健全政策支持体系，持续激发各类主体活力，为 AI 赋能数字重庆建设提供强有力支撑。

市级有关部门和单位负责人、有关行业专家和企业负责人参加。

国家数据专家咨询委员会（理论组）2025 年第一期内部交流研讨会在京召开

原载：“国家数据局”微信公众号

近日，国家数据专家咨询委员会（理论组）2025 年第一期内部交流研讨会在京召开。国家数据专家咨询委员会主任委员江小涓等委员出席会议。

会议围绕“数据要素市场化配置的理论创新与实践路径”开展深入研讨。与会委员从政策设计、理论研究和产业实践等多个角度深入交流数据基础制度的细化落地，公共数据开放中权责界定与运营机制，数据交易机构生态培育与市场活力激发，数据隐私保护、使用效率与开放共享间的平衡等问题。委员们提出，应加快完善数据产权“三权分置”政策法规，健全公共数据开放制度，细化数据提供方和使用方责任划分，加大对数据泄露等违法行为的惩处力度，强化数据交易机构登记服务和合规管理职能，支持地方政府和企业开展数据要素市场化价值化创新探索等。国家数据专家咨询委员会江小涓、申卫星、韦韬、田申、任奎、汤珂、陈荣凯、欧阳日辉、黄丽华等委员，国家数据发展研究院副院长姜江，立足各自研究领域分别发言。

国家数据局各单位相关负责同志参加会议。

国家数据专家咨询委员会（应用组）2025 年第一期内部交流研讨会在京召开

原载：“国家数据局”微信公众号

近日，国家数据专家咨询委员会（应用组）2025 年第一期内部交流研讨会在京召开。

会议围绕“数据要素跨境流动互信机制”开展深入研讨。与会委员认真梳理总结前期相关研究与实践，分析了当前数据要素跨境流动面临的问题与挑战，从技术、规则、政策等多维度提出针对性意见建议。**在技术层面，**建议构建基于域名体系的统一数据标识体系，应用隐私计算等数字技术保障“数据可用不可见”；**在规则层面，**建议积极参与国际规则制定，深化数据要素跨境规则制定的国际合作；**在政策层面，**建议推行数据分类分级，通过试点探索差异化管理路径，构建“管放结合”的数据要素跨境流动政策环境。国家数据专家咨询委员会黄先海、丁邡、王继业、余祖俊、李晓东、邵广禄、邱泳钦、林晓东、胡善勇、章根明等委员立足各自研究领域分别发言。

国家数据局各单位有关负责同志参加会议。

专家解读|金融行业跨机构核验中的数据流通安全治理——解读《基于金融业跨银行企业资金流水核验场景的安全多方计算技术应用案例》

原载：“国家数据局”微信公众号

文|清华大学电子工程系信息系统研究所副所长王钺

2025 年 1 月，国家发展改革委、国家数据局等 6 部门联合印发《关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案》（以下简称《方案》），旨在统筹数据发展和安全的内在要求，完善数据流通安全治理机制，以推动数据要

素合规高效流通。《方案》针对企业数据、公共数据、个人数据三种典型的数据流通与应用场景，梳理了安全问题，明确了安全责任、细化了安全规则，并强调通过制度、技术、市场的协同，最大化安全治理的效能。

落实《方案》任务，国家数据局组织遴选了数据流通安全治理典型案例，以具体的案例为切口，详细分析场景中数据流通的安全风险和合规问题，凝聚业务实践过程中形成的共识，规范实践行为，细化安全规则。

一、以小切口破题，细化数据流通安全规则

《基于金融业跨银行企业资金流水核验场景的安全多方计算技术应用案例》（以下简称《案例》）涉及金融行业内跨机构的数据流通安全问题。为提升金融风险管理水平，建立起银行间高效合规的数据交互与协同机制具有重要的意义。但金融行业业务复杂，数据敏感性高，监管要求严，建立金融行业数据共享生态面临巨大挑战。《案例》从贷款申请时跨银行的资金流水核验这一小场景切入，尝试打通银行之间的数据壁垒，推动数据在银行间的安全流动。

小切口破题是推动数据流通安全治理工作的要点。《案例》依据业务需求，将跨主体的数据查询简化成为数据核验服务，这种简化带来了两方面的好处：首先，核验由申请贷款的对公客户发起，查询银行与客户签署了信息查询使用授权书、客户借款合同等文件，这些明确的授权操作，保障了数据使用的合规；其次，核验服务只需返回一致与否的简单结果，可以避免复杂明文查询信息的交互，降低敏感信息直接流通的风险，更便于引入隐私计算等技术手段保护数据主体的权益。场景和问题聚焦之后，才能够进一步从安全技术、制度保障等方面细化落实数据流通安全治理的具体操作。

引入上述跨行核验服务后，对公客户申请贷款时，不再需要客户往返于银行间办理各种证明材料，而是转为委托贷款申请的受理银行进行跨行的资金流水核验，简化了贷款申请的流程，同时也丰富了银行识别、监测客户真实经营活动的方式和手段。跨主体的数据流通和交互，即便只是最简单的数据核验，也切实地体现出了数据的价值。

二、以技术为手段，提高数据流通安全保障能力

聚焦于跨主体的数据核验服务，需要细化具体的安全规则和技术要求。《案例》以具体的数据流通技术手段细化落实了国家、行业数据安全管理要求。《案例》采用安全多方计算技术实现银行间最小必要的数据交互。一方面，被查询银行不知道查询的是哪个主体、哪笔流水；另一方面，所有核验计算均在密态下进行，确保被查询银行对外提供的是密文计算的比对结果，而非原始敏感数据。最终实现银行间的数据安全交互。

更进一步，《案例》对数据流通的技术要求进行了细化。要求查询银行与被查询银行按照统一标准对资金流水数据进行预处理，按照统一标准部署安全多方计算节点，按照统一的协议进行加密和安全传输。同时，为保障数据保密性、完整性、可用性，还要求系统建设与应用单位从架构安全、传输安全、算法安全、系统安全等方面依据《金融业数据能力建设指引》（JR/T 0218-2021）等要求开展技术安全性评估。

三、以制度为核心，加强数据流通安全治理

近年来，商业银行不断提升自身数据治理水平，通过内控管理和风险管理的细化，提升整体合规管理的效能。数据流通安全治理不仅仅关系到安全技术的应用、安全平台的建设，还必须配套相关的安全管理制度，控制业务合规风险，确保数据流通全过程的安全可控。实践中，经常存在对数据流通安全治理复杂性低估的问题，认为只要运用了隐私计算等安全技术，实现了“原始数据不出域、数据可用不可见”，就实现了数据流通的安全合规。事实上，在安全治理过程中，还需要技术体系建设与制度建设深度融合，用技术控制风险、用制度推动合规。

《案例》中，与系统建设相配套，增加了以下管控措施：一是开展技术安全性评估，从架构安全、传输安全、算法安全、系统安全等方面对安全技术

和系统进行评估，出具“基于隐私保护计算技术的他行资金流水核验服务”技术安全性评估报告；二是开展业务合法合规性评估，由系统应用单位出具合法合规性评估报告；三是建立风险补偿机制，制定了风险补偿方案，明确风险认定方式、制订风险赔付机制；四是明确退出机制，确保一旦发生安全事件，银行可根据多方签署的相关协议中约定的期限，在保障用户资金和信息安全的前提下，进行系统平稳退出。这一系列措施的细化落实，强化了《案例》场景中的风险管控能力。

专家解读|公共数据授权运营下的数据安全与利用平衡机制——解读《基于城市交通信号智能协调场景的数治模式应用案例》

原载：“国家数据局”微信公众号

文|对外经济贸易大学数字经济与法律创新研究中心主任许可

2025 年 1 月，国家发展改革委、国家数据局等 6 部门联合印发的《关于完善数据流通安全治理更好促进数据要素市场化价值化的实施方案》（以下简称《方案》）特别提出“加强公共数据流通安全管理”，为公共数据合规高效流通指明了方向。为应对快速迭代的公共数据流通场景和不断涌现的公共数据流通需求，国家数据局近期推出了《基于城市交通信号智能协调场景的数治模式应用案例》（以下简称《案例》）等数据流通安全治理典型案例，为数据安全政策法规提供具象化实施路径参考。

一、“三位一体”的公共数据流通安全解决方案

《案例》中，交通运输管理部门将出租车、公交车等营运车辆单车实时位置数据以公共数据授权运营的形式授权特定企业，被授权企业在数据汇聚融合和分析转化后，将加工后的数据提供给城市交通治理部门，助力其制定交通信号管理方案。鉴于出租车、公交车等营运车辆单车实时位置数据较为敏感，如何在确保数据安全的前提下，满足交通指标计算的需求，成为公共数据流通安全的关键问题。

为化解上述问题，《案例》提出了安全技术、管控措施、法律机制三位一体的解决方案。其中，“安全技术”即对敏感数据进行二次编码，并通过聚类算法将该数据聚类分析后生成群体性路口画像数据，如此确保了数据加工处理过程中的数据安全，并且，处理后的数据转化为群体数据，从而无法关联原始单一车辆信息。“管控措施”包括但不限于“三审核三隔离”机制，其以穿透式管理为核心，覆盖数据流通的主要环节，使资质审查、算法验证、结果校验与权限隔离、数据隔离、人员隔离等各种措施深度融合。“法律机制”一方面指向了公共数据授权运营协议、数据安全承诺书等法律文件，另一方面指向了数据安全负责人、管理部门的组织机制以及提交公共数据授权运营年度报告的信息披露机制。《案例》通过三重保障，探索了公共数据合规使用新模式，释放出了公共交通数据要素的价值。

二、公共数据授权运营安全规则的有益探索

《案例》系公共数据流通安全治理的实践，与立足于统一性的“标准”不同，实践以多样性的探索为特征，不强求唯一做法，而是着眼于实践约束条件和特定场景下达到既定目标的行动模式。数据流通安全治理典型案例遴选、发布和推广，体现了企业自我合规和国家强制合规的协力，发挥着公私共治的功能。从这一视角观察本案例，不难发现其对公共数据治理的示范意义。

其一，《案例》是对“数据安全管理风险评估”的有益探索。《方案》明确提出，数据接收方应按照“谁经手、谁使用、谁管理、谁负责”的原则，承担数据接收后的安全管理责任，探索建立数据接收方“数据安全管理风险评估”制度。《案例》在管控措施中使用的“合法合规性评估”可视为上述“数据安全管理风险评估”的自发性尝试。《案例》中，被授权企业在申请公共交通数据过程中，

严格遵循“业务必需、最小范围”原则，明确数据使用的目的和方式，并经过多方专家论证，确认申请数据合法合规。同时，数据提供方还对被授权企业定期开展项目审计，以确保符合法律法规文件及应用规范。

其二，《案例》是对“原始数据不出域、数据可用不可见”的有益探索。《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》提出，鼓励公共数据按照“原始数据不出域、数据可用不可见”的要求，以模型、核验等产品和服务等形式向社会提供。《案例》一方面由政府部门将其持有的公共交通数据脱敏后汇聚至公共数据授权运营计算域的可信执行环境中；另一方面采用时空 Transformer 模型（深度学习模型）技术，找到其中上下游“时间与空间”联系，向使用方提供反映交通态势的数据产品，最终打造出通行效率倍增的标准化数智绿波产品。

其三，《案例》是对“公共数据运营期限限制”的有益探索。国家发展改革委、国家数据局发布的《公共数据资源授权运营实施规范（试行）》第十四条规定：“授权运营期限，原则上最长不超过 5 年。”这是因为，较诸公共数据开放，公共数据授权运营是为兼具高风险和高价值的数据所设置的特别规则，一旦被授权运营的数据经评估不再具有高风险属性，就应根据《中共中央办公厅 国务院办公厅关于加快公共数据资源开发利用的意见》的要求，向社会公众开放。《案例》明确设置退出机制，这是公共数据运营期限限制的有力体现。一旦授权运营终止，公共数据主管部门就将及时关闭被授权企业的授权运营域使用资格，有力保障数据的安全性。

国家互联网信息办公室发布《数据出境安全评估申报指南（第三版）》

原载：“网信中国”微信公众号

为了指导和帮助数据处理者规范有序申报数据出境安全评估，国家互联网信息办公室编制了《数据出境安全评估申报指南（第三版）》，对数据处理者申报数据出境安全评估需要提交的相关材料进行了优化简化，明确数据处理者申请延长数据出境安全评估结果有效期的条件、流程、材料等内容。

数据处理者因业务需要向境外提供重要数据和个人信息，符合数据出境安全评估适用情形的，应当根据《数据出境安全评估办法》和《促进和规范数据跨境流动规定》，按照申报指南申报数据出境安全评估。评估结果有效期届满，符合申请延长评估结果有效期条件的，数据处理者可以在有效期届满前 60 个工作日内提出延长评估结果有效期申请。

数据处理者可以通过线上方式申报。请直接访问“数据出境申报系统”（网址：https://sjcj.cac.gov.cn），也可从中国网信网（https://www.cac.gov.cn）首页“全国网信政务办事大厅”栏目访问“数据出境申报系统”。

关于印发《网信部门行政处罚裁量权基准适用规定》的通知

原载：“网信中国”微信公众号

关于印发《网信部门行政处罚裁量权基准适用规定》的通知

国信办通字〔2025〕3 号

各省、自治区、直辖市互联网信息办公室，新疆生产建设兵团互联网信息办公室：

为了规范网信部门行政处罚行为，保护公民、法人和其他组织的合法权益，现将《网信部门行政处罚裁量权基准适用规定》印发给你们，请认真遵照执行。

国家互联网信息办公室

2025 年 6 月 26 日

网信部门行政处罚裁量权基准适用规定

第一条 为了规范网信部门行政处罚行为，保护公民、法人和其他组织的合法权益，根据《中华人民共和国行政处罚法》、《中华人民共和国网络

安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《网信部门行政执法程序规定》等法律、法规、规章和国家有关规定，结合网信工作实际，制定本规定。

第二条 网信部门依据行政处罚裁量权基准行使行政处罚裁量权，适用本规定。法律、法规、规章另有规定的，从其规定。

第三条 本规定所称行政处罚裁量权基准，是指网信部门在实施行政处罚时，按照裁量涉及的违法行为的事实、性质、情节、社会危害程度、当事人主观过错等因素，对法律、法规、规章中的原则性规定或者具有一定弹性的执法权限、裁量幅度等内容进行细化量化而形成的具体执法尺度和标准。

第四条 网信部门适用行政处罚裁量权基准，应当遵循法制统一、公平公正、过罚相当、处罚与教育相结合等原则。

第五条 网信部门行政处罚裁量权基准划分为不予处罚、减轻处罚、从轻处罚、一般处罚、从重处罚等裁量阶次。

不予处罚是指因法定原因对实施违法行为本应给予行政处罚的当事人不再给予行政处罚。

减轻处罚是指减少并处法律、法规、规章规定的行政处罚种类或者低于最低限度的处罚幅度，对当事人实施行政处罚。

从轻处罚是指在法律、法规、规章规定的行政处罚种类和处罚幅度内，适用较轻、较少的种类或者较低的幅度，对当事人实施行政处罚。

一般处罚是指在法律、法规、规章规定的行政处罚种类和处罚幅度内，适用适中的种类或者幅度，对当事人实施行政处罚。

从重处罚是指在法律、法规、规章规定的行政处罚种类和处罚幅度内，适用较重、较多的种类或者较高的幅度，对当事人实施行政处罚。

第六条 有下列情形之一的，应当不予处罚：

（一）违法行为轻微并及时改正，没有造成危害后果的；

（二）当事人有证据足以证明没有主观过错的，法律、行政法规另有规定的，从其规定；

（三）其他依法不予处罚的情形。

初次违法且危害后果轻微并及时改正的，可以不予处罚。

依法不予处罚的，网信部门可以根据情节采取相应的行政监管措施，并应当对当事人进行教育。

第七条 有下列情形之一的，应当从轻或者减轻处罚：

（一）主动消除或者减轻违法行为危害后果的；

（二）受他人胁迫或者诱骗实施违法行为的；

（三）主动供述网信部门尚未掌握的违法行为的；

（四）配合网信部门查处违法行为有立功表现的；

（五）其他依法从轻或者减轻处罚的情形。

第八条 有下列情形之一的，应当从重处罚：

（一）违法行为严重危害网络信息内容安全、网络运行安全、网络数据安全的，违法处理个人信息或者处理个人信息未履行个人信息保护义务情节严重的；

（二）因同种违法行为一年内受到网信部门两次以上行政处罚的；

（三）教唆、胁迫、诱骗他人实施违法行为的；

（四）拒不配合、阻碍、以暴力威胁网信部门执法人员依法执行公务的；

（五）隐匿、毁损、伪造、篡改有关证据的；

（六）对证人、举报人、网信部门工作人员进行打击报复的；

（七）违法行为引起群众强烈反映，引发群体性事件或者造成其他严重不良社会影响的；

（八）违反未成年人保护相关规定情节严重的；

（九）性质恶劣、情节严重、社会危害性较大的其他情形。

第九条 违法行为不具有不予处罚、减轻处罚、从轻处罚或者从重处罚情形的，应当给予一般处罚，法律、法规、规章另有规定的除外。

第十条 当事人同时存在减轻处罚、从轻处罚或者从重处罚等情形的，应当根据案件具体情况综合考量进行处罚。

第十一条 罚款有一定幅度的，在相应的幅度范围内分为从轻处罚、一般处罚、从重处罚。

从轻处罚的罚款数额应当在法定最低限至法定最高限幅度或者倍数区间低于 30%的数额；一般处罚的罚款数额应当在法定最低限至法定最高限幅度或者倍数区间的 30%至 70%的数额；从重处罚的罚款数额应当在法定最低限至法定最高限幅度或者倍数区间超过 70%的数额。

在确定具体处罚数额时，综合考量违法行为的性质、情节和本地区经济社会发展状况等因素，结合执法实践和执法案例，可以以前款规定的百分比为基础上下浮动十个百分点。

第十二条 依法单独处警告、通报批评、没收违法所得的，仅适用不予处罚、一般处罚两种裁量阶次。

第十三条 单位实施违法行为的，对直接负责的主管人员和其他直接责任人员的处罚，应当综合考量相关责任人员的岗位职责、任职时间、履职行为与违法行为的关联性、主观过错程度、主次责任，以及是否对违法行为采取整改措施等因素，参照对单位行政处罚裁量阶次，确定适当的行政处罚。

第十四条 网信部门适用行政处罚裁量权基准，判断违法行为性质、情节以及社会危害程度等，应当综合考量以下因素：

（一）违法行为的具体方法或者手段，当事人实施违法行为的主观过错程度；

（二）违法行为的持续时间、发生次数，违法行为造成的社会影响、危害后果；

（三）违法行为的危害对象及其数量；

（四）当事人本年度内的处罚情况；

（五）当事人获取的违法所得；

（六）当事人的生产经营类型规模、经营情况及其影响力；

（七）当事人改正违法行为的主观态度、配合检查的情况、所采取的整改措施及效果；

（八）法律、法规、规章规定的其他因素。

第十五条 对当事人的同一个违法行为，不得给予两次以上罚款的行政处罚。同一个违法行为违反多个法律规范应当给予罚款处罚的，按照罚款数额高的规定处罚。有两个以上应当给予行政处罚违法行为的，应当分别裁量，合并处罚。

第十六条 省、自治区、直辖市和设区的市、自治州网信部门可以结合工作实际制定本行政区域内的行政处罚裁量权基准。对同一行政执法事项，上级网信部门已经制定行政处罚裁量权基准的，下级网信部门原则上应当直接适用；如下级网信部门不能直接适用，可以结合本地区经济社会发展状况，在法律、法规、规章规定的行政处罚裁量权范围内进行合理细化量化，但不能超出上级网信部门划定的阶次或者幅度。下级网信部门制定的行政处罚裁量权基准与上级网信部门制定的行政处罚裁量权基准冲突的，应当适用上级网信部门制定的行政处罚裁量权基准。

第十七条 网信部门作出行政处罚决定前，应当告知当事人拟作出的行政处罚的内容及事实、理由、依据，并在行政处罚决定书中对行政裁量权基准的适用情况予以明确。

第十八条 网信部门实施行政处罚，适用本部门制定的行政处罚裁量权基准可能出现明显不当、显失公平，或者行政处罚裁量权基准适用的客观情况发生变化的，经本部门主要负责人批准或者集体讨论通过后可以调整适用，批准材料或者集体讨论记录应当列入处罚案卷归档保存。

适用上级网信部门制定的行政处罚裁量权基准可能出现前款情形的，报请上级网信部门批准后，可以调整适用。

第十九条 上级网信部门应当通过行政执法情况检查、行政执法案卷评查等方式，对下级网信部门行使行政处罚裁量权工作进行监督。

因不规范适用行政处罚裁量权基准造成严重后果的，应当依规依纪依法严格追究有关人员责任。

第二十条 本规定自 2025 年 8 月 1 日起施行。

国家互联网信息办公室发布《网信部门行政处罚裁量权基准适用

规定》

原载：“网信中国”微信公众号

近日，国家互联网信息办公室发布《网信部门行政处罚裁量权基准适用规定》（以下简称《规定》），自 2025 年 8 月 1 日起施行。国家互联网信息办公室有关负责人表示，出台《规定》，旨在规范网信部门行政处罚行为，保护公民、法人和其他组织的合法权益。

《规定》明确，行政处罚裁量权基准是指网信部门在实施行政处罚时，按照裁量涉及的违法行为的事实、性质、情节、社会危害程度、当事人主观过错等因素，对法律、法规、规章中的原则性规定或者具有一定弹性的执法权限、裁量幅度等内容进行细化量化而形成的具体执法尺度和标准。明确网信部门适用行政处罚裁量权基准，应当遵循法制统一、公平公正、过罚相当、处罚与教育相结合等原则。

《规定》提出，网信部门行政处罚裁量权基准划分为不予处罚、减轻处罚、从轻处罚、一般处罚、从重处罚等裁量阶次。明确不予处罚、减轻处罚、从轻处罚、从重处罚等具体适用情形。规定违法行为不具有不予处罚、减轻处罚、从轻处罚或者从重处罚情形的，应当给予一般处罚。

《规定》明确，省、自治区、直辖市和设区的市、自治州网信部门可以结合工作实际制定本行政区域内的行政处罚裁量权基准。上级网信部门应当通过行政执法情况检查、行政执法案卷评查等方式，对下级网信部门行使行政处罚裁量权工作进行监督。

关键信息基础设施商用密码使用管理规定

原载：“网信中国”微信公众号

国家密码管理局

国家互联网信息办公室

中华人民共和国公安部

令

第 5 号

《关键信息基础设施商用密码使用管理规定》已经 2025 年 4 月 21 日国家密码管理局局务会议审议通过，并经国家互联网信息办公室、公安部同意，现予公布，自 2025 年 8 月 1 日起施行。

国家密码管理局局长 刘东方

国家互联网信息办公室主任 庄荣文

公安部部长 王小洪

2025 年 6 月 11 日

关键信息基础设施商用密码使用管理规定

第一条 为规范关键信息基础设施商用密码使用，保护关键信息基础设施安全，根据《中华人民共和国密码法》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《商用密码管理条例》和《关键信息基础设施安全保护条例》、《网络数据安全管理条例》等有关法律、行政法规，制定本规定。

第二条 依据《中华人民共和国网络安全法》、《关键信息基础设施安全保护条例》等法律、行政法规和国家有关规定认定的关键信息基础设施的商用密码使用管理，适用本规定。

第三条 国家密码管理部门会同国家网信部门、国务院公安部门负责规划、指导和监督全国的关键信息基础设施商用密码使用管理工作，建立关键信息基础设施商用密码使用管理信息共享机制。

县级以上地方各级密码管理部门会同网信部门、公安机关负责指导和监督本行政区域的关键信息基础设施商用密码使用管理工作。

第四条 关键信息基础设施保护工作部门（以下简称保护工作部门）在职责范围内负责监督管理本行业、本领域关键信息基础设施商用密码使用工作，单独编制本行业、本领域商用密码使用规划或者纳入本行业、本领域的关键信息基础设施安全规划并组织实施，指导本行业、本领域关键信息基础设施运营者（以下简称运营者）开展商用密码相关制度、人员、经费等保障工作。

保护工作部门应当于每年 3 月 31 日前向国家密码管理部门、国家网信部门、国务院公安部门报

告上一年度本行业、本领域关键信息基础设施商用密码使用管理情况。

关键信息基础设施发生涉及商用密码的重大网络安全事件或者发现涉及商用密码的重大网络安全威胁时，保护工作部门应当及时向国家密码管理部门、国家网信部门、国务院公安部门报告，指导运营者开展应急处置，必要时开展商用密码应用安全性评估。

第五条 运营者应当按照相关法律、行政法规和国家有关规定，遵循国家商用密码管理、网络安全等级保护、关键信息基础设施安全保护等制度要求，使用商用密码保护关键信息基础设施，同步规划、同步建设、同步运行商用密码保障系统，并定期开展商用密码应用安全性评估。

运营者应当于每年 1 月 31 日前向所属的保护工作部门报告上一年度关键信息基础设施商用密码使用以及商用密码应用安全性评估开展情况。

第六条 运营者应当加强关键信息基础设施商用密码使用制度保障，建立商用密码使用、应急处置、重大事件报告等关键信息基础设施商用密码使用管理制度。

运营者的主要负责人对关键信息基础设施商用密码使用管理负总责，负责关键信息基础设施商用密码使用和涉及商用密码的重大网络安全事件处置工作。

第七条 运营者应当加强关键信息基础设施商用密码使用人员保障，配备取得密码相关专业学历或者密码相关国家职业技能等级认定证书的专业人员分别承担密钥管理员、密码操作员等职责，配备具有安全审计专业能力的人员承担密码安全审计员职责。

运营者应当对密码相关专业人员进行安全背景审查，并定期组织其参加密码相关业务技能培训，提高密码相关专业人员的商用密码使用能力。

第八条 运营者应当加强关键信息基础设施商用密码使用和应用安全性评估经费保障，将商用密码使用和应用安全性评估经费纳入网络安全和信息化经费安排。

第九条 关键信息基础设施使用的商用密码产品、服务应当经检测认证合格，使用的密码算法、密码协议、密钥管理机制等商用密码技术应当通过国家密码管理部门审查鉴定。

运营者采购涉及商用密码的网络产品和服务，影响或者可能影响国家安全的，应当按照《网络安全审查办法》进行网络安全审查。

第十条 关键信息基础设施应当按照国家数据安全保护、个人信息保护有关要求，使用商用密码对其存储、使用、传输的核心数据、重要数据和个人信息进行保护。

第十一条 关键信息基础设施规划阶段，其运营者应当依照相关法律、行政法规和标准规范，根据商用密码应用需求，制定商用密码应用方案，规划商用密码保障系统并纳入关键信息基础设施安全规划统筹部署。

运营者应当自行或者委托商用密码检测机构对商用密码应用方案进行商用密码应用安全性评估。商用密码应用方案未通过商用密码应用安全性评估的，不得作为商用密码保障系统的建设依据。

第十二条 关键信息基础设施建设阶段，其运营者应当按照通过商用密码应用安全性评估的商用密码应用方案组织实施，落实商用密码安全防护措施，建设商用密码保障系统。建设过程中需要调整商用密码应用方案的，应当重新开展商用密码应用安全性评估，评估通过后方可按照调整后的商用密码应用方案继续建设。

关键信息基础设施运行前，其运营者应当自行或者委托商用密码检测机构开展商用密码应用安全性评估。关键信息基础设施未通过商用密码应用安全性评估的，运营者应当进行改造，改造期间不得投入运行。

第十三条 关键信息基础设施建成运行后，其运营者应当自行或者委托商用密码检测机构每年至少开展一次商用密码应用安全性评估，确保关键信息基础设施商用密码的正确使用和商用密码保障系统的有效运行。关键信息基础设施未通过商用密码应用安全性评估的，运营者应当进行改造，并

在改造期间采取必要措施保证关键信息基础设施运行安全。

第十四条 本规定施行前正在建设的关键信息基础设施，其运营者应当加强商用密码应用方案编制论证，建设完善商用密码保障系统，并按照本规定第十二条开展商用密码应用安全性评估。

