中国人民大学法学院
数字法学教研月报

2025 年第 4 期（总第 16 期） 2025 年 4 月 21 日

本期看点

【数字法治大事件】中国人民大学法学院张新宝教授、主持编制**《数据安全技术　大型互联网企业内设 个人信息保护监督机构要求》国家标准**发布，该标准实施将推动企业加强个人信息保护能力建设，促进行业标准化发展，并为用户权益保护和社会信任构建提供制度保障。

国家在数据领域持续发力，政策法规密集出台。国家数据局发布**《数据领域常用名词解释（第二批）》**，进一步统一数据领域术语，为数据产业发展筑牢语言基础；**《数据出境安全管理政策问答（2025 年 4 月）》**解答跨境数据流动关键问题，为企业合规运营指明方向。**《中华人民共和国网络安全法（修正草案再次征求意见稿）》**公开征求意见，强化网络安全法律责任；**《人脸识别技术应用安全管理办法》**出台，规范人脸识别技术应用，全方位保障数据安全与个人信息权益。地方层面，合肥推进数据标注产业与人工智能协同发展，江苏省出台培育壮大数据企业专项政策，区域数字经济发展活力迸发。

【研究动态】本期研究动态聚焦数字法学多领域前沿问题。基础理论研究深入剖析刑事数据调取、金融稳定风险防范等课题；个人信息保护领域围绕数据交易合法性审查、神经数据保护等展开探讨；数据确权与流通研究涉及数据产权制度、数据持有权等关键内容；人工智能研究涵盖犯罪刑法应对、生成式人工智能侵权责任等热点。此外，平台治理、数字行政与司法、虚拟财产等领域也有诸多新研究成果，为数字法治建设提供坚实理论支撑。

【教研活动】第二届科技与法治论坛成功举办，多领域专家齐聚共探科技与法治协同发展；“人工智能将如何重塑法律版图” 讲座引发学界业界深度思考；俄罗斯国立人文大学法学院院长到访中国政法大学数据法治实验室，促进国际学术交流；北京数字司法与数据合规调研巡礼推动理论与实践深度融合；第三届人工智能法治论坛在广州举行，为人工智能法治发展凝聚智慧。

【数字法评】

《作为举报治理的通知删除：避风港规则反思》，《法学论坛》2025 年第 2 期，作者：丁晓东。

《数据权益之权能体系的再思考》，《法学评论》2025 年第 2 期，作者：阮神裕。

《数据可以占有吗？——兼论数据持有的法律构造》，《华东政法大学学报》2025 年第 2 期，作者：阮神裕。

本期目录

学术顾问：王利明

编 委 会：张新宝 丁晓东 王 莹 张吉豫

编 辑 部：阮神裕 卞 龙 艾 薇 邓语鑫 何 芮 梁因格 李佳丽 林诗敏 麻卓妍 乔彩霞 王 昊 朱恬馨

联系方式：RUCdigitallaw@163.com

本期排版：王昊

数字法治大事件

导言：中国人民大学法学院张新宝教授主持编制《数据安全技术 大型互联网企业内设 个人信息保护监督机构要求》国家标准，该标准已于 2025 年 3 月 28 日公布，于 10 月 1 日施行。

在数字化浪潮奔涌的当下，数据已然成为驱动社会发展与经济增长的核心要素。国家数据局发布的《数据领域常用名词解释（第一批）》，精准锚定数据、原始数据、数据资产、数据交易等 40 个可信数据空间相关名词，为数据领域搭建起通用语言体系。在数据安全与法规建设层面，数据出境安全管理政策问答（2025 年 4 月）针对数据跨境流动中的关键问题予以解答，为企业合规开展跨境数据业务提供指引，严守数据安全国门。《中华人民共和国网络安全法（修正草案再次征求意见稿）》公开征求意见，此次修订秉持问题导向，强化网络安全法律责任，在网络运行安全、网络信息安全、个人信息和重要数据安全等维度完善法律责任制度。《人脸识别技术应用安全管理办法》为人脸识别技术应用划定安全边界，从源头防范信息泄露、滥用等风险。地方层面，合肥积极推进数据标注产业与人工智能协同发展；江苏省出台省级层面培育壮大数据企业专项政策，从资金扶持、技术创新、人才培养等多维度发力，助力数据企业茁壮成长，为区域数字经济发展注入强劲动力。这一系列政策法规与地方实践致力于构建一个安全有序、创新活跃、开放共赢的数据生态环境，推动数字经济高质量发展，引领社会迈向更加智能、高效、安全的数字时代。

张新宝教授主持编制《数据安全技术 大型互联网企业内设 个人信息保护监督机构要求》（GB/T 45404-2025）国家标准发布

2025 年 3 月 28 日，国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告(2025 年第 6 号)，全国网络安全标准化技术委员会归口的 6 项国家标准正式发布。具体清单如下：

序号	标准编号	标准名称	实施日期
1	GB/T 45409-2025	网络安全技术 运维安全管理产品技术规范	2025/10/1
2	GB/T 45389-2025	数据安全技术 数据安全评估机构能力要求	2025/10/1
3	GB/T 45392-2025	数据安全技术 基于个人信息的自动化决策安全要求	2025/10/1
4	GB/T 45396-2025	数据安全技术 政务数据处理安全要求	2025/10/1
5	**GB/T 45404-2025**	**数据安全技术 大型互联网企业内设个人信息保护监督机构要求**	**2025/10/1**
6	GB/T 45406-2025	网络关键设备安全技术要求 可编程逻辑编辑控制器(PLC)	2025/10/1

《数据安全技术 大型互联网企业内设个人信息保护监督机构要求》（GB/T 45404-2025）标准由**中国人民大学法学院教授、博士生导师，教育部长江学者特聘教授，中国人民大学信息法中心主任张新宝教授**主持编制，该标准针对我国互联网企业，特别是大型互联网企业个人信息保护工作中出现的**个人信息保护合规标准不明、监督机制缺失与监督机构独立性不足，应对高危险场景的规则空白，透明度与问责机制薄弱**等问题，通过规范大型互联网企业内设监督机构的独立性、专业性和工作机制等个人信息保护中的监管难题，系统性给出解决方案。其实施将推动企业加强个人信息保护能力建设，促进行业标准化发展，并为用户权益保护和社会信任构建提供制度保障。

数据领域常用名词解释(第二批)

原载：“国家数据局”微信公众号

为凝聚广泛共识，在社会各界的大力支持下，我们认真研究形成了数据领域常用名词解释（第二批）。后续我们还将结合实践需求和发展需要迭代完善名词解释，欢迎社会各界持续关注。附件：数据领域常用名词解释（第二批）

数据领域名词解释起草专家组

2025 年 3 月 29 日

数据领域常用名词解释（第二批）

1.数据产权，是指权利人对特定数据享有的财产性权利，包括数据持有权、数据使用权、数据经营权等。

2.数据产权登记，是指数据产权登记机构按照统一的规则对数据的来源、描述、内容等的真实性、合规性、准确性等情况进行审核，记载数据权利归属等信息，并出具登记凭证的行为。

3.数据持有权，是指权利人自行持有或委托他人代为持有合法获取的数据的权利。旨在防范他人非法违规窃取、篡改、泄露或者破坏持有权人持有的数据。

4.数据使用权，是指权利人通过加工、聚合、分析等方式，将数据用于优化生产经营、提供社会服务、形成衍生数据等的权利。一般来说，使用权是权利人在不对外提供数据的前提下，将数据用于内部使用的权利。

5.数据经营权，是指权利人通过转让、许可、出资或者设立担保等有偿或无偿的方式对外提供数据的权利。

6.衍生数据，是指数据处理者对其享有使用权的数据，在保护各方合法权益前提下，通过利用专业知识加工、建模分析、关键信息提取等方式实现数据内容、形式、结构等实质改变，从而显著提升数据价值，形成的数据。

7.企业数据，是指企业在生产经营过程中形成或合法获取、持有的数据。

8.数据交易机构，是指为数据供方、需方提供数据交易服务的专业机构。

9.数据场内交易，是指数据供方、需方通过数据交易机构达成数据交易的行为。

10.数据场外交易，是指数据供方、需方不通过数据交易机构达成数据交易的行为。

11.数据交易撮合，是指帮助数据供方、需方达成数据交易的行为。

12.数据第三方专业服务机构，是指为促进数据交易活动合规高效开展，提供数据集成、质量评价、数据经纪、合规认证、安全审计、数据公证、数据保险、数据托管、资产评估、争议调解、风险评估、人才培训、咨询服务等第三方服务的专业化组织。

13.数据产业，是指利用现代信息技术对数据资源进行产品或服务开发，并推动其流通应用所形成的新兴产业，包括数据采集汇聚、计算存储、流通交易、开发利用、安全治理和数据基础设施建设等。

14.数据标注产业，是指对数据进行筛选、清洗、分类、注释、标记和质量检验等加工处理的新兴产业。

15.数字产业集群，是指以数据要素驱动、数字技术赋能、数字平台支撑、产业融通发展、集群生态共建为主要特征的产业组织新形态。

16.可信数据空间，是指基于共识规则，联接多方主体，实现数据资源共享共用的一种数据流通利用基础设施，是数据要素价值共创的应用生态，是支撑构建全国一体化数据市场的重要载体。可信数据空间须具备数据可信管控、资源交互、价值共创三类核心能力。

17.数据使用控制，是指在数据的传输、存储、使用和销毁环节采用技术手段进行控制，如通过智能合约技术，将数据权益主体的数据使用控制意愿转化为可机读处理的智能合约条款，解决数据可控的前置性问题，实现对数据资产使用的时间、地点、主体、行为和客体等因素的控制。

18.数据基础设施，是从数据要素价值释放的角度出发，面向社会提供数据采集、汇聚、传输、加工、流通、利用、运营、安全服务的一类新型基

础设施，是集成硬件、软件、模型算法、标准规范、机制设计等在内的有机整体。

19.算力调度，本质是计算任务调度，是基于用户业务需求匹配算力资源，将业务、数据、应用调度至匹配的算力资源池进行计算，实现计算资源合理利用。

20.算力池化，是指通过算力虚拟化和应用容器化等关键技术，对各类异构、异地的算力资源与设备进行统一注册和管理，实现对大规模集群内计算资源的按需申请与使用。

专家解读 | 以标准化引领国家数据基础设施高质量建设

原载：“国家数据局”微信公众号

文|中国信息通信研究院副院长 魏亮

党的二十届三中全会明确提出“建设和运营国家数据基础设施，促进数据共享”。2024 年底，国家发展改革委、国家数据局、工业和信息化部联合印发了《国家数据基础设施建设指引》（以下简称《指引》），明确了建设目标。

标准化是推动数据基础建设落地的关键一环，全国数据标准化技术委员会设置数据基础设施标准工作组，以标准规范为抓手，为数据基础设施建设提供技术指导。近日，国家数据局数字科技和基础设施建设司、全国数据标准化技术委员会秘书处联合发布国家数据基础设施建设有关技术文件（以下简称“技术文件”），进一步推动了数据基础设施标准化进展，为构建横向联通、纵向贯通、协调有力的国家数据基础设施提供基础支撑。

一、国家数据基础设施建设走深向实

国家基础设施建设已进入部署实施、走深向实新阶段，将夯实数据互联互通基础，加速数据价值释放，促进产业协同，助力全国一体化数据市场建设。

一是国家数据基础设施建设进入部署实施阶段。党的二十届三中全会明确了建设和运营国家数据基础设施的部署要求，《指引》明确了国家数据基础设施建设的目标路径、总体功能、总体架构、重点方向等内容。《数据基础设施 参考架构（试行）》《数据基础设施 互联互通基本要求（试行）》《数据基础设施 用户身份管理和接入规范（试行）》《数据基础设施 标识管理规范（试行）》《数据基础设施 接入连接器技术要求（试行）》《数据基础设施 数据目录描述规范（试行）》等 6 项技术文件首次提出了技术标准要求，标志着国家数据基础设施建设从规划阶段正式进入部署实施阶段，国家数据基础设施建设进一步深化。

二是深化数据基础设施建设加速数据价值释放。数据要素流通利用是数据要素价值释放的重要途径，我国数据要素流通领域的探索正不断扩展和深入，然而某些场景下仍存在“找不到、用不了、理不清、控不住”等问题，阻碍数据要素流通进一步发展。直击这些堵点、痛点问题，数据基础设施“统一目录标识、统一身份登记、统一接口要求”的标准化，将有利于跨平台、跨技术路线的互联互通，促进数据资源泛在接入，为数据发现、可信认证、数据查询、数据交互、供需交易提供基础支撑，加速数据价值释放。

三是深化数据基础设施建设加快全国一体化数据市场构建。深化数据基础设施建设将加速数据要素跨区域、跨行业流通，拉动经济增长。据测算，数据流通量每增加 10%可带动 GDP 增长 0.2%，数据流动对各行业利润增长的平均促进率为 10%左右。明确数据基础设施技术标准要求即是“书同文、车同轨”，将催生更多跨区域和跨行业的协同应用，深化产业合作，降低运营成本，活跃数据产业生态，助力全国一体化数据市场建设。

二、标准先行拉动国家数据基础设施高质量建设

标准在国家数据基础设施建设中具有重要的基础性、规范性和引领性作用。推进国家数据基础设施建设标准化进展，为建设集约高效、可信互联的数据基础设施夯实技术基础。

一是明确框架逻辑。通过标准化，规范数据基础设施的参考框架和互联互通基本要求，规范数据基础设施相关方角色定位和功能层级结构，规范各

类设施、数据及业务在数据基础设施中的对接交互逻辑和接口要求，将进一步避免重复建设，打破孤岛，降低异构系统对接成本，为跨区域、跨行业数据流通利用扫清技术障碍。

二是构筑数据地图。通过标准化，规范数据目录描述，构建统一标识管理规范，实现数据全生命周期追踪与管理，提升数据的可发现性与可用性，实现“目录可查、地址可循”，将进一步降低数据流通交易成本，提升数据供需匹配效率，驱动数据要素高效配置。

三是构建信任链路。通过标准化，规范用户身份管理和接入连接器等要求，建立数据流通“身份信任链”和可信交付体系，解决数据流通中的权责归属与信任问题，确保数据流通链路的稳定性与安全性，实现“身份可信、如约交付”，进一步降低数据流通信任成本，增强市场信心。

四是推动技术应用。通过标准化，规范可信数据空间、数场、数联网、数据元件、隐私保护计算、区块链等技术设施的标准要求，鼓励其通过标准化接口要求和流程规则接入和应用，保证高价值、高敏感数据“可用不可见”“可控可计量”“可溯可审计”，支持分布式数字身份（DID）等接入应用实现跨域身份互认和可信身份自主管理，探索大模型融合应用，促进数据应用智能化创新加速。

三、务实推进国家数据基础设施标准建设

下一步，要坚持问题导向、务实管用原则，逐步完善标准体系，结合实际不断迭代优化标准技术文件，适时开展标准实施效果评估评价，不断丰富应用场景，构建多方参与生态，以标准化引领国家数据基础设施高质量建设。

一是完善标准体系。围绕数据领域发展需求，开展相关国家标准的立项编制工作，有效指导国家数据基础设施建设。及时总结区域、行业、企业的实际建设和运营经验，密切跟踪国内外前沿数据流通技术和模式的发展应用，不断迭代优化标准技术文件。依据标准技术文件，开展标准实施效果的测试验证和能力评估，推动标准贯彻实施，确保标准文件有效落地执行。

二是丰富标准应用。坚持应用牵引，聚焦重点领域的数据流通利用场景，率先推动技术文件相关标准要求的先行先试。围绕实体经济数字化转型需求，深化数据要素在跨层级、跨行业、跨领域场景中的融合应用，打造一批具有示范性、可推广的数据基础设施架构方案、建设路径，形成覆盖数据全生命周期的典型实践，赋能数据流通利用和价值释放。

三是构建多方生态。依托《数据基础设施 参考架构（试行）》等标准技术文件构筑的多方参与架构和角色定位，充分发挥行业协会、联盟组织、专业智库等桥梁纽带作用，引导产学研用各方深化协同创新。壮大数据基础设施服务商力量，支持多元主体参与数据产品开发、技术服务和管理，推动构建开放共享的产业生态。谋划构建国家数据基础设施产业生态组织，健全技术创新、标准研制、应用推广的联动机制，凝聚各方共识、形成发展合力，培育可持续发展的良性市场生态。

数据出境安全管理政策问答（2025 年 4 月）

原载：“网信中国”微信公众号

国家互联网信息办公室持续加强数据出境安全管理政策宣贯，指导和帮助数据处理者高效合规开展数据出境活动。经对近期收到的咨询问题进行研究，现将一些有代表性的问题和答复公布如下。

1. 如何理解中国数据出境安全管理制度设计？

答：随着数据跨境流动活动的日益频繁，世界上许多国家和地区从本国、本地区实际出发，对数据跨境流动安全管理作了制度性探索，制定出台了一系列法律法规和规则标准。中国建立数据出境安全管理制度，是法律作出的规定。《网络安全法》《数据安全法》《个人信息保护法》在法律层面对数据出境活动作出明确规定。相关规定不是针对所有数据，只限于重要数据和个人信息。对于确需出境的重要数据，法律作了制度上的安排，经数据出境安全评估认为不会危害国家安全和社会公共利益的，可以出境。对于个人信息出境，法律规定了

数据出境安全评估、个人信息保护认证、个人信息出境标准合同等多种途径。总的来看，中国法律关于数据出境管理的规定，旨在保证在华企业因业务需要的数据跨境安全、自由流动，同时对涉及国家安全和公共政策目标的个人信息和重要数据跨境流动进行必要的监管。对于不涉及个人信息或者重要数据的一般数据可以跨境自由流动，重要数据和达到规定数量的个人信息通过数据出境安全评估后可以依法跨境流动。　　落实法律规定，国家互联网信息办公室先后出台实施《数据出境安全评估办法》《个人信息出境标准合同办法》《促进和规范数据跨境流动规定》，发布《关于实施个人信息保护认证的公告》及配套认证规则，明确数据出境安全评估、个人信息出境标准合同、个人信息保护认证等制度的实施路径，会同各地、各部门依法有序开展数据出境安全管理工作。

2.如何保证不同自贸试验区制定数据出境负面清单标准的一致性？

答：《促进和规范数据跨境流动规定》明确，自贸试验区可在国家数据分类分级保护制度框架下自行制定数据出境负面清单，经省级网络安全和信息化委员会批准，报国家网信部门、国家数据管理部门备案后实施，负面清单外数据出境将免予申报安全评估、订立标准合同、通过保护认证，是促进和便利自贸试验区数据跨境流动的一项创新举措。负面清单制定过程中将充分征求相关主管部门意见，负面清单备案时国家互联网信息办公室会同国家数据局对清单进行审核，针对同一领域，如果已经有自贸试验区发布负面清单，其余自贸试验区可以参照执行，不再重复制定。上述工作确保负面清单符合国家数据分类分级保护制度要求，保证不同自贸试验区负面清单标准的一致性。