本规定施行前已经投入运行的关键信息基础设施，其运营者应当按照本规定第十三条开展商用密码应用安全性评估。

第十五条 开展关键信息基础设施商用密码应用安全性评估，应当符合《商用密码应用安全性评估管理办法》有关规定。

关键信息基础设施商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评加强衔接，避免重复评估、测评。

第十六条 国家密码管理部门负责建设和管理国家关键信息基础设施商用密码运行安全管理基础设施，统筹保护工作部门建设本行业、本领域关键信息基础设施商用密码运行安全管理基础设施，会同国家网信部门、国务院公安部门分析研判关键信息基础设施商用密码运行安全态势，协同应对处置重大商用密码运行安全威胁。

第十七条 密码管理部门应当定期组织开展关键信息基础设施商用密码使用情况监督检查。保护工作部门应当定期对本行业、本领域关键信息基础设施商用密码使用情况进行检查并提出改进措施，必要时可以自行或者委托商用密码检测机构等专业机构进行商用密码应用安全性评估。

运营者对密码管理部门和保护工作部门开展的关键信息基础设施商用密码使用情况监督检查应当予以配合，根据监督检查意见及时进行整改并向保护工作部门报告整改情况，保护工作部门应当将整改情况向国家密码管理部门报告。

开展关键信息基础设施商用密码使用情况监督检查应当加强协同配合、信息沟通，避免不必要的检查和交叉重复检查。监督检查不得收取费用，不得要求被监督检查单位购买、使用指定单位或者指定品牌的商用密码产品、服务。

第十八条 密码管理部门、有关部门、商用密码检测机构及其工作人员对其在履行职责中知悉的国家秘密、商业秘密和个人隐私承担保密义务，不得泄露或者非法向他人提供。

第十九条 运营者违反《中华人民共和国密码法》、《中华人民共和国网络安全法》、《商用密码管理条例》、《关键信息基础设施安全保护条例》和本规定有关条款，有下列情形之一的，由密码管理部门责令改正，给予警告；拒不改正或者有其他严重情节的，处 10 万元以上 100 万元以下罚款，对直接负责的主管人员处 1 万元以上 10 万元以下罚款：

（一）未按照要求使用商用密码保护关键信息基础设施，同步规划、同步建设、同步运行商用密码保障系统的；

（二）关键信息基础设施使用的商用密码产品、服务未经检测认证合格的；

（三）关键信息基础设施使用的密码算法、密码协议、密钥管理机制等商用密码技术未通过国家密码管理部门审查鉴定的；

（四）关键信息基础设施规划阶段，未制定商用密码应用方案，或者未对商用密码应用方案进行商用密码应用安全性评估的；

（五）关键信息基础设施建设阶段，未按照通过商用密码应用安全性评估的商用密码应用方案建设商用密码保障系统的；

（六）关键信息基础设施运行前，未开展商用密码应用安全性评估，或者未通过商用密码应用安全性评估且未进行改造的；

（七）关键信息基础设施建成运行后，未定期开展商用密码应用安全性评估，或者未通过定期开展的商用密码应用安全性评估且未进行改造的。

第二十条 运营者违反《中华人民共和国密码法》、《中华人民共和国网络安全法》、《商用密码管理条例》、《关键信息基础设施安全保护条例》和本规定第九条，使用未经安全审查或者安全审查未通过的涉及商用密码的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额 1 倍以上

10 倍以下罚款；对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款。

第二十一条 运营者违反《中华人民共和国密码法》、《中华人民共和国网络安全法》、《商用密码管理条例》、《关键信息基础设施安全保护条例》和本规定第十七条，无正当理由拒不接受、不配合或者干预、阻挠密码管理部门、有关部门的商用密码监督管理的，由密码管理部门、有关部门责令改正，给予警告；拒不改正或者有其他严重情节的，处 5 万元以上 50 万元以下罚款，对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款；情节特别严重的，责令停业整顿。

第二十二条 运营者违反本规定，有下列情形之一的，由密码管理部门、有关部门依据职责责令改正：

（一）未按照要求报告上一年度关键信息基础设施商用密码使用以及商用密码应用安全性评估开展情况的；

（二）未建立关键信息基础设施商用密码使用管理制度的；

（三）未按照要求配备密钥管理员、密码操作员、密码安全审计员的；

（四）未保障关键信息基础设施商用密码使用和应用安全性评估经费的。

第二十三条 从事关键信息基础设施商用密码使用监督管理工作的人员滥用职权、玩忽职守、徇私舞弊，或者泄露、非法向他人提供在履行职责中知悉的商业秘密、个人隐私、举报人信息的，依法给予处分。

第二十四条 属于国家政务信息系统的关键信息基础设施的商用密码使用管理，除应当遵守本规定以外，还应当按照《国家政务信息化项目建设管理办法》（国办发〔2019〕57 号）等有关规定要求执行。

第二十五条 本规定自 2025 年 8 月 1 日起施行。

关于发布生成式人工智能服务已备案信息的公告（2025 年 4 月至 6 月）

原载：“网信中国”微信公众号

促进生成式人工智能服务创新发展和规范应用，网信部门会同有关部门按照《生成式人工智能服务管理暂行办法》要求，持续开展生成式人工智能服务备案工作。4 月至 6 月，新增 93 款生成式人工智能服务在国家网信办完成备案，对于通过 API 接口或其他方式直接调用已备案模型能力的生成式人工智能应用或功能，由地方网信办开展登记，本阶段新增 74 款完成登记。截至 2025 年 6 月 30 日，累计有 439 款生成式人工智能服务完成备案，233 款生成式人工智能应用或功能完成登记。现将相关信息予以公告。

提供具有舆论属性或者社会动员能力的生成式人工智能服务的，可通过属地网信部门履行备案或登记程序。已上线的生成式人工智能应用或功能，应在显著位置或产品详情页面公示所使用已备案或登记生成式人工智能服务情况，注明模型名称、备案号或上线编号。

关于征求《数据安全技术 电子产品信息清除技术要求》强制性国家标准（征求意见稿）意见的通知

原载：“国家数据局”微信公众号

根据国家标准化管理委员会标准制修订计划，中央网络安全和信息化委员会办公室已组织完成了《数据安全技术 电子产品信息清除技术要求》强制性国家标准的征求意见稿，现公开征求意见。请于 2025 年 9 月 13 日前将意见反馈给组织起草部门。

联系人：王秉政

联系电话：010-64102746

联系邮箱：lingjingbin@cac.gov.cn

中央网络安全和信息化委员会办公室

2025 年 7 月 14 日

地方动态|辽宁省人民政府办公厅关于印发《辽宁省数字政府建设实施方案（2025—2027 年）》的通知

原载：“国家数据局”微信公众号

辽宁省人民政府办公厅关于印发《辽宁省数字政府建设实施方案（2025—2027 年）》的通知

辽政办发〔2025〕13 号

各市人民政府，省政府各厅委、各直属机构：

《辽宁省数字政府建设实施方案（2025—2027 年）》已经省政府同意，现印发给你们，请认真贯彻执行。

辽宁省人民政府办公厅

2025 年 7 月 2 日

辽宁省数字政府建设实施方案

（2025—2027 年）

为深入贯彻落实党中央、国务院关于数字政府建设的决策部署，加快构建数字化、智能化政府运行新形态，推进政府治理体系和治理能力现代化，结合我省实际，制定本方案。

一、总体要求

以习近平新时代中国特色社会主义思想为指导，坚持统筹集约、数据赋能、利企惠民、安全可控，着力构建与国家治理体系和治理能力现代化相适应的数字政府体系。到 2027 年，全省一体化基础设施高效集约，一体化数据资源开放共享，“一网通办”、“一网协同”、“一网统管”应用数智赋能，一体化安全防护体系动态防御，“1131”数字政府运行工作体系基本建成。

二、建设完善一体化基础支撑体系

（一）强化云网设施支撑

1. 提升政务云统揽能力。统筹整合政务云资源，推进非涉密政务系统向政务云迁移，建立统一调度机制，开展效能评估、动态调配。完善省政府数据中心异地数据灾备和数据备份功能。（责任单位：省数据局等有关单位，各市政府、省沈抚改革创新示范区管委会。以下均需各市政府和省沈抚改革创新示范区管委会落实，不再列出）

2. 提升电子政务网络支撑能力。强化电子政务网络统筹建设管理，深化非涉密业务专网与电子政务外网整合。提高省级政务外网互联网出口带宽，推进省政务外网互联网协议第 6 版（IPv 6 ）地址部署和应用，提升电子政务外网的移动接入能力。（责任单位：省数据局等有关单位）

（二）强化共性应用支撑

3. 完善数字政府基座系统。聚焦应急、水利、生态环境等领域，基于共性支撑平台，结合人工智能技术，通过跨技术集成、跨主体协作和跨场景适配，打造防汛减灾、气象监测等个性化应用场景。（责任单位：省数据局、省自然资源厅、省生态环境厅、省水利厅、省应急厅等有关单位）

（三）强化人工智能支撑

4. 增强一体化基础大模型服务能力。统筹算力资源，聚焦政务服务、社会治理、机关办公等领域，搭建“人工智能中台”，提供知识库、接口调用等基础能力，探索智能问答、政策匹配、数据分析等应用。（责任单位：省数据局等有关单位）

三、建设完善一体化数据资源体系

（一）推动公共数据高质量供给

5. 推行公共数据统一目录管理。规范化梳理现有数据资源目录，实现全省公共数据资源“一本账”管理。推进人口数据、法人数据、电子证照数据、信用数据、自然资源与空间地理数据等基础数据库共建共用。建设教育服务、文化旅游、医疗健康等重点领域专题库。（责任单位：省数据局、省发展改革委、省教育厅、省公安厅、省民政厅、省自然资源厅、省文化和旅游厅、省卫生健康委、省市场监管局等有关单位）

6. 强化公共数据源头治理。推动各地区、各部门整合内部业务系统，建立集成的一体化应用系统。推进业务数据整合，核心职责业务全部建立专题数

据库。开展公共数据供给能力提升行动，推进高频重点数据归集，构建数据质量标准体系。（责任单位：省数据局等有关单位）

（二）促进公共数据高效率流通

7. 完善公共数据管理机制。健全数据资源管理统筹协调机制，明确数据归集、共享、开放、应用、安全、存储、归档等责任。出台公共数据资源登记管理制度，建设省公共数据资源登记平台，积极融入全国一体化公共数据资源登记体系。（责任单位：省数据局等有关单位）

8. 健全公共数据供需对接机制。制定供需对接管理规范，动态编制数据共享需求和责任清单。推进数据直达基层，为“高效办成一件事”、基层报表数据“只报一次”等基层数据创新应用提供支撑。（责任单位：省数据局等有关单位）

（三）深化公共数据高水平应用

9. 推动公共数据高效共享。依托一体化数据资源管理系统，实现政府信息系统与党委、人大、政协、法院、检察院等信息系统互联互通和数据按需共享。支持各地区、各部门创新大数据科学辅助决策应用，促进政务运行高效协同。（责任单位：省数据局等有关单位）

10. 促进公共数据开发利用。完善省公共数据资源开放平台功能，动态更新公共数据开放目录，建立公共数据开放需求受理反馈机制。围绕医疗健康、城市治理、应急管理等行业领域，培育一批典型应用场景。（责任单位：省数据局、省住房城乡建设厅、省卫生健康委、省应急厅等有关单位）

四、建设完善“三网”数智应用体系

（一）推进政务服务“一网通办”

11. 提升线上服务效能。依托全省一体化政务服务平台，统筹整合各类网上办事入口，拓展电子证照和电子印章应用范围，丰富“辽事通”应用场景。推动“高效办成一件事”重点事项落地。（责任单位：省数据局等有关单位）

12. 扩展涉企增值服务。依托“辽企通”平台向企业提供全生命周期服务，推广扫码入企应用，推动更多优惠政策免申即享、直达快享。强化 12345 政务服务便民热线“1 号键”企业服务专线建设，完善涉企诉求问题高效闭环解决机制。（责任单位：省数据局等有关单位）

13. 创新智慧政务应用。围绕省市政务服务网、12345 政务服务便民热线等应用场景，探索人工智能大模型创新应用。聚焦文化旅游、医疗健康、教育服务、养老助残等领域，提升数字惠民服务水平。（责任单位：省数据局、省教育厅、省民政厅、省农业农村厅、省文化和旅游厅、省卫生健康委、省残联等有关单位）

（二）推进机关运行“一网协同”

14. 健全一体化协同办公体系。推进非涉密办公业务系统、公车用房等机关事务管理系统接入“辽政通”。推动电子公文标准化，逐步实现相关业务全程电子化单轨运行。推进机关单位数字档案室和数字档案馆建设。（责任单位：省数据局、省委机要局、省档案局、省机关事务局等有关单位）

（三）推进社会治理“一网统管”

15. 提升城市治理能力。推动人、地、事、物、组织等多维度数据融合，创新社会防控、公共安全、基层治理、市场监管、应急管理等领域应用，提升态势实时感知、风险智能研判、处置及时协同等能力。（责任单位：省数据局等有关单位）

16. 提升经济调节能力。推动人口、就业、产业、投资、消费、贸易、区域等经济领域关键数据的归集、治理和应用，构建经济治理基础数据库。推动经济运行监测系统建设，提升财政、税收、就业、工业、统计、审计等领域数字化监测预警水平。（责任单位：省发展改革委、省工业和信息化厅、省财政厅、省人力资源社会保障厅、省农业农村厅、省商务厅、省卫生健康委、省审计厅、省统计局、省税务局等有关单位）

17. 提升市场监管能力。加强“互联网+监管”系统建设，实现监管执法部门、事项、人员等应接尽接。加强重点领域数字化追溯监管，拓展“食安辽宁”一体化智慧监管服务平台、药品智慧监管系统应用场景。推动部门联合“双随机、一公开”监管转入常态。（责任单位：省市场监管局、省药监

局等有关单位）

18. 提升社会管理能力。提升网上行政复议、网上信访、网上调解、智慧法律援助等水平。构建新型基层管理服务平台，推进智慧社区建设。完善公安大数据智能化应用和智能感知体系，推动智慧公安建设。构建省应急管理综合数字化平台，深化智慧应急建设。（责任单位：省委社会工作部、省公安厅、省司法厅、省应急厅、省信访局、省法院、省检察院等有关单位）

（一）完善网络安全保障体系

20. 建立健全网络安全事件应急预警处置和协同联动机制。常态化开展网络安全监督检查、安全预警、应急演练工作，提升安全防护能力。落实关键信息基础设施保护、网络安全等级保护等制度，推进政务系统商用密码应用改造和密码应用评估工作。（责任单位：省委网信办、省委机要局、省公安厅、省数据局等有关单位）

（二）提升数据安全保护能力

21. 构筑公共数据全生命周期安全防护体系。对公共数据开展分级分类保护，强化全生命周期监管，建立安全防护管理制度。常态化开展安全风险评估、制度执行情况监督检查。（责任单位：省委国安办、省委网信办、省数据局等有关单位）

（三）加强人工智能风险防范

22. 推动人工智能安全发展。建立人工智能安全评估、风险防范机制，促进大模型应用安全合法，实施分类管理，推动协同治理，强化问题处置。（责任单位：省委网信办、省委保密办、省发展改革委、省工业和信息化厅、省公安厅、省国家安全厅等有关单位）

六、保障措施

（一）强化工作机制统筹。省数字辽宁建设工作领导小组要统筹抓好重要任务落实。各级政府要将数字政府重大改革、重点项目、重要任务纳入重要议事日程。设立数字政府首席数据官，协调推动数字政府建设。（责任单位：省数据局、省发展改革委、省财政厅等有关单位）

（二）强化标准规范统筹。组建省数据标准化专业技术委员会，推动制定实施数据基础通用标准，健全完善数据流通利用安全标准体系。完善省级政务信息化项目管理办法，推动共性项目统建、特色项目自建。（责任单位：省数据局、省发展改革委、省市场监管局等有关单位）

19. 提升生态环境保护能力。打造全省生态环境业务综合平台，强化大气、水、土壤等数据资源综合开发利用。健全水利智能监测感知体系，统筹推进数字孪生水利建设。构建精准感知、智慧管控的协同治理体系，完善省自然资源和空间地理基础数据库一体化服务平台功能。（责任单位：省生态环境厅、省自然资源厅、省水利厅等有关单位）

五、建设完善一体化安全防护体系

（三）强化效能评价统筹。建立数字政府建设评价指标体系，定期组织评价并对相关指标进行动态调整，加强评价结果分析和跟踪指导，强化经验总结和宣传推广。（责任单位：省数据局等有关单位）

（四）强化运维运营统筹。建立数字政府运维保障机制，组建专业化运营队伍，提升全域全层级运营服务能力，优化用户使用体验，以运营促建设，以运营促提升。（责任单位：省数据局等有关单位）

（五）强化数智育才统筹。将提高数字治理能力作为各级党校（行政学院）的重要教学培训内容，创新数字政府建设人才引进培养使用机制。统筹政府、高校、科研院所等各方力量，持续激发数字人才创新活力。（责任单位：省委组织部、省教育厅、省科技厅、省人力资源社会保障厅、省数据局等有关单位）

美国法院：购买书籍用于 AI 训练属于合理使用

原载：“HexCode 数据何规”微信公众号

美国加州北区联邦地区法院在 Anthropic 版权侵权案裁定：准予 Anthropic 关于大模型训练行为及购买后扫描属合理使用；驳回其关于盗版图书馆副本可豁免的请求；盗版责任问题进入审判程序。”

该案明确区分 AI 训练行为与数据获取方式，确立“技术中立，手段须正”原则，为全球生成式 AI 版权合规提供标杆规则。

裁判文书在这里：

https://www.documentcloud.org/documents/25982181-authors-v-anthropic-ruling/，以下是核心裁判观点：

1、LLM 训练行为：复制作品训练 AI 是否构成《版权法》第 107 条合理使用（fair use）？**支持 Anthropic，构成合理使用。**

2、图书馆副本合法性：

(a)盗版副本：能否因后续用于训练豁免侵权？支持原告，构成侵权。

(b)扫描副本：购买实体书后转换为数字格式是否侵权？支持 Anthropic，构成合理使用。

3、未用于训练的盗版副本保留行为是否侵权？未决

一、基础事实及争议焦点

（一）基础事实

1、盗版行为

Anthropic 于 2021 年通过盗版网站（Books3、LibGen、PiLiMi）下载超过 700 万本受版权保护书籍的数字副本，包含每位原告至少两部作品。

2、购买扫描行为

2024 年，Anthropic 花费数百万美元购买实体书（多二手），委托服务商进行破坏性扫描（destructive scanning），流程为：剥离装订→切页→扫描为 PDF→丢弃纸质书。

3、中央图书馆建设

整合盗版与扫描副本建立“通用研究库”，计划永久保留所有书籍，即使部分永不用于 AI 训练。

4、大模型训练

（1）复制子集：从图书馆选取书籍子集

（2）清洗（cleaning）：移除页眉/页脚等冗余文本

（3）分词化（tokenization）：将词语转为数字标记（token）

（4）压缩存储：将统计关系映射至 LLM，近乎“记忆”原作。

“Each trained LLM retained ‘compressed’ copies.....mapped almost verbatim.”（页 7）

译文：“每个训练完成的 LLM 保留‘压缩’副本...近乎逐字映射原作。”

（二）争议焦点

1、LLM 训练行为：复制作品训练 AI 是否构成《版权法》第 107 条合理使用（fair use）？

2、图书馆副本合法性：(a)盗版副本：能否因后续用于训练豁免侵权？(b)扫描副本：购买实体书后转换为数字格式是否侵权？

3、责任范围：未用于训练的副本保留是否需独立追责？

二、美国合理使用制度

（一）法律渊源

《版权法》第 107 条确立四要素检验标准（four-factor test），判断合理使用时需考量：(1) 使用目的与性质；(2) 作品性质；(3) 使用数量与实质；(4) 对潜在市场的影响。

（二）四要素检验法要点

1、使用目的与性质（Purpose and Character）

（1）变革性（Transformative）为核心：二次使用是否“增加新表达、意义或功能”（Google v.Oracle,593 U.S.1(2021)）。

（2）商业性质非绝对障碍：但商业用途需更强变革性证明（Campbell v. Acuff-Rose, 510 U.S. 569 (1994)）。

（3）主观意图无关：以客观行为（objective inquiry） 界定用途（Warhol v. Goldsmith, 598 U.S. 508, 544-45 (2023)）。

2、作品性质（Nature of Work）

（1）创造性梯度：虚构作品（如小说）比事实作品（如传记）受更强保护。

（2）发表状态：未发表作品保护力度高于已发表作品。

3、使用数量与实质（Amount and Substantiality）

（1）比例原则：复制量需与合理目的相称，

但全文复制未必侵权（如搜索引擎缩略图，见 Perfect 10 v. Amazon 案）。

（2）关键焦点：所取内容是否构成原作“核心精华”（Harper & Row v. Nation Enters., 471 U.S. 539 (1985)）。

4、市场影响（Effect on Market）

（1）核心关切：是否替代原作市场（market substitution）或侵害潜在授权市场（potential licensing market）。

（2）新兴市场争议：版权人不可垄断与版权无关的新兴市场（Sega v. Accolade, 977 F.2d 1510 (9th Cir. 1992)）。

5、司法适用原则

（1）整体权衡（weighed together）：四要素无优先级，需综合评估（Campbell, 510 U.S. at 578）。

（2）情境敏感（context-specific）：无机械公式，依个案调整（Warhol, 598 U.S. at 525）。

三、法院裁判观点

（一）大模型训练行为：构成合理使用

1、高度变革性

页码 14：使用版权作品训练 LLM 生成新文本具有本质变革性...旨在创造不同事物。

训练 LLM 生成新文本是高度变革性使用：类比人类学习写作过程，旨在创造不同作品，非复制原作。

2、作品性质

页 24：“第二要素（作品性质）对合理使用不利.....但主要功能在于辅助评估其他要素。”

承认作品含创造性表达（不利因素），但此要素单独不决定结果。

3、全文复制的合理性

页 26：因使用海量作品具合理必要性，使用任一作品训练 LLM 的合理性与其他作品无异。”

复制全书具有合理性：训练需海量文本，且无证据显示输出内容替代原作。合理必要≠严格必要（reasonably necessary ≠strictly necessary）。

4、无市场替代

页 28：原告主张训练将导致竞争作品激增...但此竞争性替代非版权法关切类型。该法旨在促进原创作品，而非保护作者免于竞争。

（1）不损害现有市场：AI 输出与原作无竞争关系

（2）不保护新兴市场：版权法不赋予作者控制“AI 训练”用途的权利，“AI 生成竞争作品不属版权法保护范畴（not protect authors against competition）”。

结论：

训练行为属合理使用。除作品性质外，其余要素均支持此结论.....涉案技术技术本身是我们毕生所见最具变革性的之一（among the most transformative many of us will see）。当输出未侵权时，训练行为如同人类阅读后创作新作品，属合理使用。

(二) 购买后扫描行为：构成合理使用

核心逻辑：格式转换系空间节约与可搜索性（space-saving and searchability） 的物理性调整，不涉内容衍生。

页 15：“存储与可搜索性非作品创造性属性，而是围绕作品的物理属性。”

页 25：“数字副本应被视同正版印刷副本。”

1、变革性认定

页 16：“存储与可搜索性非作品的创造性属性，而是围绕作品的物理属性或关于作品的信息属性...转换目的系节约空间并实现搜索功能，属变革性使用。”

2、限制条件

页 16：“每本购得实体书的复制均以一对一替换：纸质原件销毁，数字副本未向公司外部分发、展示或出售。”

3、类比先例

页 15：若 Texaco 公司将期刊文章复制为微缩胶片以节省空间，此用途可能构成有说服力的变革性使用”（引 Texaco 案）。

结论：

页 31：实体书转数字副本系合理使用... 第一

要素强烈支持，第三要素支持，第四要素中立，仅第二要素轻微不利。

（三）盗版图书馆副本：不构成合理使用

1、要素一：非变革性独立用途

页 18："Anthropic 未将盗版副本仅用于训练...建立中央图书馆本身即独立用途.....盗版构建研究图书馆而不付费的行为，系非变革性使用。"

页 19：盗版构建研究图书馆而不付费，本身即独立用途——且非变革性。

页 21："盗版意图明确：为建立本可付费的图书馆却拒不付费。"

主观恶意，盗版意图明确：高管邮件称"避免法律/业务麻烦"（avoid "legal/practice/business slog"）。

法律定性：副本留存"直至永远"（store everything forever），即使永不用于训练。

2、全文复制

页 27："Anthropic 复制了数百万本书籍（含原告作品）.....第三要素对盗版副本的合理使用不利。"

复制全书且直接替代正版市场。

3、市场影响

页 30："盗版图书馆副本显然挤占了原告作品的市场需求：一本抵一本（copy for copy）.....若纵容此类行为，将摧毁整个出版市场。"

盗版替代正版：Anthropic 本可购买或借阅（如 Google Books 模式），却选择侵权。

4、反驳"最终用途正当化"论点

页 19-20："Anthropic 主张'最终用途正当化手段'，但最高法院要求客观评估每一复制行为的用途... 其盗版时的自述（'建立研究图书馆'）恰恰证明该独立用途的非变革性。"

最高法院要求逐项评估用途（use-by-use analysis），不因最终目的豁免前期侵权。

结论："盗版副本不适用合理使用..... 所有要素均不利。Anthropic 需承担侵权责任。"（页 31）

(四)其他裁决

1、非训练用途副本

页 31："针对从图书馆副本复制的非训练用途行为（如员工搜索或其他用途），因证据不足不予即决判决，留待审判解决。"

因证据不足，不予即决判决。

2、赔偿责任

页 32："Anthropic 事后购买正版不免除盗版责任... 将就盗版副本进行侵权与赔偿审判，包括实际损失或法定赔偿（含故意侵权加重赔偿）。"

Anthropic 事后购买正版不免除盗版责任（含故意侵权加重赔偿）进入审判程序。

四、总结

Anthropic 案既承认购买正版书用于大模型训练行为（类比人类学习过程）属于合理使用，又严厉否定盗版数据获取，斥为"固有且不可豁免的侵权"，更斩断企业以训练之名囤积盗版资源库的后路。判决通过四要素的精密切割（训练行为合法/购买正版书转换合法/盗版行为违法），为 AI 产业划定"创新可嘉，盗版必究"的红线，既避免版权成为技术枷锁，又捍卫创作市场秩序。

（技术编辑：何芮）

研究动态

基础理论

1. 数字时代合同合意的制度困境及其解决机制（杨彪）

来源：《比较法研究》2025 年第 3 期

平等协商下的合同合意作为交易公平性的根基，是确保市场持续繁荣的关键要素，探讨合同合意问题有助于深度理解数字场景下交易行为的变化及其影响。低质量的格式交易泛滥，从过去的条款同意到今天的条款通知，表明合同合意制度已经形同虚设，互联网市场和消费市场的效率正在严重流失。强化提示说明义务和事后合同解释的治理思路无法解决形式主义立法带来的合同单方支配问题。未来的合同法改革应高度重视认知因素和技术因素，对合同合意制度进行彻底的体系化再造，以重拾日渐消亡的交易共识。数字时代合同合意制度困境的解决思路是采取更强势的事前行政监管和干预，将治理的重心放在商家而非消费者一端，激励其提供更贴近认知决策心理、更简单、更透明的合同。

2. 数字法律行为的逻辑构成与类型分析（郑智航）

来源：《当代法学》2025 年第 3 期

数字法律行为是指通过网络、数据和算法等为主要呈现或表达方式而实施的能够引起法律关系产生、变更和消灭的活动。技术与人的行为的深度结合，使法律行为的手段与方法得到了数字化重塑，并体现为交易的智能化、权力主体行为的智能化。网络空间的数字化和即时性使法律行为摆脱了物理空间的束缚。数字科技正在重塑法律行为的构造性要素，并对法律行为的规范性、意志性和主体性提出挑战。数字法律行为的表达特征主要体现在虚实同构的行为表达空间、人机互动的行为表达方式以及二元治理的表达约束机制。数字法律行为主体的主观状态不仅受到自身现实场域的影响，还受到网络规则及虚拟场域所形成的压力或影响的限制。数字法律行为的行为过程具有更高的技术性、自动性和不可控性的特点。数字空间中跨时空的人际交互模式导致数字法律行为可能会引发更加多样化的社会性风险。数据处理、算法决策、线上交易和虚拟社交是数字法律行为的主要类型。数据处理与算法决策的行为主体一般为大型互联网企业、

平台或公权力机关等掌握数据技术和资源的组织，而线上交易与虚拟社交的行为主体还包括了不掌握数据技术和资源的普通数字用户。

3. 论我国数字经济政策的法律化（宋保振）

来源：《东方法学》2025 年第 3 期

数字经济政策法律化是基于我国数字经济治理法治化目标，对数字经济领域既有“政策—立法”二元治理模式的优化。当下数字经济政策法律化面临着“政策体系繁杂、内容抽象且稳定性不足”“欠缺转化为具体法律规范的理据和标准”，以及“政策的时效性和程序性限制了转化进程”三重困境，这些困境包括多项具体问题。立法中的央地关系构成数字经济政策法律转化的现实逻辑，基于央地立法互动，可以从“转化为不同法律规范”以及“优化促进型立法”两方面，开展数字经济政策法律化的路径设计。当下我国数字经济政策的法律转化可从三方面具体展开：第一，构建“法源性”数字经济政策的识别标准；第二，明确转化为不同类型法律规范的具体要求；第三，完善立法规划和立法审议阶段的操作机制。

4. 算法合同重大误解的救济机制（杨勇）

来源：《东方法学》2025 年第 3 期

相较于一般交易场景中的重大误解，算法合同重大误解呈现较多特殊性。算法用于订立合同时，当事人对合同订立的介入度降低，相对人更不易察觉交易异常状况。自主化决策算法加剧了算法系统出现重大误解的风险。无法借助代理法规则解决算法合同重大误解问题。风险归责思想对于解决自动化算法中的重大误解，仍具有重要价值，但可能会忽视信赖保护价值。对自主化决策算法而言，风险归责思想意义有限。算法作出的决策，偏离算法使用人的预期，构成动机错误，并非排除算法使用人基于重大误解撤销权的正当理由。相对人不存在合理信赖时，在能够实现算法使用人真意保护与相对人信赖保护平衡的基础上，可赋予算法使用人以撤销权。与此同时，自动化算法使用人应对相对人的信赖利益损失承担基于过错的损害赔偿责任，自主化决策算法使用人则应承担无过错责任。

5. 新技术新应用风险规制的结构性反思与法律理念的重塑（汪庆华）

来源：《法律科学(西北政法大学学报)》2025 年第 3 期

新技术新应用是数字经济发展的主要动力。对于人工智能等新技术新应用，我国没有采取统一立法的模式，而是针对特定技术和行业应用，出台专门的规则。我国对新技术新应用的规制经历了从最初的规制不足，到目前的及时跟进、动态均衡。在风险规制的视野下，我国的新技术新应用立法呈现出即时性、行为规制以及法律效力的溢出性等特征，具有作为预防手段、非对称监管、动态监管等结构性要素。就风险规制合宪性的一般分析框架而言，新技术新应用的立法需要满足法律保留原则、比例原则和明确性原则。

6. 可信数字身份的法律保障（李晓楠）

来源：《法律科学(西北政法大学学报)》2025 年第 3 期

数字身份是现实世界中自然人身份在数字空间的映射，其可信性构成了数字空间安全的重要保障、数字经济的信任基础、数字治理的有效工具。当前法律规制未能有效满足数字身份的可信性需求，包括安全、互操作和个人控制等，制度碎片化有余而体系化不足、纵向规范有余而横向标准支撑不足、风险防控有余而个人控制不足。随着数字身份法律内涵的不断扩张，通过法律规制实现可信数字身份构建应当注重规范与标准的融合、个人控制与数字身份处理的协调、安全性与效率性的平衡。在具体制度层面上，应在基于全流程的数字身份安全监管制度、基于认证效力互认的数字身份互操作制度、基于权益保障的数字身份个人控制制度等方面进行适应性的制度体系革新。

7.“数字逝者”技术的媒介性与关系型规制（陈曦宜）

来源：《法学家》2025 年第 3 期

“数字逝者”技术对现世性的法律规范构成冲击，引发独有的悼念秩序困境和规制难题。既有的研究提出三种规制方案：确定“数字遗存”的归属；引入生前意思自治制度；预先限制技术用途。此三种方案将技术客体化而忽略了技术对社会秩序的建构性，且因具有个体主义倾向，而对生者与死者以及生者之间的关系互动关注不足。“数字逝者”技术具有超越主客体二分的媒介性，其正当性基础不在于死者人格利益的延续抑或生者情感利益的满足，而在于“维持联结”这一以关系而非个人为基本单位的精神利益。以上述技术定位和法理证成为基础，应将“维持联结”作为技术监管原则，区分“私人悼念”“共享空间中的集体悼念”“个体行动公开化后的公共悼念”这三种不同关系情境下的制度安排，并从生前个人意思自治制度向多方协商制度转变。

8.“权力—权利”视角下数字分配正义的法律实现（宋保振）

来源：《法学论坛》2025 年第 3 期

数字分配正义是基于数字正义理念，信息和数据被赋予特定价值后，社会资源、要素、机会等的均衡配置。数字分配正义包括狭义的数据要素收益合理分配，以及数字化社会生产、生活及治理中，不同公民主体对数字红利的公共占有与共享，是实现数字社会公平正义和国家共同富裕目标的重要理论保障。数字分配正义缺失的原因，外在表现为利益范式下的数字资本垄断，内在根源于结构范式下不同社会主体的“权力—权利”失衡。利益分配过程中“权力—权利”关系变化的发生逻辑为：首先，信息数据的有价性、虚拟和集聚性改变了权力/权利衍生与发展的社会条件；其次，相关法律和政策安排将调整的社会结构与社会关系上升为制度设计；最后，技术参差赋权直接引发数据控制者与被控制者间权力/权利失衡及不同公民数字权利的实现差异。法律作为分配正义的重要制度保障，应积极进行如下回应：第一，经由法律化路径，配置数据信息生产环节不同主体的数据权属；第二，通过再赋权机制，平衡数据控制者与被控制者的数据权力与权利关系；第三，结合权利体系，设置保障数字弱势群体权利的国家与平台义务。

9.数字时代仇恨犯罪的代际变更与治理革新（陈禹衡）

来源：《法学论坛》2025 年第 3 期

数字社会的变革导致传统仇恨犯罪逐渐迭代升级为数字仇恨犯罪，因此要基于本土化视角来明确数字仇恨的概念，并根据数字仇恨治理现状来推动治理模式转型升级。当前数字仇恨兴起的原因在于数字社会的形势变化提供了数字仇恨的生成环境，数字鸿沟成为数字仇恨的新兴来源并放大了损害后果，而数字技术与数字仇恨的共轭关系则导致数字仇恨的治理难度增加。当前数字仇恨在代际变更后的特征复杂，具体包括实质内涵扩张、损害范围增加、行为模式多样且生成节点多元。当前数字仇恨治理模式的整体革新要在规范刑法学的基础上积极引入犯罪学新兴理论。一方面，基于“看门人规则”来优化数字平台的义务责任分配路径；另一方面，针对数字仇恨构建引入敏捷治理模式的情境犯罪预防体系，同时基于犯罪控制理论来对数字鸿沟进行内部控制与外部控制，并通过行动者网络理论来从行动者、转译、网络这三个层面削弱数字仇恨生成节点多元化趋势。

10.中国与 DEPA 数据跨境流动：规制差异及制度对接探究（齐鹏）基础理论

来源：《法学评论》2025 年第 3 期

中国加入 DEPA 是构建新发展格局、深化全球数字贸易伙伴关系的重要战略举措，不仅彰显了我国开放创新包容的发展理念，也是推动引领全球数字经济治理的重要举措。为有效弥合与 DEPA“新式”数据治理规则之间的张力分歧，有必要围绕 DEPA 模块 4 中“个人信息保护、数据跨境流动及

数据本地化存储”三个核心议题展开深入研究。通过系统梳理全球数据跨境多极治理格局及 DEPA 运行现状，比对中国与 DEPA 数据跨境流动规则的差异，进而探索具有中国特色的数据跨境流动“中式”方案：一是在个人信息安全保护规则方面，扩大个人信息保护边界，构建个人信息保护法律体系，强化数据跨境传输中个人信息保护机制兼容互认；二是在数据跨境流动规则方面，秉持“构建数字空间命运共同体”价值理念，强化国际合作筑牢数据跨境流动安全防线，准确把握数据流动和安全发展的平衡点；三是在数据本地化存储规则方面，形成与 DEPA 各国立法互相尊重的透明规则，推进与 DEPA“本地化为原则+合法公共政策为例外”的数据跨境本地化模式的制度衔接。

11. 计算机信息系统作为财产的私法保护（张浩然）

来源：《法学研究》2025 年第 3 期

数字经济催生各种新型财产形态而要求完善财产权制度，理论上多通过逐一界定客体属性构造财产权模型，非物质财产形态的多样化与动态性使传统制度模式面临困境。不同于传统工业经济，数字经济的市场交易形式由商品交换转变为平台提供服务，企业将各种生产要素纳入平台组织整合开展竞争，财产保护需求由控制单一生产资料转变为控制要素活动系统，可整体性地确认计算机信息系统的财产权益而实现对各类财产要素的保护。按照“有体—无体”的财产二分框架，计算机信息系统的物理硬件可受物权法保护，代码内容的保护则主要依靠知识产权法上的技术措施制度，无法及于非版权内容，制度扩张的前提取决于计算机信息系统之上能否成立私人财产权。回归物权法视角，计算机信息系统物理层、应用层、网络层整体作为“物”成为财产权客体，所有人和占有人有权排除他人非法访问、破坏和控制计算机信息系统，限制访问系统可排除破坏技术措施的非法侵入行为，公开访问系统则对一般公众访问负有容忍义务。在此产权框架下，权利人可通过技术措施自主进行计算机系统资源的配置、利用、收益和处分，实现平台自治与法律保护的激励相容。

12. 智能时代的知识产权制度和理论发展（张吉豫）

来源：《法制与社会发展》2025 年第 3 期

进入 21 世纪以来，人类社会快速步入智能时代。智能时代具有数字化、智能化、全球化、法治化等鲜明特征，为知识产权制度和理论提出了强烈的发展需求和变革性挑战。当前，知识产权制度在主体的模糊与扩张、保护对象的界定、权利保护的方式方法等方面面临重大的变革性挑战。智能时代的知识产权法应从知识产权法保护对象理论的体系化建构、创新方式变革引发的对保护条件的反思重塑、面向智能时代创新特点的知识产权制度调适、智能科技与知识产权法治建设的有机融合、围绕国际知识产权规则开展对话和协调等重点方面展开，探索智能时代知识产权规则、制度、实践创新，推动知识产权法学理论发展。

13. 元宇宙中的专利：范围与挑战分析（Prajakta Kale）

来源：International Review of Law, Computers & Technology, Vol.39, Issue 2 (2025)

“元宇宙”有望成为一项颠覆性技术，即将对教育、娱乐、医疗、商业等众多领域的运作方式带来革命性变革。该技术的核心特征在于将物理世界融入虚拟世界。元宇宙在某种程度上源于虚拟现实（VR）和增强现实（AR）技术，这些技术本质上是模拟现实世界并在数字世界中增强现实体验。知识产权（IP）作为保护无形资产的手段，在元宇宙背景下具有重要意义。本研究以元宇宙为背景，分析专利作为知识产权形式的特点。专利因其商业优势及相较其他知识产权形式更高的保护水平而成为吸引人的选择。随着人工智能（AI）和区块链等新兴技术专利申请量的激增趋势，元宇宙领域也可能呈现类似现象。本文通过宏观视角审视元宇宙与专利领域，评估其潜在范围与挑战。分析基于美国、欧盟及印度专利法律，以呈现全球范围内的全面图景。

14. 做好互联网治理的全球合作：未来战略路线图（Miriam F. Weismann）

来源：International Review of Law, Computers & Technology, Vol.39, Issue 2 (2025)

除了一项网络犯罪条约外，目前尚无任何具有国际约束力的条约规范国家间在网络空间中的关系。其原因包括碎片化、互操作性和本地化等挑战。这些挑战因条约协调问题而进一步加剧，许多国家尚未制定禁止特定行为的国内立法，或在人权和隐私保护问题上存在分歧。国家间的不信任以及对主权削弱的日益警惕，也为多边合作与条约协议设置了政治障碍。大量研究探讨了全球网络安全合作模式，但成果参差不齐。探讨条约谈判法律复杂性的文献寥寥无几，且未能提供关于当前全球法律、文化、经济和政治挑战综合影响的深刻洞见，这些挑战正构成阻碍有意义条约合作的障碍。本研究通过调查和分析未来全球网络安全协议的适当范围和广度方面的多样化观点，以及考虑当前全球战略建议以实现通过条约或其他方式的互联网治理，为全球网络安全治理文献做出了贡献。研究结果显示，这些战略有一个共同点：需要集体全球响应。

15. 元宇宙中的商标困境：利益相关者之间的相互作用（Alona Yarmak）

来源：Journal of Intellectual Property Law & Practice, Vol.20, Issue 5 (2025)

元宇宙中利益相关者的对立利益产生了越来越多的法律不确定性。作者将利益相关者之间的关系定义为对立利益的三角形，其中每个利益都塑造了元宇宙的发展。如果我们为开发者提供了太多的表达自由，但很少关注感兴趣的商标持有人发现自己的知识产权许可，那么元宇宙就会因为假冒数字商品的不受控制的流通而崩溃。在这种情况下，开发人员对整个 IP 系统施加了压力。数字商品的价值下降，这给元宇宙带来了负面的声誉后果。相比之下，来自商标持有人的限制也是危险的，因为元宇宙将停滞不前，设计师将锁定有限的创意选择。在这种不确定性中，我们需要平衡利益冲突，并修改商标和技术历史的经验教训。这个问题需要对欧盟和美国的判例法和学术评论进行审查，因为法院实践往往限制商标的合理使用，有利于商标持有人。相比之下，学者们指出这种方法的潜在问题在于过度限制了艺术表达的自由。

个人信息保护

1. 信息主体任意撤回同意的性质、正当性及限制（王成）

来源：《当代法学》2025 年第 3 期

信息主体的同意及撤回同意，其性质均应为意思表示。民法上有多种任意撤回意思表示的规则。任意撤回权利的行使多有限制，而且多数情况下应当赔偿对方由此造成的损失。信息主体任意撤回同意是一个例外。泛泛意义的个人信息与人格尊严的关联不足以使得任意撤回所有个人信息都具有正当性。同意及撤回同意涉及的场景类型复杂多样。对信息主体任意撤回规则应当在类型化的基础上做限缩解释。类型化角度应当从个人信息与人格尊严和人格自由关联的密切程度入手，仅在涉及敏感个人信息时可以任意撤回。对于非敏感个人信息的撤回，应当进一步类型化。在以个人信息作为对价而获得服务的场景中，应类推适用肖像权许可撤回的规则。

2. 个人信息保护合规审计的基本框架与制度衔接（赵精武）

来源：《法律科学(西北政法大学学报)》2025 年第 3 期

我国近期公布的《个人信息保护合规审计管理办法》旨在落实《个人信息保护法》第 54 条和第 64 条规定的个人信息保护合规审计制度。然而，现有研究并未对该类合规审计机制的功能定位和具体内容进行系统性讨论，甚至存在将合规管理与合规审计等同看待的概念认知误区。个人信息保护合规审计机制不同于个人信息保护影响评估、数据安全风险评估等个人信息保护制度，而属于面向个人

信息业务合规的专项合规审计活动，其“审计”属性大于“合规”属性。个人信息保护合规审计机制是以传统的合规审计理论为起点，基于风险管理的传统理论建立的机制，其功能包括合规监督、合规鉴证和合规评估，规范包括审计基本原则、审计证据规则和审计报告规则等。个人信息保护合规审计制度中规定的前期证据调取、合规管理事实评定、审计报告出具和后期审计建议整改监督有助于促成个人信息保护合规审计与其他个人信息保护配套制度的相互支撑。

3. 信息信义关系的法律保护（刘亚菲）

来源：《法律科学(西北政法大学学报)》2025 年第 3 期

数据、信息、知识与智慧，共同构成数字时代的知识生产机制循环。在整个以信息流转为核心的闭环或开放系统中，应将属于自然人人格权益的个人信息权益作为最重要的权益加以保护。然而在智能化时代，信息处理者处理个人信息的方式更为隐蔽，对权益的侵害也更为隐蔽。现有告知同意规则与个人信息保护监管制度在保护个人信息权益方面虽然均发挥了重要作用，但其中却隐藏着一个需要在个人与信息处理者之间产生内生性信赖关系的地带。信息信义关系是弥合个人与信息处理者之间不对等地位以及建立信赖关系的重要纽带。信息信义关系既包括理念上的信任与信赖，也包括具象化的信息信义义务。这一义务构造以忠实义务为基础，以注意义务为拓展，进一步强化信息处理者积极履行保护个人信息合法使用的义务。信息信义义务之实现建立在明确信义关系的构造、明确目的限制原则、构建损害赔偿责任体系的基础上，进而作用于个人与信息处理者信任关系之建立。

数据确权流动

1. 数据授权中的管理权研究（武腾）

来源：《当代法学》2025 年第 3 期

数据授权包含两种情形，一是授予数据财产权，二是授予数据事务的管理权限。对于经过深加工后产生的数据产品，主要通过确认、授予数据财产权来实现数尽其用。对于数据资源，控制者不得基于纯粹利己的目的任意使用和处分；此时，管理权的授予和行使对于数据资源的合理利用至关重要。如果将数据授权仅理解为授予财产权，便难以解释对数据资源使用的目的、方式进行全过程限制的重要性，也难以揭示行权过程中构建程序性规则的必要性。数据事务管理的目的既可能是纯粹利他的，也可能兼具利他性与利己性。在大型平台企业作为数据资源事务的管理组织时，应建构集体缔约制度，以保障个人、中小企业对数据资源相关事务的知情和参与。在标准化组织制定有关数据资源保护和利用的国家标准时，应完善公共协商机制，保障各类利益相关者能够充分表达意见。

2. 数据法治三人谈（李鸣捷、王年、刘欣琦）

来源：《东方法学》2025 年第 3 期

2025 年 4 月 29 日，国家数据局发布的《数字中国发展报告（2024 年）》显示，2024 年我国数据生产量已达 41.06 泽字节（ZB），同比增长 25%，高质量数据集量质齐升。随着数据要素市场加速扩容，“公共数据”正在被寄予更高的价值释放期待。本期“数据法治三人谈”聚焦公共数据资产权益担保、公共数据产权构造与政府数据授权运营三大前沿议题，展现法学界对数字中国建设重要命题的深度回应。李鸣捷从融资视角切入，提出以抵押或权利质押方式构造公共数据资产权益担保，并详细论证其体系定位、设立要件、登记效力等方面，为公共数据信用融资提供可落地的制度方案。王年回归确权问题，针对公共数据产权的理论争议，提出“国家所有、用途区分”的法律构造方案，将公共数据细分为“公用”与“私用”两类，分别对应自由使用和许可使用，为后续利用开发奠定产权基础。刘欣琦则聚焦运营终端，提出政府在授权运营中应转变为“运营效果担保者”，据此重塑监管、接管与赔偿三大义务，并通过正当程序与责任豁免机制统筹好有效市场和有为政府的关系。三位作者

立足现实难题，提出法治化解决方案，期待能为数据治理领域的理论创新与实践探索贡献力量。

3. 环境数据的刑法保护（李梁）

来源：《法商研究》2025 年第 3 期

环境数据是指用于表达环境质量和生态状况的各种符号。在数字化时代，环境数据实际上就是环境大数据。从形成环境数据的目的和环境法的法权结构来看，环境数据属于公共数据。环境数据能够为国家开展生产活动、生态环境监督管理部门的决策和执法、司法机关作出司法裁判以及实现生态环境保护的公众参与提供基本依据。在我国，环境刑法和数据刑法对环境数据提供了一定的保护，但具有明显的附带性、片段性和间接性特点，同时在保护方式上呈现出立法与司法解释之间的“中介性”特点。在数字化和生态文明建设交汇的当下和未来，应当提出和确立环境数据法益，使其与环境秩序法益和环境本体法益一道成为环境法益序列，并通过构造破坏环境数据犯罪以使其得到有效保护。

4. 人工智能时代财产权刑法保护模式的完善（刘宪权）

来源：《法学论坛》2025 年第 3 期

人工智能时代将会出现传统财产权刑法保护模式难以保护的新型犯罪对象、难以调整的新型社会关系、难以评价的新型权利主体以及难以规制的新型犯罪主体。人工智能技术的发展导致传统财产权刑法保护模式明显存在滞后性。为了平等保护各种类型的新型数字财产，刑法必须适时调整相关规定，确立以数字财产权为核心的全新财产权刑法保护理念，逐步构建能够全面保护有形财产、无形财产以及数字财产的财产权刑法保护体系。在被数字化之后，相关事物的原本属性仍然是主要属性，而数据属性则主要来源于技术层面的依托且只能被作为相关事物的次要属性。数字财产权是一种与物权、债权和知识产权相并列的财产权，其既包括基于算法、算力等数字技术而存在的新型财产权，也包括被数字化之后的物权、债权和知识产权。数字财产权的归属应当遵循创作者优先原则和合同约定原则。侵犯相关数字财产权的行为可能构成侵犯著作权罪或者财产类犯罪。

5. 数据犯罪的刑事风险区分与应对——以数据关系理论的三权分置为切入（杨猛）

来源：《法学论坛》2025 年第 3 期

对于数据犯罪的研究，已经从物权属性的上位概念逐渐细化渗透到了数据类型化保护的具体领域。通过对数据关系理论中纵、横向数据关系所承载的数据权利主体类型的梳理及其权属性质的确证，可将具有财产性价值的数据权利分置为数据持有权、使用权以及经营权。在以上数据三权分置背景下，以权利类型作为逻辑起点，以刑法法益作为跨法域连接要素，在规范保护目的价值引导下，会形成以典型数据法益作为保护对象的刑法规制领域：一是数据持有权与基本物权法益内容相关联，进而涉及财产性犯罪的刑法规制与法益保护；二是数据使用权与知识产权法益内容相关联，进而涉及知识产权犯罪的刑法规制与法益保护；三是数据经营权与金融法益内容相关联，进而涉及金融类犯罪的刑法规制与法益保护。因此，以数据关系作为数据犯罪类型化规范治理的前提基础，可对数据权利进行更具针对性、更为细致的保护与利用。

6. 印度数据保护的轮廓：同意的困境（Aafreen Mitchelle Collaco）

来源：International Review of Law, Computers & Technology, Vol.39, Issue 2 (2025)

随着印度数字技术的快速发展，数据保护和数字隐私问题日益引起关注。2023 年《数据保护与隐私法》（DPDP Act 2023）也体现了对健全隐私实践的高度重视。本文探讨了同意原则的有效性，这一原则是数据隐私制度中的核心要素，也是诸多争议的焦点。尽管同意原则是全球隐私制度的基石，但基于同意的隐私保护模式存在显著局限性。例如，其二元特性仅允许“是”或“否”的回应，且

无法确保数据主体能够做出明智的选择。本研究以印度政府加强数据保护措施的努力及频发的数据泄露事件为背景展开。研究还通过分析构成《2023 年数据保护与隐私法》基础的根本理念，探讨了同意的理论与法律层面，以保护同意框架。它质疑当前法律形式是否与具有里程碑意义的隐私判决相一致。最后，研究探索了在印度语境下有效解决特定问题的替代性、更具适应性的信息隐私实施机制，并从中汲取了欧盟等其他司法管辖区的灵感。

7. 如何减少跨境数据流动的不必要限制？印度尼西亚在个人数据保护法实施后的立场与挑战（Faiz Rahman, Cora Kristin Mulyani）

来源：International Review of Law, Computers & Technology, Vol.39, Issue 2 (2025)

在数字化快速发展的时代，数据作为“燃料”在重塑和创造数字领域的新机遇中发挥着至关重要的作用，尤其是在数字经济领域。印尼数据的重要性可从各行业产生的、收集的和分析的数据量中看出。然而，印尼近年来也面临数据泄露问题，这些问题对社会造成危害，需要立即关注。本文探讨了印尼的数据和跨境数据流动的监管与制度框架及其实施挑战，特别是随着近期《个人数据保护法》（PDP 法）的颁布，该法律主要借鉴了欧盟《通用数据保护条例》（GDPR）。本文指出，印尼正朝着比以往监管制度更宽松的数据流动监管方向发展，但仍处于数据流动监管的规范性与限制性光谱之间。本文认为，《个人数据保护法》的颁布可成为印尼评估现有监管框架的契机，以确保印尼的监管措施不会因设置不必要的限制而导致实施复杂化，从而阻碍数据利用带来的益处。

8. 数据知识产权登记及救济：银木（上海）科技有限公司诉书聚堂（北京）科技有限公司案（Hong Wu, Yupeng Dong）

来源：Journal of Intellectual Property Law & Practice, Vol.20, Issue 5 (2025)

“数据知识产权”是中国数据财产法中一个独特的概念。银木（上海）科技有限公司诉书聚堂（北京）科技有限公司案首次澄清，就涉案数据集取得的《数据知识产权登记证》可以作为书聚堂公司享有与该数据集相关的所有权权益的初步证据。它还可以作为数据收集活动或数据集来源合法性的初步证明。本案确立了数据集侵权案件的裁判框架：如果数据集是公开的，并且在内容的选择和编排上表现出独创性，则首先应作为汇编作品进行保护。如果相关领域的专业人士不容易访问数据集，则可以将其作为商业秘密进行保护。如果数据集是公开可用的，并且数据的选择或安排缺乏原创性，那么，在没有版权或商业秘密保护的情况下，它可以根据情况受到《反不正当竞争法》第 2 条的保护。最后，本文提出了立法改革，以解决数据集产权确认和保护问题。

人工智能

1. 生成式人工智能服务提供者注意义务研究（杨利华）

来源：《比较法研究》2025 年第 3 期

生成式人工智能服务提供者是否尽到注意义务，是判定其是否存在主观过错进而构成间接侵权的关键因素。基于促进人工智能产业发展的政策考量，设置生成式人工智能服务提供者注意义务，需兼顾权利义务一致与禁止权利滥用的法理、利益平衡与产业激励的考量以及“守门人”理论与科技向善的技术理性。生成式人工智能服务提供者注意义务的内涵应包括：“注意”内容上的致害后果的预见与避免，“注意”程度上的基于同业平均水平高度的注意标准，“注意”基准上的现有技术水平和“注意”要素上的客体、主体和服务模式。生成式人工智能服务提供者注意义务的具体规则应涵盖事前语料、模型风险的防范规则，事中用户行为监督与高危风险提示的干预规则，以及事后区分场景与内容的人工智能生成内容标识规则和针对用户举报、投诉的处置规则。

2. 生成式人工智能的法律定位与侵权归责路径（李雅男）

来源：《比较法研究》2025 年第 3 期

生成式人工智能具有自主性、不透明性、不可预测性等特征，这也导致了学界认为人工智能侵权归责需脱离产品责任，理由主要为产品责任为严格责任，生产者难以控制人工智能运行过程中存在的风险，要求其承担严格责任并不公平；生成式人工智能大多以服务的形态存在，因此其不符合产品的定义。然而，从法律属性来看，生成式人工智能提供者与网络服务提供者二者存在实质差异。生成式人工智能系统符合产品的定义，产品责任契合生成式人工智能系统多层次、多样态的特征，能够实现与监管的良性互动。在产品责任框架下，开发者与运营者可以类比为产品责任中生产者与销售者的地位，可以根据生成式人工智能的生命周期、层次属性确定制造缺陷、设计缺陷、警示缺陷、跟踪观察缺陷，确定发展风险抗辩适用的条件与标准。

3. 人工智能统一立法宜缓行（付新华）

来源：《东方法学》2025 年第 3 期

在技术变革与社会风险的双重驱动以及国际科技竞赛与规则竞争双重博弈的推动下，人工智能统一立法的呼声日益高涨。然而，人工智能技术的复杂性、发展路径的不确定性和应用场景的差异性，使统一立法面临法律滞后、规制僵化、监管错配和创新受阻等挑战。基于技术哲学、渐进社会工程理论与社会系统论的交叉论证，人工智能立法应遵循渐进式治理模式，审慎推进统一立法。我国人工智能立法应构建“时间—空间”双重弹性框架，增强法律适应性与治理韧性，在促进技术发展与防范风险之间寻求最佳平衡。在时间维度上，应采取渐进式立法路径，结合技术成熟度监测、“试错法”治理模式和反身性法律框架，实现法律监管与技术发展的双向互动与协同演进，避免过早规制锁定技术发展路径；在空间维度上，需实施分层治理，依托国家、行业和地方三层次治理体系，结合政策试验区、行业自律和监管沙盒，探索灵活适应的法律监管模式。