3.自贸试验区数据出境负面清单适用范围如何覆盖更多领域？

答：落实《促进和规范数据跨境流动规定》，国家互联网信息办公室、国家数据局先后完成天津、北京、海南、上海、浙江等地自贸试验区（港）数据出境负面清单备案，对汽车、医药、零售、民航、再保险、深海业、种业等 17 个领域数据跨境流动发挥促进作用。国家互联网信息办公室会同有关部门正在指导各自贸试验区结合各自产业发展特点制定数据出境负面清单，随着更多负面清单的发布实施，覆盖的领域会越来越宽。关于自贸试验区数据出境负面清单发布实施情况，可以关注国家互联网信息办公室官网（www.cac.gov.cn）和相关地方自贸试验区网站进行了解。

4.如何理解和判断个人信息出境必要性？

答：《个人信息保护法》第六条规定，“处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息”；第十九条规定，“除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间”。

根据上述法律规定，判断“必要性”的考量因素包括与处理目的直接相关、对个人权益影响最小、限于实现处理目的的最小范围、保存期限为实现处理目的所必要的最短时间等 4 方面。落实法律规定，国家互联网信息办公室在开展数据出境安全评估工作中，将充分考量数据处理者申报事项的业务场景和实际需求，对个人信息出境必要性进行评估，评估要点主要包括出境活动本身的必要性、涉及自然人规模的必要性以及出境个人信息数据项范围的必要性等。

数据出境涉及众多行业领域，国家互联网信息办公室会同相关行业主管部门，逐步细化明确具体行业领域的数据出境业务场景以及个人信息出境必要范围，为企业机构数据出境提供更为细化的政策指引。

5.如何识别重要数据？

答：根据《网络数据安全管理条例》第六十二条规定，重要数据是指特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。《数据安全技术 数据分类分级规则》（GB/T

43697-2024）附录 G《重要数据识别指南》提出了重要数据识别方法。数据处理者可依据相关法律法规、技术标准等识别申报重要数据。

6. 重要数据是否意味着不能出境？

答：对于确需出境的重要数据，法律作了制度上的安排，经数据出境安全评估认为不会危害国家安全和社会公共利益的，可以出境。截至 2025 年 3 月，国家互联网信息办公室共完成数据出境安全评估项目 298 个，其中，44 个申报项目涉及重要数据，评估结果为不通过的 7 个，不通过率为 15.9%；44 个申报项目涉及 509 个重要数据项，评估后准予出境的重要数据项为 325 个，占申报数据项总数的 63.9%。

特别说明的是，《促进和规范数据跨境流动规定》明确，数据处理者按照相关规定申报重要数据，未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。

7. 行业技术标准制定过程中如何发挥外资企业的作用？

答：国家互联网信息办公室指导有关专业机构在制定行业技术标准过程中，高度重视并积极鼓励中外企业等各方参与，确保标准制定工作充分考虑国内外相关方需求。一是参与机制公开透明。国家互联网信息办公室指导全国网络安全标准化技术委员会坚持开放合作、广泛参与的原则，面向社会长期公开征集工作组成员单位。委员及下设工作组成员覆盖了一批有代表性的外资企业，其拥有和国内企业机构在标准参与、研讨方面平等的权利义务，作为工作组成员单位的外资企业能够全程参与，可在标准研制各环节充分提出意见和建议。二是标准工作程序公开透明。通过面向社会公开征集标准需求和标准参编单位、就标准草案面向社会公开征求意见等方式，确保各相关方公平公正参与标准制定。

8. 集团公司跨境传输个人信息有无更加便利的渠道？

答：一方面，境内多家子公司如同属一家集团公司且数据出境业务场景相似，可以由集团公司作为申报主体合并申报数据出境安全评估或者备案个人信息出境标准合同，提高数据出境工作效率。另一方面，国家互联网信息办公室正在推动出台个人信息出境保护认证相关管理办法，指导第三方专业认证机构对个人信息出境活动进行认证，境内企业和境外接收方任意一方通过认证，企业即可在认证范围内开展个人信息出境活动，对于通过认证的跨国集团，可在集团内开展个人信息出境活动，无需分别与各国子公司单独签订个人信息出境标准合同。

9. 申请延长数据出境安全评估结果有效期有无具体流程？

答：《促进和规范数据跨境流动规定》将数据出境安全评估结果有效期由原来的 2 年延长至 3 年，同时明确有效期届满，需要继续开展数据出境活动且未发生需要重新申报数据出境安全评估情形的，数据处理者可以在有效期届满前 60 个工作日内通过所在地省级网信部门向国家网信部门提出延长评估结果有效期申请，经国家网信部门批准，可以延长评估结果有效期 3 年。目前，国家互联网信息办公室正在积极听取各方意见，加快研究延长评估结果有效期的流程，计划通过修订发布相关政策文件的方式予以明确，为企业机构数据出境创造更为便利的条件。

关于公开征求《中华人民共和国网络安全法（修正草案再次征求意见稿）》意见的通知

原载：“网信中国”微信公众号

为了做好《中华人民共和国网络安全法》与相关法律的衔接协调，完善法律责任制度，保护个人、组织在网络空间的合法权益，维护国家安全和公共利益，根据《十四届全国人大常委会立法规划》，我办会同相关部门进一步研究起草了《中华人民共和国网络安全法（修正草案再次征求意见稿）》，现向社会公开征求意见。公众可通过以下途径和方式反馈意见：

1. 通过电子邮件将意见发送至：

law@cac.gov.cn。

2.通过信函将意见寄至：北京市西城区车公庄大街 11 号国家互联网信息办公室网络法治局，邮编：100044，并在信封上注明“《网络安全法》意见”。

意见反馈截止时间为 2025 年 4 月 27 日。

国家互联网信息办公室

2025 年 3 月 28 日

中华人民共和国网络安全法（修正草案再次征求意见稿）

一、将第五十九条修改为：“网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处一万元以上五万元以下罚款；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处五万元以上十万元以下罚款；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

有前两款行为，造成大量数据泄露、关键信息基础设施丧失局部功能等严重危害网络安全后果的，由有关主管部门处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款；造成关键信息基础设施丧失主要功能等特别严重危害网络安全后果的，由有关主管部门处二百万元以上一千万元以下罚款，并责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员处二十万元以上一百万元以下罚款。”

二、增加一条，作为第六十一条：“违反本法第二十三条规定，销售或者提供未经安全认证、安全检测或者安全认证不合格、安全检测不符合要求的网络关键设备和网络安全专用产品的，由有关主管部门责令改正或者停止违法行为，给予警告，没收违法产品和违法所得；违法所得十万元以上的，可以并处违法所得一倍以上三倍以下罚款；没有违法所得或者违法所得不足十万元的，可以并处三万元以上十万元以下罚款。”

三、增加一条，作为第六十四条：“有本法第六十条第一项、第二项和第六十三条行为，造成本法第五十九条第三款规定的后果的，依照该款规定处罚。”

四、将第六十五条改为第六十七条，修改为：“关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令限期改正、消除对国家安全的影响，并处采购金额一倍以上十倍以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。”

五、将第六十八条、第六十九条第一项合并，作为第六十九条，修改为：“网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录、向有关主管部门报告的，或者违反本法第五十条规定，不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告、通报批评，可以处五万元以上五十万元以下罚款；拒不改正或者情节严重的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

网络运营者有前款规定的违法行为，造成特别严重影响、特别严重后果的，由有关主管部门处二百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销

相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处二十万元以上一百万元以下罚款。

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前两款规定处罚。”

六、将第六十四条第一款、第六十六条、第七十条合并，作为第七十一条，修改为：“有下列行为之一的，依照有关法律、行政法规的规定处理、处罚：

（一）发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的；

（二）违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的；

（三）违反本法第三十七条规定，关键信息基础设施的运营者在境外存储个人信息和重要数据，或者向境外提供个人信息和重要数据的。”

七、增加一条，作为第七十二条：“网络运营者存在主动消除或者减轻违法行为危害后果、违法行为轻微并及时改正且没有造成危害后果或者初次违法且危害后果轻微并及时改正等情形的，依照《中华人民共和国行政处罚法》的规定从轻、减轻或者不予行政处罚。有关主管部门依据职责制定相应的行政处罚裁量基准，规范行使行政处罚裁量权。”

八、对部分条文作以下修改：

（一）将第六十一条改为第六十二条、第六十二条改为第六十三条，将其中的“关闭网站”修改为“关闭网站或者应用程序”。

（二）将第六十四条第二款改为第六十六条。

此外，对条文序号作了相应调整。

关于《中华人民共和国网络安全法（修正草案再次征求意见稿）》的说明

党中央高度重视维护国家网络安全。习近平总书记多次作出重要指示，强调“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障”。党的二十大和二十届三中全会对加强重点领域、新兴领域、涉外领域立法和增强立法系统性、整体性、协同性、时效性等作出了重要部署。为贯彻党中央决策部署，落实《十四届全国人大常委会立法规划》，适应网络安全新形势，我办会同相关部门起草了《中华人民共和国网络安全法（修正草案再次征求意见稿）》（以下简称《网络安全法（修正草案再次征求意见稿）》）。有关情况说明如下。

一、修改背景

《网络安全法》自 2017 年施行以来，为维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，提供了有力的法律保障。随着网络和信息技术日益融入社会生产生活，网络安全风险进一步凸显。2021 年以来，《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》）等网络安全相关立法相继制定实施，《中华人民共和国行政处罚法》（以下简称《行政处罚法》）修订出台，《网络安全法》需要适应形势加强与新出台法律的衔接协调，对相关法律责任制度作出科学优化，进一步保障网络安全。

2023 年 9 月，《十四届全国人大常委会立法规划》发布，明确将“网络安全法（修改）”列入了“第一类项目：条件比较成熟、任期内拟提请审议的法律草案”。2025 年 3 月，《全国人民代表大会常务委员会工作报告》将修改网络安全法列入 2025 年的立法工作任务。修改工作启动以来，我办会同相关部门密切沟通，共同推进修改《网络安全法》工作，先后开展了调查研究、修正草案起草、征求中央和国家机关有关单位、面向社会公开征求意见等工作。在认真听取有关方面意见的基础上，形成了《网络安全法（修正草案再次征求意见稿）》。

二、修改思路

在《网络安全法（修正草案再次征求意见稿）》起草过程中，着重把握以下几点：一是坚持以习近平新时代中国特色社会主义思想为指导，深入贯彻习近平法治思想和习近平总书记关于网络强国的

重要思想。二是坚持问题导向，重点强化网络安全法律责任，加大对违法行为处罚力度。三是坚持体系化衔接，加强与《数据安全法》《个人信息保护法》《行政处罚法》等相关法律有机衔接，在行政处罚的种类、范围、幅度等方面作出合理安排。四是坚持分类施策，科学设置网络运行安全、网络信息安全等不同类型违法行为的法律责任。

三、修改的主要内容

（一）关于网络运行安全的法律责任。结合实践中危害网络安全后果的情况，增加造成大量数据泄露、关键信息基础设施丧失局部功能等严重危害网络安全后果的和造成关键信息基础设施丧失主要功能等特别严重危害网络安全后果的情形，并参照《数据安全法》调整了现行《网络安全法》第五十九条罚款幅度，增加相应处罚规定；新增销售或者提供未经安全认证、安全检测或者安全认证不合格、安全检测不符合要求的网络关键设备和网络安全专用产品的法律责任；明确关键信息基础设施运营者使用未经安全审查或者安全审查未通过的网络产品或者服务行为的处置处罚措施。

（二）关于网络信息安全的法律责任。为防范新形势下网络信息内容安全风险对国家安全、政治安全带来的风险挑战，结合近年来网络信息内容执法实践，借鉴国外相关立法法律责任制度的新调整，完善现行《网络安全法》第六十八条、第六十九条针对的违法情形，调整未向有关主管部门报告和不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息停止传输、采取消除等处置措施情形的法律责任，明确对造成特别严重影响、特别严重后果的违法情形的处置处罚措施。

（三）关于个人信息和重要数据安全的法律责任。鉴于《数据安全法》《个人信息保护法》等有关法律、行政法规对现行《网络安全法》第六十四条第一款、第六十六条涉及的个人信息和重要数据违法行为的处罚作出了新的专门规定，明确转致适用的规定。

（四）关于从轻、减轻或者不予行政处罚的情形。统筹考虑《网络安全法》和《行政处罚法》的适用关系，专门新增一条衔接规定，明确网络运营者存在主动消除或者减轻违法行为危害后果、违法行为轻微并及时改正且没有造成危害后果或者初次违法且危害后果轻微并及时改正等情形的，依法从轻、减轻或者不予处罚；明确有关主管部门依据职责制定相应的行政处罚裁量基准。

中央网信办、工业和信息化部、公安部、市场监管总局关于开展 2025 年个人信息保护系列专项行动的公告

原载：“网信中国”微信公众号

《中华人民共和国个人信息保护法》施行以来，中央网信办会同有关部门持续组织开展个人信息保护相关工作，建立健全工作机制，研究制定标准规范，依法依规查处各类违法违规行为，加强正面典型示范引领，督促指导个人信息处理者不断提升合规水平，取得了积极治理成效。2025 年，中央网信办将会同工业和信息化部、公安部、市场监管总局等部门，进一步深入治理常用服务产品和常见生活场景中存在的违法违规收集使用个人信息典型问题，切实维护人民群众在网络空间合法权益，着力提升人民群众满意度、获得感。相关部门将围绕以下重点问题开展系列专项行动：

1.App（含小程序、公众号、快应用）违法违规收集使用个人信息。聚焦 App（含小程序、公众号、快应用）未提供个人信息收集使用规则，未按照个人信息收集使用规则处理个人信息，无相关功能或未使用相关功能时调用位置、媒体文件、通讯录、设备等非必要权限或收集非必要个人信息，未提供个人信息相关投诉渠道，未提供有效的更正删除个人信息及注销账号功能，提供个性化信息推送等功能但未提供便捷的拒绝方式，以及开屏等场景频繁“意外”跳转广告页面等问题开展治理。

2.SDK 违法违规收集使用个人信息。聚焦 SDK 未提供个人信息收集使用规则，未按照个人信息收集使用规则或与 App 明确的规则处理个人信息，未使用 SDK 相关功能时调用位置、媒体文件、通讯录、

设备等非必要权限或收集非必要个人信息，未提供个人信息相关投诉渠道，提供个性化信息推送等功能但未向 App 提供停止收集个人信息或关闭该功能的选项等问题开展治理。

3. 智能终端违法违规收集使用个人信息。聚焦智能手表、智能手环等穿戴产品，智能音箱、智能门锁、智能摄像头等家居产品，智能平板、智能学习机等学习终端，未提供个人信息收集使用规则，高频次、高精度、长时段超范围收集非必要个人信息，以及相关功能开启后需在后台持续收集个人信息或者需在云端计算和分析的，但未向用户进行显著提示等问题开展治理。

4. 公共场所违法违规收集使用人脸识别信息。聚焦交通运输、住宿旅游、教育培训、文化体育、物流商贸、休闲娱乐等公共场所使用人脸识别技术处理人脸信息，但未履行单独或书面告知同意等法律义务，未设置显著提示标识，未采取加密等严格保护措施，以及未依法开展个人信息保护影响评估等问题开展治理。

5. 线下消费场景违法违规收集使用个人信息。聚焦自动售卖、扫码点餐、出行乘车、入场停车、商超支付、扫码充电、房屋租赁等线下消费场景中，强制关注公众号、强制注册会员，强制收集非必要的手机号、生日、性别等信息，物业前台收集个人信息用于用户授权以外的目的，未经同意向第三方提供用户个人信息，以及上述场景中个人信息处理者未尽有效保护义务造成泄露等问题开展治理。

6. 个人信息相关违法犯罪案件。聚焦网络借贷、求职招聘、出行购票、教育、医疗、旅游住宿等领域个人信息违法犯罪活动，通过暗网电报等境外渠道以及境内渠道违规售卖公民个人信息，以及个人信息泄露或被攻击窃取等违法犯罪案件开展治理。

中央网信办、工业和信息化部、公安部、市场监管总局等有关部门将有序推进系列专项行动中的各项任务，集中治理各类典型违法违规问题，对拒不整改的依法从严处理；同时，有关部门将根据实际工作需要及时调整重点治理问题，确保专项行动取得实效，切实保护公民个人信息安全。

特此公告。

中央网信办 工业和信息化部公安部

市场监管总局

2025 年 3 月 28 日

国家互联网信息办公室、公安部联合公布《人脸识别技术应用安全管理办法》

原载：“网信中国”微信公众号

近日，国家互联网信息办公室、公安部联合公布《人脸识别技术应用安全管理办法》（以下简称《办法》），自 2025 年 6 月 1 日起施行。

国家互联网信息办公室有关负责人表示，人脸识别技术应用与人脸信息安全紧密相关，受到社会各方高度关注。为了规范应用人脸识别技术处理人脸信息活动，保护个人信息权益，国家互联网信息办公室、公安部联合出台《办法》，对应用人脸识别技术处理人脸信息的基本要求和处理规则、人脸识别技术应用安全规范、监督管理职责等作出了规定。

《办法》明确了应用人脸识别技术处理人脸信息的基本要求。应用人脸识别技术处理人脸信息活动，应当遵守法律法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行个人信息保护义务，承担社会责任，不得危害国家安全、损害公共利益、侵害个人合法权益。

《办法》明确了应用人脸识别技术处理人脸信息的处理规则。一是应当具有特定的目的和充分的必要性，采取对个人权益影响最小的方式，并实施严格保护措施。二是应当履行告知义务。三是基于个人同意处理人脸信息的，应当取得个人在充分知情的前提下自愿、明确作出的单独同意。基于个人同意处理不满十四周岁未成年人人脸信息的，应当取得未成年人的父母或者其他监护人的同意。四是除法律、行政法规另有规定或者取得个人单独同意外，人脸信息应当存储于人脸识别设备内，不得通过互联网对外传输。除法律、行政法规另有规定外，

人脸信息的保存期限不得超过实现处理目的所必需的最短时间。五是应当事前进行个人信息保护影响评估，并对处理情况进行记录。

《办法》明确了人脸识别技术应用安全规范。一是实现相同目的或者达到同等业务要求，存在其他非人脸识别技术方式的，不得将人脸识别技术作为唯一验证方式。国家另有规定的，从其规定。二是应用人脸识别技术验证个人身份、辨识特定个人的，鼓励优先使用国家人口基础信息库、国家网络身份认证公共服务等渠道实施。三是任何组织和个人不得以办理业务、提升服务质量等为由，误导、欺诈、胁迫个人接受人脸识别技术验证个人身份。四是在公共场所安装人脸识别设备，应当为维护公共安全所必需，依法合理确定人脸信息采集区域，并设置显著提示标识。任何组织和个人不得在宾馆客房、公共浴室、公共更衣室、公共卫生间等公共场所中的私密空间内部安装人脸识别设备。五是人脸识别技术应用系统应当采取数据加密、安全审计、访问控制、授权管理、入侵检测和防御等措施保护人脸信息安全。