4. 诊疗式人工智能的医疗产品责任认定（候曼曼）

来源：《东方法学》2025 年第 3 期

在人工智能“服务—产品”二元框架下，诊疗式人工智能不论是否依托物质载体，均属产品责任法中的“产品”。诊疗式人工智能致害锚定产品责任体系符合矫正正义和分配正义的要求。在责任成立层面，研发者、生产者和销售者违反注意义务的行为可作为产品缺陷的判定因素；诊疗式人工智能致害因果关系的判断应区分风险增加的可能性与实质性，前者是事实因果关系的判断标准，后者是法律因果关系中融入价值判断的通道。诊疗式人工智能产品缺陷引发的风险是否超出生产者等主体可预见范围应结合法定义务违反、人工智能自主性和医务人员介入行为分析。事实推定规则可以缓解人工智能技术引发的产品缺陷与因果关系证明困境。在责任承担层面，专业中间人规则并非当然免除诊疗式人工智能生产者和销售者的责任，医疗机构以及医疗器械的注册人、备案人亦为医疗产品责任主体。直接责任主体对外承担连带责任后可向有过错的最终责任主体追偿。

5. 生成式人工智能平台自治规则的体系化构建（邓栩健）

来源：《东方法学》2025 年第 3 期

当前我国在 AIGC 领域确立了“分层治理、审慎监管”的治理思路，AIGC 平台的自治规则作为平台履行责任和义务的制度工具，与传统的互联网平台规则在内容和效力上都存在显著差异。AIGC 平台自治规则应当由关于合规与自律的“平台规则”、关于规范生成内容的“模型规则”以及关于规范用户行为的“用户规则”构成，并在事实上产生拘束力、说服力和证明力三大法律效果。当前，有必要设立权力与权利清单以厘清平台的权力边界，建立分类机制以明确规则的效力审查标准，同时，探索敏捷治理路径以完善回应性监管机制，构建起平台、用户以及监管部门多主体共治和多要素

制约的权力制衡体系。

6. 人工智能立法的动态演化框架与制度设计（李学尧）

来源：《法律科学(西北政法大学学报)》2025 年第 3 期

如何构建兼具稳定性与灵活性的人工智能立法框架是一个全球性议题。针对规范方法论主导下的人工智能立法思路可能引发的制度适用问题，应采取“适应型法”的立法思路。为了实现法律规则与技术演进的动态适配，还应结合本土实践探索人工智能立法的“适应性法治”路径：审慎对待体系化、部门法化的立法目标，尽量在传统部门法的实体法框架中采用立改废释的方式实现人工智能的立法目标；动态适应性原则应是人工智能立法的核心原则；条款拟制应从“义务本位”转向“行为激励”；学理阐述需把重点放在如何建立“法治化”“中央底线规则+地方差异化试点+司法判例引导”的多层治理体系，进一步优化“软硬法协同”在内的中国式法治实践。这样既可以延续中国改革开放以来“试验—推广”的制度创新传统，也可尝试为全球技术治理贡献具有普适价值的制度分析工具。

7. 深度伪造技术滥用行为的刑法回应（郑高键）

来源：《法律科学(西北政法大学学报)》2025 年第 3 期

深度伪造技术的滥用已然超越了纯粹的人工智能技术边界，迈入违法犯罪的灰色地带。深度伪造技术在社会生活中的不当和非理性适用，带来了一系列刑事治理层面的疑难问题。为回应这一问题，在学理层面，应当阐明深度伪造技术滥用的不法形式和危害样态，揭示技术发展与刑法之间的治理鸿沟，形塑全新的刑法理念和解释规则，理顺刑法规制深度伪造技术滥用行为的制度逻辑；在治理路径方面，应当将技术原理作为法益界定的重要基础，构建符合涉罪特质的法益保护体系，依托刑法体系进行合理解释，并坚持刑法文本的规范指引作用，明确不法行为的认定标准，为相关行为的刑法治理提供坚实的理论支撑和有效的实践框架，以实现对深度伪造技术滥用行为的有效规制。

8. 人工智能时代劳动者隐私权的侵害风险及其保护路径（侯玲玲）

来源：《法学》2025 年第 4 期

劳动者隐私权保护是人格尊严、言论自由、公平正义等基本权利得以保障的基础。用人单位将人工智能技术应用到人力资源管理，虽有利于提高企业管理效率，但也急剧增加了劳动者隐私权被侵犯的风险。我国现有的劳动者隐私权保护以意思自治为中心的民法保护为主，无法有效保护数据化和自动化工作场所的劳动者隐私权。将劳动者隐私权纳入劳动法予以特殊立法，既不会削弱劳动关系的性质，也能兼顾其从属性特征，从而实现劳动者隐私利益与用人单位管理需求之平衡。具体而言，要确立合法性原则、合理期待理论及目的限定原则作为限制用人单位数据收集和处理的基本原则；赋予劳动者对用人单位收集和处理数据的知情同意权，以及同意撤回权；建立数据保护局作为劳动者隐私权保护集中执法机构；赋权工会代表劳动者提起侵犯隐私权的集体诉讼，利用专业数据审计机构辅助工会集体诉讼。个案裁判应妥善运用公平原则、比例原则，根据社会变化调整对劳动者隐私期待评估等，积极探索裁判新标准。通过发布指导案例和示范判决，逐步实现裁判规则的一致性，并确立劳动争议案件的非法证据排除规则，用人单位非法获得的劳动者隐私信息不得作为劳动争议处理的合法证据。

9. 透明度作为开发边境管控风险评估人工智能技术的核心特征（Jonida Milaj, Jeanne Pia Mifsud Bonnici）

来源：International Review of Law, Computers & Technology, Vol.39, Issue 2 (2025)

根据欧盟当前的《人工智能法案》草案，用于移民、庇护和边境管控管理的人工智能系统被归类

为高风险人工智能。该法案草案对这些系统的开发和使用提出了严格要求，包括必须使用高质量数据来训练算法，以减轻对基本权利和安全构成的风险。基于在 H2020 CRiTERIA 项目框架下开展的研究，本研究从法律理论角度分析了社交媒体平台提供的开源数据是否符合高质量数据要求，以及当前在透明度要求方面面临的挑战。在遵循所有旨在减轻高风险人工智能对基本权利和安全构成风险的要求后，社交媒体开放数据是否符合高质量数据要求的问题被提出。由于透明度被视为区分高风险与不可接受风险人工智能的关键界限，因此认为若未采取适当保障措施，使用社交媒体开放数据进行风险评估边境控制人工智能系统可能对基本权利保护构成不可接受的风险。

10. ChatGPT 用于善？在生成式人工智能的监管中认真对待“beneficence”（Krishna Deo Singh Chauhan）

来源： International Review of Law, Computers & Technology, Vol.39, Issue 2 (2025)

生成式人工智能平台如 ChatGPT 近期因其生成文本、图像等内容的能力而备受关注。围绕 ChatGPT 的伦理与法律问题已引发诸多讨论。本文将探讨生成式人工智能的本质与发展背景，并将其置于人工智能历史发展的语境中进行分析。随后，作者探讨了主要研究问题：人工智能伦理学文献中是否充分关注了“beneficence”原则，以及对其含义是否存在理论上的清晰阐述？作者指出，尽管关于生成式人工智能可能带来的危害及其防范措施的讨论甚嚣尘上，但关于“人工智能向善”（AI-for-good）的具体内涵，尤其是在人工智能伦理与监管文献中，却鲜有深入探讨。即便存在相关讨论，也往往直接提出具体解决方案，而未充分探讨其建议为何具有益善性的根本问题。作者论证了生物医学伦理学和人权框架中对益善原则的理解，对生成式人工智能伦理学具有有限的适用性。这些人工智能监管中的缺口尤为突出，因为它们可能阻碍生成式人工智能的长期发展及其潜力的充分实现。

11. 控制与补偿：用于训练生成式人工智能的版权例外条款的比较分析（Katharina de la Durantaye）

来源： IIC-International Review of Intellectual Property and Competition Law, Vol.56, Issue 4 (2025)

全球各地的立法者和行政机构正在讨论使用受版权保护的内容进行人工智能训练是否需要或应当获得权利持有人的同意。本文探讨了美国、加拿大、英国、欧盟、以色列、中国、新加坡和日本在这一问题上的立法和政策辩论。控制权、补偿、透明度和法律确定性等议题主导了讨论。各国正试图重新调整利益平衡，或倾向于支持人工智能公司，或通过支持权利人来实现——例如，通过实施与版权相关的透明度义务。欧盟的版权法为人工智能公司提供了相对有利的环境。然而，最终，版权法并非人工智能公司在选择训练设施地点时决定性的因素。

12. 中国对 AI 生成内容归属的监管：基于开放式方法的探索（Xinhang He, Pingji Shan）

来源：Journal of Intellectual Property Law & Practice, Vol.20, Issue 5 (2025)

本文探讨了中国现行版权法下人工智能生成内容的版权归属问题，特别关注 2020 年版权法修正案引入的开放式分类系统及其实际影响。该修正案标志着中国版权法从封闭式方式转变为开放式方式，从而将版权保护扩展到非传统作品，例如 AI 生成的内容。尽管纳入了包罗万象的规定并完善了作品分类的标准，但在原创性和分类层次结构的要求方面仍然存在歧义，继续引发关于 AI 生成内容的可版权性的辩论。本文分析了涉及人工智能生成内容的代表性版权争议案件，以说明中国法院的裁判立场。法院在原创性和智力成就的标准方面存在重大差异，裁决通常严重依赖于个别法官对技术和创作过程的解释，这导致了相当大的自由裁量权。此外，传统作品类别和包罗万象的规定之间的模糊关系有助于将 AI 生成的内容归类为一种新型作品，这可能导致版权保护的不当扩大。本文从立法和司法角度提出了建议，建议在立法中建立“传

统工作类别优先适用”原则，发布司法解释以阐明人工智能在创作中的工具性作用，并倡导在法庭上进行谨慎和实质性的评估，以确定人工智能生成的内容是否符合受保护作品的特征。

13. 了解人工智能辅助作品中的作者身份（Johannes Fritz）

来源：Journal of Intellectual Property Law & Practice, Vol.20, Issue 5 (2025)

生成式人工智能（AI）的出现带来了作品创作方式的重大转变，人类和机器驱动的创作过程之间的界限变得模糊成为一个突出的挑战。这就引出了一个问题，即此类作品是否存在作者身份，如果存在，应该归属于谁。本文重点介绍了欧盟法院和选定的欧盟成员国法院的现有判例法，以找到关于在欧洲版权系统中审查 AI 辅助作品的作者身份时应考虑哪些因素的指示。最终，提出了一个四步测试，有助于评估具体作品中是否存在作者身份以及应该归属于谁。第一步询问创建过程涉及哪些人员，然后确定（作为第二步）使用的 AI 系统类型。第三步分析相关人员是否对作品的构成进行了足够的主观判断。最后一步确定他们是否对执行有足够的控制权。

平台治理

1. 从平台责任到合作规制——互联网规制模式转型及其正当程序规范（赵鹏）

来源：《法商研究》2025 年第 3 期

近年来，立法开始通过公法强化互联网平台对其用户违法、侵权和其他有害行为的治理义务。伴随着立法和监管实践中“主体责任”“安全保障义务”“风险防控责任”等监管要求的提出，互联网合作规制模式开始形成。公法规制框架的强化回应了互联网生态中的问题以及平台经济的现实，有其合理性。与此同时，当平台扮演事实上的监管者角色时，法律需要强化对平台权力行使的正当程序规范。但是，相应的规则设计需要考虑平台技术和生态方面的特点。法律可以要求平台制定更为详细的平台规则，同时关注平台规则在通过算法自动化执行时可能出现的落差。在平台规则实施层面，既需要从“系统”层面提高平台权力行使的透明度，又要求平台对有重大影响的个案处理决定在陈述、申辩和救济等方面提供更充分的程序保护机制。

2. 数字私权力与平台自我优待的法律规制（黄绍坤）

来源：《法学家》2025 年第 3 期

为保障数字经济创新发展，提升平台国际竞争力，应减少使用反垄断法规制平台自我优待。平台自我优待为平台组织化和内部权力化的产物，本质上属于数字私权力的不当行使。而反垄断法作为平台外部规制工具，在应对平台自我优待时，存在适用前提、条件、效果上的不足。平台自我优待是对平台中立义务的违反，属于过错推定责任类型，其违法性需借助比例原则进行个案判断。在进行具体判断时，应区分为资源配置型自我优待、秩序维护型自我优待，并由此导向不同判断标准。从平台自我优待的数字私权力滥用定性出发，可以在事前、事中和事后阶段，通过程序设置、商家权利赋予、平台内部决策民主化、平台主体责任强化、侵权责任与行政处罚等制度，实现平台自我优待的综合规制。

3. 互联网平台处罚权的法律规制（刘权）

来源：《法学研究》2025 年第 3 期

当前平台处罚已经成为平台维护网络公共空间秩序的基本手段，实现平台处罚正义是确保平台经济高质量发展的关键。平台处罚权并非源于国家授权或委托，而是源于用户让渡的权利和国家设定的法定义务。平台处罚的实质并非追究违约责任，而是平台对违反平台规则行为实施的惩戒，是新型社会规范设定的制裁措施。平台既是市场经营者也是市场规制者，容易滥用和不当行使处罚权。为减少平台处罚权的失范风险，应对平台处罚的设定和实施加以规制。鉴于平台具有双重主体身份，对平

台处罚的规制应采公私法融合的路径，平台处罚既要符合私法上的公平原则、禁止权利滥用原则，也要受公法上的过罚相当原则、比例原则等约束。为了保证平台处罚正义的完整实现，还需为平台处罚设定最低限度的正当程序要求。鉴于平台相对于用户处于优势地位，法院在司法审查中不应过于偏向平台自治，而应对平台处罚的实体公正性和程序正当性进行必要的实质性审查。

4. 标准化 Cookie 横幅：解决 Cookie 同意问题的方案（Paarth Naithani）

来源：International Review of Law, Computers & Technology, Vol.39, Issue 2 (2025)

Cookie 是当今互联网不可或缺的一部分。在欧盟，根据《电子隐私指令》（与《欧盟通用数据保护条例》一并适用），使用 Cookie 需事先获得用户知情同意。通常，网站会通过 Cookie 提示栏来满足知情同意的要求。然而，由于欧盟各国在 Cookie 法律上的不协调、不同成员国数据保护机构制定的 Cookie 指南存在差异，以及网站对 Cookie 同意要求的实施方式不一，用户在不同网站上会遇到不同的 Cookie 提示栏。面对不同的 Cookie 提示栏，用户需要额外投入认知努力和时间来阅读、理解、评估并选择每个提示栏中的选项。此外，获取同意的方式仍然具有误导性。网站通过暗黑模式、模糊语言、积极表述和行为引导等手段诱使用户同意。本文提出采用标准化 Cookie 横幅以解决 Cookie 同意横幅的各种问题。本文建议，标准化横幅必须具备统一的显示时机、网站位置、文本与语言、呈现方式、同意选项以及同意方式。

数字行政与司法

1. 论行政算法规则的双重审查模式（陈晓敏）

来源：《东方法学》2025 年第 3 期

行政算法规则是自动化行政的依据，“依法行政”在一定程度上演变为“依算法行政”。自动化行政中的正义价值蕴含在“普遍正义—个案正义”范畴之中，前者体现在算法规则的制定中，后者体现在司法裁判中。行政算法规则与行政规范性文件在指令结构、内涵和效力上具有的同质性，使其不能逃脱依法行政原则的约束。对行政算法规则的合法性审查存在备案审查和司法审查双重模式，分别构成审查的第一阶段和第二阶段。将行政算法规则的合法性审查嵌入现有备案审查和司法审查结构中，依据其技术规范的特性实现对既有结构的突破。继而对双重审查模式展开体系化塑造，勾勒出一个抽象与具体相结合的审查体系。结合对司法审查模式中风险防范与控制、法院审查能力、审查启动动力等现实因素的考量，构建备案审查为主、司法审查为辅的双重体系更适应现阶段数字法治政府建设的需要。

2. 科技企业参与人工智能司法应用及其规制（郑曦）

来源：《法商研究》2025 年第 3 期

科技企业参与人工智能司法应用，是在法院沉重的案件数量压力和企业追求商业利益本能这两方面驱动力作用下的必然现象。在人工智能司法应用中，科技企业除了扮演产品研发者、系统维护者、平台运营者等技术角色外，还实质上担任数据处理者、程序控制者和裁判参与者等角色。这可能与审判基本原理发生冲突，导致诉讼模式改变，并带来其他外部政策性风险。针对这些风险，应当合理区分科技企业参与人工智能司法应用中的公私界限，明确“有限参与”的基本要求，并对其参与过程进行必要监管。据此，可以通过调适法院与科技企业的关系、确立相应的技术标准、科以数据安全保护义务等措施，合理规制科技企业在人工智能司法应用中的参与程度，使其参与符合法治的基本要求。

3. 数字时代刑事证据制度的“开放化”转型逻辑（谢澍）

来源：《法学》2025 年第 4 期

数字时代的刑事证据制度面临着多重机遇与挑战，而制度转型的基本前提在于通过细致的理论

分析，厘清转型逻辑：一是从“物理空间”到“网络空间”的发展趋势呈现出证据收集立体化的转型逻辑，需要在制度层面明确多元主体的立体参与、海量证据的立体抽样和跨境证据的立体衔接；二是从“口供中心”到“数据指引”的发展趋势呈现出证明效果协同化的转型逻辑，应当在制度上体现传统证据与电子数据的协同处理、线下证据与线上证据的协同呼应以及过程证据与结果证据的协同认知；三是从“逻辑证成”到“智能校验”的发展趋势呈现出事实认定交互化的转型逻辑，需要制度保障内心确信与机器赋能的交互作用、逻辑涵摄与数据整合的交互作用以及认知决策与认知提示的交互作用。对此，《刑事诉讼法》再修改时应当以开放的姿态予以回应，推动数字时代刑事证据制度的“开放化”转型。

4. 数字时代刑事侦查程序的逻辑转变与制度回应（裴炜）

来源：《法学家》2025 年第 3 期

犯罪及犯罪治理的数字化深刻转变着刑事侦查程序的内在逻辑，尤为集中地体现为犯罪“嫌疑”的概念被重构，侦查对象呈现出量化拓展的趋势，侦查行为的涉外属性不断强化，以及侦查权在私主体的深入参与下被不断稀释。在国家启动新一轮《刑事诉讼法》修订的背景下，采用法典化的修法思路意味着需要对侦查程序进行体系化的调适，从而与演变中的数字侦查逻辑相适应。基于此，侦查制度的调整应当遵循“技术导向”向“权利导向”回归的总体路径，重构侦查行为的基点，采用透明化的全流程控制的规制视角，通过引入涉外法治思路来应对犯罪治理全球化这一外部生态，并在此基础上整合和修订刑事诉讼法相关制度。

虚拟财产

1. 数字经济视阈内网络虚拟财产的识别标准与类型构造（谢潇）

来源：《法商研究》2025 年第 3 期

在数字经济视阈内，《中华人民共和国民法典》第 127 条中的“网络虚拟财产”应当被认定为契合网络虚拟性、价值性、特定性与独立性、可支配性与排他性以及合法性要件的新型无形财产。而以此为据，或可将网络虚拟财产区分为物品型网络虚拟财产、营业型网络虚拟财产、账号型网络虚拟财产、空间型网络虚拟财产以及加密型网络虚拟财产。与此同时，由于网络虚拟财产系属蕴含网络虚拟属性的无形财产，因此欠缺网络虚拟性的其他无形财产应当被排除在网络虚拟财产的范围之外。此外，一般意义上的数据亦与网络虚拟财产有所不同，数据产品原则上亦不可归于网络虚拟财产之列，而具有个人信息因素的网络虚拟物如若不符合网络虚拟财产的识别标准，亦不得被认定为网络虚拟财产，其仅可适用个人信息与隐私保护规则以获得妥当的私法保护。

（技术编辑：李佳丽、麻卓妍）

教研活动

2025 全球数字经济大会知识产权与数字经济生态建设论坛举办

7 月 2 日下午，2025 全球数字经济大会知识产权与数字经济生态建设论坛在北京国家会议中心举办。本次论坛由北京市知识产权局、北京市人民检察院、北京知识产权法院和中国人民大学法学院共同承办。中国人民大学未来法治研究院、教育部哲学社会科学创新团队“新科技革命与未来法治创新团队”为本次会议提供了支持。来自国家、北京市有关部门负责人，高校、知识产权服务机构以及数字经济领域企业等单位代表参加论坛。

论坛现场

国家知识产权局战略规划司司长梁心新、北京市人民检察院检察长朱雅频、北京市人民政府副秘书长丁章春出席论坛并致辞。致辞环节由北京市知识产权局局长孟波主持。

主旨演讲环节，中国人民大学法学院吴玉章高级讲席教授、数字法学学科带头人、中国法学会网络与信息法学研究会副会长张新宝，中国国家创新与发展战略研究会副会长、中国科学院大学经管学院教授吕本富，美国南卡罗来纳大学法学院、工程学院（特邀）副教授布莱恩特·沃克·史密斯，北京市海淀区人民检察院检察长姜淑珍，北京互联网法院副院长赵长新，华为技术有限公司副总裁樊志勇，360 集团总法律顾问刘晓庆，美国科文顿·柏灵律师事务所合伙人冉瑞雪等 8 位中外嘉宾围绕数据属性探讨、知识产权保护和运用、知识产权纠纷预测和解决机制构建等议题，分享研究成果与实践经验，为知识产权更好融入数字经济发展建言献策。

中国人民大学法学院吴玉章高级讲席教授、
数字法学学科带头人、
中国法学会网络与信息法学研究会副会长张新宝
以“作为知识产权的数据与作为数字经济要素的数据之“并联包容”关系探讨”为题做主题演讲

美国南卡罗来纳大学法学院、
工程学院（特邀）副教授布莱恩特·沃克·史密斯
以“数字经济领域专利纠纷预测”为题做主题演讲

成果发布环节，中国人民大学纪检监察学院教授、未来法治研究院研究员邓矜婷介绍了“法图知产规则 AI 知识共享平台”，相关部门和单位发布了《标准必要专利纠纷企业应对指引》《北京市人民检察院关于商业秘密保护与风险防范指引》、北京市检察机关知识产权法律监督模型、《数字经济产业专利蓝皮书》、专利检索分析系统 AI Pat+、数据知识产权保护十大典型案例等系列成果，展示知识产权与数字经济深度融合的探索与实践，引导相关产业高质量发展。

中国人民大学纪检监察学院教授、
未来法治研究院研究员邓矜婷
介绍“法图知产规则 AI 知识共享平台”

签约共建环节，北京市人民检察院第四检察部与中国人民大学法学院举行人工智能赋能涉外知识产权保护共建仪式，强化涉外知识产权保护检校共建机制；北京知产宝网络科技发展有限公司与京东科技信息技术有限公司合作签约，联合推出“云捕手”外观设计专利侵权检测系统；知识产权出版社有限责任公司与北京国际大数据交易所合作签约，在数据交易、价值转化、金融服务等方面协同发力。

北京市人民检察院第四检察部刘晶主任与
中国人民大学法学院副院长万勇教授
举行人工智能赋能涉外知识产权保护共建仪式

讲座 | 哈佛法学院 Lawrence Lessig 教授：人工智能的民主治理

2025 年 7 月 9 日，一场关于人工智能与西方民主制度关系的学术讲座于中国人民大学明德法学楼 725 会议室热烈举行。本次讲座由中国人民大学法学院、中国人民大学未来法治研究院、中国人民大学涉外法治研究院、中国人民大学公法研究中心主办，中国人民大学法学院数字法学教研中心、教育部哲学社会科学创新团队“新科技革命与未来法治创新团队”及国际数字法学协会协办。

讲座由哈佛大学法学院洛伊·福尔曼法律与领袖讲席教授（Roy L. Furman Professor of Law and Leadership）劳伦斯·莱斯格主讲。作为知识共享（Creative Commons）项目的创立者，他荣获众多奖项，包括自由软件基金会颁发的自由奖以及美国法律界最高荣誉奖“Fastcase 50”。其作品《代码：塑造网络空间的法律》和《思想的未来：网络时代公共知识领域的警世喻言》被誉为迄今为止网络法、知识产权领域最为重要和具有里程碑意义的论著。

本次讲座由中国人民大学法学院副院长丁晓东教授主持。劳伦斯·莱斯格教授深入探讨了人工智能商业模式对西方民主制度的影响。中国人民大学法学院副教授王春燕、中国人民大学法学院教授李琛、中国人民大学法学院教授金海军、中国人民大学法学院副教授、未来法治研究院执行院长张吉豫、中国人民大学法学院副教授喻文光、上海交通大学法学院教授郑戈、北京师范大学法学院教授汪庆华分别发表了与谈意见。

讲座 | 技术发展与产品责任之间的互动关系

2025 年 7 月 8 日，一场关于美国产品责任法的学术讲座于中国人民大学明德法学楼 502 教室热烈举行。本次讲座由中国人民大学法学院、中国人民大学未来法治研究院、中国人民大学涉外法治研究院主办，中国人民大学法学院数字法学教研中心、教育部哲学社会科学创新团队“新科技革命与未来法治创新团队”及国际数字法学协会协办。

讲座由美国南卡罗来纳大学法学院教授、美国南卡罗来纳大学工程学院特邀教授、斯坦福大学互联网与社会研究中心特邀学者 Bryant Walker Smith 教授主讲。

本次讲座由中国人民大学法学院副教授、中国

人民大学未来法治研究院执行院长张吉豫副教授主持。Bryant Walker Smith 教授从技术视角切入，介绍了美国产品责任法。从追溯早期发明（包括火车、汽车与流水线）如何催生现代人身损害赔偿理论出发，阐释可预见性、行业最新技术标准、产品误用等关键教义问题与科学知识的关联；并探讨了生成式人工智能、物联网、黑客技术等新兴科技发展。本次讲座为国内学者和学生提供了一个与国际学者交流的平台，拓宽了大家在新兴科技与法律、政治交叉领域的研究视野，对推动相关领域的学术研究具有重要意义。

哥伦比亚大学法学院李本教授访问法学所国际法所并发表学术演讲

2025 年 7 月 8 日，美国哥伦比亚大学法学院副院长、中国法律研究中心主任李本（Benjamin L. Liebman）教授到访中国社会科学院法学研究所、国际法研究所，并以“美国法治现状（The State of Rule of Law in the United States）”为主题作讲座。

演讲现场

讲座开始前，法学研究所国际法研究所联合党委书记李洪雷研究员、法学研究所所长莫纪宏研究员会见了李本教授。双方回顾了法学研究所与哥伦比亚大学法学院及中国法律研究中心之间长期友好、深入的学术交流历程，并就进一步加强合作达成广泛共识。法学研究所副所长谢增毅研究员参加会见。

在讲座中，李本教授结合其长期从事中美法制比较研究的经验，介绍了近年来美国法治领域的制度变化与发展趋势。讲座由李洪雷主持，莫纪宏致辞。来自法学研究所、国际法研究所以及中国社会科学院大学、清华大学、西安交通大学的四十余人参加，并就有关问题与李本教授进行了交流探讨。

美国哥伦比亚大学法学院副院长、

中国法律研究中心主任

李本教授（Benjamin L. Liebman）

北京大学首届“数字法治的理论视野与实务前沿”暑期学校成功举办

2025 年 7 月 7 日至 9 日，由北京大学法学院、北京大学数字法治研究中心主办的首届“数字法治的理论视野与实务前沿”暑期学校成功举办。本次暑期学校为北京大学“研究生教育创新计划”项目，并由北大英华科技有限公司（北大法宝）和长春吉大正元信息技术股份有限公司作为协办支持单位。暑期学校邀请了北大数字法治研究中心研究人员及校内外高水平专家，通过理论研讨、实务论坛和智能工具应用实训等形式，为近六十位来自全国各地的青年教师、硕博研究生学员提供了接触数字法治领域前沿新知、共同切磋学习研究心得的优质平台。

部分教师、学员合影

开营式

7 月 7 日上午，“数字法治的理论视野与实务前沿”暑期学校在北京大学法学院 B102 会议室正式开幕。仪式由北京大学法学院长聘副教授、副院长、北京大学数字法治研究中心副主任戴昕主持，北京大学数字法治研究中心主任王锡锌教授出席开幕式并致辞。

北京大学数字法治研究中心主任 王锡锌教授

理论研究工作坊（7 月 7 日上午及下午）

北京大学法学院副教授、北京大学数字法治研究中心研究员胡凌讲授的讲座题目为《信息匹配与错配》。中国海洋大学法学院副教授王博阳、贵州大学法学院副教授曲君宇作为学员代表，针对胡凌的讲座提出问题和评论。