《办法》明确了监督管理职责。个人信息处理者应当在应用人脸识别技术处理的人脸信息存储数量达到 10 万人之日起 30 个工作日内向所在地省级以上网信部门履行备案手续。网信部门会同公安机关和其他履行个人信息保护职责的部门，建立健全信息共享和通报工作机制，协同开展相关工作。

《办法》同时对违反《办法》规定的法律责任、相关术语的含义等作出了规定。

《人脸识别技术应用安全管理办法》答记者问

原载：“网信中国”微信公众号

近日，国家互联网信息办公室、公安部联合公布了《人脸识别技术应用安全管理办法》（以下简称《办法》）。国家互联网信息办公室有关负责人就《办法》相关问题回答了记者提问。

问 1：请介绍一下《办法》的出台背景？

答：随着云计算、大数据、物联网、人工智能等互联网技术飞速发展，人脸识别技术应用在消费、金融、出行等社会各领域快速普及，在促进数字经济发展、方便人民生活的同时，也引发了公众对侵犯隐私、泄露个人信息的担忧，受到社会各方高度关注。《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》《网络数据安全管理条例》等法律、行政法规对个人信息处理规则作出了规定。同时，《中华人民共和国个人信息保护法》第六十二条规定，国家网信部门统筹协调有关部门针对人脸识别等新技术、新应用制定专门的个人信息保护规则。制定出台《办法》是落实法律、行政法规规定的重要举措，目的是规范应用人脸识别技术处理人脸信息活动，保护个人信息权益。

问 2：《办法》如何处理发展与安全的关系，在保护个人信息权益的同时促进人脸识别技术发展？

答：《办法》坚持发展与安全并重，妥善处理促进创新和依法治理之间的关系，在保护个人信息权益的同时鼓励人脸识别技术的应用和创新。一方面，《办法》规定应用人脸识别技术处理人脸信息的基本要求和具体规则，建立人脸识别技术应用监督管理制度，规范人脸识别技术应用，切实保护广大人民群众的个人信息权益。另一方面，《办法》明确在中华人民共和国境内为从事人脸识别技术研发、算法训练活动应用人脸识别技术处理人脸信息的，不适用本办法的规定，为开展人脸识别技术的攻关研究和应用创新预留空间，有利于推动相关产业安全健康发展。

问 3：《办法》的主要内容是什么？

答：《办法》主要对下列内容进行了规定：一是明确应用人脸识别技术处理人脸信息的基本要求，规定应用人脸识别技术处理人脸信息活动，应当遵守法律法规，尊重社会公德和伦理，遵守商业道德和职业道德等。二是明确应用人脸识别技术处理人脸信息的处理规则，规定应用人脸识别技术处理人脸信息，应当具有特定的目的和充分的必要性，个人信息处理者应当履行告知、进行个人信息保护

影响评估等义务。三是明确人脸识别技术应用安全规范，规定实现相同目的或者达到同等业务要求，存在其他非人脸识别技术方式的，不得将人脸识别技术作为唯一验证方式，明确在公共场所安装人脸识别设备的具体要求。四是明确监督管理职责和法律责任，规定个人信息处理者应当在应用人脸识别技术处理的人脸信息存储数量达到 10 万人之日起 30 个工作日内向所在地省级以上网信部门履行备案手续，明确违反本办法规定的法律责任。

问 4：《办法》对应用人脸识别技术处理人脸信息活动提出了哪些基本要求？

答：《办法》规定，应用人脸识别技术处理人脸信息活动，应当遵守法律法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行个人信息保护义务，承担社会责任，不得危害国家安全、损害公共利益、侵害个人合法权益。

问 5：《办法》对应用人脸识别技术处理人脸信息规定了哪些处理规则？

答：《办法》对应用人脸识别技术处理人脸信息规定了以下处理规则：一是应当具有特定的目的和充分的必要性，采取对个人权益影响最小的方式，并实施严格保护措施。二是应当履行告知义务，处理残疾人、老年人人脸信息的，还应当符合国家有关无障碍环境建设的规定。三是基于个人同意处理人脸信息的，应当取得个人在充分知情的前提下自愿、明确作出的单独同意。基于个人同意处理不满十四周岁未成年人人脸信息的，应当取得未成年人的父母或者其他监护人的同意。四是除法律、行政法规另有规定或者取得个人单独同意外，人脸信息应当存储于人脸识别设备内，不得通过互联网对外传输。除法律、行政法规另有规定外，人脸信息的保存期限不得超过实现处理目的所必需的最短时间。五是应当事前进行个人信息保护影响评估，并对处理情况进行记录。

问 6：《办法》对人脸识别技术应用规定了哪些安全规范？

答：《办法》对人脸识别技术应用规定了以下安全规范：一是实现相同目的或者达到同等业务要求，存在其他非人脸识别技术方式的，不得将人脸识别技术作为唯一验证方式。国家另有规定的，从其规定。二是应用人脸识别技术验证个人身份、辨识特定个人的，鼓励优先使用国家人口基础信息库、国家网络身份认证公共服务等渠道实施。三是任何组织和个人不得以办理业务、提升服务质量等为由，误导、欺诈、胁迫个人接受人脸识别技术验证个人身份。四是在公共场所安装人脸识别设备，应当为维护公共安全所必需，依法合理确定人脸信息采集区域，并设置显著提示标识。任何组织和个人不得在宾馆客房、公共浴室、公共更衣室、公共卫生间等公共场所中的私密空间内部安装人脸识别设备。五是人脸识别技术应用系统应当采取数据加密、安全审计、访问控制、授权管理、入侵检测和防御等措施保护人脸信息安全。

问 7：针对群众普遍关心的强制刷脸问题，《办法》作出了哪些规定？

答：人脸信息是敏感个人信息，一旦泄露，容易对个人的人身和财产安全造成重大危害，甚至威胁公共安全。针对“刷脸”住宿、“刷脸”进小区等人脸识别技术应用场景泛化、强制使用等问题，《办法》明确了人脸识别技术应用的非强制原则，规定实现相同目的或者达到同等业务要求，存在其他非人脸识别技术方式的，不得将人脸识别技术作为唯一验证方式。个人不同意通过人脸信息进行身份验证的，应当提供其他合理、便捷的方式。国家对应用人脸识别技术验证个人身份另有规定的，从其规定。

问 8：《办法》对个人信息处理者应用人脸识别技术处理人脸信息备案提出了哪些要求？

答：《办法》从信息数量、备案时间、备案部门、备案材料、备案变更和注销五个方面对个人信息处理者应用人脸识别技术处理人脸信息备案提出了具体要求。一是信息数量方面，以“应用人脸识别技术处理的人脸信息存储数量达到 10 万人”为备案起始数量。二是备案时间方面，规定应当在应用人脸识别技术处理的人脸信息存储数量达到 10 万人之日起 30 个工作日内进行备案。三是备案

部门方面，明确向所在地省级以上网信部门履行备案手续。四是备案材料方面，明确应当提交个人信息处理者的基本情况、人脸信息处理目的和处理方式、人脸信息存储数量和安全保护措施、人脸信息的处理规则和操作规程、个人信息保护影响评估报告五项材料。五是备案变更和注销方面，明确备案信息发生实质性变更的，应当在变更之日起 30 个工作日内办理备案变更手续。终止应用人脸识别技术的，应当在终止之日起 30 个工作日内办理注销备案手续，并依法处理人脸信息。

《网络安全法（修正草案再次征求意见稿）》解读：以“四大导向”推进网安法治现代化

原载：“信息化方案提供商”微信公众号

近日，国家互联网信息办公室发布了《中华人民共和国网络安全法（修正草案再次征求意见稿）》（以下简称《修正草案再次征求意见稿》），引起社会的广泛关注和热议。《中华人民共和国网络安全法》（以下简称《网络安全法》）作为网络安全领域的基本法，于 2017 年 6 月施行。随着社会网络安全需求的不断增长及网络安全法律体系完善发展的内在要求，该法也再次迎来修订的契机。本文结合对本次修订意见的学习，简要分析如下。

一、修订历程简要回顾

《网络安全法》施行至今，共进行了两次修订征求意见。

（一）第一次修订征求意见

2022 年 9 月，国家互联网信息办公室会同相关部门起草并发布了《关于修改〈网络安全法〉的决定（征求意见稿）》，开启了对《网络安全法》的修订完善历程。

第一次修订时，主要基于两个背景。

一是做好《网络安全法》与相关法律的衔接协调，完善法律责任制度。此时的法律衔接，主要是指《网络安全法》颁行后，国家出台的多部重磅网络安全相关法律，主要包括《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》等。保持不同法律之间的协同，是网络安全法修订的主要动因之一。

二是保护个人、组织在网络空间的合法权益，维护国家安全和公共利益。随着数字化发展的深入，个人、组织乃至国家面临的网络安全风险和威胁形势也日益严峻。近年来除了常规的网络风险因素之外，以勒索软件、供应链攻击、基于 AI 技术的攻击等为典型代表的网络安全威胁日益增多。通过修订法律以强化法律责任机制和合规要求，无疑是加强对网络安全合法权益保护的有效途径之一。

（二）第二次修订征求意见

2025 年 3 月，国家互联网信息办公室发布了会同相关部门进一步研究起草的《修正草案再次征求意见稿》。

结合通知内容，有三个重要问题需特别留意。

一是关于第一次修订征求意见的结果。按照《全国人大常委会 2024 年度立法工作计划》，“网络安全法（修改）”位列 23 项“初次审议的法律案”之中，而时至今日未有正式消息表明其已修订通过并颁布实施。这或许也是第二次修订征求意见稿出台的重要原因。

二是法律修订的时限。《通知》阐明了法律衔接和保护权益两个修订工作目标之外，还补充了一条工作依据即《十四届全国人大常委会立法规划》。根据该项立法规划，“网络安全法（修改）”位列“条件比较成熟、任期内拟提请审议的法律草案（79 件）”之中，可见网络安全法的修订工作正常情况下应当在十四届全国人大任期结束前，即 2028 年 3 月之前提请审议。

三是征求意见时间比上次更长。与第一次征求意见相比，本次征求意见的时间为 30 个自然日（2025 年 3 月 28 日-4 月 27 日），明显长于上次的 15 个自然日（2022 年 9 月 14 日-9 月 29 日）。这也在一定程度上反映了主管部门对本次征求意见充分性所作的预期考量。

二、内容比较

通过比较《网络安全法》和《修正草案再次征求意见稿》，我们可以发现：除了对于同类违法行

为处罚条款的合并、提升措辞准确性、调整法条序号等行文方面的修改之外，对实质内容方面的修订充分反映了本次法律修订重要导向。以下分析概括为 4 个方面。

导向一：强化执法严肃性

一是提升了对相关违法行为的处罚力度。主要体现在《修正草案再次征求意见稿》第一条和第五条，对于网络运营者、关键信息基础设施运营者违反网络安全保护和网络安全管理义务的行为，提高了罚款处罚额度。

二是增加处罚裁量选项。主要体现在《修正草案再次征求意见稿》第一条和第五条，对于网络运营者、关键信息基础设施运营者违反网络安全保护和网络安全管理义务的行为，在给予警告等处罚的同时，还“可以处”一定金额的罚款。赋予执法部门根据违法行为具体情况做出并行处罚的裁量权。

导向二：强化分级处罚

主要体现为增加了加重处罚的情节。《修正草案再次征求意见稿》第一条、第三条、第五条，对于网络运营者、关键信息基础设施运营者违反网络安全保护和网络安全管理等义务的行为，增设了造成“严重危害网络安全后果”、“造成特别严重影响、特别严重后果”等加重处罚情节，体现了对违法行为按照所产生的后果进行分级处罚的思路。

导向三：完善产品服务使用合规责任体系

主要体现在增加了对网络产品服务使用合规的责任和处罚规定。《修正草案再次征求意见稿》第二条，增加对使用不合规网络产品和服务等行为的处罚规定。从而将涉及网络产品、服务的合规使用要求与相应法律责任直接挂钩衔接，无疑将进一步增强对产品服务合规使用日常监管的执法力度。

导向四：鼓励违法者主动采取补救措施

体现在增加了对违法者主动改正行为的鼓励条款。《修正草案再次征求意见稿》第七条，明确将网络运营者“主动消除或者减轻违法行为危害后果、违法行为轻微并及时改正且没有造成危害后果或者初次违法且危害后果轻微并及时改正”等 3 种情况，作为从轻、减轻或者不予行政处罚的情形。而这 3 种情形都以行为人主动采取一定补救或改正措施为必要条件，这也是本次法律修订的一个重要特点。

三、思考和影响

（一）完善思考和建议

《修正草案再次征求意见稿》目前正在征求意见阶段，对于其内容的完善有以下粗浅思考。

一是停止损害的前置性问题。《修正草案再次征求意见稿》第四条规定了对关基运营者使用违规产品的处罚方式，包括责令改正、消除影响和罚款三种形式。与原法律条文相比，不再采用“责令停止使用”的表述。这从修改内容来看，或许“责令限期改正”也可作包含了“责令停止使用”含义的理解。但在实际操作中，“责令停止使用”等停止损害措施作为及时止损的有效方式，有其存在的现实意义，是有必要在规定中明确提出，值得商榷。

二是消除影响的范围问题。《修正草案再次征求意见稿》第四条对于消除影响的规定为“消除对国家安全的影响”，结合本条关基运营者使用违规产品的行为来看，其潜在的影响除了国家安全，可能还有对系统正常运行、相关经济社会利益的损害等多个方面。是否扩充消除影响的范围和种类，可能也有必要进一步研究。

三是处罚原则的一致性问题。《修正草案再次征求意见稿》第六条为转致性规定，其将个人信息保护、数据安全等违法行为的处罚明确转致适用《数据安全法》、《个人信息保护法》等有关法律的罚则规定。但目前后者对于此处涉及的违法行为处罚，并未细化、也未规定诸如“可以并处一定罚款”等威慑性的可裁量处罚方式。因此，本条内容转致适用后，可能带来不同法律之间处罚导向不尽一致的问题。如何体现法律之间处罚原则和导向保持协调一致，或需统筹考虑。

（二）行业影响观察

《修正草案再次征求意见稿》体现了宽严相济、加重对违法行为处罚、完善相关罚则体系等重要特点导向。或将对网络安全行业产生至少两个方面的切实影响。

一方面，对违规行为加大处罚力度，进一步强化了法律要求的合规威慑，促使以网络运营者为主的各类主体严格履行法律义务。这对于网络安全运行合规咨询、网络安全监测和审计、个人信息和重要数据保护等无疑将带来综合促进。

另一方面，对于法律责任的补充，尤其是对使用合规网络产品和服务等责任的规定，对于相关网络产品认证服务、数据产品认证服务、网络和数据产品设备采购等业务或将带来明显的提振。

四、小结

《网络安全法》是奠定我国网络安全管理制度基础性法律，其发挥着开先河、集大成、定框架的重要作用。如何完善发展立法，构建符合数字中国时代特征、满足中国式现代化发展要求的网络安全法律制度体系，事关经济社会发展的各个领域，需要产、学、研、用各领域集思广益，发挥集体智慧。绿盟科技一向重视深入学习研究国家网络安全法规政策，并认真将相关要求贯彻到技术创新和业务发展的全过程，努力发扬绿盟科技“专攻术业、成就所托”的宗旨愿景，持续为国家网络安全体系和能力的提升贡献力量。

专家解读丨完善法律责任制度 筑牢网络安全屏障

原载：“网信中国”微信公众号

《网络安全法》作为我国网络安全领域的基础性法律，自 2017 年施行以来，在维护网络空间主权、国家安全、社会公共利益以及保护公民、法人和其他组织合法权益等方面发挥了重要作用。然而，随着网络空间的复杂性和不确定性不断增强，网络攻击、数据泄露、关键信息基础设施威胁等事件频发，有关法律制度已难以适应新的风险挑战。近日，国家网信办会同相关部门起草了《网络安全法（修正草案再次征求意见稿）》（以下简称“征求意见稿”），从征求意见稿来看，主要是做好与《数据安全法》《个人信息保护法》等相关法律法规的衔接协调，完善法律责任制度，将进一步保障网络安全。

一、推进依法治理，有效应对网络安全形势需要

近年来，网络攻击手段不断升级，我国面临的网络安全形势日益严峻复杂。**一是**个人信息和重要数据泄露风险频发。贩卖个人信息和重要数据获利成为黑产的主要手段之一，一些联网数据库存在未授权访问或弱口令漏洞，容易导致姓名、身份证号、手机号等数据泄露。**二是**勒索软件攻击呈持续增长趋势。勒索攻击的主流威胁形态已经演变成“勒索软件即服务（RaaS）+定向攻击”收取高额赎金的模式，制造、医疗、金融、建筑、能源和公共管理等行业频繁成为勒索攻击的目标。2024 年全球公开披露的勒索软件攻击事件超过 5700 起，我国某金融机构驻外子公司被勒索组织 Hunters 攻击，泄露数据量达 6.6TB。**三是**网络安全漏洞风险依然严峻。2024 年，国家信息安全漏洞共享平台（CNVD）共收录通用软硬件漏洞 1.8 万个，其中高危漏洞占比达 46.4%。“微软蓝屏”事件虽然并非安全漏洞，但也导致全球超过 850 万台设备运行故障，造成巨大经济损失。随着大数据、云计算、人工智能等新技术的广泛应用，网络安全技术的应用场景也越来越广泛，势必也将引入新的安全风险。

在此形势下，增强法律威慑力已成为修改《网络安全法》的必然要求。部分企业为追求经济利益，忽视网络安全责任，导致数据泄露、网络攻击、安全漏洞等事件和风险频发。而现行《网络安全法》对违法主体的处罚额度较低，这对其经济利益影响较为有限，也远低于数据泄露所造成的经济损失和社会影响。

此次修改拟完善法律责任制度，规定造成严重或特别严重危害网络安全后果等违法情形的法律责任，并通过提高罚款金额、增加处罚种类等措施加大了相关违法行为的处罚力度。**一是**拟明确对造成数据泄露严重后果的处罚措施。对网络运营者不履行网络安全保护义务造成大量数据泄露等严重危害网络安全后果的，拟规定最高可处以二百万元罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销