对外经贸大学法学院教授张欣为学员们带来题为《从云端到终端：端侧智能治理的挑战与应对》的讲座。中国计量大学法学院讲师黄丽和上海交通大学凯原法学院博士后冉高苒作为学员代表，针对张欣的讲座提出问题和评论。

中国人民大学法学院教授熊丙万作题为《数据产权：场景、样态与学术问题》的报告。中南财经政法大学法与经济学院讲师李胡兴和中华女子学院法学院讲师涂艳辉作为学员代表，针对熊丙万的讲座提出问题和评论。

北京大学法学院助理教授、院长助理、北京大学数字法治研究中心研究员王华伟以《网络暴力语境下人肉搜索的刑法规制》为主题开展讲座。天津大学法学院副教授李倩和华东政法大学法律学院副教授王静作为学员代表，针对王华伟的讲座提出问题和评论。

特邀学者主题学术报告（7 月 8 日上午）

7 月 8 日上午，当代著名法学家、美国哈佛大学法学院 Roy·L·Furman 法学与领导力讲席教授劳伦斯·莱西格（Lawrence Lessig）以“人工智能与民主政治”为题，在北京大学法学院凯原楼学术报告厅作学术演讲。北大法学院副院长、长聘副教授戴昕担任本次演讲的主持人，中国政法大学数字法治研究院教授张凌寒和北大法学院副教授胡凌担任本次活动的与谈人。校内外学生、学者和行业实务专家约 160 余人到场参加活动，反响热烈。在与谈环节中，戴昕、张凌寒、胡凌分别发表了与谈意见。

实务专家授课研讨（7 月 8 日下午及 7 月 9 日上午）

阿里研究院人工智能治理中心主任傅宏宇以《DeepSeek 时刻以来人工智能全球发展应用和治理挑战》作学术分享，并由中国社会科学院大学法学院副教授刘晓春作为特邀与谈人与谈。上海政法学院人工智能法学院讲师鲍坤和中共黑龙江省委党校政治和法律教研部讲师陈可作为学员代表，针对傅宏宇的讲座提出问题和评论。

抖音集团互联网法律研究中心主任丁道勤的讲座以《平台治理权边界的思考》为主题，由北京大学智能学院、人工智能研究院助理研究员辜凌云担任特邀与谈。北京交通大学法学院讲师陈子君和中南财经政法大学法学院讲师闫申作为学员代表，

针对丁道勤的讲座提出问题和评论。

法律 AI 实训课（7 月 7 日及 7 月 8 日晚间）

北大法宝结合其新型技术工具前沿研究的能力与丰富资源，为学员们带来四场法律 AI 实训课。

北大法宝科研发展办公室主任梁鸿翔博士以《面向企业出海的数字法治智能技术讨论》为题，探讨企业在出海过程中面临的数字法治挑战以及应对经验。北大法宝智能产品负责人郭世聪以《AI 时代，重塑知识管理新范式》为题，分享借助大模型及相关技术提升法律领域知识管理效率与应用价值。北大法宝智慧法务研究院秘书长、研究员蔡治博士作《“数智融合”赋能企业法务合规创新实践》主题报告。北大法宝总经理助理郭璐进行北大法宝大数据实证分析案例介绍。

学员代表研究展示

7 月 9 日下午，八位学员代表分享了自己的研究成果。北京大学法学院长聘副教授、副院长、北京大学数字法治研究中心副主任戴昕、北京大学法学院长聘副教授、北京大学人文社会科学研究院副院长、北京大学数字法治研究中心副主任阎天两位老师从选题类型、研究结构、写作技巧与投稿建议等多个维度进行点评。

结业仪式

7 月 9 日下午，首届“数字法治的理论视野与实务前沿”暑期学校举行结业仪式。仪式由北京大学法学院长聘副教授、副院长、北京大学数字法治研究中心副主任戴昕主持，北京北大英华科技有限公司（北大法宝）副总经理何远琼出席，一同为学员颁发结业证书。本次暑校推进数字技术和人工智能相关新兴法律议题的学术研究与实务交流，拓展法学专业研究生及青年教师的学术视野，促进相互学习交流，提升其结合新型技术工具开展前沿研究的能力，为数字法治领域的人才培养和学术研究注入了新的活力。

北京大学法学院长聘副教授、副院长、

北京大学数字法治研究中心副主任 戴昕 和北京北大英华科技有限公司（北大法宝）副总经理何远琼

清华大学计算法学课题组参加第 20 届国际法律人工智能学术大会（ICAIL2025）

2025 年 6 月 16 日至 20 日，计算法学 2021 级硕士毕业生陈卿静、计算法学 2024 级硕士研究生马佳羽受邀前往美国芝加哥西北大学参加第 20 届国际法律人工智能学术大会（ICAIL 2025）。

国际法律人工智能学术大会（ICAIL, International Conference on Artificial Intelligence and Law）是法律人工智能领域顶会。自 1987 年创办以来，ICAIL 一直是该领域最具影响力的国际学术会议，由国际法律人工智能协会（IAAIL）组织。本届大会在美国芝加哥西北大学法学院召开，大会聚焦人工智能在法律领域的前沿应用与理论创新，涵盖法律文本分析与挖掘、法律知识表示与推理、法律文本生成、伦理规范与可解释性与多语言法律 AI、法律 AI 的实际应用、法律 AI 竞赛与挑战等主题。会议持续五天，共收录 35 篇长论文、25 篇短论文、12 篇演示摘要，来自世界各地的 250 余位学者与会。第 21 届 ICAIL 将于 2026 年举办，这是 ICAIL 首次连续两年举办。此次会议也将首次在亚洲举行，由新加坡管理大学承办。

第 20 届国际法律人工智能学术大会现场

6 月 17 日，陈卿静在会上作题为 EVENS: Equality versus Equity Notion Spectrum of LLMs 的论文报告，该论文由刘云、申卫星等担任通讯作者。

6 月 19 日，马佳羽（由陈卿静代为报告）在会上作题为 Multi - agent Cooperative Mechanisms for Legal Adjudication: The Crucial Role of Automatic Prompt Optimization 的报告。该论文由刘云担任通讯作者。

两项研究均获得国际学术界的积极反馈，并收获了对未来研究方向具有重要启发意义的建设性建议。论文全文收录于由美国计算机学会（ACM）出版的会议论文集，EI 检索。

“数治领航，知行合一” 国家市场监督管理总局竞争政策协调司党支部与中国政法大学数据法治研究院党支部共建活动顺利举行

2025 年 6 月 20 日，国家市场监督管理总局竞争政策协调司党支部与中国政法大学数据法治研究院党支部在中国政法大学海淀校区联合举办“数治领航，知行合一”主题党建共建活动，取得圆满成功。

活动伊始，在中国政法大学数据法治研究院党支部时建中教授的引导下，双方支部党员共同参观了中国政法大学校史展。追溯法大文脉传承，赓续法治精神绵延。

中国政法大学数据法治研究院党支部 时建中教授

在教育部哲学社会科学实验室——中国政法大学数据法治实验室的交流环节，**时建中**教授重点展示了实验室的建设成果，特别是“数据法治致公平台”在数据治理、公平竞争审查及合规实践应用等领域的创新机制与运行成效，生动体现了实验室推动数据法治理论与实务融合发展的探索路径。

国家市场监督管理总局竞争政策协调司党支部代表随后进行了专业深入的座谈发言。二级巡视员**刘凤双**充分肯定了数据法治实验室的信息化建设成果，并强调了数治融合对竞争政策创新发展的重要赋能作用。

公平竞争审查二处负责人**果铭**、一处负责人**刘辉**、国际合作处负责人**胡馨月**等同志结合市场监管总局信息化建设实践，围绕数据获取与分析技术、公平竞争审查数字化系统建设、数据安全、政务数据运营机制及系统效能优化等关键议题，提出了宝贵的建设性意见。数据法治研究院党支部师生代表积极参与了互动研讨，现场交流气氛热烈。

本次党建共建活动以党建为引领，有效搭建了行政实务部门与高校科研机构之间的沟通桥梁，凝聚了智慧监管领域的研究合力。活动为深化公平竞争审查政策研究、推动数据法治建设提供了重要的智力支持和实践指导，是“知行合一”理念的生动实践。

活动在全体参会党员同志的热烈掌声与合影留念中圆满落幕。

“数治领航，知行合一”主题党建共建活动顺利举行

第四届“数字法学与数字司法”研讨会

开幕式

2025 年 6 月 28 日，第四届“数字法学与数字司法”研讨会在青岛西海岸新区隆重举行。开幕式由山东科技大学文法学院院长孙法柏教授主持。本届论坛聚焦“全球数字治理与数字法治发展”这一重大时代主题，围绕数字权利与数字人权，数字司法与数字法治，数据共享、数据垄断与数据治理三个议题展开深入研讨。会议伊始，孙法柏院长介绍了出席开幕式的专家领导，并对出席本次会议的各位领导、嘉宾、专家、学者、朋友们表示热烈欢迎和诚挚感谢。

研讨会现场

山东科技大学党委副书记刘明永代表主办方致辞，首先向与会嘉宾、同仁表示诚挚欢迎，向长期关心支持学校发展的领导专家致以衷心感谢。刘明永强调，本届研讨会紧密围绕全球数字治理体系的核心法律问题与我国数字法治建设的现实需求，通过与会专家学者深入研讨，必将激荡思想、凝聚共识，搭建高效交流平台，推进数字法治理论创新与实践发展，为构建中国自主数字法学知识体系、贡献中国式数字法治智慧发挥积极作用。

山东科技大学党委副书记 刘明永

青岛市中级人民法院审判委员会专职委员曹波代表青岛中院发表致辞。曹波指出，当前正值落实习近平总书记关于“推动大数据、人工智能等科技创新成果同司法工作深度融合”要求的关键时期，大语言模型已成为人工智能进步的核心驱动力，深度赋能司法服务的精准化、普惠化与便捷化。在此背景下，本届研讨会汇聚智慧，共商数字法治发展大计，彰显出对理论创新与实践探索的双重引领价值。

青岛市中级人民法院审判委员会专职委员 曹波

中国法学会网络与信息法学研究会会长姜伟发表讲话，肯定了本届论坛聚焦“全球数字治理与数字法治发展”重大命题具有深远意义。姜伟强调，中国的倡议与实践，同联合国双契约理念高度契合。数字法学研究须立足国情，总结中国经验，提炼原创性理论概念，着力构建中国数字法学自主知识体系。

中国法学会网络与信息法学研究会会长 姜伟

第一单元：数字权利与数字人权

研讨会第一单元由华东政法大学数字法治研究院副院长、副教授、《数字法学评论》副主编韩

旭至副教授主持。中国人民大学法学院张新宝教授，清华大学法学院程啸教授，《中国法律评论》余亮亮编辑，山东科技大学文法学院李宗录教授，东南大学人权研究院执行院长龚向和教授，广州大学人权研究院刘志强教授分别进行了会议演讲。

在自由发言阶段，张新宝教授围绕人格权商品化及财产利益保护问题展开了论述。广州大学人权研究院博士生李越开围绕数字人权问题提出了观点。龚向和教授在自由发言阶段回应时指出，人权是随着时代发展而不断变化的，从近代的第一代自由权、现代的第二代社会权到当代的第三代发展权，数字时代也可能产生第四代人权——数字人权。

第二单元：数字司法与数字法治

研讨会第二单元由中国石油大学文法学院院长王学栋教授主持。本单元围绕数字司法与数字法治中的理论问题和实践路径展开。中国人民大学法学院教授陈景辉，西南政法大学教授、《现代法学》副主编董彦斌，上海政法学院人工智能法学院讲师余圣琪，上海市普陀区人民法院院长刘力，浙江省人民检察院第十一检察部主任劳伟刚，上海师范大学哲学与法政学院副教授杨帆进行了主旨发言。

第三单元：数据共享、数据垄断与数据治理

研讨会第三单元由青岛大学法学院王静教授主持。中国政法大学数据法治研究院张凌寒教授，山东科技大学文法学院单娟副教授，黑龙江大学法学院牛丹彤老师，山东科技大学文法学院赵丽莉教授，山东科技大学文法学院孙明泽副教授分别在本单元进行了会议演讲。

闭幕式

闭幕式上，华东政法大学数字法治研究院院长、《数字法学评论》主编马长山教授做了会议总结。闭幕式由山东科技大学文法学院李伟教授主持。

第四届“数字法学与数字司法”研讨会圆满结束

“数字法治政府建设与治理现代化”学术研讨会成功召开

2025 年 7 月 5 日，由中国法学会网络与信息法学研究会主办，西南政法大学行政法学院、西南政法大学数字法治政府研究院、大理大学法学院、大理大学经济与管理学院承办，北京植德律师事务所协办的“数字法治政府建设与治理现代化”学术研讨会在大理大学召开，来自全国人大常委会、中国社会科学院、清华大学、南开大学、南京大学、中山大学、中国政法大学、西南政法大学、华东师范大学、云南大学、宁波大学、广州大学、重庆邮电大学、大理大学等机构 40 余位专家学者，就数字法治政府建设与治理现代化问题进行研讨。

研讨会现场

开幕式

开幕式由西南政法大学数字法治政府研究院执行院长、人工智能法学院教授冯子轩主持。中国法学会网络与信息法学研究会会长、最高人民法院咨询委员会副主任委员姜伟，中国法学会法理学研究会会长、中国法学会学术委员会副主任，中国社

会科学院学部委员、法学研究所研究员李林，大理大学党委书记李涛，作开幕致辞。

第一单元　数字治理的法治框架与制度创新

本单元由全国人大常委会法制工作委员会研究室王洪宇处长主持。

中国法学会行政法学研究会顾问、清华大学公共管理学院于安教授，中山大学法学院高秦伟教授，大理大学法学院杜永波副教授分别发表了主题演讲。云南大学法学院副院长刘国乾教授，南开大学法学院王瑞雪教授，清华大学公共管理学院陈天昊长聘副教授，西南政法大学教务处副处长、《政法教育评论》执行主编武夫波副教授，对三位报告人的报告进行了与谈。

第二单元　数字法治政府的制度架构与治理现代化

本单元由中国社科院信息情报院第八编研室副主任李延枫编审主持。

宁波大学法学院张亮教授、西南政法大学行政法学院杨靖文副教授、南京大学法学院金健助理教授分别发表了主题演讲。华东师范大学王军副教授，西南政法大学行政法学院杨国栋副教授，西南政法大学行政法学院陈子祯讲师对三位报告人的报告进行了与谈。

第三单元　数字立法的创新路径与人工智能治理

本单元由云南大学法学院副院长刘国乾教授主持。

北京植德律师事务所管委会委员、合伙人沙骏律师，宁波大学法学院副教授金耀，大理大学经济与管理学院贾婷特聘副教授分别发表了主题演讲。重庆邮电大学网络空间安全与信息法学院韩兵教授，西南政法大学人工智能法学院冯子轩教授，广州大学法学院狄行思讲师对三位报告人的报告进行了与谈。

闭幕式

闭幕式由中国社会科学院法学研究所宪法与行政法研究室主任、研究员，中国法学会行政法学研究会副秘书长、政府规制专业委员会副秘书长李霞主持。大理大学法学院院长杨运星教授作闭幕致辞。

“数字法治政府建设与治理现代化”研讨会圆满落幕

（技术编辑：林诗敏）

数字法评

论人工智能法律规制的内部路径

此处删除了原文脚注，全文请参见《河北法学》2025 年第 8 期，转载或引用请注明出处。

作者：邓矜婷

摘要：人工智能具有海量、高效、黑箱的特点，使得规制人工智能相关人员权利义务责任的外部路径存在规制效能不足、规制限制发展的困境。应当利用人工智能的特点，构建以人工智能规制人工智能的内部路径，补充外部路径。内部路径是在人工智能行为被直接影响和约束的层面进行规制，包括通过发布可以直接调用的法律规则要件体系和关系图表、通用的合规审查基座模型、用以自动检测的标注数据集和指标体系、构建人工智能执法司法辅助系统等方法。其核心是将法律规则的要求融入人工智能底层的技术，实现运用人工智能技术帮助规制人工智能应用。因此，内部路径具有高效、精准规制的特点，可以补充外部路径，缓解规制人工智能的两大困难。

一、人工智能法律规制的困境

人工智能的迅猛发展为人类带来了新的机遇，同时风险也迅速滋生。如何抓住机遇，规避风险，是具有滞后性的法律需要面临的挑战。人工智能的发展对传统法律产生了巨大冲击，与一般技术引发的治理风险相比，人工智能技术引发的风险更具复杂性、系统性，带来的立法挑战更具颠覆性。具有滞后性的法律难以规制以月为单位变化的人工智能技术格局，此外，人工智能的信息不对称性让立法机构无法针对性地制定法律，人工智能治理范式不可避免地从单一的以国家为中心、以命令和控制为核心的“硬法”模式向基于多中心主体参与的“软法”模式转变。[1]

为了应对人工智能带来的挑战，国家各部门以及地方政府相继出台大量的规范性法律文件，以应对冲突、促进发展。在国家层面，主要集中于数据治理。人工智能作为一种数据密集型技术，需要海量的数据支撑，这些数据中包含国家数据、个人信息、商业数据、政府数据和公共数据等，2017 年起施行的《中华人民共和国网络安全法》（以下简称《网络安全法》）要求为了网络安全和数据保护，企业和个人必须采取技术措施保护个人信息和重要数据。为保障数据安全和个人信息权益，2021 年国家相继出台了《中华人民共和国数据安全法》（以下简称《数据安全法》）、《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）。在具体应用层面，《中华人民共和国电子商务法》针对“大数据杀熟”、算法的信息披露义务等作出了规定，《中华人民共和国反不正当竞争法》（以下简称《反不正当竞争法》）的“互联网专条”针对企业间数据获取和使用作出了规定。我国尚未出台针对人工智能应用的专门立法，但有司法解释和部门规章出台，最高人民法院为推动人工智能同司法工作深度融合，发布《关于规范和加强人工智能司法应用的意见》，国家互联网信息办公室、工业和信息化部和公安部于 2022 年联合发布《互联网信息服务深度合成管理规定》。在地方层面，深圳、上海作出了立法尝试，为未来人工智能领域的法律规制提供了经验。[2]

关于人工智能的法律规制，学界也有诸多研究和讨论。包括人工智能的基础理论和具体适用问题，比如人工智能的法律地位，人工智能法律规制的前提是明确人工智能在法律关系中的地位，目前有三种理论观点：客体说[3]、有限主体说[4]和完全主体说[5]。传统的侵权责任体系以过错归责为原则，但人工智能造成的侵权责任因人工智能法律地位尚未明确，致害主体和因果关系认定复杂，对侵权责任的认定带来极大挑战。作为人机交互的算法决策机制，学界逐步对其深入研究，如算法黑箱、算法歧视、数据垄断、信息茧房、大数据杀熟、算法共谋等现象[6]。对于算法风险的治理，有学者主张通过有效提升算法透明度和加强监管来解决，[7]有的学者主张既要实现数据开发和算法透明，也要将法律与道义嵌入算法设计，优化算法，强化伦理审查。[8]有学者主张将算法决策嵌入网络社会架构，采用

分类分级的精准化治理方法，兼用“软”“硬”法作为协同治理工具，[9]有学者主张要建立双轨制的规制路径，调整对象升级为算法设计与部署应用的结果，和调整算法自主决策本身，采用平台责任和技术责任双轨并用的责任承担方式。[10]在人工智能具体应用领域，如智慧司法，其内嵌技术具有本源性缺陷，可能会导致过度依赖、主体弱化、算法歧视与数字鸿沟的异化风险，损害司法公开、司法公正等基本原则，为了规制这些风险，有学者主张建立事前评估和事后检验相结合的算法论证规则，设立完善的算法解释规则，嵌入案件预警纠偏机制，并探索运用区块链技术。[11]也有学者主张要对应智慧司法系统的投用全流程，建构伦理与道德的设计审查、裁量标准的统一性尺度、增强算法决策的可解释性与重构责任分配规则的权利保护新体系。[12]

尽管《网络安全法》《数据安全法》《个人信息保护法》等法律的出台作为底层的规则基石为人工智能的健康发展提供了坚实保障，学者也作出了诸多有益的讨论，但是对于人工智能风险的规制仍显乏力。一方面是出台的文件和提出的学说不足以解决人工智能迅猛发展带来的问题，并且预期法律成本过高。如对于算法崛起所带来的法律挑战，传统法律规制主要采取三种方式加以应对：算法公开、个人数据赋权与反算法歧视，但是算法公开或者算法的可解释性面临技术上无法实现、公开无意义、用户算计与侵犯知识产权等难题，个人数据赋权面临个人难以行使数据权利、过度个人数据赋权导致大数据与算法难以有效运转等难题，反算法歧视面临非机器算法歧视、身份不可能完全中立、社会平等难以实现等难题。[13]人工智能的发展建立在数据的收集与利用基础之上，进而会诱发数据安全风险，包括数据投毒、数据深度伪造[14]、数据过度采集、数据滥用分析等方面的威胁，如前所述，我国针对数据保护出台了大量法律法规，但是人工智能内在的局限性，即算法风险，以及数据在人工智能应用中历经数据采集、数据传输、数据储存、数据处理、数据交换再到数据销毁的动态周期过程，所涉及的个人、企业、其他组织、政府等多主体的利益难以调和，引发的隐私保护、可解析性和公平性等问题无法根本解决。[15]此外，根据摩尔定律，互联网等高科技的更新周期大约在两年。[16]2023 年 3 月，AI 领域便发生了一场震撼人心的革命，从斯坦福大学推出的 Alpaca 到 ChatGPT Plugins，实现实时数据获取仅花了 12 天时间，立法的速度难以与之匹敌，导致法律滞后现象出现。对此，已有学说指出，与规则和指令相比，当颁布一项规则或者指令带来的预期法律成本过高时，立法机关应当以标准作为更有效率的规制方式。[17]

另一方面，人工智能亟须发展，各种规范性法律文件过多，会成为人工智能发展和创新的掣肘。据统计，我国目前已经制定出台网络领域立法 140 余部。[18]但人工智能立法应是规范与发展并行的立法。在信息控制者激励失衡的背景下，如果立法缺乏科学性，只是简单施加各种强制性外部要求，忽视信息控制者内在激励机制设计，会抑制大数据开发利用。[19]有企业智库的研究人员通过对美欧日韩立法的对比研究，主张法律天平的一端是产业发展和互联网创新，另一端是私权、用户保护和公共利益，加重平台责任必然与互联网创新背道而驰。现在即使需要对互联网加强监管，合理的监管方式也不是将传统的法律监管框架延伸到互联网，而是探索新的监管范式，协同发挥各方力量，共同治理互联网。[20]

目前大量的规范性法律文件的出台，使得人工智能产业的发展成本也急剧上升，如企业数据的合规管理。企业不仅要遵守数据保护相关的法律法规，还要遵守国家政策、商业惯例、公司章程以及道德规范等，需要配合各个部门密集的监管行动进行整改，无暇顾及数据保护能力的提升。知情权、许可权与删除权等新设权利增加了企业的合规负担，如仅仅针对 GDPR（《通用数据保护条例》，General Data Protection Regulation）的要求，全球便有 20% 的企业因违反要求而导致破产，甚至出现了美国洛杉矶时报及芝加哥论坛报等企业因 GDPR 合规成本过高而直接退出欧盟市场的现象。[21]对于需要大量收集和使用个人信息的企业来说，个人数据保护

机制的建立和完善需要投入的资金巨大，并且需要考虑建成之后每年的维护费用，这都对公司财政状况提出挑战。Telos 开展的一项企业合规治理的成本调查显示：每家企业要做到数据的管理符合法律法规的要求，平均需要遵守至少 13 个不同的 IT 安全或隐私法规，并且每年在合规性活动上要花费高达 350 万美元。[22]

本文认为，当前人工智能的法律规制主要是按照人的特点，通过构建权利义务责任，影响人工智能相关人员的行为和意图的方法来实现对人工智能的规制。相对于人工智能本身而言，这种规制路径是通过对人工智能外部人员的规制来实现，本文因而称之为人工智能法律规制的外部路径（简称“外部路径”）。这种规制路径确实是当前应对人工智能风险必要的也是主要的手段。不过由于外部路径主要考虑的是人的特点，所以在应对人工智能高效、海量、黑箱等特点带来的风险时存在难以有效规制的困境。数量众多、边界不明的规制又导致对技术创新的限制。人工智能较为智能，而且强人工智能已经开始显现。虽然这种智能本质上与人的智能是不同的，但是它还是具有一定的自主性，其在行动和决策上是自动的。但是人工智能不是人，不能理解权利义务责任，难以通过这些方法影响其行为和意图。如果能够在人工智能会被影响的层面和方式上，将法律法规对其行为和目的的要求通过计算机语言和方法来表达，使得人工智能能够直接被影响，并且主动遵循，就可以极大地降低人工智能应用的法律风险，减少人工智能的规制需要。在此基础上，如果能够建立可信人工智能的执法和司法系统，就可以有效地利用人工智能来规制人工智能。这两方面的规制是直接规范人工智能本身的，本文称之为人工智能法律规制的内部路径（简称“内部路径”）。内部路径虽然旨在让人工智能“懂”法律，但是这是为了更有效地约束人工智能，让人工智能更好地服务于人，而不是认为人工智能具有跟人一样的主体地位。要实现内部路径，核心就是通过计算机语言和方法来充分表达法律规则。只有这样，人工智能才能一定程度地理解法律规则，或者说，人工智能的行为和目的才能被法律规则影响。在充分表达的基础上，可以出台权威数据标注规则框架、权威标注数据集、权威法律法规关系图表，搭建人工智能应用可以对接的权威法律规则运维平台，提供人工智能对法律规则遵循程度的检测体系及平台等。此外，只有在充分表达的基础上，才能构建可信的人工智能司法和执法系统，实现以人工智能规制人工智能。而法律规则作为一种抽象的存在，既然可以通过自然语言来表示，也应当可以通过计算机语言和方法来表示。一方面自然语言的词义目前已经有很多复杂的以词向量为代表的表示方法，另一方面，法律规则的逻辑含义也有不少以逻辑变量为代表的表示方法。虽然距离法律规则的充分表达还较远，但是该领域在不断发展，以之作为外部路径的补充未尝不可。况且，当前的外部路径已经在这方面作出了尝试，开始针对算法、标注、预训练数据集等作出一些原则性的规定。不过面对人工智能的不断发展和广泛应用，以及强人工智能的显现，只有原则性的规定不足以实现有效的内部路径。实践中已经出现了相关人员随意构建法律知识图表、使用粗糙的标注数据集等做法。法学界应当在这一领域展开正式的研究，指导和引领实践。

二、人工智能法律规制困境的原因在于当前规制仅采取外部路径

（一）当前人工智能法律规制采取的是外部路径

现代社会已经进入了数字时代，人工智能技术在多个领域广泛应用，人工智能越来越成为我们生活中不可缺少的科技力量，我们的生活逐渐被人工智能渗入。但我们在发展人工智能、利用人工智能的时候，也很容易受到人工智能的影响，陷入人工智能介入可能产生的困境之中。

人工智能深刻影响了法律的发展，法律需要对这种强势力量作出一定的回应，立法者已经采用了多种方法规制人工智能，但这些方法无一例外都属于外部路径。即，当前法律对人工智能的调整，是通过设计一种法律机制，配置人工智能相关人员在

法律上的权利义务以及规定违反法律规定所应承担的法律责任，来设定主体的行为模式，引导相关人员在法律所许可的范围内开展与人工智能相关的活动，从而把人工智能相关人员的活动引入可调控的法律秩序之中。

目前人工智能法律规制的方法有：首先，立法者通过制定相关法律法规，明确人工智能技术的应用范围、责任承担等方面的规定。例如，出台《网络安全法》《数据安全法》等法律法规，对人工智能在网络安全、数据安全等领域的应用进行了规范。其次，通过设立相关机构，如中央网络安全和信息化委员会、中国网络空间安全协会人工智能安全治理专业委员会等，加强对人工智能领域的监督和管理。这些机构负责制定和实施相关政策、标准和规范，确保互联网平台等主体对人工智能技术的合规应用。最后，通过加强对人工智能相关行业从业人员的管理，确保他们符合相应的资格要求和技术标准。例如，国家新一代人工智能治理专业委员会发布的《新一代人工智能伦理规范》等文件，对从事人工智能管理、研发、供应、使用等相关活动的自然人、法人和其他相关机构等主体的人工智能伦理问题进行了规范。[23]但以上对人工智能的规制均采用了外部路径，即通过构建人工智能相关人员的权利义务责任的方式来进行调整。