营业执照。**二是**拟明确对违法销售或提供网络关键设备和网络安全专用产品的处罚措施。对违反本法第二十三条销售或者提供未经安全认证、安全检测或者安全认证不合格、安全检测不符合要求的网络关键设备和网络安全专用产品的，拟规定由有关主管部门责令改正或停止违法行为，给予警告、没收违法产品和违法所得，根据违法所得金额处以不同数额的罚款。**三是**拟加大对网络运营者等主体不履行网络信息安全管理义务的处罚力度。造成特别严重影响、特别严重后果的情形拟明确最高可处以一千万元罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，同时对直接负责的主管人员和其它责任人员最高处以一百万元罚款。这将提高违法成本，促使主动建立健全网络安全管理制度，提升网络安全技术防护能力，落实网络运营者主体责任，并对潜在的违法者形成更强的威慑，有效遏制网络违法犯罪行为的发生。

二、细化责任体系，加强关键信息基础设施安全防护

关键信息基础设施是关系到国家安全、国计民生和公共利益的重要基础设施，受地缘政治和国家间冲突的影响，某些组织通过分布式拒绝服务（DDoS）攻击、系统漏洞、网络钓鱼、勒索软件等方式，对我国能源、交通、金融、公共、通信、科技等重要领域实施网络攻击，窃取重要敏感数据，将网络空间演变成为国家博弈的重要战场。2023 年 5 月起，我国某大型高科技企业遭疑似境外机构网络攻击，其邮件服务器被控制并植入后门程序，并以此为跳板攻击该公司及下属企业 30 余台设备，大量邮件数据和商业秘密信息被窃取。2024 年 8 月，我国某研究单位遭疑似境外机构网络攻击，270 余台主机被控，大量商业秘密信息被窃取。

强化关键信息基础设施运营者的网络安全主体责任，是保障国家网络安全的关键环节。此次修改进一步完善了关键信息基础设施安全保护的法律责任制度，有利于推动其更好地落实网络安全主体责任、加强安全防护。**一是**明确对不履行义务导致关键信息基础设施丧失功能情形的处罚措施。关键信息基础设施运营者不履行网络安全保护义务，造成关键信息基础设施丧失局部功能等严重危害网络安全后果的，拟规定最高可处以二百万元罚款，造成丧失主要功能等特别严重危害网络安全后果的，最高可处以一千万元罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员处以相应罚款。**二是**优化对违规使用网络产品或服务的处罚措施。关键信息基础设施运营者违规使用未经安全审查或者安全审查未通过的网络产品或者服务的，其处罚措施拟由现行法律规定的“责令停止使用”调整为“责令限期改正、消除对国家安全的影响”，为关键信息基础设施运营者兼顾安全与发展提供了空间。**三是**优化对违规存储或传输个人信息和重要数据的处罚措施。针对关键信息基础设施运营者违规在境外存储个人信息和重要数据、或者向境外提供个人信息和重要数据的情形，拟将其处罚措施调整为“依照有关法律、行政法规的规定处理、处罚”，将增强《网络安全法》与《数据安全法》《个人信息保护法》的衔接，提升了网络安全法律体系的整体协调性。

三、引入从轻、减轻、不予行政处罚情形，激励运营者主体参与网络安全治理

网络安全是一项系统工程，涉及的领域广、方面多，大多数网络安全事件和风险都具有跨地区、跨部门、跨行业的特点。仅仅依靠单一个体防御已经无法应对复杂的网络安全形势，迫切需要发挥政府、企业、社会组织等各种主体作用，加强网络安全协作。其中，网络运营者承担着网络和信息系统安全防护的实际工作，在网络安全事件应对、风险防范等工作中占有重要地位，网络运营者的参与对加强网络安全防护至关重要。

此次修改拟引入情节轻微情形下的豁免机制，即对网络运营者存在主动消除或减轻违法行为危害后果、违法行为轻微并及时改正且没有造成危害后果或者初次违法且危害后果轻微并及时改正等情形的，依照《行政处罚法》的规定从轻、减轻或

者不予行政处罚。这一机制的引入具有重要意义，一方面，它有利于引导运营者主体自觉遵守法律法规，减轻其合规负担，避免因轻微违法而面临严厉处罚；另一方面，它能够有效打消运营者主体的顾虑，激励其主动配合网络安全管理，积极履行网络安全义务，更好地发挥其主体作用。

《网络安全法》的修改是适应新时代网络安全需求的重要举措。在全球网络安全形势日益严峻的背景下，为进一步加强网络威胁发现及防御能力，有效应对国家级有组织网络攻击，需要综合发挥各方作用，共同打造国家网络安全纵深防御体系。此次修改结合当前网络安全工作实际，通过增强法律威慑力、细化责任体系、引入豁免机制等创新举措，加强了网络安全领域相关法律法规的协同性，提升了法律的威慑力和执行力，促进了运营者主体履行网络安全义务的积极性，将为维护国家网络安全、建设网络强国提供更坚实的法治保障。

关于《上海市网络数据分类分级和重要数据目录管理办法（征求意见稿）》公开征求意见的通知

原载：“网信上海”微信公众号

为建立健全网络数据分类分级制度及重要数据目录管理机制，保障网络数据安全，促进网络数据开发利用，依据有关法律法规，上海市网信办会同市数据局起草了《上海市网络数据分类分级和重要数据目录管理办法（征求意见稿）》，现向社会公开征求意见。公众可以通过以下途径提出反馈意见：

1. 通过电子邮件将意见发送至：wxbwac@shxc.gov.cn。

2. 通过信函方式将意见寄至：上海市徐汇区宛平路 315 号上海市互联网信息办公室网络安全处，邮编 200030，并在信封上注明“网络数据分类分级和重要数据目录管理办法征求意见”。

意见反馈截止日期为 2025 年 4 月 28 日。

上海市互联网信息办公室

2025 年 3 月 28 日

上海市网络数据分类分级和重要数据目录管理办法（征求意见稿）

第一章　总则

第一条　目的和依据

为建立健全网络数据分类分级制度及重要数据目录管理机制，保障网络数据安全，促进网络数据开发利用，保护个人、组织的合法权益，根据《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》《上海市数据条例》等法律法规要求，结合本市实际，制定本办法。

第二条　适用范围

本办法适用于在本市范围内开展的各行业、各领域的网络数据分类分级规则制定、网络数据分类分级实践、重要数据识别处理、网络数据安全保护体系建立等工作及其安全监管行为。

开展核心数据的网络数据处理活动，按照国家有关规定执行。

开展涉及国家秘密、工作秘密的网络数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

第三条　定义

本办法所称网络数据，是指通过网络处理和产生的各种电子数据。

重要数据，是指特定领域、特定群体、特定区域或达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。

个人信息，是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

公共数据，是指本市国家机关、事业单位，经依法授权具有管理公共事务职能的组织，以及供水、供电、供气、公共交通等提供公共服务的组织，在履行公共管理和服务职责过程中收集和产生的数据。

网络数据处理者，是指在网络数据处理活动中

自主决定处理目的、处理方式的个人、组织。

网络数据安全，是指通过采取必要措施，确保网络数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

第四条　管理原则

本市实行网络数据安全工作与业务工作协同管理，网络数据分类分级和重要数据目录管理应当结合网络数据所属行业领域特点，按照谁主管谁负责、属地管理的原则，坚持“谁收集谁负责、谁持有谁负责、谁使用谁负责”，统筹促进网络数据开发利用与保障网络数据安全。

第五条　部门职责

我市数据安全工作协调机制负责统筹协调网络数据安全重大事项和重要工作。

市网信部门负责统筹协调本市网络数据安全和相关监督管理工作，推进网络数据分类分级和重要数据目录管理。

市数据部门负责组织协调数据发展管理，推动公共数据资源开发利用，指导市大数据中心结合公共数据上链、数据开发利用等要求，推动各部门落实本市公共数据分类分级和重要公共数据目录管理。

本市各主管部门负责承担本行业、本领域网络数据安全监督管理职责，统筹本行业、本领域网络数据分类分级、重要数据目录确定、指导重要数据处理者履行安全保护责任等工作。

各部门对本部门工作中收集和产生的网络数据及网络数据安全负责，推进本部门数据分类分级和重要数据目录确定。

市公安机关、国家安全机关在各自职责范围内承担网络数据安全监管职责。

各区有关部门按照职责分工参照执行。

第二章　网络数据分类分级

第六条　网络数据分类分级原则

网络数据分类分级应当遵循国家有关规定，按照网络数据所属行业领域要求，依据科学实用、边界清晰、就高从严、点面结合、动态更新等原则进行。

如所属行业、领域没有主管部门认可的网络数据分类分级标准规范，或存在相关行业、领域规范未覆盖的网络数据类型，参照国家网络数据分类分级标准进行网络数据分类分级。

第七条　网络数据分类规则

网络数据分类应当根据网络数据管理和使用需求，结合网络数据所属行业领域已有的网络数据分类基础，灵活选择业务属性将网络数据逐级细化分类。

涉及法律法规有专门管理要求的网络数据类别（如个人信息、公共数据），应按照有关规定和标准进行识别和分类。

第八条　网络数据分级规则

网络数据分级应当根据网络数据在经济社会发展中的重要程度，以及一旦遭到泄露、篡改、破坏或者非法获取、非法利用、非法共享，对国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益造成的危害程度，将网络数据从高到低分为核心数据、重要数据、一般数据三个级别。

一般数据级别可根据本单位网络数据管理和使用需求进一步分级。公共数据、行业数据等有明确分级要求的从其规定。

当网络数据业务属性、重要程度和可能造成的危害程度变化时，应当对网络数据的级别进行动态更新。

第九条　网络数据分类分级流程

网络数据分类分级工作可以按照梳理网络数据资产、制定网络数据分类分级内部规则、实施网络数据分类、实施网络数据分级、形成网络数据资产清单、按有关程序上报重要数据目录等步骤开展。所属行业、领域有明确网络数据分类分级流程的从其规定。

第十条　网络数据分类分级保护

完成网络数据分类分级后，不同类别、级别的网络数据应当根据法律法规要求采取不同的保护措施，建立重要数据重点保护、一般数据全周期分级保护体系。

第三章　重要数据识别及目录管理

第十一条　重要数据识别依据

重要数据识别主要依据相关法律法规，行业、领域重要数据识别指南，数据分类分级相关国家标准等。各部门应当将相关重要数据识别依据报送至市网信部门。

第十二条　开展重要数据识别

网络数据处理者应当对所处理的数据情况进行盘点、梳理和分类分级，并判断其对国家安全、经济运行、社会稳定、公共健康和安全可能造成的影响，按照国家有关规定识别、申报重要数据。

各主管部门根据本行业、领域实际，审核申报情况，对确认为重要数据的，应当及时向网络数据处理者告知或者公开发布，同时将相关网络数据处理者纳入到重要数据处理者名单。

第十三条　重要数据目录制定

各主管部门应当结合实际，按照下列方式之一组织开展本行业、领域重要数据目录制定工作：

（一）对照国家部委明确的本行业、领域重要数据目录，排摸掌握本行业、领域属地重要数据处理者底数及重要数据底数，形成我市本行业、领域重要数据目录；

（二）根据本行业、领域数据分类分级标准规范及重要数据识别规则或数据分类分级相关国家标准，组织本行业、领域数据处理者报送重要数据识别情况，形成我市本行业、领域重要数据目录；

（三）国家部委另行规定的重要数据目录制定方式。各部门应当结合实际，参照行业、领域重要数据目录制定方式，形成本部门重要数据目录。第

十四条　重要数据目录更新

各主管部门应当要求重要数据处理者在数据的业务属性、重要性和可能造成的危害程度发生变化时，重新开展重要数据识别，并上报变更情况。

各部门应当在本部门以及相关行业、领域数据重要程度和可能造成的危害程度变化、或重要数据处理者掌握数据发生变化时，更新本部门以及相关行业、领域重要数据目录。

第十五条　重要数据目录报告

各部门应当在重要数据目录制定完成或发生重大变化时，及时报告市网信部门。

第十六条　重要数据保护

重要数据处理者应当履行网络数据安全保护责任，明确网络数据安全负责人和网络数据安全管理机构，对重要数据进行重点保护。

重要数据处理者应当每年度对网络数据处理活动开展风险评估，并向主管部门报送风险评估报告，有关主管部门应当及时通报市网信部门、市公安部门。

各主管部门应当排摸掌握本行业、领域重要数据出境情况，涉及重要数据出境的，应当指导督促网络数据处理者通过市网信部门申报数据出境安全评估。

第四章　公共数据分类分级及开发利用

第十七条　公共数据分类分级

各部门在公共数据目录编制过程中，应当同步完成公共数据分类分级和重要公共数据识别，依托市大数据资源平台开展重要公共数据目录编制、上链工作。

公共数据中的重要数据目录，由各部门通过市大数据资源平台统一标记，并纳入本市公共数据统一管理。

第十八条　强化数据安全便捷共享

各部门应当按照相关规定，明确不同级别公共数据的共享应用场景、数据应用模式、共享方式，完善权限管理和审核机制，推动公共数据安全、便捷共享。

因数据分级需调整原有公共数据共享属性的，各部门应当提供依据，报市数据部门同意。

对于重要数据和较高级别的一般数据，各部门在确保安全可控的前提下，通过隐私计算、数据脱敏、匿名化等技术手段，可以依场景运用公共数据，充分促进数据要素流通利用。自然人、法人和非法人组织明确授权使用其公共数据的，应当按照授权依法提供。

第十九条　促进数据要素流通利用

纳入公共数据开放和授权运营范围的公共数据，应当优先完成数据分类分级和重要数据识别，

保障公共数据资源安全开发利用。

第五章 监督考核

第二十条　监督检查

市网信部门定期会同数据管理等相关部门开展网络数据安全检查，形成检查结果并进行通报，督促网络数据处理者做好网络数据分类分级相关工作。

各主管部门对本行业、领域数据分类分级、重要数据保护行为进行监督，确保网络数据处理者能够依照规定识别申报重要数据，并加强重点保护。

第二十一条　绩效考核

市网信部门综合运用日常监督和评估结果，将各部门网络数据分类分级和重要数据目录管理工作纳入绩效考核。

第六章 附则

第二十二条　保障措施

各区、各部门应当加强组织领导、资金投入、人才队伍建设和法律法规宣传，合理保障网络数据分类分级、重要数据目录管理工作。

第二十三条　解释

本办法由市网信部门、市数据部门负责解释。

第二十四条　实施时间

本办法自 年 月 日起施行。

地方动态 | 推进数据标注产业与人工智能协同发展

原载：“国家数据局”微信公众号

数据标注是对数据进行添加标记、说明、解释、分类和编码的过程。这一过程是提升人工智能算法与模型核心能力的关键环节。近日，我国首个数据标注产业专项规划——《合肥数据标注产业发展规划（2025—2027 年）》（以下简称《规划》）发布。

《规划》立足安徽合肥产业基础，以打造国际领先的数据标注创新基地为目标，为推进城市数字化转型提供核心支撑。”合肥市数据资源管理局党组成员、总工程师彭辉在接受科技日报记者采访时表示，预计到 2027 年底，合肥标注数据规模将达到 3000TB，产业规模突破 30 亿元，支撑相关产业规模迈上千亿元台阶。

产业优势与多元需求融合

位于合肥高新区的飞友科技有限公司，是一家深耕民航大数据的科技企业。3 月 30 日，该公司首席技术官朱睿向记者介绍：“以安全事件监管为例，传统的人工巡检和视频回放方式效率低下，实时性欠佳。然而，通过对航空器保障视频画面进行采集标注，我们可实现运行节点的自动提取和安全事件的实时监测，工作效率大大提高。”

“在合肥，还有许多类似的大数据企业，为相关行业政策的制定提供了‘源头活水’。”彭辉说，早在 2017 年，合肥就在全国率先启动大数据企业认定工作。目前，合肥市大数据企业存量达 2246 家，涌现出一大批行业领先者。

“合肥数据标注产业优势明显，相关企业也有迫切发展需求。”彭辉介绍，合肥依托人工智能、智能网联汽车等战略性新兴产业集聚优势，数据标注应用场景丰富。如科大讯飞等企业在人工智能数据标注方面，比亚迪、蔚来等智能网联汽车企业在自动驾驶数据标注等方面，为数据标注产业提供了多样化的业务场景。

此外，合肥地处人工智能产业集中的长三角区域，如上海、杭州等地的自动驾驶、金融科技产业对高质量标注数据需求旺盛。

截至目前，合肥的数据标注总规模已达 933.3TB，相关企业总数突破 35 家，数据标注总产值累计达 8.63 亿元，初步形成了覆盖数据采集、清洗、标注、应用的全链条产业生态。

为人工智能行业提供支撑

“如果把人工智能模型比作学生，那么数据标注员就是老师。”安徽飞数信息科技有限公司常务副总经理、合肥市数据产业协会秘书长谭昶形象地比喻道，标注员通过详细地标注数据，为模型提供准确的指导和示范，帮助模型认识不同的模式和特征。

“比如，我们为讯飞星火大模型标注了大量科普知识问答和评价数据。在这些‘老师’的指引下，模型逐渐学会了如何准确回答不同问题。”谭昶举

例说。

去年 4 月，全国数据工作会议提出，探索建设数据标注基地，充分发挥地方配套支撑作用，在数据标注产业的生态构建、能力提升和场景应用等方面先行先试，集聚龙头企业，促进区域人工智能产业生态发展。次月，国家数据局发布承担数据标注基地建设任务的首批城市名单，合肥位列其中。

“合肥的数据标注产业，已为人工智能产业发展提供了有力支撑。”彭辉介绍。2024 年 5 月，合肥启动建设“人机协同多模态众智标注平台”。目前，该平台开发进度达 90%，功能完备性实现 100%，技术指标处于行业前列。

另外，合肥围绕工业制造、医疗、教育、城市治理、地理信息等八大重点领域，构建了多模态数据标注服务体系，已为安徽省政务服务大模型、豆包大模型等 18 个大模型提供数据支撑。

“下一步，合肥将充分发挥区域优势，实现以合肥为总部基地，覆盖全省、服务长三角，推动形成数据标注产业与国家人工智能重大生产力协同发展的格局。”彭辉表示。

地方动态丨江苏省出台省级层面培育壮大数据企业专项政策

原载：“国家数据局”微信公众号

近日，省数据局、省委金融办、省发展改革委、省教育厅、省科技厅、省工业和信息化厅等 12 个部门，联合印发《江苏省培育壮大数据企业行动方案（2025-2027 年）》，这是继 2024 年国家发展改革委、国家数据局等部门印发《关于促进数据产业高质量发展的指导意见》、省政府办公厅印发《关于加快释放数据要素价值 培育壮大数据产业的意见》后，全国首个省级层面出台的培育壮大数据企业专项落实文件。