当前的外部路径已经取得了一定的成效。然而，由于人工智能技术的快速发展和应用领域的不断扩大，外部路径已经无法满足人工智能应用发展的需要。因此，需要继续探索和完善相关法律制度，以适应新发展形势下人工智能技术的发展需要。

（二）外部路径不直接规制人工智能本身

1．外部规制路径仅规范人的行为，与人工智能技术保持距离

如上文所述，现阶段法律对于人工智能的规制，主要是传统的调整人的权利义务责任的外部路径，只能够从规制人工智能的创造者和使用者的角度来规制人工智能。但人工智能有自身的运行逻辑，有自身的发展要求和规律，现有人工智能已经可以作出一定程度的独立自主的判断和行为。[24]针对人工智能发展所带来的法律挑战，仅有外部路径难以跟上人工智能技术的发展步伐。

外部法律规制路径强调法律与技术要保持距离。法律作为一种社会规范，具有抽象性和稳定性。法律是通过一系列的规则和原则的设置来调整法律主体的行为，这些规则和原则是高度抽象和概括化的，它们构成了法律体系的基本框架。相比之下，技术发展中出现的问题则有具体性、多样性和不断变化的特点。法律太接近技术被认为会损害法律本身的稳定性和可预见性。

因而，外部路径下法律具有一定的滞后性。法律通常是在一定的社会、经济和文化背景下制定的，并且受到特定历史时期的社会价值观和文化传统的影响。因此，法律往往落后于技术的变化，需要在新的社会情况和技术发展要求下改变。大数据时代，人工智能技术高速发展，当今的人工智能已经从单纯的技术工具逐步升级为复杂的自主性体系，并通过嵌入社会权力结构发挥作用。[25]外部路径下法律的这一局限性在当今时代表现得更加明显，外部路径越来越难以追上技术的发展速度，可能导致法律在新的网络时代无法充分保护公民的权益。技术导致的多主体性、主体与客体的模糊性也使得法律更加难以理解和实施。

因此，由于外部路径下法律与技术需要保持一定的距离，进而难以完全适应社会的变化和技术的发展，所以需要引入其他的法律规制路径作为补充。

2．外部规制路径仅解决人工智能相关人员的价值判断问题

根据拉兹对于法律作用的分类，法律具有规范作用和社会作用。当法律作为行为规范作用于人工智能领域时，主要通过对人工智能相关人员的行为起到导向和引导的作用，即引导相关人员进行价值判断来进行规制。法律具有指引、评价、预测、教育和强制作用。法律是通过规定人工智能的相关人员在法律上的权利和义务以及违反法律规定应承担的责任来调整主体的行为的。通过法律，人工智能的相关人员可以知道什么是应当做、可以做的，什么是不能做的。法律可以防止人工智能相关人员

作出违反法律指明的行为，鼓励人工智能相关人员从事法律所容许的行为。同时，根据法律规定，人工智能相关人员可以预先估计到他们相互间将如何行为，国家机关及其工作人员将如何行为。人工智能相关人员因而可以根据法律来确定自己的行为方向、方式、界限，合理地作出安排，采取措施。[26]

结合现在的法律和法学理论，外部路径已经解决了一部分价值判断问题。例如关于人工智能技术运用中个人信息保护问题，《中华人民共和国民法典》《个人信息保护法》都针对互联网平台对个人信息的权利、义务、责任范围等作出了规定。《刑法》《行政法》等也通过设置惩罚方式为个人信息保护提供充分的规则供给。[27]又如，《反不正当竞争法》对互联网平台涉数据不正当竞争行为进行规制，从而达到间接保护网络消费者个人信息的目的。[28]再如人工智能应用的前沿领域——自动驾驶问题，自动驾驶在迅猛发展的同时，也遇到了自动驾驶汽车的主体地位和责任认定等伦理和法律挑战。[29]有学者认为，在民法意义上，汽车故障导致的事故引发侵权责任，可以使用现有的机动车交通事故责任规则和产品责任规则来进行规制。[30]有学者认为对于自动驾驶模式下发生的交通事故侵权，从救济与预防目标来看，应由制造商一方承担产品责任。[31]有学者认为司法机关应当通过利用刑罚有效性原则排除主体争议。[32]在刑法方面，有学者认为可以基于既有刑法教义学进行追责，具体的刑事归责方面，可以类型化为：非法利用自动驾驶汽车作为犯罪工具者的故意责任、驾驶人的过失责任、系统故障导致的生产销售者的产品责任以及驾驶人与系统存在过失竞合的责任等四种情况。[33]

学者和立法者通过现有法律，解决了部分人工智能的相关人员哪些行为可以为、哪些行为必须为、哪些行为不能为的价值判断问题。然而，由于人工智能具有一定的智能性，仅仅通过规制人工智能相关人员这种外部路径不足以应对人工智能的规制需要，不能达到像规制其他技术那样的效果，所以在对人工智能的规制时经常出现规制失效、规制限制发展的情况。

三、人工智能法律规制内部路径的提出

面对权利义务责任模式的外部路径在一些人工智能治理场景下的失效，需要有适应人工智能特点的规制路径来克服人工智能高效、海量、黑箱等特点带来的难以有效规制的困境。基于此，本文提出了一种新的人工智能法律规制的内部路径，对外部路径进行补充，协调人工智能规制和发展的需要。

（一）内部路径直接规制人工智能本身

人工智能法律规制的外部路径和内部路径是相对于人工智能本身而言的。如前所述，外部路径是指以构建权利义务责任的方式，通过影响人工智能相关人员的行为和意图来实现对人工智能的规制。以国家互联网信息办公室起草的《生成式人工智能服务管理办法（征求意见稿）》为例，[34]该草案主要规制对象是利用生成式人工智能产品提供聊天和文本、图像、声音生成等服务的组织和个人，规定其遵守法律法规、尊重社会公德、公序良俗等义务，如利用生成式人工智能生成的内容不得含有危害国家安全的内容以及歧视的内容，履行个人信息保护义务等。组织和个人违反规定的，应当根据相关法律法规和本草案承担相应的刑事责任和行政责任。外部路径以人工智能相关人员为主体，将人工智能视为技术、工具或者平台，以技术中立或者工具中立的观点，认为人工智能违反法律的本质是使用人工智能的人违反法律，规范使用人工智能的人的行为，能促进人工智能的健康发展和规范应用。

然而人工智能并非以往的技术或者工具，其具有一定的智能性，尤其是强人工智能已经开始显现，在算法和数据的支持下，人工智能在一定程度上能够自主行为和决策。在这种背景下，提出内部路径是可能的，也是必须的。内部路径是指直接规制人工智能本身，在人工智能会被影响的层面和方式上，将法律的要求通过计算机语言和方法来表达，使得人工智能能够理解，并且主动遵循。内部路径相对于外部路径来说深入人工智能内部，建立在人工智能具有一定智能性的基础之上，以人工智能本身为

规制对象，即在程序、算法层面约束人工智能无法违反法律，即使其使用者要求其违反法律或将其用于实施违法行为。目前，我国一般采取外部路径规制人工智能，但部分法律法规中体现出了内部路径的精神，如，《生成式人工智能服务管理办法（征求意见稿）》中已经开始注意会直接影响人工智能行为的几个因素，并对其规定了一些基本要求，包括对人工智能的预训练过程、大模型的调用、训练集的要求等。[35]

（二）内部规制路径通过在技术底层融入法律规则的要求实现对人工智能的直接规制

既然要直接规制人工智能，那就要让人工智能理解法律规则，其行为和决策直接受法律规则约束。所以内部路径与外部路径本质的区别是，外部路径是让人懂法律规则，而内部路径是让人工智能“懂”法律规则。因此，内部路径的核心是法律规则的计算机表达。只有通过计算机充分准确地表达了法律规则，人工智能才能理解和遵循。值得一提的是，人工智能虽然有智能化的表现，但是跟人还是有本质的不同。而且让人工智能“懂”法律，是为了更有效地约束人工智能，让人工智能更好地服务于人，而不是认为人工智能具有跟人一样的主体地位。所以所谓让人工智能理解和遵循法律规则，其实是指在人工智能能够被直接影响的层面按照法律规则的要求予以规范，换言之，在能够直接影响人工智能的层面将法律规则的要求表达出来，使得人工智能直接受到法律规则的约束和规范。

现有的智慧法治、数字法治实践也是沿着这个方向在不断努力，让计算机能够获取法律知识，自动完成法律任务。[36]虽然这些实践的目的是研究如何将人工智能技术应用到法律领域，而不是研究如何规范人工智能技术本身，但是为了更好地完成这些法律任务，已有研究在不断地完善法律规则相关知识体系的计算机表达。因为法律规则的相关知识越能较好地被计算机获取和处理，计算机完成相关法律任务的能力已经被证明就会越好，就越能得到认可。虽然人工智能无法像人类那样理解法条、进行三段论式的法律推理，但是人工智能有适应其特点的三段论适用法律的方式。在理解、确定适用的法律规范（大前提）方面，已有不少研究取得较大进展。[37]可以通过构建法律规则的要件体系并将其标签化、构建法律规则体系的图表、对结构化的判决书中的裁判说理和裁判依据部分进行自动处理等方法将关于法律规则的知识转变成计算机可以自动获取和学习的知识，训练计算机在法律规则体系中寻找、确定与案件事实相关的可能适用的大前提的能力，训练计算机将大前提要件化。在分析、识别关键性事实（小前提）方面，已有研究也有不少成果。[38]可以通过进一步丰富要件体系、构建关键性事实的标签体系、有效运用通用自然语言大模型、自动生成标注的法律事实数据集等方法训练计算机自动识别、抽取关键性事实的能力。在根据大、小前提进行演绎得到结果方面，已有研究的尝试显示，可以通过自动获取关键性事实与裁判依据及争议焦点的对应关系表、构建法律规则体系的图表、设定逻辑规则等方法训练计算机进行法律推理、确定法律适用路径、得到法律适用结果的能力。

除了法律适用，人工智能还可能在具体行动的过程中获取法律知识、受到法律规则的约束。总结已有研究，本文认为法律规则计算机表达具体包括法律规则的标签化、法律任务的要件化、法律知识的数据化、法律规则体系的图表化、法律规则表达效果的指标化等。法律规则的标签化是指将法律规则的理解转换成标签体系，通过标注数据，让计算机自动获取。法律任务的要件化是指将法律规则的行动预期和适用等任务进一步分解为相关法律规则的要件及要件之间的逻辑关系，让计算机自动获取法律规则的要件及逻辑结构知识，分步完成这些任务。法律知识的数据化是指将法律知识通过数据表示出来，运用像正则表达式、通用自然语言大模型、标注数据等方法让计算机通过数据获取法律知识。法律规则体系的图表化是指将法律规则之间的对应关系、先后的变化关系，法律规则的要件逻辑关系、优先级和权重等让计算机通过像知识图谱、决策树、回归模型等方法自动获取。法律规则表达效果的指标化是指在检验人工智能完成法律任务

的效果指标中增加反映其对法律规则理解能力的指标，对非法律任务的人工智能完成效果的检测也适当考虑增加该场景相关的法律规则遵循效果的指标。

通过这些方法，法律规则的计算机表达已经在不断实践，而且在不断完善。这些方法都旨在让计算机能够获取法律知识，并在完成任务时运用这些知识。在完成像类案检索、辅助司法裁判等司法类任务时，人工智能可以通过前述方法在理解法律规则的基础上进行检索、给出建议。在完成像合同生成、协议审查、法律智能问答等公共法律服务类任务时，人工智能可以通过前述方法根据获取的法律知识，撰写符合法律要求的合同，审查协议的合法性，给出符合法律规定的回答和行动建议。在完成像自动驾驶、自动交易、自动分享传播、自动推荐、自动筛查等行动类任务时，人工智能可以自动选择符合法律规定的方法来完成任务，避免不合规定的驾驶行为，阻止虚假欺诈的交易，及时删除侵权数据的分发，阻止侵犯个人信息的收集处理行为，防止内容违法犯罪的数据传播。

在法律规则计算机表达的不断发展下，可以预见会有两种模式的内部路径。一是国家主导的模式，具体以国家机关组织、国家资助高校科研院所研发、企业负责工程建设的路径展开。这样的模式可能形成一些基础类的工具，比如通用的法律规则要件标签体系、法律规则体系的图表、基础的标注数据集、通用的合同协议生成模型等。还可能发布一些排除高风险的具体任务的基座模型，比如建议的自动驾驶基本要求基座模型、高风险内容及可疑交易自动判断筛查基座模型等。以及在立法、司法、执法工作中运用的人工智能工具，用以辅助识别、规制人工智能行为。二是市场主导的模式，具体以国家政策支持和引导、市场多主体参与、企业投资研发、良性竞争的路径展开。这样的模式可以一定程度参与和支持第一种模式，更重要的是可以产生丰富多样的人工智能产品和服务，直接促进人工智能技术向善，推动社会经济生产生活高速发展。比如形成可以为人工智能应用直接调用的相关领域法律要求的法律法规要件标签体系、基座模型、白名单数据、通用算法规则，发布可以用来检测人工智能应用对法律规则遵循效果的通用标注数据集和指标体系，产生可以直接调用、与人工智能应用结合完成合规审查的任务模型等。

四、人工智能法律规制困境需要内部路径的补充

（一）外部规制路径存在规制失效、监管成本过高的情况

随着人工智能技术的不断发展，其在社会生活中的应用越来越广泛，但同时也引发了一系列的法律问题。现有的基于权利义务责任分配的外部路径是规制人工智能的主要路径，但其难以有效应对人工智能的高效、海量和黑箱特性，即法律只能解决人的权利和义务，但不能使人工智能得到有针对性地调整，法律与技术始终保持着距离，这已成为当前面临的困境之一。

第一，责任主体的认定较为困难。随着人工智能技术的不断进步，越来越多的个人数据、个人信息被收集、记录和储存，这也意味着越来越多的个人信息、个人数据可能存在被泄露的风险，甚至会进一步导致个人隐私泄露、大数据杀熟等违法行为的出现。然而，由于人工智能技术所涉及的利益方众多，存在着复杂的权利义务关系，在这些违法犯罪行为发生时，存在着责任主体识别困难、责任承担难以落实等困境。有的学者认为，网络侵权行为涉及主体众多，包括算法开发者、算法使用者（即平台）、算法消费者，在某些情形下，算法开发者与算法使用者甚至会出现重合。[39]有的学者认为，“监管机构—平台—用户”的监管路径可能会出现平台责任边界不清的风险。[40]有的学者认为，要求平台为算法部署和应用的不利后果承担责任，可能会因为没有评判算法部署和应用是否合理的法定标准，而使平台责任范畴模糊。[41]在这种情况下，我们需要通过更加科学的方式来确定责任，而不是仅仅依靠传统的权利义务分配方式来规制人工智能。

第二，人工智能监管成本较高。由于人工智能

犯罪产生的数据海量，以及人工智能犯罪的高技术性和隐蔽性，导致人工智能监管成本较高。人工智能犯罪与传统犯罪相比，具有犯罪行为发生的随机性、犯罪过程迅速、犯罪后果呈裂变式等特点，[42]因此监管机构对其监管成本较高。人工智能犯罪的监管难度也在于其技术手段的复杂性。由于人工智能系统具有高度的复杂性和不确定性，人工智能应用已不仅仅是技术化的工具，而是越来越具有类似于人类思维的能力，监管机构需要投入大量的技术资源来分析和识别犯罪行为。[43]人工智能系统还具有自我学习和自我修复的能力，这也增加了监管难度。随着人工智能技术的快速发展，如何对其进行有效监管已经成为一个重要的课题，监管机构需要采用更加高效、精准的监管手段来应对人工智能犯罪带来的挑战。

第三，人工智能存在黑箱问题，加重了责任主体认定的困难。由于人工智能技术本身的特性，其决策过程往往是黑箱化的，这使得人们很难了解其内部决策的原因和依据。有学者认为人工智能的规则设计和运作，有时会出现用户甚至开发者无法理解的秘密状态。[44]有学者认为在人工智能系统输入的数据和其输出的结果之间，存在着人们无法洞悉的“隐层”，这就是“算法黑箱”。[45]从算法决策和人类决策的特性可以发现，算法危机的产生并非全由算法黑箱导致，人类决策同样具有“黑箱性”。[46]有学者认为算法的不可解释性使得其对现有的法律责任体系适用困难。[47]目前尚无完整的技术方案对黑箱算法进行全局解释，虽然存在局部补充解释工具作为替代性解释方法，但该类解释的可信度一直面临质疑。[48]这也给法律规制带来了困难，因为很难确定哪些决策是合法的，哪些决策是非法的。因此，需要采用更加科学的方式来评估人工智能技术的合法性，并对违法决策进行惩处。

（二）外部规制路径容易造成规制限制发展的情况

第一，责任主体范围过大以及平台责任过重。外部路径是通过人工智能相关人员来规制人工智能，所以要确定责任主体，但是人工智能相关人员的范围过于宽泛，包括关键基础设施运营者、个人信息处理者，后扩展至互联网服务提供者，再后扩展至任何主体及个人。而由于责任主体过于宽泛，所有人工智能相关人员都成为监管对象。此外，由于责任边界的模糊，容易一刀切地由互联网平台来承担责任，导致平台责任过重。《数据安全法》《网络安全法》《个人信息保护法》等多部法律都对人工智能相关人员的责任作出了规定，刑法也设置了帮助信息网络犯罪活动罪和拒不履行信息网络安全管理义务罪来对互联网平台进行规制。当今时代，互联网平台不仅要对算法的设计负起责任，同样也要对算法在部署和应用中产生的不利法律后果承担责任。[49]人工智能技术的研发在当前外部路径下存在不确定性和一定风险，人工智能产业的发展受限。

第二，规制的边界不确定，合规治理的成本过高。人工智能技术在研发和运用过程中，个体和机构的很多行为都很容易触犯相关法律，企业、个人难以界定哪些行为是违法行为，容易导致人工智能企业创新能力的下降。例如，从研发角度，《中华人民共和国刑法修正案（九）》专门规定了帮助信息网络犯罪活动罪和拒不履行信息网络安全管理义务罪，网络服务提供者等主体为他人基于信息网络技术实施犯罪行为提供了网络技术与网络结算等各类支持与帮助，或者不履行信息网络安全管理义务的消极不作为方式提供技术支持、帮助，将受到刑法的规制。然而，何为促进犯罪活动的技术支持、帮助行为，何为正常的技术活动，在司法实践中界限还较为模糊，这容易构成信息网络服务者经营活动的重大刑事法律风险，对各类创新性的信息网络技术构成了压力与限制。[50]又如，研发数据的获取、处理、分析、应用就涉及多个主体和多部法律的要求，数据合规涉及的法条众多，数据的获取、处理、分析、应用等多个阶段都要重复受到法律的限制，这使得人工智能研发企业难以确定哪些研发行为、预训练、数据、数据获取和处理分析行为及算法是合法的。随着我国不断加强互联网平台等主体责任的落实，平台方越来越需要加强内部监管，

从而走向另一个极端——过度审查，这会导致企业合规成本过高，还会降低互联网平台经济的发展质量，阻碍平台经济中信息、数据等关键资源的自由流通。[51]

可以看出，当前的外部路径在一定程度上存在着过度干预的风险。这种过度干预不仅表现在法律对于人工智能研发的宽泛管制，也表现在法律对于人工智能企业的多方面审查和干预。这可能会限制企业的自由和创新能力，从而阻碍人工智能的发展。

（三）内部路径的特点可以补充外部路径，更加准确、有效地规制人工智能

前述两点表明，人工智能所带来的挑战需要我们采用更加全面、科学的法律规制路径来应对。我们需要在充分考虑各种权利义务责任的同时，采用高效、精准的内部规制路径加以补充，以确保人工智能技术在社会生活中得到合理、有效地监管。内部规制路径具有穿透式规制和以人工智能规制人工智能的特点，可以更加准确、有效地规制人工智能应用。

1．穿透式规制

内部路径具有穿透式规制的特点，即相对于外部路径通过规制人工智能相关人员间接规制人工智能，内部路径穿透人工智能相关人员，直接规制人工智能。在工具不智能、完全隶属于人的情况下，法律无法规制工具本身，工具的活动实际上反映人的行为，法律只能通过调整人的行为避免工具对他人造成妨碍或危害。但是人工智能相对于普通工具具有海量、高效和黑箱的特点，能力极其强大，所以造成前文分析的规制困境。此外，在人工智能已彰显一定智能甚至强智能的情况下，人工智能的行为具有一定的自主性，在有些时候可能超越其使用者的意图或者目的，其能力和副作用可能超出其设计者的预设。此时，人工智能的行为实际上在人工智能理解人的指令和人工智能本身的自主决策双重支配之下。因此，外部路径的实现是由人工智能相关人员理解法律的要求，从而调整人工智能的程序、算法，规制人工智能的行为，具有间接性；内部路径的实现是将法律的要求直接转化为人工智能的程序、算法，由人工智能理解并执行，具有穿透性、直接性。

内部路径的穿透式规制特点在自动驾驶系统中有较好的体现。考虑到自动驾驶的汽车和人驾驶的汽车将长期混合存在的情况，自动驾驶汽车必须和人驾驶的汽车遵守同一套交通规则体系，在交通规则体系下由自动驾驶系统代替人从事驾驶活动，因此，将由自然语言表述的交通规则转化为自动驾驶系统能理解和执行的计算机语言是必要的。目前，学者已开展了将自然语言表述的交通规则转化为自动驾驶系统可以理解和执行的数字化交通规则的研究。[52]

2．以人工智能规制人工智能

内部路径的另一大特点是以人工智能规制人工智能。该特点有两方面内容。一是，在人工智能能够被直接影响的层面进行规制，具体包括出台通用的法律知识图谱或决策树、回归的基础工具和基座模型，发布标注规则体系的建议，提供通用的标注数据集，以及法律规则表达是否准确充分的检测指标体系等。这些方法可以加强对法律规则的计算机表达，使得人工智能在运行时能够直接获取法律的知识，受到法律的约束，在法律的框架之内执行其使用者的指令，提高其活动的合法性。

二是构建人工智能的法治系统，通过人工智能法治工具，自动识别、规范、处理人工智能应用的行为，并通过反馈机制让人工智能自动改善自己的行为，提高合法性。通过前文的方法，不断提高计算机自动获取法律知识、进行法律规则适用判断的能力，构建和完善能够理解并遵守法律规则的人工智能司法、执法系统，在司法活动中可以辅助司法人员更高效地裁决涉人工智能案件，在执法活动中可以帮助执法人员更加有效地进行法律监督，按照法律规则的要求开展执法活动，实现以人工智能规制人工智能应用。

五、内部路径可以克服人工智能规制困境的理由

如前所述，在使用外部路径规制人工智能时会陷入两方面的困境，而内部路径则可以利用其自身

所具有的特性，在外部路径“失效”的场景中发挥作用，从而对外部路径起到有效补充，最终将二者相结合，实现对人工智能的有效规制。

（一）内部路径可以提升外部路径规制的有效性

前文已经分析了通过外部路径规制人工智能时存在明显不足的原因，主要是因为算法黑箱的存在使算法具有天然屏障、从弱人工智能向强人工智能的技术革新使人工智能应用场景中的责任主体越发模糊、权利义务关系难以准确判断，以上一系列因人工智能自身“智能”特性所引发的规制难点，使现有通过调整人（主要为人工智能开发者、运营者、提供者等）而影响人工智能的外部路径难以对人工智能实现有效规制。因此需要内部路径的补充，弥补外部路径存在的不足。

1．内部路径可以有效地确定规制的对象

内部路径的“内部”体现为一种穿透式的规制，即越过相关人员，直接规制人工智能本身。这一路径的核心在于通过法律规则的计算机表达，使计算机能够理解、遵循事先内置于其中的法律规则，从而让人工智能的运行、生成结果符合已经预先内置于代码中的法律规则，即将法律的指引作用运用到人工智能的运行过程中。由于内部路径是利用计算机技术表达法律规则的要求，所以可以通过一些在数据的收集处理和模型的搭建训练检测层面的指标和方法来直接检测人工智能应用对一般性法律规则的符合程度。这样可以快速、便捷、自动地检测出可能存在问题的人工智能应用，更加有效地确定需要规制的人工智能及相关人员。一方面，可以让数据的准确和模型的搭建训练尽量减少黑箱的部分，增加让人理解的步骤。另一方面，可以通过检测指标和方法避开黑箱的影响，确定规制的对象。

关于此类以技术规制技术的方法，已经有学者在区块链治理领域中提出，并将其总结为“以法入链”和“以链治链”。[53]内部路径也是将现有的法律规则通过计算机语言表达，让人工智能直接遵循已经被计算机语言和方法表达的法律规则，从而弥补外部路径“与技术保持一定距离”的不足，提升新发展形势下人工智能治理效率。

内部路径的底层逻辑为“代码创设了算法的运行方式，其亦具有反向管理算法的权能”，因此人工智能算法规制在一定程度上可借助代码规制实现。[54]从认识层面看，很长一段时间里，算法被视为脱离于价值判断的纯粹的运算程序，是纯粹的技术问题，在“技术中立”“算法黑箱”掩护下肆意生长。但是，随着技术的发展尤其是算法不利后果的凸显，人们逐渐认识到算法其实是携带价值取向或数据偏见的复杂运行程序。这种取向或偏见可能源于设计者、研发者，也可能源于任务完成的训练过程。在计算运行的过程还可能会强化这种偏见或不道德，即“自我实现的歧视性反馈循环”，最终形成消极后果。因此有研究已经提出应当为机器进行双重意义的编码，将人类想要人工智能遵循的法律规则写入代码、写入控制机器的软件。[55]比如在第一层编码的基础上进行第二层编码，并让第二层编码符合第一层编码内含的法律、伦理规范。[56]不过，具体如何实现还需要计算机科学研究者在法律规则计算机表达理论的发展指导下进行。内部路径使人工智能在被设计之初便能够做到符合现行法律要求，并且因为其已经内置有需要被遵守的法律规则，因此在面对生成式人工智能迅猛发展的现状下也能较好地发挥作用，即可以实现让人工智能后续生成内容在脱离人为控制的前提下，仍然可以符合相关法律、伦理规范。

2．内部路径可以实现高效的规制过程

内部路径可在实现法律规则计算机表达的基础上，进一步提升人工智能规制效率。外部路径通过规制人工智能相关人员影响人工智能的方法没有充分考虑强人工智能的发展方向，同时在现有的人工智能算法设计、开发背景下，外部路径也存在着规制效率不高、过程过于烦琐等明显不足。而内部路径选择将人工智能需要遵守的一系列法律规则通过计算机表达的方式内置于人工智能算法，可以实现一次设置、多次重复使用，从而大幅提升了人工智能规制的效率。并且除了通过事先预设程序进行事前规制，以法律规则的计算机表达为基础建

设的可信人工智能司法、执法平台，也可以在实现数据共享、相关标准共同制定、知识图谱共建的基础上对后续开发的人工智能进行快速合规检测，从而将人工从现有的外部路径所要进行的烦琐、低效的监管工作中解放出来，实现对人工智能的高效规制。

外部路径通过人规制人工智能，存在规制低效、失效的困境，因为人的反应远远慢于人工智能。内部路径通过计算机表达法律规则，将法律规则的要求转化成具体的人工智能检测指标和方法。这样，一方面，可以直接、自动检测人工智能应用对一般性法律规则的符合程度；另一方面，可以搭建人工智能执法、司法辅助系统，自动地发现、检测、处理在实际应用中存在问题的人工智能，高效地锁定需要规制的相关人员及技术应用。

（二）内部路径可以平衡规制和创新

外部路径存在的另一问题是因规制而限制技术创新，这主要是因为人工智能所具有的技术特性使外部路径在试图提升其规制效率时无法兼顾精准监管，从而导致外部路径容易在规制时产生一刀切或者监管边界不明限制创新的问题。而在内部路径的补充下，这些问题会随着内部路径有效提高对人工智能的规制能力、达到预设规制目的而迎刃而解。并且内部路径可以在实现高效规制的基础上更好地进行精准监管，通过为人工智能设置其能理解并遵循的行为规范，制定符合人工智能特点的规制规则，避免一刀切，实现不限制人工智能有益发展的监管。

1．内部路径可以明确规制边界

内部规制的逻辑为用人工智能规制人工智能。如果我们将法律条文编程输入智能机器构成法律编码，那么软件代码不允许逾越法律层编码所设定的权利义务边界。这就要求法律编码必须表意明确，如此人工智能算法才能按照代码执行。[57]而此种编码化的法律规则相较于自然语言表达的法律规则少了一些模糊性与抽象性，变得更为清晰、明确，从而有助于提升相关法律规则的稳定性，使得规制过程中法的确定性、一致性以及法的可预期性得到了进一步提升。并且内部路径将在法律计算机表达的基础上建设可信人工智能司法、执法平台，通过平台明确人工智能行为边界、对人工智能进行合规检测。这一平台的建设可以让多方主体群策群力，相关可信人工智能标准的制定、法律规则代码的编写可以由更广泛的开发者、法学专家参与。通过此种方式得出的内部路径可以满足人工智能精准规制的需求，也容易得到相关从业人员的认可。这种方法也可以打消其他想要进入人工智能领域的从业人员的顾虑，增强了从业人员信心，为市场注入了活力。

2．内部路径可以降低合规治理的成本

内部路径面向人工智能本身，尽可能减少对开发者的直接规制。外部路径中关于人工智能规制的法律规则，大多为笼统、原则性的规定，许多规定在制定时并未能充分考虑相关技术的现实应用的场景，从而导致其可能对开发者提出了一些较高的、不切实际的要求。已有研究指出目前人工智能外部监管体系存在要求过于严苛、合规治理的成本较高等问题。[58]因此在当前的外部路径中，开发者不得不在开发人工智能产品时尽到相当高的注意义务，在数据训练、模型设计的每一环节都需要做到符合现行法律，这无疑是加重了开发者的责任，使其在设计程序时还需要尽可能熟悉相关法律，从而提高了人工智能技术的合规成本与进入门槛。而在内部路径的补充下，通过由法学界与开发者共同建设前文所述的可信人工智能司法、执法平台、共建数据共享平台、法律规则计算机表达知识图谱，让开发者不需要再去深入了解法律，而只需要将已经合规的规制程序、数据集嵌入现有的人工智能算法，让人工智能自己去学习、遵循相关的法律规则，这大大降低了人工智能合规治理的门槛与开发者的学习成本。

此外从学理上来看，外部路径将规制重心置于人工智能背后的开发者或其他相关人员，试图通过规制相关人员的行为来影响其所设计、开发出的人工智能，但是应当看到在此种规制路径中，人工智能作为处于高速发展变化中的技术，法律自身所具

有的滞后性与其特性存在明显差异。并且因为法律制度的发展与变革，每一过程的路径选择和规则设计，其法律思维一般都是客观事实分析与主观价值判断的综合。就法律制度建设而言，如果总是基于技术及其效应的充分显现，以此形成以技术事实为基础的社会规范，那么法律制度的滞后现象将会十分严重，最终导致技术法律对技术“匡正”的失效和无力。[59]因此在人工智能技术迅猛发展的现状下，试图仅通过外部路径实现有效规制人工智能的目标，实际上是不符合技术发展规律的。面对此类正处于高速发展变化中的技术，在进行立法规制时不仅要考虑其法律效果，还需要考虑规制可能产生的社会效果，即应当综合考虑技术的本质与发展现状来探索规制路径。因此，只有在内部路径的补充下，才能更好地适应人工智能技术发展现状，既实现对人工智能的有效规制又不过分限制其创新发展。

结语

本文中，人工智能法律规制的内部路径是指将法律规则通过计算机语言和方法来表示，使得人工智能能够理解和遵循。具体手段包括官方出台权威法律知识图谱或决策树加回归的模型，权威标注规则体系，权威标注数据集，权威的法律规则表达是否准确充分的检测指标体系等。这不是说要出台权威的人工智能应用，而是要提供接口让人工智能应用可以对接，以便理解和遵循这些法律规则的要求。这些手段听起来不可思议，无法想象，而且面对的是弱人工智能，所以只是作为补充手段，旨在克服前文所述的外部路径困境，帮助外部路径更好地规制人工智能。

人工智能正在以不可思议的速度发展进步，强人工智能能力已经显现。面对具有越来越强的智能的技术，只是通过其相关人员加以规制会日益捉襟见肘。一是难以锁定责任主体，难以确定权利内容；二是难以通过人来管理人工智能。另外，法律规则作为一种抽象的存在，既可以以自然语言的形式表示，也可以以计算机语言的形式表示。只不过离开了自然语言的文字含义，法律概念范畴的含义需要有更多的方法来表达。当前主要是通过多种构建方法得到与自然语言含义尽可能接近的词向量。在探索如何充分表达法律规则方面，计算机和法学界都已经进行了不少的前期积累。

在这些工作的基础上，内部路径可以让人工智能在底层技术搭建和运行原理上就主动遵循一般性的法律规则的要求，更加高效、精准地锁定出现问题的人工智能，更加高效地反应和处理。因此，通过计算机语言和方法表达的法律规则，出台人工智能可以“理解”的法规和构建人工智能司法、执法系统，搭建通用法律大模型和人工智能对接检测平台，实现以人工智能规制人工智能应用，应当作为一种补充规制路径，正式展开探索和实践。

数据财产权排除强制执行的权益结构

此处删除了原文脚注，全文请参见《中国法学》2025 年第 3 期，转载或引用请注明出处。

作者：陈爱飞

内容提要：案外人执行异议及执行异议之诉是案外数据财产权益人请求排除强制执行的程序基石，数据财产权益的实体性质与对抗效力则是其能否成为足以排除强制执行的民事权益的核心要素。基于“数据三权”分置模式，我国可在尊重和保护数据原始主体优先权益的基础上，综合运用新型财产权理论与传统物权理论，从物权本权性数据财产持有权、物债两分的数据财产使用权、以许可使用为代表的数据财产经营权等维度，确立一种三权分置型排除强制执行的权益结构。同时，考虑到三权分置型排除强制执行结构仍然与执行理论及实务中足以排除强制执行民事权益的类型界分存在适配不足，我国可进一步确立定限物权型排除强制执行结构，以提升数据财产权排除强制执行的权益结构与案外人执行异议及执行异议之诉法理的契合性。

一、引言

数据财产的形成是一个多方参与的过程，在同一数据财产上，不同主体之间形成了紧密的利益共生关系，这就使数据财产成为权利的集合体。[1]当前，我国数据市场上流通的数据财产主要是能够以货币价值呈现的数据产品或服务，但不同平台对交易的数据财产的称谓与分类存在一定的差异，例如，上海数据交易所称之为“数据产品”，且细分为数据集、数据应用、数据服务三种类型；深圳数据交易所则以“数据商品”代之，体现其商业价值属性，并进一步将其区分为数据产品、数据工具、数据服务；贵阳大数据交易所则直接以“交易标的”称之，其交易列表包括数据资源、算力资源、算法模型、数据产品和服务。一方面，基于实体法维度之分析，由于各类交易对象均涉及对相关主体的权属评价，故有必要以数据确权的方式来确定某项数据上是否存在着支配权性质的财产权。另一方面，基于执行法维度之观察，无论是“数据产品”“数据商品”，还是“交易标的”，既然能够作为交易对象，则说明具备一定的经济价值，这也是其成为金钱债权执行中责任财产的基本要件。以此为基础，需要进一步分析的问题是：案外人能否以其对某项数据财产享有实体权益为由，提出执行异议及执行异议之诉请求排除强制执行。

欲回答上述问题，须先行确认数据财产能否被强制执行。根据强制执行法的一般原理，执行开始时属于被执行人的财产均有成为执行标的的可能性。[2]尤其是在数据资产入表、数据资产质押，以及“执行难”的大背景下，将数据财产视为被执行人可供执行的财产，既符合社会经济发展需要，又能够通过扩大被执行人的责任财产范围助力“执行难”问题的解决。[3]若要将数据财产作为执行标的，应将其实体法上的稳定性、价值性、有限排他性、可转让性等转化为程序法上的可查控性、可评估性、可变价性。[4]申言之，数据财产应能够被执行机关依法处置，[5]并用于金钱债权执行中的责任财产执行。事实上，在域外法上，已经有国家表现出对数据财产强制执行的重视。譬如，新加坡将以数字化形式存在且具有一定经济价值和可交易性的数据财产均纳入其执行法律框架。对于数据财产的保全与执行，在执行程序开始前或过程中，法院可依申请作出财产保全命令，向数据财产交易平台等发出冻结令，而后在强制执行阶段，可进一步对被冻结的数据财产予以评估变价。[6]当下，我国司法实践也愈来愈重视对数据财产的强制执行，且已有相关典型案例。[7]另外，根据《最高人民法院关于民事执行中财产调查若干问题的规定》，被执行人需在收到报告财产令后向法院如实申报财产。虽然报告财产令涉及的主要是现金、固定资产等常规财产类型，但数据财产的申报与执行也已经在实践中出现。譬如，在上海市长宁区人民法院处理的某执行案件中，被执行人系某人工智能公司，该公司的核心资产为其掌握的算法数据库，在承办人的要求下，被执行人对这一数据财产进行了申报。[8]甚至，我国对数据财产强制执行问题的讨论还进一步延伸至“执破衔接”领域。正如有学者提出，破产本质上

是一种集体性的强制执行，[9]虽然我国司法实践层面尚无企业破产清算出售数据财产的案例，但并不代表对“执破衔接”程序中数据财产的处理问题的研究仅为学理层面的设想。[10]这一论断同样适用于数据财产权排除强制执行领域，并且我国司法实践中已有数据财产强制执行的实践样本，部分法院也一直在探索数据财产强制执行的理论与实务问题，充分证明研究数据财产权强制执行相关问题具有必要性与紧迫性。未来随着数据财产强制执行案件的逐渐增加，案外人以数据财产权益提出执行异议及执行异议之诉请求排除强制执行的案件也必然会不断涌现。因此，研究数据财产权排除强制执行的权益结构，明确何种数据财产权益足以排除强制执行，正当其时。

遗憾的是，我国数据财产强制执行领域仍然存在程序法与实体法衔接不足的问题。《民法典》及其司法解释未明确规定具体的数据财产权益类型，既有的民事程序法规范也未对足以排除强制执行的民事权益作体系性与一致性的规定，因而研究数据财产权益是否足以排除强制执行存在实体法与程序法的双重供给不足。且从《民法典》与《民事诉讼法》的衔接来看，实体法的规范缺失也导致难以在执行法层面确定何种数据财产权益足以排除强制执行。具体而言，在实体法上，虽然数据财产的保护、利用、交易过程难以适用单一物权保护模式，不能直接类比适用完整排他性保护，但有限的排他性保护依然很有必要。[11]《中共中央、国务院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”）提出的“数据资源持有权、数据加工使用权、数据产品经营权”均非物权意义上的绝对权，其内蕴的是“淡化所有权，强调使用权”的理念。在程序法上，数据财产权是否属于足以排除强制执行的民事权益，案外人能否据此提出执行异议及执行异议之诉，关系到我国数据财产权强制执行程序的整体建构。根据《民事诉讼法》及相关司法解释关于执行异议及执行异议之诉的规定，案外人依据《民事诉讼法》第 238 条规定提起诉讼的，须对执行标的主张足以阻止其转让、交付的实体权利（权益）。为此，有必要先行明确数据财产权属，以便于支持案外人异议，进而实现从数据财产确权至案外人执行异议及执行异议之诉的有效衔接。然而，基于数据财产客体的独特性，数据财产的所有权内涵与传统物权中的所有权内涵存在较大差异。[12]而且，数据财产具有可复制性与可共享性，同一数据财产可能出现多重持有的现象，难以明确界定数据财产的所有权主体，所以对于能否在数据上设立所有权，学界尚有争议。[13]持否定说的学者不胜枚举，代表性观点为，数据财产通常包含数据原始主体的在先权益，且该权益具有法定优先性，故不具备严格的排他性。[14]还有学者认为，数据财产上存在复杂的利益共生关系，单一主体不适合享有完整的“数据所有权”，正是因为数据原始主体法定优先权的限制，数据财产权人才难以享有绝对排他和控制的权利。[15]更有甚者提出了数据财产“所有权终结”的观点，[16]认为亦无必要为数据财产所有权制定专门的规范[17]。上述观点主要关注的是数据财产权益界定的实体法理由，未关注实体权益界分可能对诉讼程序产生影响，尤其是不便于界定案外人执行异议及执行异议之诉中何种数据财产权益足以排除强制执行。

有鉴于此，本文遵循程序法与实体法共进的分析进路，借助案外人执行异议及执行异议之诉的程序法理与新型财产权理论及传统物权理论来确定数据财产权排除强制执行的权益结构。具言之：第一，从“形式审查与实质审查”的程序适用与“数据财产权益的对抗效力”的实体基础之维度，明确数据财产权益排除强制执行的双重要件。第二，基于“数据持有权、数据使用权和数据经营权”的三权分置模式，[18]以数据财产的实体权能为立足点，确立三权分置型排除强制执行结构。第三，为了克服三权分置型排除强制执行结构在权属基础、权利体系、对抗效力等方面的局限，提升排除强制执行的数据财产权益与我国民事执行实务中足以排除强制执行的民事权益之契合性，还有必要确立定限物权型排除强制执行结构。

二、数据财产权益排除强制执行的要件

在执行程序中，若案外人将数据财产权益作为一项足以排除强制执行的民事权益提出执行异议及执行异议之诉，那么该项权益需要具备程序适用与实体基础双重要件。程序适用是一项不可或缺的引入要件，实体基础则是真正影响数据财产权排除强制执行的权益结构的核心因素。

（一）程序适用：形式审查与实质审查

一般而言，强制执行的正当性依赖于是否符合真实的实体权利义务关系，[19]案外人请求排除强制执行同样如此。当数据财产因债务人被强制执行而成为执行标的，且执行行为妨碍到案外人对该数据财产享有的实体权益时，案外人可通过执行异议及执行异议之诉请求排除强制执行。

首先，形式审查数据财产权属的权利外观。根据《民事诉讼法》第 238 条的规定，在执行过程中，若案外人提出异议，对执行标的主张实体权益并请求排除强制执行，执行法院应先行适用物权公示原则与权利外观主义对执行标的的实体权属进行形式审查，以认定执行标的是否属于债务人的责任财产。[20]其中，登记与否是数据财产权属形式审查的核心要件。实践中，数据财产权利登记契合数据确权的发展需要，[21]无论未来立法是将数据产权登记确立为设权登记还是宣示登记，都不影响对数据产权的形式审查[22]。根据《最高人民法院关于人民法院办理执行异议和复议案件若干问题的规定》（法释〔2020〕21 号，以下简称《执行异议和复议规定》）第 25 条第 5 项之规定，针对“其他财产和权利”的异议，在案外人主张其系权利人时，人民法院应当区分登记与未登记两种情形：“有登记的，按照登记机构的登记判断；无登记的，按照合同等证明财产权属或者权利人的证据判断”。从解释论视域看，可将数据财产（权）纳入“其他财产和权利”的范畴进行解释。如此一来，上述规范即可作为案外人执行异议及执行异议之诉中数据财产权属判断的一项规范性依据。然而，我国法律对于如何通过权利外观判断数据财产的实体权属并未作出明确规定，这就导致执行法院仅通过形式审查难以判断案外人是否对执行标的享有数据财产权益。

其次，实质审查可能影响数据财产权属变动的其他因素。在物权变动方面，我国依然是以债权形式主义为基石，即使在数据财产权属变动领域推行“数据财产登记新范式”，数据财产交易合同也符合登记要件，仍然可能因合同不成立、无效或被撤销等理由而无法实现数据财产权属的变动。例如，在案外人提出其与被执行人签订了书面的数据财产权合同并已完成登记，从而主张对执行标的享有数据财产权益时，申请执行人可能辩称该合同因违反法律与行政法规的强制性规定或违背公序良俗而无效。因此，法院在审查案外人是否以合同方式设立了数据财产权时，还需确认交易合同的有效性，尤其应重视对意思表示真实与否、有无违反法律与行政法规的强制性规定，或是否有悖于公序良俗等因素的审查。由此观之，登记这一要件可通过形式审查查明，但关于数据财产交易合同是否有效的实体判断，仅通过形式审查难以明确，此时，则有必要通过实质审查进行判定。

（二）实体基础：数据财产权益的对抗效力

在案外人执行异议及执行异议之诉程序中，对案外人享有的数据财产权益是否足以排除强制执行，应根据该权益的实体要件进行判断，尤其需要关注该数据财产权益的对抗效力。[23]

首先，案外人主张的数据财产权益具备对抗效力是其排除强制执行的基础。基于该效力，法院方能认定一项数据财产权益具备排除强制执行的资格。所谓足以排除强制执行的数据财产权益是指实体上具有对抗效力，且程序上适合以案外人执行异议及执行异议之诉予以救济的某种数据财产权益。该权益的真实性、优先性、对抗性是案外数据财产权益人胜诉的关键所在。[24]关于足以排除强制执行的数据财产权益的判断方法，法院可根据《执行异议和复议规定》第 24 条的规定展开：一是确认案外数据财产权益人是否对执行标的享有合法且真实的实体权益；二是如果存在实体权益，则进一步审查该权益相较于申请执行人的权益是否有优先性；三是审查该权益的对抗效力，判断其是单纯的对抗性权益，还是属于足以排除强制执行的数据财

产权益。[25]

其次，数据财产权益具备对抗效力并不意味着其一定能够排除强制执行。一方面，案外人主张的具备对抗效力的数据财产权益并非都能通过排除强制执行的方式获得救济。例如，在执行环节，案外人主张的抵押权、质押权等担保物权具备优先受偿的效力，其主要是通过参与分配及其衍生程序等方式予以救济，而不能直接适用案外人执行异议及执行异议之诉。另一方面，案外人主张权益的对抗效力仅为影响足以排除强制执行的一项因素，而非全部。譬如，当法律法规对某项财产的转让设限或该财产本身不可强制执行时，就直接决定了案外人执行异议及执行异议之诉的适用限制，但这并非因案外人所主张权益的对抗效力导致，而是因为其受到法律法规强制性规定或者该财产的本质属性的影响。尤其是对于包含个人信息权益的数据财产而言，[26]虽然它也具有一定的对抗效力，但由于个人信息权益还具有人身权性质，且人身权与财产权分属不同的权利维度，故难以评价其是否足以排除强制执行。不过，从 2022 年《中华人民共和国民事强制执行法（草案）》第 89 条第 2 款的规定来看，即使对不足以排除强制执行的案外人民事权益也应依法予以保护。该立法草案的倾向表明，案外人所主张的对抗性权益与数据财产权益的对抗效力并不等同，所以法院在认定某项数据财产权益是否具有足以排除强制执行的对抗效力时，应进行合理区分。

最后，法院须结合多重因素对案外人享有的数据财产权益的对抗效力进行评判。面对数据财产权这类新兴权利，在案外人以数据财产权益的对抗效力为依据请求排除强制执行时，法院应结合数据财产权益的性质、公示方式等多方面因素进行考量，从而判断案外人能否据此对抗申请执行人。事实上，数据财产是一种无形财产，在其基础上衍生的数据财产权益也具备无形财产权的特性，这就使其不能完全适用物权或债权的对抗效力规则。有学者提出，可以排除强制执行的方式差异为划分标准，将足以排除强制执行的民事权益分为以下两种类型：其一，以所有权为代表的“所有权型对抗性权益”，该权益对应着所有权等权益类型；其二，以限制财产使用价值与交换价值，以及限制财产处置为表现形式的“定限物权型对抗性权益”，其与执行实践中的用益物权、担保物权等权益相对应。[27]上述分类方式对于明确足以排除强制执行的数据财产权益的类型有一定借鉴作用，但由于数据财产具有非完整排他性等独特属性，故不能直接套用“所有权型对抗性权益”的分析架构。针对这一问题，可根据新型财产权理论对“数据财产权是指民事主体对其持有的数据进行使用、收益以及依法占有、处分的对世性财产权利”[28]的界定，厘清何种数据财产权益具有对抗效力，其又在何种情形下足以排除强制执行。同时，考虑到上述分析框架的局限性与数据财产权益的复杂性，依然有必要将定限物权型对抗性权益作为补充，分析数据财产用益物权与担保物权的对抗效力及排除强制执行的可能性。

三、三权分置型排除强制执行结构

基于数据三权分置模式，数据财产可被多方主体同时持有或使用，这将导致无法在数据财产上确立绝对的支配权。[29]如果仅以新型财产权理论为根基，将使执行程序中数据财产权益的对抗效力缺乏足够的实体支撑。同时，根据案外人执行异议及执行异议之诉的程序法理，若一项民事权益要足以排除强制执行，须以明确且稳定的实体权益为基础。且由于我国足以排除强制执行民事权益的类型界定主要是基于传统物权理论展开，所以对于如何判断某项数据财产权益是否足以排除强制执行，不能抛弃传统物权理论的分析框架。因此，有必要将新型财产权理论与传统物权理论相结合，以数据财产的实体权能为立足点，绕过所有权确权障碍，[30]并借鉴所有权型对抗性权益排除强制执行的经验，确立既符合数据三权分置模式，又契合案外人执行异议及执行异议之诉法理的三权分置型排除强制执行结构。该结构的核心在于：既力求通过新型财产权理论关于数据三权分置的结构设定实现数据财产权益的差异化保护，又承认传统物权理论在数据财产领域的有限适用性。直言之，三权分置型排

除强制执行结构可从物权本权性数据财产持有权、物债两分的数据财产使用权、以许可使用为代表的数据财产经营权三个维度展开。

（一）物权本权性数据财产持有权

物权本权性数据财产持有权是基于物权关系的一种权益类型，其以“本权+占有的自然状态”为依托，且只有同时满足上述两大要素，该权益才具备排除强制执行的可能。而对于不具备本权基础的数据财产持有权，则难以主张排除强制执行。数据财产持有权不以所有权为权源，强调的是对数据财产持有者合法持有状态的事实性认定，持有者能够基于对数据产品的实际控制，对他人擅自使用和流通数据产品予以禁止和排除。[31]因此，若案外人仅对数据财产享有持有状态而无本权依据，数据财产持有权则难以作为足以排除强制执行的民事权益。

首先，从民事实体权利体系化角度看，数据财产持有权是数据财产权的内核。持有权反映的是权利人对数据财产的稳定持有权能，若无法定事由或未经权利人同意，他人不得对数据财产实施访问、复制、删除等行为。[32]譬如，“数据二十条”第 7 条明确指出，要“合理保护数据处理者对依法依规持有的数据进行自主管控的权益”。然而，欲将数据财产持有权转化为足以排除强制执行的民事权益，首先需要从规范层面确立数据财产权人对数据财产的持有权。基于该权益，权利人能够依法或依约实现对数据财产的现实管控。若无权利人授权与合理使用等法定事由，任何第三方都应对权利人的数据财产持有权保持必要的尊重，不得妨碍或以非法手段侵蚀权利人对数据财产的稳定持有状态。合理使用与不得干扰的双重限制也表明，权利人对数据财产享有的持有权实际上是一种有限的排他权。

其次，数据财产持有权与传统动产所有权的占有权能均注重权利人对财产的自主控制能力，但数据财产的可复制性、可共享性等特性又使其与传统动产存在很大区别。同一数据财产可能存在多重主体持有的问题，此时交付占有的公示方式难以直接应用于数据财产权的转移。那么，数据财产持有权与占有能否等同？实践中，一般的动产占有并不能成为案外人提起执行异议及执行异议之诉的合法事由。如果将权利人对数据财产的持有权等同于占有，则案外人也不能仅仅基于非本权的事实请求排除强制执行。但是，如果在占有的同时，还存在着基础物权关系，则可能使案外人提出执行异议及执行异议之诉趋于合理化。对于传统动产，“基础物权关系+占有”为案外人执行异议及执行异议之诉创造的条件主要为权利外观的强化。占有作为物权公示手段，与基础物权结合后，将产生“事实控制+权利控制”双重效力。可以传统动产为例，对案外人能否基于占有提出执行异议及执行异议之诉进行分析。肯定说基于《民法典》第 462 条第 1 款关于占有保护的规定，认为案外人可以占有保护为由主张排除强制执行。否定说认为，占有只是一种事实而非权利，但案外人执行异议及执行异议之诉程序的启动是基于本权，而非本权衍生的事实状态，所以不能单独将占有作为排除强制执行的民事权益看待。[33]除肯定说和否定说的单向性评价之外，还存在着一种折中说，即有本权占有和无本权占有对案外人能否提出执行异议及执行异议之诉的影响有很大差别。具体而言，其一，有本权占有是指基于本权的占有，这种情况下，案外人仅主张存在“占有的自然状态”，不能提出执行异议及执行异议之诉，其须以“本权+占有的自然状态”为双重依据才初步具备请求排除强制执行的资格。其二，无本权占有则指的是无本权依据或单纯的自然事实占有，在这种情况下，虽然处分性与保全性执行措施会妨碍案外人的占有状态，但因其缺乏本权，故难以排除强制执行。如果将上述关于传统动产占有能否排除强制执行的分析适用于数据财产，则可能出现以下论断：仅以持有状态而无权利依据，原则上数据财产持有权不能作为足以排除强制执行的民事权益。若在执行程序中，申请执行人要求被执行人交付的数据财产被案外人持有，作为无权利依据的案外人，不得以执行异议及执行异议之诉为由拒绝交出该数据财产。换言之，无本权案外人对执行标的的持有状态不足以排除强制执行。

然而，数据财产持有与传统动产占有存在着本质差异。从持有与占有的属性来看，“控制”与“排他性”的分离是数据财产持有区别于传统动产占有的根本所在。[34]这就导致关于传统动产占有的论证在适用于数据财产持有时存在普适性缺陷。与数据财产持有相比较，传统动产占有具有天然的物理排他性，通常同一动产在同一时间仅能由一人实际占有，占有状态可直接公示权属，且占有本身与本权高度关联。若将数据财产持有直接等同于传统动产占有，则可能混淆事实控制与法律权利的关系，导致案外人执行异议及执行异议之诉的启动标准在数据财产持有的场景下出现偏差。具体体现为：一是多重持有下的权利冲突。一般而言，基于数据的可复制性与可共享性，数据财产持有主要体现为对相应数据的访问控制能力，同一数据可同时被多个主体持有，且持有状态未必反映本权归属。譬如，数据财产通过 API 接口共享可同时被甲、乙、丙三方持有，甲与乙订立了用益权合同但未公示，丙基于技术控制实际持有数据，在甲与丁的强制执行案件中，若甲的债权人丁申请执行该数据财产，案外人乙能否以“基础物权关系+持有”主张排除强制执行，案外人丙又能否基于实际的技术控制主张排除强制执行。若按传统动产规则，乙因未对其用益权进行公示，其占有的物权属性存在瑕疵，将难以主张排除强制执行。但在数据财产场景中，若乙的持有能够通过访问日志等技术手段证明，此时将增强其持有权益的对抗效力。面对此种情形，法庭应如何判断未公示的数据持有权益与技术实际控制的持有权益能否排除强制执行。笔者认为，乙若未公示用益权，即使通过 API 接口持有数据，其“事实控制”依然不具有对抗效力；丙的实际控制亦须以登记或技术公示为前提，否则也不能排除强制执行。二是技术控制与法律权利的分离。传统动产场景下“基础物权关系+占有”的规则，在数据财产中因权利公示方式的缺失而丧失普适性。譬如，丁通过技术手段非法获取数据财产并实际控制，但数据财产的真实权利人为戊。若丁的债权人申请执行该数据财产，戊能否主张排除执行？按传统动产规则，丁的占有属于无权占有，不足以对抗戊的本权，但若数据财产未登记，戊的权属证明可能依赖于技术证据，此时本权与占有的关联性被削弱，传统规则也难以直接适用。实际上，丁的非法控制是因缺乏合法性而无法对抗戊的登记权利，即使戊未登记，但因其本身就是实质权利人，若其能通过区块链权属链等技术证据证明原始权利，仍可尝试利用案外人执行异议及执行异议之诉程序获得救济。

为此，对于数据财产持有场景中可能出现的案外人请求排除强制执行的情形，应当区分“技术性事实控制”与“权利控制”。前者仅指通过技术手段对数据的实际访问或使用能力，不必然反映权利归属，后者则需结合权利公示与基础法律关系，形成具有对抗效力的控制状态。例如，若案外人通过合同交易且以公示的方式取得数据财产用益物权，并通过技术手段控制数据，其“权利控制”可具有对抗效力。反之，若案外人仅“技术性事实控制”数据财产而缺乏基础物权，则其控制状态的对抗效力将存在严重瑕疵，案外人仅凭此提出执行异议及执行异议之诉缺乏正当性。进而言之，基于数据财产持有权的特殊性考量，案外人执行异议及执行异议之诉程序的启动标准需跳出传统动产的类比框架，从传统动产的“占有+本权”模式转向数据财产的“登记公示+技术性控制+权利控制”模式，构建符合数据财产持有权益特性的独立规则体系，方能实现法律逻辑自洽与场景普适性的统一。