《方案》聚焦数据资源、数据技术、数据服务、数据应用、数据安全、数据基础设施等六类数据企业，提出持续开展“增、转、引、育”工作，实施鼓励新设独立经营主体、引导拓展新兴数据业务、加大数据企业招引力度、增强数据企业核心能力、营造数据企业良好发展环境等五大任务 20 条具体举措。到 2027 年，全省要建成 5 个数据产业创新联合体，打造 100 个数据企业应用场景优秀案例，培育 1000 家数据企业，形成 1000 个高质量数据集，打造 2000 个典型数据产品，建立 50 个数据产业公共服务示范平台，建立健全数据企业培育发展机制，初步形成各类企业融通发展的产业生态。

关于印发《江苏省培育壮大数据企业行动方案（2025-2027 年）》的通知

苏数发〔2025〕22 号

省各有关部门，各设区市数据局、市委金融办、市发展改革委、教育局、科技局、工业和信息化局、财政局、人力资源社会保障局、知识产权局、税务局、金融监管局，各省属企业：

现将《江苏省培育壮大数据企业行动方案（2025-2027 年）》印发给你们，请结合工作实际，认真组织实施。

江苏省数据局

中共江苏省委金融委员会办公室

江苏省发展和改革委员会

江苏省教育厅

江苏省科学技术厅

江苏省工业和信息化厅

江苏省财政厅

江苏省人力资源和社会保障厅

江苏省知识产权局

国家税务总局江苏省税务局

国家金融监督管理总局江苏监管局

中国证券监督管理委员会江苏监管局

2025 年 3 月 31 日

江苏省培育壮大数据企业行动方案

（2025-2027 年）

为落实省政府办公厅《关于加快释放数据要素价值 培育壮大数据产业的意见》，着力培育壮大经营主体，繁荣产业发展生态，制定本行动方案。

一、发展目标

坚持市场主导、创新驱动、特色发展的原则，聚焦数据资源、数据技术、数据服务、数据应用、

数据安全、数据基础设施等六类企业，持续开展数据企业“增、转、引、育”工作，推动国资国企、行业龙头等新设一批多元经营主体，引导一批传统企业拓展数据业务，招引一批国内外知名数据企业落地江苏。到 2027 年，全省建成 5 个数据产业创新联合体，打造 100 个数据企业应用场景优秀案例，引育 1000 家规上数据企业，形成 1000 个高质量数据集，打造 2000 个典型数据产品，建立 50 个数据产业公共服务示范平台，建设重点数据企业培育库，建立健全数据企业培育发展机制，初步形成各类企业融通发展的产业生态。

二、重点任务

（一）鼓励新设独立经营主体

1. 鼓励具备条件的省属企业设立专业化数据公司。完善国有企业数据治理运营体系，支持有条件的国有企业剥离数字化相关业务部门，通过新设、并购重组等方式成立数据公司，加强数据治理和创新应用。支持国有数据公司深度参与公共数据运营，协同各行业主管部门，提升数据供给能力。鼓励国有数据公司加强与中央企业合作，探索数据投资、数据授权等央地数据合作新模式。（责任单位：省国资委、省数据局）

2. 引导行业龙头、平台企业组建数据公司。鼓励行业龙头企业发挥产业链主导优势，成立一批专业性数据企业。支持产业互联网、网络销售、生活服务等平台企业发挥数据资源富集优势，组建独立的数据公司。（责任单位：省数据局、省发展改革委、省工业和信息化厅、省国资委、省市场监管局）

3. 支持高校院所孵化初创型数据企业。支持高校院所加速数据科研成果市场转化，筛选具有市场潜力的数据技术和服务创新项目，成立初创型数据企业。加强高校院所与行业龙头企业合作对接，联合建设数据技术推广应用中心和数据企业孵化中心。（责任单位：省教育厅、省科技厅、省数据局）

4. 开展数据企业认定评估。制定数据企业认定评估标准，开展数据企业认定和能力评估，定期公示我省数据企业培育和认定情况。建立重点数据企业培育库，定期遴选具有发展潜力的“种子企业”、拓展数据业务的“成长企业”和规模实力领先的“领航企业”。（责任单位：省数据局）

（二）引导拓展新兴数据业务

5. 支持系统集成、软件开发等企业拓展数据应用业务。引导系统集成企业聚焦优势行业领域，加强行业数据资源整合应用，打造具有行业特性的数据产品和服务品牌。鼓励软件开发企业加快从软件产品供应向数据价值创造转型，研发一批基于数据驱动决策的、面向大模型应用的数据产品。支持各类数字化转型服务企业发挥技术能力和市场资源优势，拓展行业数据应用。（责任单位：省工业和信息化厅、省数据局）

6. 支持网络安全企业拓展数据安全业务。推动网络安全龙头企业拓展面向动态防护要求的数据安全业务，丰富数据安全产品，构建覆盖数据全生命周期的综合业务体系。支持创新型中小企业聚焦数据可信流通技术，加快成长为技术基础好、市场占有率高、核心竞争力强的数据安全企业。（责任单位：省工业和信息化厅、省数据局、省委网信办、省通信管理局）

7. 支持数字基础设施企业拓展数据基础设施业务。鼓励基础电信运营企业发挥网络资源和技术优势，深度参与算网融合数字底座构建，助推全省一体化算力调度平台建设。引导传统信息技术企业强化在公有云、数据空间和低代码平台等领域研发投入和业务创新。支持省内数据基础设施企业参与国家数据基础设施试点任务。（责任单位：省数据局、省发展改革委、省工业和信息化厅、省通信管理局）

8. 支持传统第三方机构拓展数据服务业务。鼓励第三方服务机构开展数据咨询、数据保险、数据公证、合规认证、安全审计、质量评价、资产评估、争议仲裁、风险评估、人才培训等业务，发展数据流通交易新业态。推动法律、会计、审计和资产评估等机构面向数据资产化需求，提升专业服务能力。（责任单位：省委网信办、省数据局、省委金融办、省司法厅、省财政厅、江苏金融监管局）

（三）加大数据企业招引力度

9. 加强重点数据企业招引。聚焦先进存储、大模型、智能算法等领域，招引一批行业领先的数据技术企业。加快在智能制造、新能源、大健康等领域，招引一批聚焦细分行业的数据应用企业。聚焦数联网、数据空间建设需求，招引一批数据基础设施领域的头部企业。围绕数据动态安全防护需求，招引一批在区块链、隐私计算等领域具有竞争力的骨干企业。鼓励各地招引影响力大、实力强的省外数据企业在江苏设立综合型总部、区域总部、研发机构或数据服务基地等分支机构。（责任单位：省数据局）

10. 强化数据企业精准招引。制定全省数据产业图谱，支持有条件的地方建立健全数据企业招商清单，明确招商引资重点对象和招引计划，有针对性地开展招商推介活动。鼓励各地丰富数据企业招引政策，为重点数据企业招商项目提供“一对一”全程服务。发挥产业示范园区引领带动作用，提升数据企业招引效率。（责任单位：省数据局）（四）增强数据企业核心能力

11. 强化企业创新主体地位。鼓励数据企业强化智能计算、云原生、新型存储、数据标注、数据合成等核心技术研发攻关，聚焦隐私计算、区块链、数据空间、数场、数联网、数据元件等关键技术路线，构建自主可控的数据技术体系。支持符合条件的数据企业按规定享受研发费用加计扣除等税收优惠政策。支持龙头企业牵头组建产业创新联合体，推动龙头企业和创新联合体的研发项目纳入财政专项资金支持范围。加强数据企业知识产权保护，鼓励对经过一定算法加工、具有实用价值和智力成果属性的数据集申请数据知识产权登记，强化数据知识产权运用。（责任单位：省发展改革委、省科技厅、省工业和信息化厅、省财政厅、省数据局、国家税务总局江苏省税务局、省知识产权局）

12. 加强“人工智能+”企业培育。支持数据企业开展人工智能前沿技术研究和关键核心技术攻关，积极参与数据领域标准规范的研制和实施。支持各地引进培育参数量超千亿的通用大模型，推动人工智能技术在制造、交通、金融、医疗、教育等领域深度应用，加快培育一批融合行业数据集的人工智能大模型。（责任单位：省数据局、省发展改革委、省工业和信息化厅）

13. 提升企业专业服务水平。支持数据服务企业依托合规设立的数据交易场所，开展数据产品的上市辅导、上架保荐、发行报价以及数据发布、承销、交易撮合等业务。鼓励各地对场内数据服务企业给予交易补贴、服务补贴等激励举措。引导和推动第三方专业服务机构开展数据流通交易中介服务，提高服务水平。（责任单位：省数据局、省委金融办、省财政厅、省国资委）（五）营造数据企业良好发展环境

14. 打造高价值应用需求。支持数据企业开展“数据要素×”应用实践。面向党政机关、行业企业等征集高价值场景需求，并向数据企业公布。支持数据企业参加“数据要素×”大赛，鼓励场景需求方将需求策划为赛道方案，通过赛道机制遴选合作企业。（责任单位：省数据局）

15. 支持数据产品推广。支持行业协会等机构围绕我省重点行业，常态化开展细分行业数据产品供需对接活动。制定数据企业产品应用推广指导目录，对经认定进入目录的数据企业产品和服务，推动纳入政府采购支持科技创新政策范围。鼓励政府采购单位购买创新型数据产品和服务。鼓励国有企业等采购单位率先购买符合条件的数据产品和服务。（责任单位：省数据局、省发展改革委、省工业和信息化厅、省财政厅）

16. 强化用数用算支持。支持数据企业加强大模型研发应用，在政策允许范围内优先享受安全生产、信用服务、交通运输、医疗卫生、公共安全、社保就业等公共数据集支持。强化全省一体化算力调度平台建设运营，探索省级算力支持政策，降低数据企业用算成本。（责任单位：省数据局、省发展改革委、省工业和信息化厅、省通信管理局）

17. 拓宽企业融资渠道。强化“苏科贷”“苏知贷”“苏质贷”“人才贷”“苏服贷”“专精特新贷”等普惠金融产品对数据企业的供给。鼓励金

融机构创新开展以数据资产为核心的质押融资、保险保障等金融服务。做好数据企业上市后备梯队建设，鼓励符合条件的数据企业通过资本市场融资。充分发挥省数据产业和平台经济基金作用，支撑数据企业发展。鼓励市级产业基金参照执行，对符合条件的数据企业加大支持力度。（责任单位：省委金融办、省发展改革委、省科技厅、省工业和信息化厅、省财政厅、省数据局、人民银行江苏省分行、江苏金融监管局、江苏证监局）

18. 健全惠企利企政策。制定数据企业分类分策培育措施，综合利用财税等政策支持数据企业发展。畅通数据企业资质、试点等申报信息渠道，支持符合条件的数据企业申报认定国家重点软件企业、国家高新技术企业等，按规定享受相关优惠政策。探索设置数据企业监管执法“包容期”制度。鼓励各地结合本地实际，创新企业支持政策。（责任单位：省发展改革委、省科技厅、省工业和信息化厅、省数据局、省市场监管局）

19. 加强人才培养与引进。加大对数据领域人才的培养和引进力度，建立多层次、多渠道的人才培养体系。设立数字人才行业认证机制，开展数字职业技能等级认定。支持数据高技能人才与数字经济专业技术人才职业发展贯通。（责任单位：省人力资源和社会保障厅、省工业和信息化厅、省数据局）

20. 加快培育一体化数据市场。建立健全融入和服务全国一体化数据市场建设的基础制度、标准规范，推动数据市场设施互联、信息互通，统筹全省数据交易场所建设发展，形成全省“一个数据交易所、一套交易规则体系、一个数据交易系统”的格局。建设统一的公共资源交易公共服务系统，为各类交易和监管信息跨部门、跨地区共享提供数据通道和服务支撑，提升数据企业交易便利度。规范数据市场不当市场竞争和市场干预行为，加强数据领域重大政策措施会同审查，从源头防范妨碍统一市场和公平竞争的政策出台，为数据企业营造公平竞争的市场环境。（责任单位：省发展改革委、省市场监管局、省数据局）

三、保障措施

21. 加强统筹协调。充分发挥省数字经济发展部门统筹协调机制作用，健全跨地区、跨部门协同的数据企业培育发展机制，建立数据企业交流沟通制度，做好重点数据企业服务、关键技术攻关、典型产品推广等工作，协调推进重大项目，解决重大问题。鼓励高校院所、龙头企业、行业协会、产业联盟等开展数据产业基础理论和应用实践研究，定期发布江苏数据企业发展研究成果。（责任单位：省有关部门）

22. 强化合作推广。将数据企业培育纳入长三角数据专题合作机制，支持数据企业与国内头部数据交易机构开展合作，助力数据企业开拓省内外市场。搭建数据企业交流合作平台，支持数据企业利用展会、论坛、培训等重大平台展示优秀实践成果，宣传推广优秀数据企业和典型案例。（责任单位：省有关部门）。

（技术编辑：何芮）

研究动态

基础理论

1. 刑事数据调取的规范反思与优化

（刘文琦）

来源：《现代法学》2025 年第 1 期

刑事数据调取是常态化且效益显著的取证措施之一，涉及公民权利保护、侦查权力行使与平台协助义务三个方面。刑事电子数据规范从任意侦查的属性界定、调证文书相关性的干预范围控制，以及丰富性、绝对性与无偿性的调取配合义务三方面为数据调取构建规范框架，但上述规范在适用时存在以任意侦查替代强制侦查的权利失守缺陷、相关性约束失灵的权力扩张缺陷及配合主体陷入冲突困境的义务失衡缺陷。刑事数据调取规范缺陷的生成逻辑在于传统刑事诉讼权利保护体系无法因应新兴数据权利需求，入口型调取相关性规则的物理逻辑无法适配于虚拟场景，作为权力延伸的配合义务逻辑与案外第三方主体身份相矛盾这三个方面。优化刑事数据调取规范，应在导入个人信息权基础上对数据调取按强制属性进行分级，完善事前事后相关性的综合权力控制机制，构建协助调取的责任豁免与合理补偿机制。

2. 金融稳定风险防范的数据治理路径研究

（尚博文）

来源：《中国法律评论》2025 年第 2 期

数字化时代金融稳定风险面临着“数据鸿沟”，复杂金融市场与关联网络、数字金融创新的“破坏性”以及对金融危机事件中缺乏监管数据的反思显示出，金融稳定风险是金融数据收集短缺和无效利用引发的风险。“数据鸿沟”引发了金融监管内外部三个场景的权力失衡困境，是现有滞后、静态且单维的信息规制路径所致，有必要正确认识数据在政府治理和金融监管中的定位和功能，探索金融稳定风险防范的数据治理路径。从国际金融治理与美欧金融市场的监管实践来看，金融稳定数据治理以协同流通为原则，具备要素充足与互通共享的双层架构。应在金融法制定的契机下重构金融稳定风险防范与金融风险早期纠正制度体系，推动金融监管从信息规制走向数据治理路径，在权力失衡的三个场景中分别完善金融法治的约束、促进和协调。

3. 智能化金融市场系统性风险的法治应对——基于包容审慎监管的视角

（阳建勋）

来源：《财经法学》2025 年第 2 期

智能化金融是人工智能、大数据等新质生产力在金融领域应用而产生的创新性金融模式。鼓励、包容智能化金融发展是推动金融高质量发展和在金融领域发展新质生产力的现实需求，故应对智能化金融进行包容性监管。智能化金融面临“太大而不能倒”“过于关联而不能倒”“太快而无法挽救”等系统性风险挑战，守住不发生系统性风险的底线必须对其实施审慎监管。应当秉承包容审慎监管理念，完善智能化金融市场系统性风险监管法律制度，以实现金融安全、金融效率与金融公平之平衡。

4.打击数字仇恨言论：厘清欧盟的监管方法和障碍

（Evangelia Psychogiopoulou）

来源：German Law Journal, Vol.25,Issue 7 (2024)

数字平台和社交媒体拓展了个人行使言论自由权、获取和传播信息的途径。与此同时，它们也成为仇恨者表达和传播仇恨的主要手段，这在几年前是不可想象的。为应对这一挑战，欧盟逐步制定了一系列广泛的文书和工具，以打击网络仇恨言论。本章讨论了欧盟为打击数字仇恨言论所做安排的主要特点，揭示了这是一项多方面的艰巨监管任务。

5.欧洲健康数据空间--拟议的认证系统是否能有效防范网络威胁？ （Federica Casarosar）

来源：European Journal of Risk Regulation, Vol.15, Issue 4 (2024)

欧洲健康数据空间提案旨在创建一个共同空间，让个人可以通过可信和安全的方式控制自己的健康数据。其目的不仅在于改善医疗服务，还在于增加将健康数据用于研究和创新的机会。为了取得这些成果，该提案为欧洲健康记录系统以及健康设备和应用程序实施了一项强制性自我认证计划，设定了与互操作性和安全性相关的基本要求。虽然这是首次制定对所有成员国都具有强制性的横向框架，但立法提案中包含的安全要求还不够详细和全面。鉴于网络威胁日益增加，影响健康数据的安全事件可能会对患者的生命造成潜在影响，因此必须以最有效的方式采取和实施网络安全措施。本文将对欧洲健康数据空间提案进行分析，指出可能出现的未决问题和疑虑，并将其与拟议的《网络复原力法》进行比较，找出通过这一横向法规可能解决的问题和仍未解决的问题。

6.上瘾设计是一种不公平的商业行为：超吸引人的暗色图案案例

（Fabrizio Esposito, Thaís Maciel Cathoud Ferreira）

来源：European Journal of Risk Regulation, Vol.15, Issue 4 (2024)

这篇文章解释了为什么超吸引暗模式在欧盟应被视为非法，尽管它们在网上，尤其是在内容共享平台上非常普遍。超吸引模式是一种具有成瘾性设计的数字界面：它通过利用大数据分析和一种或多种行为特征，使用户花费更多时间与服务互动。超吸引人的黑暗模式是一种超软糖。它们利用多巴胺循环，降低用户的自主性，并可能对健康产生额外的有害影响。《反不正当商业行为指令》应被解释为将其作为一种不正当影响或根据第 5 条的一般测试予以禁止。《数字服务法》和《人工智能法》都可以在打击超吸引人的黑暗模式的传播方面发挥有益但只是补充的作用。

7.数字环境中的消费者决策自主权：重新理解国家法院评估违反公平商业惯例行为的义务

（Zanda Davida）

来源：European Journal of Risk Regulation, Vol.15, Issue 4 (2024)

数字化改变了商家在数字环境中影响消费者自主选择的可能性。欧盟的数字市场涉及多种商业行为，如暗箱操作、上瘾模式、目标广告和个性化等，这些行为会诱导消费者做出不利于他们的决定。2005 年不公平商业行为指令》的主要目的之一就是保护消费者的决策自由。然而，目前该指令在