（二）物债两分的数据财产使用权

数据财产使用权主要指的是在尊重和保护数据原始主体法定优先权益的基础上，数据财产权利人自主使用数据财产的权益，即权利人可不被干扰地自主进行数据开发利用，如分析性使用、训练性使用和加工性使用等。[35]数据财产使用权除了自主使用权益之外，还包括许可他人使用数据财产的权益，亦即权利人可通过合同交易或授权，许可他人以访问、复制等方式使用数据财产。需要明确的是，此处关于数据财产使用权益的分析仅限于自主使用，关于许可他人使用的权益，则可置于数据财产经营权中进行分析。

首先，数据财产使用权是一种限制性权益。该权益通常仅限于使用，而用益物权则包含了使用、收益的权利，并且具有更强的独立性和法律效力。笔者之所以将数据财产使用权作为三权分置型排除强制执行权益结构的一个组成部分，是基于政策性与法律性的双重考量。从“数据二十条”关于“数据加工使用权”的规定来看，其属于数据资源使用权的权能，是从经济学角度对数据处理者享有的数据财产权的一种描述。[36]数据加工使用权向数据财产使用权转化需解决两个问题：一是权利主体问题。经济学意义上的数据加工使用权不能直接等同于法律维度的数据财产使用权。前者存在一个明确的权利主体，更侧重于对数据处理者的权利确认，而后者还可能存在着授权使用的主体。二是数据资源向数据财产的转化问题。数据资源并不一定就是数据财产，其向数据产品转化需要一定条件，只有转化为具备一定货币价值的数据产品时，才能够冠之以数据财产之名。在此基础上，案外人才具有以其享有的数据财产权益提出执行异议及执行异议之诉排除强制执行的可能性。否则，若执行标的缺乏可执行的财产权益，将丧失其可以被执行的实体法基础。

其次，数据财产使用权可进行“物债”两分。关于数据财产使用权能否排除强制执行，可基于实体法将其分为两种类型：一是物权性使用权，二是债权性使用权。二者的划分依据主要源自权利人在自主使用权的基础上，是否以合同交易等形式进行了二次授权。若未进行二次授权，原始使用权人享有的是物权性使用权；若进行了二次授权，被授权者将获得债权性使用权。一般情况下，二次被授权者作为案外人不能基于债权性使用权请求排除法院的强制执行，至于原始使用权人作为案外人能否以物权性使用权请求排除强制执行还需进一步分析。可将法院的强制执行行为是否会妨碍原始使用权人自主使用权之行使作为一项考量因素。若不会，案外人则无必要提出执行异议及执行异议之诉；若会，则需对物权性使用权与债权性使用权进行对比。具体来看，若原始使用权人在保留数据财产自主使用权的基础上也许可他人使用，被许可人因金钱债务成为另案的被执行人，法院又将该项被许可使用的数据财产作为责任财产予以强制执行。那么，原始使用权人就成为许可使用权人执行案件中的案外人，且对被执行的数据财产享有的是物权性使用权，而许可使用权人仅是基于合同交易或授权许可才享有债权性使用权。原始使用权人的物权性使用权明显优先于许可使用权人的债权性使用权，且前者具备显著的物权性质。如果法院对许可使用权人仅享有债权性使用权的数据财产进行强制执行，将侵害案外原始使用权人的合法权益。因此，可尝试赋予案外原始使用权人基于物权性使用权请求排除法院强制执行之权利。

（三）以许可使用为代表的数据财产经营权

数据财产经营权主要指的是数据财产权利人能够通过许可使用、整体转让等方式对数据财产进行经营，从而处分其数据财产权益，其体现了权利人对数据财产的自主管理能力和以经营为核心的处分权能。[37]“无流通则无价值”是数据经济领域的一种重要价值观念，数据财产经营权恰好能够很好地践行这一理念。数据财产权利人可在法律规定的范围内，依法对其享有的数据财产权进行流转，整体或部分转让其持有的数据财产使用价值或交换价值。例如，权利人可以将数据财产转让或出租给其他企业。[38]虽然数据财产经营权的实现方式有很多种，但真正与案外人执行异议及执行异议之诉相关的却不多。譬如，整体转让情况下的经营权就不足以成为排除强制执行的事由。因此，就数据财产经营权是否能够成为足以排除强制执行的民事权益，本文主要以其中的许可使用权为分析对象。

首先，普通许可使用权与允许转许可的许可使用权为不具有排他性的权利。对于同一数据财产，权利人可以给予单个主体独家许可使用权，也可以让多个主体非独家许可地使用，其体现的是数据财产使用权的“有限排他性”。[39]其中，能够排除第三人效力的主要为“独家许可使用”或“禁止转许可”。前者体现的是许可使用权人在许可范围内的“排他性使用权”，权利人不得在该范围内重新许

可他人；后者体现的则是权利人仍然保有相应数据财产的“排他性经营权”。

其次，就许可他人使用而言，独占许可使用与非独占许可使用对法院强制执行的影响较为复杂。第一，在数据财产权利人成为被执行人的情形下，独占许可使用的数据财产成为执行标的，此时许可使用权人能否基于独占许可使用权请求排除法院的强制执行？此处的独占许可使用不包括权利人保留自我使用权的情形，仅指许可使用权人的独占使用。第二，在非独占许可使用的情形下，许可使用权人又能否基于单纯的使用权益请求排除强制执行？欲解决上述两个问题需重点关注以下要素：其一，数据财产权的许可使用是否有对抗效力，若有，又如何发挥其对抗效力。在我国数据财产交易登记制度尚未成熟的情况下，数据财产权的许可使用缺乏有效的公示手段，如果许可使用权人未以外部可知的方式表达其权益，又能否将使用行为本身作为一种公示手段以获得对抗第三人的效力？毋庸置疑，在存在排他和独占许可的情况下，一旦数据财产权属发生变化或他人取得使用权，将对原许可使用权人造成重大影响。这种情况下，公示对抗效力的存在能够为许可使用权人请求排除强制执行提供效力基础。虽然许可使用权人依然是以其债权性使用权来阻却对数据财产权利人的物权执行，但基于独占许可使用排他性与对许可使用权人的程序保障，可使具有公示对抗效力的独占许可使用权成为排除强制执行的民事权益。目前“数据二十条”的第 3 条和第 15 条已经提出探索建立“数据产权登记新方式”，建立数据权利登记机制，但仅有政策性宣示还不够，还需要从立法层面予以规定。2025 年 3 月 1 日起施行的《公共数据资源登记管理暂行办法》（发改数据规〔2025〕26 号）已经明确了公共数据资源登记的基本要求，其能够在一定程度上推进我国的数据财产登记实践，这也有利于数据财产强制执行的理论研究与实践发展。其二，是否存在一种即使数据财产被强制执行，也不会对其许可使用权益造成负面影响的协调方案。如果存在这种方案，那么基于许可使用权的排除强制执行则失去基础。笔者认为，一种解决方案是：可尝试在第三方中立机构的监管下，实现数据财产权转让与使用权收益的分离，使许可使用权人不会因权利人（债务人）被强制执行而影响其对数据财产的使用。与此同时，需要将许可使用费用的收益人由原来的权利人（债务人）转变为申请执行人。

最后，就权属变动方式而言，应明确数据财产排他性转让的基本模式与公示要件。第一种模式是出让方将数据财产一次性转让给受让方，约定在转让完成后，作为原数据财产权人的出让人不得保留原来存储的数据，以实现受让人的独家持有。第二种模式是以数据财产独家排他访问权的形式实现，数据财产权人不一次性转让数据财产，而仅仅提供数据访问接口与数据维护服务，保障需求方能够在特定的时间和范围内访问数据，且这种独家排他效力不仅排斥其他主体，也排斥数据财产权利人自身。若上述两种模式能够通过某种方式公示，受让方与独家排他访问方则能对抗不特定的第三方，并可基于此权益提出执行异议及执行异议之诉以排除强制执行。至于数据财产权利的具体公示方法，则存在实践与制度上的两种要件：一是在立法未定的情况下，可暂时将“技术层面对数据财产的实际控制”作为权利外观；二是采用“数据二十条”提倡的“数据财产交易登记”作为公示对抗要件。[40]

四、定限物权型排除强制执行结构

三权分置型排除强制执行结构为如何判断数据财产权益是否足以排除强制执行提供了一个基础分析框架。然而，考虑到三权分置型排除强制执行结构在与《民事诉讼法》及其司法解释规定的“足以排除强制执行的民事权益”的衔接方面尚有不足，且该结构难以覆盖所有排除强制执行的数据财产权益类型。在这种情况下，可确立与三权分置型排除强制执行结构互补的定限物权型排除强制执行结构。

（一）两种排除强制执行权益结构的关系

三权分置型排除强制执行结构与定限物权型排除强制执行结构之间为互补关系，二者的分析视角不同，前者主要是从实体法的权益视角展开，后

者则是立足于执行法的权益维度。本质上，定限物权型排除强制执行结构是数据财产定限物权在案外人执行异议及执行异议之诉中的映射，同时也是对三权分置型排除强制执行结构的补充。该结构可在化解数据财产权非完整排他性冲突的同时，克服三权分置型排除强制执行结构在权属基础、权利体系、对抗效力等方面的局限性。具体而言，两种权益结构的关系主要表现为以下几个方面：

第一是权益结构的互补性。依托于传统物权理论的数据财产定限物权能够与基于数据财产实体权能的物权本权性数据财产持有权、物债两分的数据财产使用权、以许可使用为代表的数据财产经营权形成更加完善的权益结构。实体法上，三权分置的权益结构通过对数据财产实体权能的解构与重构，将数据财产权益分解为更为精细的权益模块，逐渐形成覆盖数据财产各种复合性权益的权益体系，进一步明确了案外数据财产权益人请求排除强制执行的可能性。程序法上，数据财产定限物权权益结构在沿用用益物权与担保物权是否足以排除强制执行理论框架的基础上，对三权分置权益结构的薄弱之处予以补充，从而为案外数据财产权益人请求排除强制执行提供更为精准的权益定位。

第二是稳定性与灵活性的平衡。基于传统物权的数据财产定限物权权益结构能够发挥基础“锚定作用”，为案外人执行异议及执行异议之诉中足以排除强制执行数据财产权益的判断提供规范确定性。与之相比，三权分置的权益结构则可通过权益解构与重组的方式，灵活地适应数据财产交易中的新型权益需求，以及回应案外人执行异议及执行异议之诉中数据财产权益是否足以排除强制执行的问题。

第三是连贯性与体系性的统一。数据财产定限物权的权益结构延续了传统物权体系在案外人执行异议及执行异议之诉中足以排除强制执行的民事权益判断的连贯性，而三权分置的权益结构则通过确立契合数据财产特性的新型对抗标准，对排除强制执行的数据财产权益进行了体系化厘定。

（二）数据财产定限物权之证成

需要注意的是，数据财产定限物权排除强制执行结构存在一个前提性问题，即在数据财产上设置定限物权是否为真命题？若不是，则缺乏在数据财产上创设定限物权的可能性，也就没有必要分析其在程序法上能否排除强制执行。易言之，首先应当存在这样一类权利，否则就欠缺其足以排除强制执行的理论基础。因此，应当先从实体法维度论证在数据财产上创设定限物权的可能性，即数据财产定限物权之证成，而后以此为基础，结合数据财产用益物权与担保物权的特性，分析二者排除强制执行的可能性及局限。

定限物权是基于所有权产生的一类限制物权，在排除强制执行时具有相对对抗效力，其主要包括用益物权与担保物权两种类型，属于权利人以法律规定或合意为基础取得直接控制的部分权能。数据财产定限物权欲排除强制执行，需要回归实体法维度回应数据财产定限物权之质疑，分析能否在数据财产上设置定限物权。若可以，以何种方式设置较为适宜？

首先，数据财产可以作为物权的客体。虽然数据财产无形无体，其物理形态、生成过程及利用方式也与传统财产权遵循的“物必有体”原则不够契合，[41]但从物权标的范围来看，不动产与动产的概念亦无法涵盖所有的物权客体[42]。因为物权的客体不仅包括传统意义上以不动产与动产为表现形式的有体物，也包括以光、电、声、磁等为基本单位构成的部分无体物。譬如，当前数据交易中广泛存在的数据财产即为由代码构成的电子数据之集合，虽无形无体，但也是物质世界的一种客观存在，能够被人类所感知或支配，而这一客观存在的特性又使其具备了成为物权客体的资格。[43]

其次，数据财产的所有权争议并不会阻碍数据财产定限物权的形成。传统物权理论强调用益物权与担保物权是由所有权衍生而来的他物权，所以要确立数据财产用益物权与担保物权需回归对数据财产所有权的讨论。在理论层面，由于数据财产可能包含着人格权益等特殊性情况，理论界对于能否在其之上设置所有权存在较大争议。同时，数据对

具体场景的高度依赖性也导致数据权属在配置过程中面临选择困境，无论哪方主体对数据主张所有权均面临质疑。故而，不能照搬传统财产权中的所有权概念来界定数据所有权。在规范层面，虽然《民法典》第 127 条体现了对数据的同等保护，但其并未确认具体应以何种权利形态实现对数据财产权的保障。这就引出另一个问题，即是否存在数据财产所有权人？如果不存在这一主体，还能否在数据财产上设立用益物权与担保物权？根据《民法典》第 241 条之规定，所有权人有权在自己的不动产或者动产上设立用益物权和担保物权。该条法律规范又是否会成为在数据财产上设立定限物权的障碍？笔者认为，虽然所有权是用益物权与担保物权的源权利，但从《民法典》既有的规定来看，其关于“所有权人设立他物权”的规定主要限定在不动产与动产领域。显然，数据财产并不是不动产，至于其是否具备动产的属性，能否直接适用《民法典》关于动产物权的相关规定，在理论界和司法实践中也存在争议。有学者认为，数据财产并不完全符合传统动产的定义和属性，它不同于传统的有形财产，加之数据财产具有无形性，其权利变动方式也不同于传统意义上动产的权利变动方式。[44]虽然数据财产在可流通性、可转让性等方面与动产类似，但这仅为其部分属性。更重要的是，数据财产还具有非完整排他性、可复制性、可共享性，以及特有的流通机制等特性。因此，笔者倾向于认为，应当将数据财产视为一种新型财产。故而，不宜以《民法典》第 241 条关于所有权人在不动产与动产上设立他物权的限制，否定数据财产定限物权。且从我国数据财产的实践发展来看，数据财产质押融资担保已经成为担保物权在数据财产领域的一种新的表现形式，这也在一定程度上体现出在数据财产上设置定限物权的可能性。

最后，数据财产定限物权存在排除强制执行的可能性。在厘清数据财产定限物权的权源基础后，则需要进一步分析能否以此类定限物权排除强制执行。所有权可成为一项排除强制执行的事由，只不过就数据财产而言，数据财产权益主体的所有权属性存在瑕疵，所以案外数据财产权益人若要以所有权排除强制执行存在实体法上的阻碍。而对于属于定限物权的用益物权与担保物权而言，则不须具备绝对的排他性控制，其优势在于即使未明确界定某项数据财产的所有权，依然可尝试通过用益物权与担保物权的方式实现数据财产的经济价值与社会价值。与此同时，缺陷也较为明显，非绝对性的排他性控制使得用益物权与担保物权在对数据财产的控制方式和实现利益的途径上与所有权存在差异。因此，当数据财产附设上述两项权利而成为执行标的时，对债权人、债务人、案外人的影响也会有所不同。此时，能否通过案外人执行异议及执行异议之诉解决三者之间的权益冲突问题还需要进一步论证。

（三）数据财产用益物权排除强制执行之可能

一般而言，用益物权不足以排除强制执行，但在执行妨害案外人占有使用等特定情形下，用益物权也可成为案外人提出执行异议及执行异议之诉的一项合法事由。本质上看，用益物权是基于物的使用价值确立的权利，所以当法院的强制执行行为将损害案外人用益物权的实质行使时，案外人可主张排除强制执行。[45]当然，用益物权并不一定在所有情形下都要以排除强制执行的方式寻求救济，因其允许案外人通过对财产的占有获取利益，所以若案外人对执行标的的占有和使用不会受到法院强制执行行为的不利影响，排除强制执行则无必要。若进一步涉及标的物的交付或强制管理时，则将实质性地妨碍案外人用益物权之行使，此时案外人可提出执行异议及执行异议之诉以获得救济。[46]譬如，《北京市高级人民法院关于审理执行异议之诉案件适用法律若干问题的指导意见（试行）》（京高法发〔2011〕254 号）第 6 条规定，如果执行行为损害到案外人的用益物权，妨碍其对标的物的占有和使用，案外人有权通过执行异议之诉请求法院排除强制执行。反之，若法院的执行行为不影响案外人的用益物权，则不可通过执行异议之诉程序进行救济。[47]

在数字财产交易愈发频繁的趋势下，数据财产

的转让已成为数据流通的一种重要表现形式，这也使得用益物权的客体逐渐向数据财产领域扩张。用益物权的源权利实际上依然是所有权，但其又将所有权蕴含的使用与收益权能分割出来。若将这一观点引入数据财产交易领域，则可在搁置所有权争议的条件下实现数据权益在原始权利人和数据处理者之间的合理配置。有学者提出，可以尝试在数据上构建“所有权+用益权”的二元分置权利体系，其中，数据所有权配置给数据源发者，数据处理者则享有数据用益权。[48]在数据财产交易领域，基于对数据处理者或经营者权利的认可和保护，可以上述理论为基础，在数据财产上创设用益物权。另从权利外观的角度来看，在没有转让限制的情况下，数据财产用益物权的形成还须具备外部与内部双重要件。其中，外部要件为通过技术层面的可信机制对数据财产进行确权处理；内部要件则是在外部技术确权的基础上，通过登记等手段的公示效果来明确数据财产用益物权的权利主体身份。

就表现形式而言，数据财产的控制权、许可权、转让权等构成了数据财产用益物权的核心权能。[49]数据财产经营者可通过用益物权转让合同的形式在其持有的数据财产上设置用益物权，在约定的条件下，经许可的用益物权人可通过 API 接口等方式实现对数据的访问和获取。譬如，作为合同主体的数据财产经营者甲与用益物权人乙可以能够被外在其他主体明确感知的方式对该用益物权进行公示，该用益物权经公示可获得对抗效力。[50]有一种情形需要特别关注，如果在履约期间，数据财产经营者甲以独家许可或者全部转让的方式将该数据财产上的财产权益全部转让给第三人丙，从而使其自身丧失对该数据财产的控制、使用、收益等权能，第三人丙则相应地获得上述权能。一旦该数据财产成为第三人丙债务执行中的责任财产而被法院强制执行，显然会妨害原用益物权交易合同中用益物权人乙对数据财产的获取和使用。此时，用益物权人乙就成为第三人丙涉诉强制执行案件中的案外人。由于用益物权人乙与经营者甲之间的数据财产交易合同已经对外公示，能够取得对抗丙的效果。因此，用益物权人乙提起执行异议之诉具备诉之利益，可以其对执行标的享有数据财产用益物权为由，请求排除法院对丙持有的数据财产的强制执行。同时，对于未公示的“隐形”数据财产用益物权，应推定其不具备对抗效力。这是因为对于未完成公示程序的数据财产用益物权，其缺乏外部可识别性，此时赋予用益物权人对抗效力，与公示公信原则相冲突。即使数据财产用益物权具备对抗效力，也更多的是实体法效力的呈现，能否排除强制执行还需结合异议之诉的法理进行综合判断。直言之，如果案外人以未公示的数据财产用益物权的对抗效力主张排除强制执行，并不具备提出执行异议及执行异议之诉的正当性基础。

需要注意的是，对于在数据交易过程中获取的数据财产用益物权，如果属于案外人尚未取得数据财产的相关用益物权，则其不具备提出执行异议和执行异议之诉的正当性。基于案外人执行异议及执行异议之诉的程序法理，案外人须对执行标的享有足以排除强制执行的实体权益，[51]而尚未取得数据财产用益物权则表明案外人不具备请求排除强制执行的权利基础。原因在于，数据财产的权利期待利益不足以阻却执行。譬如，甲将数据财产质押给丁并登记后，丁的债权人申请执行该数据，此时，乙以“未来用益物权人”身份主张排除执行，但因其并未实际获得数据的相关用益物权，且将来是否能获取该用益物权还有很大的不确定性，法院将难以支持其排除强制执行的请求。换言之，案外人执行异议及执行异议之诉关注的主要是既存权益，而非期待利益。况且，如果案外人尚未取得数据财产用益物权，一般也不会出现法院错误执行案外人用益物权及妨碍其对标的物的占有和使用的情况。因此，这种情况下，数据财产用益物权人难以以期待性的用益物权对抗强制执行。

另外，就数据财产上既设有用益物权又存在担保物权的情形而言，案外人提出执行异议或执行异议之诉的正当性同样面临挑战。根据《民法典》第 414 条的规定，已登记的担保物权具有优先受偿效力。即使案外人的用益物权已成立，亦不足以对抗

已登记的担保物权人。若数据财产已设立担保物权并完成登记，担保权人的优先受偿权将排斥用益物权人的权益。譬如，甲将数据财产先质押给丁（已登记），后许可乙使用，若丁的债权人申请执行数据财产，乙主张其用益物权应优先于丁的担保物权，则缺乏法律依据。因此，在此情形下，案外人也不能以其用益物权请求排除强制执行，否则将损害担保权人的信赖利益。

（四）数据财产担保物权排除强制执行之否定

原则上，担保物权不足以排除强制执行。一般情况下，担保物的交付、转让并不会对担保物权的法律效力产生负面影响，而当担保物作为执行标的时，担保物权的优先受偿效力会阻却案外人执行异议及执行异议之诉程序的启动。实体法上，从《最高人民法院关于适用〈中华人民共和国民法典〉有关担保制度的解释》（法释〔2020〕28 号）第 45 条关于担保物权实现程序的规定来看，在满足担保物权实现程序要件的情形下，担保物权人可就担保财产进行拍卖、变卖，从而优先实现自身债权。程序法上，根据《执行异议和复议规定》第 27 条的规定，除非法律与司法解释另有规定，“申请执行人对执行标的依法享有对抗案外人的担保物权等优先受偿权，人民法院对案外人提出的排除执行异议不予支持”。这是因为在典型担保的场景下，若法院的强制执行措施不会实质性损害案外人享有的担保物权，参与分配等方式能够在一定程度上保障其优先受偿之地位，则不必再通过执行异议及执行异议之诉的方式进行救济。[52]那么，在数据财产担保领域，案外人能否因数据财产担保物权的特殊性而请求排除强制执行？欲回答这一问题，须回归至对我国数据财产担保实践与特殊性的考察。

首先，虽然数据财产具有有限排他性，但依然可成为担保标的。近年来，我国正在探索的数据资产入表、数据知识产权登记、数据资产质押融资已然能够在一定程度上反映出在数据财产上设置担保物权的可行性。权利人可将持有的数据财产作为融资担保的担保物，以质押数据财产获取贷款的形式实现其财产价值。[53]譬如，2024 年 6 月，神州数码将“神州金服云”数据产品作为数据资产纳入企业财务报表并办理质押登记，成功获得银行的授信融资，该质押融资项目是全国范围内首笔大中型数据资产质押融资案例。[54]上海市数据交易所也专门针对数据资产推出了相关的数据资产信贷服务产品“数易贷”。[55]在数据财产质押期间，出质人一般可以在法律和合同允许的范围内继续使用这些数据财产，但应确保不侵犯质权人的合法权益，并在债务得到履行或根据合同条款解除合同限制后，依法继续使用。换言之，虽然质权人会对出质人的权利进行一定的限制，但基于数据财产质押的特殊性，此种限制通常不包括出质人完全丧失对该资产的使用权限，而是保持在法律允许的范围内最大化其使用价值。

其次，由于数据财产主要是以质押的形式实现其担保价值，故数据财产担保物权是否足以排除强制执行应以数据财产质权为考察重心。如何判断数据财产质权人是否可以提出执行异议及执行异议之诉就成为下一步要关注的核心议题。理论上，我国学界对质权人能否适用案外人执行异议及执行异议之诉请求排除强制执行存在不同观点。唐力、肖建国等持肯定说，认为质权的成立是以担保财产的占有转移给质权人为前提，若法院的强制执行会导致质权人丧失对担保动产的占有，则会直接影响到质权人的实体利益，此时又难以通过优先受偿进行有效保障，那么质权人可以其享有的质权提出执行异议及执行异议之诉。[56]比较法上，德国民事诉讼法学界也以肯定说为通说，主张动产质权人可以提出案外人执行异议及执行异议之诉。[57]刘颖则持否定说，认为不应允许质权人提出案外人执行异议及执行异议之诉，依据在于《民法典》第 436 条与《最高人民法院关于人民法院民事执行中查封、扣押、冻结财产的规定》（法释〔2020〕21 号，以下简称《查封规定》）第 11 条之规定，其以《查封规定》第 11 条规定的“该财产由人民法院保管的，质权、留置权不因转移占有而消灭”为分析对象，认为即使法院的强制措施可能导致质权人丧失对担保物的占有，也不会使质权与留置权灭失。[58]

上述两种学说均有各自的合理性。

笔者对数据财产质权人基于数据财产质权提出案外人执行异议及执行异议之诉持否定态度。判断数据财产质权人可否适用案外人执行异议及执行异议之诉程序的根本要义并非是否丧失对担保财产的占有，而是质权人的担保利益是否因强制执行而受到实质影响。譬如，法院可对数据财产采用冻结之措施，指定担保权人为保管人，并不会导致其丧失质权，其可与抵押权人一样优先受偿。这是由于法院在对担保权人的占有性担保财产采取查封、扣押、冻结等措施后，会产生保管人，而保管人主要是担保权人和法院（前者更为常见），且由谁保管，并不会导致担保权人丧失质权。具体来说，在数据财产上设置质权的实质是将某些数据财产权益作为担保财产，以实现其经济价值。即便在数据财产上设定了质权，也不会直接影响到出质人的持有权与使用权，甚至为了契合数据财产的流通性，尽可能最大化地实现其商业价值，经营权都可继续保留。质权人也不必直接享有数据财产持有权、使用权和经营权。尤其是在数据财产交易中，还存在着数据财产交易平台这一中立第三方机构，它们也可以发挥一定的监管作用，实际上也能为质权人的权益保护提供证据支持。当然，依然有必要将质押登记作为对外公示的基本手段，如此质权人才有可能就该数据财产价值优先受偿。如果在执行程序中，法院在将已设立担保的数据财产折价给申请执行人时忽略了担保权人的优先受偿地位，抑或在对数据财产采取处分性执行措施之前，未将可能影响其变价的担保权人的债权作为考量因素，从而导致担保权人未足额受偿或优先受偿，作为利害关系人的数据财产质权人可通过执行行为异议获得救济，而不能提出针对执行标的的执行异议及执行异议之诉。概言之，通过对以数据财产质押为核心的数据财产担保物权的考察，可以发现，案外人原则上不能以数据财产担保物权请求排除强制执行。

五、结语

基于数据财产及其权益属性的特殊性，在数据财产权益是否足以排除强制执行方面，定限物权型排除强制执行结构能够与以数据财产持有权、使用权和经营权为内核的三权分置型排除强制执行结构形成互补。需要注意的是，无论是三权分置型数据财产权益，还是数据财产定限物权，事实上仅有少部分数据财产权益存在足以排除强制执行的可能性。进而言之，不宜不加区分地将所有的数据财产权益都确定为足以排除强制执行的民事权益；否则不仅会妨碍民事强制执行程序的正常进行，而且会影响整体性数据交易市场的良性发展。因此，未来我国在对数据财产权益进行更为精细的界定时，可通过立法构建数据财产权的公示对抗体系，明确登记的核心地位，并辅以技术手段增强权利可见性，如此方能兼顾数据流通效率与交易安全。尔后，可尝试在“数据二十条”确立的基本立场之基础上，结合传统物权理论与新型财产权理论，通过民事强制执行立法的完善，对“足以排除强制执行的数据财产权益”进行合理区分，力求做到既契合案外人的救济需要，又不阻碍数据资源要素的自由流通。

（技术编辑：艾薇）