数字环境中保障消费者选择权的能力还不够有效。本文通过禁止不公平商业行为的法律视角，分析了消费者法庭在数字环境中加强消费者决策自主权的可用手段。文章认为，禁止数字环境中不公平商业行为的法规应当现代化，在某些情况下，国家法院有义务依职权评估违反公平商业行为的行为，并颠倒论证和举证责任。

个人信息保护

1. 论个人数据交易的合法性审查义务

（程啸）

来源：《华东政法大学学报》2025 年第 2 期

个人数据交易的合法性审查是指当事人依据法律规定及合同约定所负有的对个人数据来源合法以及防止个人数据交易侵害个人信息权益的注意义务，具体包括两个层次：一是个人数据来源的合法性审查义务，即个人数据处理者负有保证其个人数据收集行为是合法的结果性义务，并对此负有证明责任；二是个人数据交易行为的合法性审查义务，即在个人数据转让、授权许可使用以及委托处理等各类个人数据交易活动中，转让人、许可人、委托人与受让人、被许可人、受托人依据《个人信息保护法》等法律法规负有的合法性审查义务。数据交易中介服务机构无法对数据来源合法性进行实质性审查，只要根据个案的情形可以认定其尽到相应的注意义务即可。明确个人数据交易中的合法性审查义务，有利于降低个人数据交易中当事人的认知难度，使人们的行为更具有可预期性并合理地确定法律责任，做到既能充分保护个人信息权益，又能促进个人数据的流通利用，助推我国网络信息科技与数字经济的发展。

2. 神经数据开放共享中的个人信息保护

（杨嘉祺）

来源：《华东政法大学学报》2025 年第 2 期

通过脑机接口技术系统收集到的神经数据本身具有生物识别能力，且从中可推断出与个人的健康状态、心理状态等相关的信息，应被界定为敏感且私密的个人信息。神经数据因具有高度的生物识别能力而面临匿名化难题，因此不能通过单一的匿名化技术与静态匿名化评估方法让神经数据自由流通，而应采取多种先进的隐私技术保护方法，对匿名化进行动态评估，实现匿名化数据与未匿名化数据之间的流动转换。对于未匿名化的神经数据，不能直接作为个人健康医疗数据进行开放共享，应考虑到神经数据的私人属性大于公共属性，通过订立数据共享协议的形式取得个人的书面同意，就经济利益的分配取得个人授权。对于数据的滥用，未来可考虑通过立法予以明确规制。

3. 处理者法律地位流变分析

（温昱）

来源：《政法论坛》2025 年第 2 期

处理者在个人信息处理法律关系中的法律地位会随着信息生命周期演进而发生变化。处理者的个保义务法律地位是由承担伦理基础作用的负担性义务、个人信息权对应的指向性义务以及法律直接规定的独立义务所组成的义务群。处理者数据财产权法律地位是由其个保义务法律地位转化而来。处理者取得数据财产权法律地位的道德辩护理由在于已经履行了在先的个保义务。处理者数据财产权法律地位的证立要在突破对处理者智慧劳动的事实描述基础上，提升其价值创造的规范品格。对个人信息权益的保护、特别是对人格利益的尊重，是处理者数据财产权的内在理由。

4. 已公开个人信息处理规则及其重构

（丁道勤）

来源：《政法论坛》2025 年第 2 期

已公开个人信息的不当处理易引发隐私保护、不正当竞争、侵害公民个人信息违法犯罪、数据安全和国家安全风险等法律问题，其具体处理与利用规则仍存在诸多有待明晰之处，如个人自行公开的范围和公开主体的判定存在一定难度、其处理是否需要符合“初始目的原则”、是否遵循一般个人信息的知情同意原则、大模型场景下如何维护公开个

人信息保护利用和公共利益平衡、未成年人公开信息的二次利用的风险防范等。因此，为促进已公开个人信息的流通利用，我国未来人工智能法在做好与民法典个人信息保护法等的衔接基础上，规定专门章节，从“上下文”善意目的限制原则、符合合理隐私期待、人格权益和未成年人优先保护、不产生实质性替代效果和 FRAND 授权原则、维护社会公共利益平衡等方面重构已公开个人信息处理利用规则。

5. 论敏感个人信息的界定标准

（张光明）

来源：《中国法律评论》2025 年第 2 期

《个人信息保护法》第 28 条第 1 款以“定义+列举”的方法对敏感个人信息进行界定。但上述立法定义仍较为模糊，需要进一步厘清其内涵和外延。对此，应在客观判断路径的基础上，基于法定类型诠释、处理场景要素和规范目的运用三重维度，进一步构建敏感个人信息的三重界定方法体系，以确保在规则弹性与可操作性之间实现平衡，并通过上述主要识别因素实现对敏感个人信息的准确界定。此种三重界定方法尊重实证法确立的评价体系，以处理场景的要素和规范目的运用作为补充，避免单一评价体系的不足，能够更好地平衡敏感个人信息的保护与利用之间的紧张关系。

数据确权与流通

1. 数据产权与交易法律制度研究

（程啸）

来源：《华东政法大学学报》2025 年第 2 期

随着数字经济的迅猛发展，数据作为新型生产要素的重要性日益凸显。数据的流通与利用不仅极大地推动了大数据、人工智能等科技创新和产业升级，也在如何构建科学合理的数据产权与数据交易制度以及加强个人数据保护方面带来越来越多的新情况与复杂问题。自 2022 年 12 月 2 日《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》颁布以来，法学界围绕着数据产权、数据要素流通与利用、数据要素收益分配制度以及数据要素治理制度等方面进行了卓有成效的研究，提出了很多新的观点，为我国数据基础制度的构建提供了有力的理论支撑。

2. 论数据持有权

（张素华）

来源：《华东政法大学学报》2025 年第 2 期

当前无论是欧盟还是中国，在数据权属制度上均以“数据持有权”为核心构建权利体系和规则，以此来沟通和协调数据生产、流通和利用过程中的利益冲突。就我国而言，应立足于数据产权结构性分置的政策框架，以数据产权“双阶二元结构”为理论基础来分析和建构数据持有权。在“双阶二元结构”中，数据持有权并非数据产权的一项权能，而是数据产权结构中的一项核心权利，具有中心地位，旨在确认和保障数据初始生产者对其合法持有数据予以自主管控和对外流通的能力。数据持有权既不同于数据生成时的数据来源者权，也区别于数据流通后的数据使用权，具有承上启下的功能。基于数据的来源和生成特征，数据持有权除在一般意义上表现为数据生产者享有的对数据以持有、使用、经营、收益等为内容的数据产权，在一些特定的生成场景中也表现为平行结构、代持结构和衍生结构等。

3. 数据可以占有吗?—兼论数据持有的法律构造

（阮神裕）

来源：《华东政法大学学报》2025 年第 2 期

数据占有论将数据持有视为物之占有，通过直接适用或者类推适用占有制度解决数据利用引发的纠纷，从而在不创设新型权利的前提下对数据提供较为全面的法律保护。然而，占有保护、占有的权利推定效力和善意取得以及多层次的占有关系无法准确适用于数据场景。数据占有论忽视了占有制度只能用于保护竞争性利益的隐藏条件。数据兼具竞争性利益和非竞争性利益，其中非竞争性利益无法通过占有制度得到调整。数据持有的法律构造

应当具备二元结构：一方面，数据的竞争性利益可以通过类推适用占有制度加以调整；另一方面，数据的非竞争性利益则应当通过建构以数据访问权为核心的法律制度加以调整。

4. 确权背景下数据产权的变动规则研究

（李东民）

来源：《法律适用》2025 年第 3 期

数据产权是区别于传统物权、债权与知识产权的新型财产权。数据产权的主体应区分数据来源者与数据处理者，其客体应限定为数据而非信息。数据来源者的数据所有权系基于事实行为而取得，登记非对抗或生效要件。数据资源持有权的首次登记可采登记对抗主义规则，移转数据产权时则采登记生效主义规则。但如果数据资源持有者为国家，则无须进行登记。对数据加工利用权、数据产品经营权的设立、变动与消灭，可采登记生效主义规则。对于登记制度的实现，可通过开设数据所有权账户实现数据所有权的登记，通过登记生效规则实现数据用益权的登记。

5. 公共领域视野下大模型数据使用行为的著作权定性 （黄汇翟、鹏威）

来源：《知识产权》2025 年第 1 期

大模型数据使用行为著作权定性的分歧突显了学理上对该问题之本质尚缺乏统一的认知，而公共领域的研究视角有助于实现从行为合理性的主观评估向客体合法性的客观判断推进。基于大模型产业分层的考量、利益市场的可分割性以及法效果评价的精准化目标，其著作权定性宜在公共领域视角下实施差异化规制。大模型数据训练的真实对象系非作者价值之元知识，对其使用未造成著作权法意义上可认知的损害，其应归入公共领域范畴。但在输出端，若大模型生成内容与训练作品构成实质性相似，则助长了著作权法的逆向激励，不利于著作权对公共领域反哺价值的实现，因此应受到著作权法的严格规制。最后，大模型模仿创作风格的行为则应视情况区分其究竟属于公共领域的利用行为抑或具有不正当竞争性质的搭便车行为，以合理划定其行为的合法性边界。

人工智能

1. 人工智能犯罪的刑法应对

（陈兴良）

来源：《国家检察官学院学报》2025 年第 2 期

人工智能浪潮正在席卷全球，我国高度重视人工智能在培育新质生产力、塑造新动能方向上发挥的重要作用。作为未来可能的颠覆性技术，人工智能在催生新产业、新模式、新动能，服务经济社会发展的同时，技术被滥用或者失控也给人类生命、财产、数据、隐私带来诸多风险。面对人工智能犯罪，需要刑法理论积极回应，明确刑法基本立场，调适刑法价值取向，提供破解涉及财产犯罪和经济犯罪的基本路径，助力人工智能驶向更加安全、有序、普惠人类社会的未来。

2. 生成式人工智能财产犯罪的特点与应对

（刘仁文）

来源：《国家检察官学院学报》2025 年第 2 期

近年来，生成式人工智能（Generative AI）研发取得突破，被视为可能是印刷术发明以来最具革命性的知识生产与传播技术。其主要的技术特征是通过深度学习和自然语言处理技术，从大量数据中学习潜在的规律和模式，从而生成类似于人类创作的内容。该项技术的演进及应用场景拓展将给人类生产生活方式带来深刻变革，对教育科研、工业制造、交通、娱乐等各个领域造成颠覆式重构，同时也引发了包括财产犯罪在内的多种犯罪形态和模式的演变与升级。依托深度学习和神经网络算法，聊天机器人 ChatGPT、人工智能绘画工具“中途”Midjourney、人工智能绘画工具“稳定扩散”Stable Diffusion 等人工智能 AI 工具在文本、图像和视频生成领域取得突破性进展，但这些技术也容易被恶意利用并引发各种犯罪。就财产犯罪而言，深度伪造（Deepfake）、合约操纵、精准诈骗等犯罪形式日益增加，给财产法益保护带来新的挑

战，凸显包括刑法在内的各种法律法规规范的紧迫性。

3. 人工智能时代的财产犯罪课题

（张明楷）

来源：《国家检察官学院学报》2025 年第 2 期

人工智能时代的到来，给财产犯罪的研究提出了许多课题。在现行刑法将财产犯罪的对象仅表述为“财物”的立法例之下，既存在如何合理确定财物范围的问题，也存在是采用“法律—经济的财产概念”还是采用“本权说—占有说”，抑或采取其他保护法益论的问题；随着财产类型的增加，对相关财产犯罪的构成要件行为需要重新界定；从立法论而言，刑法除规定骗免债务等明显不属于盗窃罪的诈骗犯罪外，能否将其他通过欺骗方法使他人交付、转移财产的行为都归入盗窃罪，形成广义的盗窃罪概念，也可以探讨；能否维持对个别财产的犯罪与对整体财产的犯罪的区分，财产损失的判断重点应否从客观价值转向主观价值，刑事立法应否仅规定行为类型而不设置数额规定，同样需要认真对待。

4. 人工智能迭代发展对财产犯罪刑事责任的影响

（刘宪权）

来源：《国家检察官学院学报》2025 年第 2 期

人工智能迭代发展对财产犯罪刑事责任的影响主要包括：财产犯罪侵害的法益内容（财产权）的扩充与确定，财产犯罪行为类型增加与行为性质认定，相关财产犯罪（或涉财产犯罪）刑事责任的分配与转移。根据“劳动—占有理论”的要旨，劳动是创造并合法拥有财富的基础。普通人工智能机器人在本质上属于权利主体通过劳动创造并拥有财产的工具，而不能成为实施劳动的主体。以生成式人工智能为代表的弱人工智能机器人可以成为创造财产的主体（即劳动主体），只是因时下尚不具备权利主体资格而无法享有相关财产权。弱人工智能的发展会对传统财产权的权利主体、权利客体以及权利内容变化造成重大影响。在强人工智能时代，我们应当逐步承认强人工智能机器人的权利主体以及责任主体地位。人工智能技术的迭代发展加速了万物数字化的进程。人工智能时代将会出现财产犯罪的新型犯罪对象（数字财产权），以及新型社会关系（基于数字财产的新型财产权关系）。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. 生成式人工智能服务中“信息错误”的民事责任

（郭金良）

来源：《政法论坛》2025 年第 2 期

作为人工智能技术的创新应用，ChatGPT 在生成成果上的创造性特征引发了社会的广泛关注，“信息”是服务的核心要素。在生成式人工智能服务提供过程中可能产生“信息错误”，包括训练数据的信息错误、技术缺陷导致的信息错误、服务使用者提示的信息错误以及服务提供者故意造成的信息错误。“信息错误”可能产生违约责任和侵权责任，传统民事责任规则的适用存在诸多法律困境，如 ChatGPT 是否具有法律责任主体资格的争论、违约行为认定标准模糊、侵权责任归责原则适用不合理、因果关系及损害的认定规则不清晰等。应当以民事责任控制理论为基础，重塑生成式人工智能服务民事责任制度。一方面，通过明确服务提供者与使用者之间的协议类型，明确不同“信息错误”情形下违约责任的规则适用；另一方面，侵权责任规则的塑造包括确立侵权责任归责原则分类适用规则，对不同类型的侵权行为确定差异化的因果关系认定规则，通过“其他合理方式计算”合理认定间接损害。

6. 生成式人工智能价值链行政监管与侵权责任的匹配

（谢尧雯）

来源：《政法论坛》2025 年第 2 期

生成式人工智能价值链具有多主体参与、机器自主学习的特征，法律规制需要实现行政监管与侵权责任的效率匹配。行政监管旨在预防系统性风险，为基础模型研发者、专业模型研发者、服务提

供者设定基础行为义务，增强价值链透明度，从而促进价值链各主体形成秩序互动与协同治理。行政监管设置的风险预防规则将影响侵权责任归责原则与构成要件的判定，侵权责任则需要发挥其获取场景信息的规制优势，弥补行政监管回应科技发展的制度缺陷。生成式人工智能服务提供者应适用产品责任，通过完善产品缺陷认定实现侵权与监管的衔接。法院以行政监管设置的绩效标准与内部管理型标准为框架，判断行业守则与标准是否符合合理技术设计要求，并激励行业层面不断完善自我规制、探寻最佳技术实践，实现软法与硬法的互动。

7. 人工智能法律治理的路径拓展

（张凌寒）

来源：《中国社会科学》2025 年第 1 期

人工智能的法律治理正处在规则形成期。基于风险的法律治理路径的“简单化”与人工智能法律治理需求“复杂化”存在矛盾，我国既有立法实践进行的本土化改良仍无法克服其固有局限。随着我国人工智能法律治理进入系统集成阶段，围绕实现人工智能高质量发展和高水平安全良性互动的治理主旨，要引入适应性治理理念统筹安全发展，应对人工智能多重属性构成复杂系统的治理需求，并高度容纳技术发展的不确定性和未知前景。在此基础上构建具有适应性的人工智能法律治理框架、方案、工具，拓展形成符合我国本土制度环境、技术产业基础与发展目标的法律治理路径。

8. 类型化视角下人工智能侵权责任的归结思

（刘成杰）

来源：《法律适用》2025 年第 3 期

随着人工智能的广泛应用，其侵权责任的归结对现行侵权法律制度提出了新的挑战。人工智能的可解释性，对于查明因果和合理归责至关重要。基于可解释的类型化方式，传统侵权理论的归责原则及现有法律框架足以因应当前人工智能侵权责任的归结问题。人工智能客体论视角下，“白箱”“灰箱”与“黑箱”三种类型的人工智能，依次可采取过错责任、过错推定与无过错责任的归责原则。同时，为有效平衡技术发展创新、赔偿受害方损失和维护公共利益之间的关系，应立足法律适应技术发展的原则和创新制度供给的维度，试点推动“黑箱”人工智能的法律主体化，尝试和观测其侵权责任的独立归结。

9. 续章与新篇：中国人工智能法治研究 2024 年度观察

（张凌寒、杨建军、文禹衡、程莹、郑志峰、赵精武、韩旭至、徐小奔）

来源：《法律适用》2025 年第 3 期

2024 年可视为中国人工智能法治研究的新元年，进一步夯实了人工智能法治研究的中国叙事结构和自主知识体系。在研究议题上，呈现出“续章出新篇”的特点。在“续章”方面，决策式人工智能（算法）持久不衰，人工智能生成内容的版权问题重者恒重，智慧司法、自动驾驶、具身智能和元宇宙等人工智能应用场景平分秋色，人工智能法律责任研究仍然侧重民刑。在“新篇”方面，生成式人工智能风险治理堪称学术热点，人工智能数据语料库建设成为焦点，人工智能法治进入研究元年。

10. 新科技革命背景下人工智能知识产权问题的立体因应 （单晓光）

来源：《知识产权》2025 年第 1 期

新科技革命引发了社会经济关系变化，必须探索新的利益平衡和激励机制。人工智能输入、处理和输出三个维度的知识产权问题既相互独立，又是一个立体整体。中国的因应方案要结合中国在新科技革命中的地位和国际竞争态势：在人工智能输入端依托数据资源优势，在优化推进数据资产，特别是数据知识产权登记基础上，构建数据和文本挖掘例外制度；在人工智能处理过程中调整公开性、软件技术性特征要求等专利授权条件，避免商业秘密无序扩张；对于人工智能输出端，绝对排除人类智力贡献的人工智能生成内容并不科学，赋予人类智

力贡献趋少直至极限值的人工智能生成内容相应知识产权，既是科技革命和社会发展的历史必然，也有利于维护我国在新科技革命中的竞争力。

11. 人工智能要素的政府供给：法理基础与制度因应 **（苏宇）**

来源：《财经法学》2025 年第 2 期

数据、算力与算法三要素对人工智能发展具有重要支撑作用。人工智能三要素均不同程度上具有公共物品属性，政府供给人工智能要素具备法理上的正当性基础。公共物品属性存在基于分享潜力效应和区分受益机制的两种消解途径，但非公共物品也在市场失能、市场缺位和资源依赖三种例外情形下需要政府供给。数据、算力与算法的公共物品属性和政府供给需求各不相同，政府供给机制亦须适应此种差别。法律应对政府供给机制作差异化授权，厘定政府供给人工智能要素的政策空间，并就政府供给的退出机制预作规定。

12. 论我国人工智能领域包容审慎监管的法治维度 **（黄锫）**

来源：《财经法学》2025 年第 2 期

包容审慎监管已逐步成为我国人工智能领域的主导性监管理念。人工智能技术具有的“破坏性创新”特征决定了包容审慎监管的法治理念内核。即“包容性监管”主要是为了呵护人工智能的创新性，促进我国人工智能技术与产业的快速发展，适用于人工智能发展中遭遇的法律规则突破与法律规则空白两种情形。“审慎性监管”主要是为了应对人工智能的破坏性，防范人工智能发展中对人的权益侵害的伴生风险，适用于人工智能导致的权益侵害广度扩张与深度拓展两种情形。实现包容性监管的法治路径主要包括：通过法律解释逸脱法律规则的适用范围、灵活运用从轻/减轻/不予处罚规则、设置法定观察期等。实现审慎性监管的法治路径主要包括：将监管沙盒制度与改革试验区模式结合运用、依法划定权益保护的安全红线、设定必要的从重处罚规则等。这些研究结论都可以为我国人工智能法的立法提供参考。

13. 论生成式人工智能服务提供者侵权损害赔偿 **（徐伟）**

来源：《财经法学》2025 年第 2 期

生成式人工智能侵害人格权是否会导致损害，须结合具体人格权类型加以判断。基于生成的侵权内容而发生的下游损害不应纳入服务提供者应承担的损害范围；潜在的再次生成侵权内容的损害需视再次发生的几率来决定是否予以赔偿。因被侵权人的损失和侵权人的获利难以准确计算，酌定赔偿或法定赔偿是确定赔偿金的主要方式。在生成阶段，服务提供者侵权的过错程度是过失，人机交互的侵权方式使得侵权影响范围往往有限，故服务提供者应承担的损害赔偿金不宜高，且通常也不应承担精神损害赔偿。消除影响、恢复名誉的责任承担方式在生成式人工智能场景中可以表现为服务提供者向接触过侵权内容的使用者推送澄清声明或专门开辟页面来发布澄清声明，且不宜再适用赔礼道歉。相较于传统损害赔偿理论，生成式人工智能侵权的特殊之处在于改变了事实基础、冲击了价值选择和影响了治理逻辑。

14. 在人工智能时代的算法社会中重新认识宪政 **（Matej Avbelj）**

来源：German Law Journal, Vol.25, Issue 7 (2024)

本文致力于探讨近代以来宪政所面临的最重大考验之一。它探讨了在我们这个新兴的算法社会中，人工智能（AI）影响下的深刻技术变革给宪政带来的理论和实践挑战。人工智能技术前所未有的迅猛发展不仅使传统的现代宪政理论变得过时，而且还造成了宪政理论中的认识论空白。因此，我们显然需要一种新的、令人信服的宪法理论，通过准确捕捉技术变革的规模、与之互动，并最终以一种在概念和规范上令人信服的方式对其做出回应，从而充分说明技术变革的规模。

15. 相互竞争的法律未来--从个人数据到人工智能的 "商品化赌注”

（Marco Giraudo, Eduard Fosch-Villaronga & Gianclaudio Malgieri）

来源：German Law Journal, Vol.25, Issue 7 (2024)

本文探讨了人工智能（AI）驱动的创新对各行各业的影响，强调了由此产生的法律不确定性。尽管人工智能在医疗保健、零售、金融等领域产生了变革性影响，但监管部门对这些发展的反应往往相互矛盾，导致人工智能业务的法律基础不透明。我们的文章指出了在法律不确定的情况下将人工智能工具商业化的普遍趋势，利用创新的合同解决方案来确保索赔。随着时间的推移，这些创新引发了被忽视的法律冲突，有时由于对一些基本权利和民主治理产生负面影响，导致对人工智能产品的直接禁止。我们这篇文章的核心论点是，过度依赖共同监管策略（如《欧洲人工智能法案》提出的策略）会加剧新兴技术市场的法律不稳定性。当替代性法律预期并存时，这种全景图创造了一个“扩展的法律现在”，从而导致经济和政治的不确定性，并可能在未来引发法律不稳定性。我们引入了“相互竞争的法律未来”这一概念，以说明在无法保证法律未来一定会实现的情况下，经济行为者如何必须将赌注押在法律未来上。为了帮助分析这一复杂的叙述，我们提出了一个理解法律、技术和经济动态的理论框架，强调了共同监管模式下市场交换的异常现象。尽管本文关注的是欧洲的发展，但其实践和理论影响却超越了欧盟，这使得本文与更广泛地理解人工智能和数字创新带来的法律-经济挑战息息相关。最后，我们提出了改正方向的论点，建议在不确定情况下对法律创新进行弹性治理的制度多样化。

16. 在人工智能调查员时代处理聊天数据

（Damir Kahvedžić）

来源：ERA Forum, Vol.25, Issue 4 (2024)

我们使用技术的方式正在改变数字取证和电子发现的面貌。过去的电子邮件现在变成了快速短信。过去是面谈，现在是录制视频和转录的 Zoom 通话。我们生成了大量的短信息，而不是过去的长篇传统文档。数据非常复杂，聊天记录与视频记录、图像、表情符号等紧密相关。电子取证和数字取证领域不能再依赖团队手动审查这些数据的能力。传统上，自动化流程会忽略聊天记录，也不是针对其复杂性而设计的。然而，就在问题的规模变得难以承受时，计算机辅助审查工作流和流程的发展提供了帮助。法律领域已经开始利用最先进的分类和文档摘要算法来迎接生成式人工智能革命。本文追溯了聊天数据的演变过程、聊天数据如何以及为何成为法律领域的难题，以及如何利用 GenAI 提供帮助。

平台治理

1. 论消费者滥用网络评价行为的合作规制

（林慰曾）

来源：《华东政法大学学报》2025 年第 2 期

消费者滥用网络评价的行为扰乱了互联网市场的竞争秩序，不利于网络评价信息与经营者信用之间的互动形成良性循环。我国现行法律体系要求经营者不得雇佣消费者从事美化或虚假评价行为，但相关规定忽视了消费者作为评价主体的互助关系与消费者对交易秩序的社会责任。互联网平台通过构建经营者与消费者双向、多维度的评价体系，制定消费者网络评价的主体与行为规范，提供替代性争议解决机制，填补了消费者滥用网络评价的责任疏漏。实践中逐渐形成了平台主导初次规制、行政机关主导后续规制的合作规制模式。该模式对消费者滥用网络评价的行为进行了分类处置，符合大众预期和比例原则，能推动多元主体合作治理。为了进一步发挥合作规制的积极作用，一方面需要明确不同主体在规范消费者网络评价领域的职能分工，另一方面需要优化平台规制、行政规制以及司法裁判之间的衔接，引导消费者通过网络评价合理行使监督权，完善互联网市场良性竞争的长效机制。

2. 生成式人工智能平台的著作权侵权责任

（熊琦）

来源：《环球法律评论》2025 年第 2 期

在生成式人工智能平台如何承担著作权侵权责任的问题上，由于我国相关治理文件中未能对提供内容与提供服务加以明确区分，致使平台在主体属性和归责事由上出现法源选择和适用的双重难题。根据域外和我国长期适用“避风港”规则的司法经验，法院一般以类推适用信息存储空间服务提供者版权侵权认定规则涵摄新兴网络服务提供者类型。虽然生成式人工智能平台在内容来源、生成过程和使用方式等方面都不同于传统的信息存储空间和搜索链接服务，但在著作权侵权责任的认定上，仍有必要类推适用。就主体定位而言，在现有法律体系内，生成式人工智能平台仍属于网络服务提供者的范围。对于事前必要措施和事后必要措施的解释，一方面当特定提示语和侵权内容之间出现稳定复现时，可将修改相关模型参数纳入必要措施范围；另一方面在延续适用“通知—必要措施”的基础上针对合规通知的侵权内容中涉及他人作品的部分，增加内容标注义务。

3. 平台经济时代用人者责任制度的反思与完善

（田野）

来源：《现代法学》2025 年第 1 期

平台经济领域损害事故频发，如何认定和分配用人者责任成为难题。在新的时代背景下对平台用人者责任的正当性基础加以反思和再定位，一方面应肯定算法控制亦是一种有效的用人控制，另一方面应识别平台企业运营给社会带来的增量风险及其组织体过失。平台用人者责任背后的用人关系的性质有待厘清，用人关系不限于劳动（雇佣）关系，在新的“劳动三分法”下不完全劳动关系亦可构成用人关系。劳动者依托平台自主经营型的民事关系通常不构成用人关系，但也存在例外。执行工作任务的认定应结合平台劳动的特点，依据内在关联标准，以类型化视角展开。对于平台经济场景下涉多数用人者的责任分配难题，应创造性地采取用工共同体思想，平台企业与合作者形成分工协同的统一组织网络，应共担用人者责任。即使在业务外包之后，平台企业基于算法管理仍然对劳动者保有一定的控制，应承担与其过错相应的补充责任。

4. 知识产权侵权平台责任论：从被动免责到主动治理

（彭学龙、刘小威）

来源：《知识产权》2024 年第 12 期

在电子商务蓬勃发展的数字时代，避风港规则预设的适用场景已不复存在。以先进网络科技为支撑的电商平台远非昔日技术中立的传输通道和存储空间。得益于智能科技，平台过滤和预防知识产权侵权的能力极大提升。平台内经营者均属具备相应资质、资本的注册用户，平台制止侵权的紧迫性远不如侵犯网络著作权的案件。因此，对于平台内经营者知识产权侵权，平台应否承担帮助侵权责任，其裁判理当回归传统的过错责任原则，“红旗标准”和“通知—删除”规则可在过错认定中发挥重要的辅助作用。只要直接侵权者能够被查证并具备赔偿能力，法院就应判令其承担全部赔偿责任。作为敦促平台经营者加强平台治理的连带责任，只能在极其例外的情形下适用。

5. 短视频二次创作使用作品合法性危机的化解方案

（孙山）

来源：《知识产权》2024 年第 12 期

平台用户未经许可使用他人作品进行二次创作所面临的合法性危机，已经成为短视频产业发展的焦点法律问题之一。在我国现行法框架下，绝大多数未经许可使用他人作品进行二次创作的行为既不构成合理使用，也不属于法定许可。连接著作权人、集体管理组织和平台用户的短视频平台企业是解决问题的关键。短视频平台企业兼具经营者和管理者双重身份，应将维持产业的生态平衡定位为其经营目标及管理计划的重要组成部分。在“效率优先”的作品创作场景下，具有营利性质的平台用户二次创作行为只能由法定许可制度进行规制。因此，我国应创设法定许可为主的作品利用方式以便在提升短视频产业运行效率的同时，有效化解二次创作使用作品的合法性危机。

6. 版权过滤认定为“必要措施”的解释论反思与矫正 （焦和平、梁龙坤）

来源：《知识产权》2025 年第 1 期

“通知—删除”规则是网络版权治理的重要制度。司法实践和理论研究中均有观点认为，该规则中的“必要措施”包含版权过滤这一防范侵权措施，由此导致网络服务提供者的版权过滤义务有进一步法定化解释的趋势。但在解释论视角下，法律适用中将“必要措施”解释为包含版权过滤，存在超越“必要措施”涵摄范围、改变法律条文体系定位、特殊规则普遍适用和架空“反通知”规范的意义等问题。合理解释“必要措施”，应从遵循体系解释规则、维护立法的体系设定、防范衍生普遍义务和受到“反通知”规则的限制四个方面把握。依循这一解释进路，应反思和调整“必要措施”的法律解释路径，以防范法律解释的合理空间异化为径行创设义务的造法风险。

7. 网络企业对网络用户版权侵权的替代责任 （吴伟光）

来源：《知识产权》2025 年第 1 期

Web 1.0 时代的“安全港与通知—删除”责任模式已经不适应 web 2.0 时代的网络环境了。Web 2.0 时代的平台已经成为非中立的、复杂的和功能性的社会组织，网络企业对平台内网络用户的行为有很强的控制和管理能力，应该对网络用户的版权侵权行为承担替代责任，网络用户不再是版权侵权的直接责任主体而只是平台内规章的执行者。网络企业的替代责任应该受到一定限制，履行了注意义务的网络企业应该减免其赔偿责任。网络企业承担替代责任使得版权法恢复专业性法律的特征，网络用户不再受到版权侵权责任的困扰。网络企业承担替代责任有利于促进其承担更高的版权保护义务，并将版权人对版权保护的外部要求转变为平台的内部规范，实现版权保护的自治与共治相呼应的局面。

8. 让系统性风险评估发挥作用：DSA 如何创造良性循环以应对内容节制的社会危害 （Niklas Eder）

来源：German Law Journal, Vol.25, Issue 7 (2024)

欧盟的《数字服务法案》（DSA）引入了一种新的监管方法，以解决在线平台的社会危害问题：系统风险评估。虽然系统风险评估是《数字服务法案》的核心组成部分，但该法规只是概括性地概述了系统风险评估的标准和流程。目前仍不清楚这些系统性风险评估在实践中的具体内容。本文就如何实施系统性风险评估提出了建议。它将系统性风险评估定位为实现平台问责制的关键一步，因为它们能解决社会危害问题，而现有的方法，如补救机制，只能保护用户权利。风险评估涉及无形伤害以及对言论和公共话语的监管，也带来了重大挑战。内容节制监管的传统参照点，如条款和条件、契约自由、基本权利和专业知识，并不能为具体化风险评估义务提供切实可行的合法依据。欧盟委员会等公共行为者也应避免界定实质性标准，因为他们直接受言论自由保障的约束。本文认为，欧盟委员会应建立一个程序性框架，即一个 “良性循环”，赋予公民社会权力，使其能够随着时间的推移明确和完善系统性风险的标准。在这一框架的基础上，文章解释了系统性风险评估如何修复 “多方利益相关者主义”，而“多方利益相关者主义 ”又如何帮助系统性风险评估发挥作用。

9. 宪法反射器？评估 Meta 监督委员会中的社会宪政和数字宪政 （Lucas Henrique Muniz Da Conceição）

来源：Global Constitutionalism, Vol.13, Issue 3 (2024)

本文探讨了宪法叙事在社交媒体平台治理中的应用，涉及数字宪政的概念。文章旨在阐明数字宪政如何在平台中体现，以及对这些治理环境民主化的影响。文章认为，数字宪政主义揭示了平台治理的三个目标：（1）在私人领域类比应用宪法价值；（2）渗透到多个规范性层面的意识形态框架；以及（3）将监管工作与基本价值对称起来的政策考虑。

这三个目标都以自由和规范的宪政方法为基础，脱离了宪政民主核心的政治和社会考量。文章认为，在考虑社交媒体平台的跨国性及其用户的本地化问题时，这会导致广泛的合法性问题。本文认为，（数字）宪政的社会视角必须指导该机构的目标和程序，以促进合法性和问责制。这种社会视角揭示了既定自我参照系统的可靠性问题。它还允许对公司制定的新兴社会宪法中传统宪法原则的混合进行分析。

数字行政与司法

1. 上海范式：数字检察的定位与展开

（盛勇强）

来源：《国家检察官学院学报》2025 年第 2 期

在中国式现代化、数字中国建设和社会治理数字化转型背景下，对数字检察的内涵和外延需要在理论上不断深入研究。对标数字中国建设和《中共中央关于加强新时代检察机关法律监督工作的意见》要求，对标社会治理数字化转型方向和数字检察的现实需求，对数字检察的认识，应回归中国式现代化、数字中国建设背景中深化；应基于检察权内涵，以及数据赋能的广度和深度来界定；应当从数字检察本体、数字检察的核心要素、数字检察运行体系三个方面展开。由此数字检察是以数据要素驱动检察履职方式、运行体系的系统性、革命性重塑，是涵盖四大检察履职以及党务、政务、队伍建设等在内的检察工作全方位、立体式数字化转型。在建设路径上，围绕数据生产与采集、汇聚与治理、应用与赋能的数据全生命周期推进建设，同时从组织架构、制度供给、运维体系、安全防范、队伍建设等方面完善数字检察配套运行体系，支撑数字检察建设行稳致远。

虚拟财产

1. 刑事涉案虚拟货币的制度化处置

（陈如超）

来源：《中国刑事法杂志》2025 年第 1 期

公安机关先行处置涉案虚拟货币面临实践合理性与制度合法性矛盾。这一矛盾逐渐驱使公安机关倾向采取涉案虚拟货币的间接处置模式，即要求、允许犯罪嫌疑人直接委托第三方公司到境外处置涉案虚拟货币。间接处置模式虽然形式上表现为犯罪嫌疑人与第三方公司的委托代理关系，但实质上仍主要由公安机关主导控制涉案虚拟货币的处置过程。然而，公安机关主导之下的间接处置模式在涉案虚拟货币处置的启动、实施、监督等环节存在结构性问题，并且忽略了犯罪嫌疑人的实质参与性与其他主体的过程监督性。基于实践合理性与制度合法性的双重逻辑，侦查阶段公安机关对涉案虚拟货币的先行处置，应当实现处置规则明确、犯罪嫌疑人充分参与、其他主体有效监督的制度化机制。

（技术编辑：李佳丽、麻卓妍）

教研活动

第二届科技与法治论坛成功举办

3 月 30 日，由北京市司法局主办，北京市科委中关村管委会、清华大学法学院联合主办的 2025 中关村论坛科技与法治论坛在中关村展示中心举办。本次论坛旨在展示科技法治领域的最新发展成果，精准对接创新主体的法治诉求与期待，推动科技与法治的协同进步，为构建更加公平、高效、普惠的科技发展环境贡献法治力量。

第二届科技与法治论坛现场

北京市政府副秘书长尹航向莅临论坛的各位嘉宾表示热烈欢迎，他介绍了北京市发展科技与法治的优势与使命，对大力发展新质生产力，不断推进科技治理体系和治理能力现代化，以法治方式引领、规范、促进和保障科技创新提出了构想。

北京市政府副秘书长 尹航

中国科学院院士、清华大学化学系教授、博士生导师王梅祥向长期支持、关心中国科技与法治事业发展的同仁致以诚挚的感谢，希望科技法治与科技学术形成合力，鼓励科技工作者在创新突破中怀揣法治信仰，法律工作者在社会治理中拥抱科技思维，将科技创新的蓬勃动力与法治建设的坚实保障深度融合。

中国科学院院士、清华大学化学系教授、博士生导师王 梅祥

北京市司法局党委书记、局长崔杨代表市司法局向各位领导和嘉宾的到来表示热烈欢迎和诚挚感谢，期待通过这一平台，聚焦“推动基础研究高质量发展”“优化前沿科技治理体系”“提升科技发展普惠性”等关键议题深入探讨，以全球视野凝聚共识，为构建包容、安全、创新的科技治理生态贡献智慧。

北京市司法局党委书记、局长 崔杨

为更好地建设国家高水平科技智库，支撑首都科技法治建设，护航首都高质量发展，北京市司法局与清华大学法学院签订共同推动科技法治创新发展的合作备忘录。双方将按照“优势互补、共建共享、互利共赢”的原则，在平台建设、法治发展、智库咨询、人才培养等方面开展长期合作。

立法解读

在立法解读环节，主办方邀请行业专家对《国家自然科学基金条例》进行解读。

《国家自然科学基金条例》于 2025 年正式实施，共 7 章 45 条，这一条例为进一步强化基础研究，增强自主创新能力，培养科学技术人才，规范国家自然科学基金的使用与管理，进一步发展新质生产力培育新动能，加快实现高水平科技自立自强提供了坚实的法治保障。国家自然科学基金委员会地球学科部常务副主任、计划与政策局副局长姚玉鹏围绕确立科学基金资助原则和导向、健全管理体制、完善资助制度、加强科研诚信建设等方面对条例内容进行了立法解读。

国家自然科学基金委员会地球学科部常务副主任、计划与政策局副局长 姚玉鹏

主旨演讲

在主旨演讲环节，论坛邀请了 7 位科技法治实务工作者国内外专家学者科技企业代表等展开深入研讨。

第十四届全国人大常委会委员、宪法和法律委员会副主任委员、清华大学法学院院长**周光权**讲述了科技法治的中国经验及未来展望。北京化工大学教授、英国皇家化学会会士**戴伟**（David Geraint Evans）分享了优化科技治理体系，提升科技普惠性的相关思考。北京市科学技术委员会、中关村科技园区管理委员会副主任**张宇蕾**围绕以科技立法护航基础研究高质量发展进行演讲。北京知识产权法院副院长**宋鱼水**围绕以优质专业化审判赋能新质生产力发展，与大家进行分享。北京市人民检察院第四分院检察长**刘惠**以法治护航数智经济新时代为题进行演讲。奇安信集团副总裁**段继平**分享了 AI+安全方案助力人工智能治理的相关构想。小米集团产业标准研究部总经理、集团技术委员会办公室主任**周珏嘉**以支持基础研究发展、提升原始创新能力为题，与大家进行分享。

主题探讨

在主题探讨环节，两位主持人和七位嘉宾围绕“人工智能时代的法治探索”主题分别展开分享。

清华大学法学院党委书记、教授**邓海峰**作为本环节第一部分主持人，从人工智能技术和应用角度对相关嘉宾的发言进行了点评，并分享了相关思考。香港中文大学法学院前院长、教授、中英法律对比研究专家**邬枫**(Lutz-ChristianWolff)围绕人工智能在法学教育领域的应用可行性及可控性探究，与大家进行了分享。北京大学法学院教授、北京大学电子商务法研究中心主任**薛军**分享了促进数字经济发展的基础性法律制度思考。伦敦大学法学院副院长、副教授、科技法律领域专家**迈克尔·维勒**(Michael Veale)分享了欧盟人工智能监管的挑战、《人工智能法案》及其未来的展望。中国人民大学法学院教授、未来法治研究院副院长**丁晓东**围绕建构人工智能促进型的数据制度作了分享。

清华大学法学院教授、知识产权法研究中心主任**崔国斌**作为本环节第二部分主持人，从知识产权法律实务角度对相关嘉宾的发言进行了点评，并分享了相关思考。天普大学-清华天普中国项目主任、教授**麦泰伦**(Tarrant Mahony)分享了《联合国国际贸易销售合同公约》规范下的软件合同相关思考。北京市律协数字经济与人工智能领域法律专业委员会主任**朱芸阳**分享了政务领域人工智能应用探索及法律规范指引的相关内容。清华大学智能法治研究院院长、法学院教授**申卫星**分享了中国人工智能立法的路径和重点问题。

圆桌与谈

“自动驾驶汽车法治实践”圆桌与谈环节邀请专家大咖齐聚一堂共话发展。

与谈由清华大学法学院党委书记、教授**邓海峰**主持，中国科学院科技战略咨询研究院研究员**肖尤丹**、北京市经济和信息化局研究室（政策法规处）主任**祝珺**、清华大学法学院教授**余凌云**、公安部道路交通安全研究中心法规室副主任**黄金晶**、文远知行副总裁**罗琳**分别围绕主题展开交流研讨，集聚智慧、凝聚共识。

与谈现场

在全球化浪潮下，中国与世界紧密相连，相互依存。北京市司法局通过中关村论坛这一平台和桥梁，积极拓展科技法治领域的国际交流，来自不同国家、不同文化背景的专家学者汇聚，群策群力，分享经验，为科技创新发展提出了集聚多方智慧的法治对策。

相关政府部门负责同志，立法、司法、研发机构等科技法治实务工作者，国内外知名专家学者，企业代表，高校师生代表等共 400 余人参加论坛。

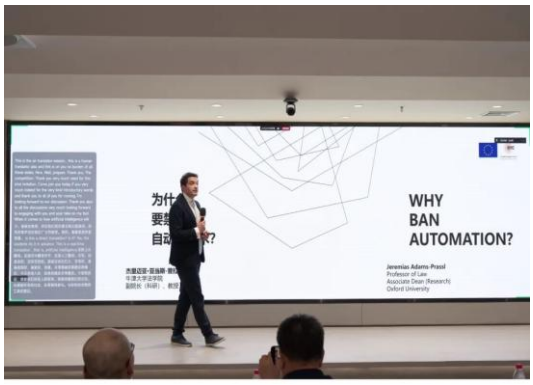
“人工智能将如何重塑法律版图”讲座顺利举行

2025 年 3 月 26 日下午，中国政法大学博士后学术前沿系列讲座第二十六讲——“人工智能将如何重塑法律版图”在海淀校区综合楼 209 顺利举行。本次讲座由杰里迈亚·亚当斯-普拉斯尔教授主讲，叶逸群博士主持。中国政法大学副校长、数据法治研究院院长时建中出席讲座并发表致辞。参与本次讲座的嘉宾既包括来自牛津大学、北京大学、中国政法大学的学者，亦包括来自科技行业和政府机构等部门的代表，专业知识涵盖宪法、劳动法、网络法、经济学和社会学等领域。

在致辞环节，时建中教授指出“人工智能对法律的重塑”主要源于两个方面：一是其对经济和社会发展的重塑，引发生产力革命，进而促使生产关系和社会关系变革，改变了法律调整的对象；二是人工智能对法治工作各环节的赋能，为法治建设提供了新工具，在数字化时代，法学研究有了新对象和新工具。

时建中教授发表致辞

在主讲环节，牛津大学法学教授杰里迈亚·亚当斯-普拉斯尔（JeremlasAdams-Prassl）担任本次讲座的主讲人。他以“为什么要禁止自动化？”（WhyBanAutomation?）为主题展开演讲，深入探讨法律体系中“人类的决策”这一核心要素。通过研究计算机科学文献与法律文献，普拉斯尔教授探究在高维计算世界里人类决策的权利与意义。他介绍了为禁止自动化决策提出的人工介入环节（Humansintheloop）概念及其争议焦点，还详细解读了法律规范对自动化决策的禁止，如欧盟《通用数据保护条例》（GDPR）第 22 条。尽管该条款存在模糊性并引发诸多难题，但可参考欧盟法院相关判例加以理解。普拉斯尔教授认为，应超越现有规定，针对不同领域制定具体规范，明确自动化决策的边界与保障措施，并介绍了欧盟《平台工作指令》在这方面的实践。



牛津大学法学教授

杰里迈亚·亚当斯-普拉斯尔（JeremiasAdams-Prassl）

在与谈环节，学者们从不同角度对演讲内容进行反思与提问，涵盖人工智能决策与人类决策的差异、法律规定中的原则与例外、劳动法研究的拓展、言论自由与内容管制、自动化决策的效率与监管、法律体系中人类与机器的关系等多个方面。

与谈现场

北京大学法学院副教授**胡凌**提出了两点反思：一是人工智能与人类决策的结构性差异尚不明确，二者决策情况有相似处，严格限制自动化决策的必要性有待探讨；二是个人数据保护涉及财产和责任问题，应务实平衡数据处理与面临的挑战。

北京大学法学院副教授**阎天**提出了两个问题：一是关于《通用数据保护条例》第 22 条中禁止自动化决策的原则与例外，这些例外及具体规定或破坏法律完整性，该条款规则是否受衡平法管辖等需探讨；二是能否将工作场所法律与劳动法研究相连接以促进学科发展，构建普遍法律原则。

北京大学法学院副教授**左亦鲁**讨论了人工智能时代言论自由和内容管制问题，指出传统言论监管特点在新时代改变，人类介入自动化决策或致更糟结果，机器和算法在内容审核上或更优。对此，普拉斯尔教授回应：一是明确人类特定与机器驱动问题，强调人类代理在法律体系中的核心地位；二是指出人们利用技术复杂性逃避责任给法律体系带来挑战；三是新兴领域规则制定要有技术意义；四是自动化决策在内容审核上因可改善人工审核环境而受青睐。

中国政法大学法学院副教授**沈伟伟**提出了两个问题：一是担心严格监管自动化决策会降低效率，询问欧盟及欧洲各国是否有类似减少监管的声音；二是探讨具体领域规定能否推广形成一般性理论。

中国政法大学数据法治研究院讲师**王申**从经济学视角进行了思考，认为关键挑战是理解法律体系中人类与机器关系及冲突时的决策权，算法与人类竞争体现在法律人格、决定人类情感、决策效率与公平等层面，可引入人类竞争约束人工智能决策，共同设计法律体系。

中国政法大学人权研究院讲师**王也**从社会学和法学视角指出了矛盾，即追求自动化决策高效又想用人类监督，现阶段更倾向人类决策，因其有回顾反思能力，还提出自动化决策监督、透明度及算法解释对象的问题。对此，普拉斯尔教授再次回应：一是法律执行要平衡效率与风险，不同场景出错成本不同；二是机器意识创造力取决于意识定义；三是协调机器与人类决策关系；四是自动化决策解释对象及解释权存在争议，相关研究不足。

此次讲座为与会者提供了多元视角，以理解人工智能技术带来的法律冲击，促进了学界与业界对相关问题的深入交流与思考，对推动人工智能与法律领域的交叉研究具有积极意义。

“人工智能将如何重塑法律版图”讲座圆满结束

俄罗斯国立人文大学法学院院长、俄罗斯前副总理谢尔盖·沙赫赖到访中国政法大学数据法治实验室

2025 年 4 月 7 日下午，俄罗斯国立人文大学法学院院长、俄罗斯前副总理谢尔盖·沙赫赖（Sergey M. Shakhray）到访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，与中国政法大学副校长、数据法治研究院院长时建中，数据法治研究院教授王立梅，数据法治研究院教师王煜婷等进行交流。

交流会成员合影

时建中教授对沙赫赖院长到访数据法治实验室表达热烈欢迎，并详细介绍了中国政法大学数据法治实验室的研究成果。他指出，当前数据已成为重要生产要素，数据法治实验室作为教育部首批哲学社会科学实验室，聚焦数据安全、个人信息保护、数据主权、数据权属等新兴法律问题，区别于对传统法律的研究，通过实验的方法探索数字化时代下的法律问题。

交流会现场

沙赫赖院长对时建中教授的欢迎表示感谢，并高度赞赏了数据法治实验室在新兴法律问题上的研究范式创新。他分享了俄罗斯的大学在法律与其他学科融合建设上的经验，并欢迎中国政法大学派出更多的学者进行访问与学习等活动。

此后，王立梅教授针对司法系统的数字化这一主题进行了分享。她指出中国司法数字化实践以《最高人民法院关于规范和加强人工智能司法应用的意见》为指引，明确司法系统中人工智能技术“辅助法官办案、提升司法效率”的核心定位，通过数据赋能实现司法流程的智能化升级。

会后，双方相互赠送书籍，并期待进一步的交流与合作。

交流会圆满结束

北京数字司法与数据合规调研巡礼

为了及时了解数字司法、数据合规的最新实践创新动态，深入推进数字法治理论研究，华东政法

大学数字法治研究院与黑龙江大学数字法治研究院于 2025 年 3 月 24-25 日前往中国司法大数据研究院、京东集团总部、人民法院出版社进行学习调研。

华东政法大学数字法治研究院院长马长山教授，华东政法大学科研处处长陆宇峰教授，华东政法大学法治中国战略研究院杨显滨教授、张迪副研究员，华东政法大学数字法治研究院副院长张文龙副教授、副院长韩旭至副教授、李莉特聘研究员，黑龙江大学数字法治研究院副院长邓齐滨教授，黑龙江大学俄罗斯研究院副院长宫楠副教授，黑龙江大学法学院潘丹丹副教授、卢艳玲、牛丹彤、赵国谚老师，上海政法学院余圣琪老师参加了此次调研活动。

在中国司法大数据研究院的调研活动中，研究院社会治理发展研究部部长李俊慧，互联网司法研究中心副主任李一帆，互联网司法研究中心法律研究员王瑜与调研组进行了深入的研讨交流，会上李一帆副主任讲解了司法大数据的开发利用情况和研究体系，马长山教授针对大模型伦理风险的法律控制做了理论介绍。双方就涉人工智能相关法律问题进行了充分交流。

中国司法大数据研究院的调研活动现场

在京东数据合规调研的活动中，京东集团法律研究院执行院长李丽、副院长何忠凯、秘书长徐迪，京东科技法律合规部负责人郑慧媛，京东科技首席数据合规官潘景燕，京东科技法律合规部高级法律顾问韩绮霄，京东科技法律合规部法律顾问桑田，京东集团知识产权顾问马悦红、李欣博与调研组进行了深入的座谈对话，会上就金融数据合规、隐私合规检测、人工智能治理框架等问题展开了深入讨论和交流。

京东数据合规的调研活动现场

在人民法院出版社的调研活动中，人民法院出版社总编辑助理、人民法院电子音像出版社常务副总编辑张承兵，人民法院出版社编审、丛书编辑部兼《数字法治》编辑部主任兰丽专，人民法院电子音像出版社副社长石鹏，人民法院出版社副编审、《数字法治》编辑部主任助理黄晓云，《数字法治》期刊编辑周利航，人民法院电子音像出版社新媒体营销中心副主任张艳华与调研组进行了深入的对话交流，会上就法答网、法信网、法信法律基座大模型的建设与运行等问题进行了充分的探讨。

人民法院出版社的调研活动现场

通过本次深度调研，调研团队深刻认识到我国数字司法与数据合规建设中所彰显的创新引领性与体系重塑性，并从中洞悉到数字法治领域具有范式意义的核心理论命题。此次调研活动在数字法学理论建构与智慧司法实践探索间架设起了对话桥梁，形成了产学研深度融合的良性互动机制，取得

了良好的效果。

第三届人工智能法治论坛在广州举行

由中国法学会网络与信息法学研究会主办，广东财经大学法学院承办的第三届人工智能法治论坛 29 日在广州举行，主题为“新质生产力与人工智能：环球视野下的法治融合发展”。

论坛开幕式由中国法学会网络与信息法学研究会常务副会长兼秘书长、中国社会科学院法学研究所研究员周汉华主持。广东财经大学党委书记郑贤操，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，广东省法学会专职副会长兼秘书长金艳致辞。

论坛特别设置“成果发布”环节，彰显了理论研究与实践应用的深度融合。在广东财经大学副校长鲁晓明的主持下，先后由中国法学会网络与信息法学研究会常务副秘书长、中国社会科学院法学研究所网络与信息法研究室副主任（主持工作）周辉发布《人工智能示范法 3.0》，广州互联网法院院长宋伟莉发布《广州互联网法院关于以高质量司法服务保障粤港澳大湾区可信数据空间建设的意见》。

论坛“主题演讲”环节由中国社会科学院学部委员、法学研究所研究员、《法学研究》主编陈甦主持。澳门特别行政区个人资料保护局局长杨崇蔚、香港特别行政区助理个人资料私隐专员王雅媛、腾讯公司副总裁徐炎、深圳大学大数据系统计算技术国家工程实验室特聘研究员潘颖慧先后以《人工智能与个人信息保护——澳门特区个人资料保护监管当局视角初探》《在人工智能时代保障个人资料私隐：香港视角》《人工智能时代著作权的挑战与机遇：腾讯的实践与思考》《人工智能与法律的共生演进》为题作主旨演讲。当日下午，会议分为十个分论坛和一个青年论坛继续展开。

与会的政产学研媒各界专家代表一致认为，当前人工智能技术快速发展，为社会带来巨大挑战，也带来了新的机遇，应当立足中国国情，借鉴国际经验，加强人工智能法治研究和应用，推动制度创新，促进人工智能健康发展，为新质生产力发展提供有力法治保障。

技术编辑：林诗敏

数字法评

作为举报治理的通知删除：避风港规则反思

此处删除了原文脚注，全文请参见《法学评论》2025 年第 2 期，转载或引用请注明出处。

作者：丁晓东

摘要：以通知删除规则为核心的避风港制度存在挑战。其制度存在不同版本，其适用可能存在冲突，其各方权益保护存在紧张。这些挑战的根本原因在于典型的平台间接侵权具有大规模治理型侵权的特征，区别于传统的二对一共同侵权，也无法被分割为独立的个体性传统共同侵权。只有在平台特定参与个案的少数情形中，平台间接侵权才类似传统共同侵权。在典型的平台间接侵权中，通知删除规则具有举报治理的特征，即应将平台收到的通知视为举报，将其采取措施视为针对举报的治理机制。避风港制度应进行重构，无论是通知要求、平台接到通知后的反通知等措施，还是平台采取的通知删除、通知过滤等措施，不同版本的制度都无必然优劣，都应根据平台治理需求与特征而设计。法律也应给予平台以通知删除的自治性空间，当法律对平台规则进行规制时，其干预应使平台利益与社会利益对齐。

一、问题的提出：避风港规则的挑战

在网络平台间接侵权中，通知删除规则与避风港制度已经被广泛接受。1998 年，美国《数字千年版权法案》（DMCA）在著作权间接侵权领域确立了以通知删除规则为核心的避风港制度，[1]对欧盟与我国等全球网络间接侵权产生重要影响。2006 年，我国立法在《信息网络传播权保护条例》中首次引入通知删除规则；[2]2009 年，我国《侵权责任法》（《民法典》生效后废止）将通知删除规则确立为网络侵权的一般规则。2018 年《电子商务法》将通知删除规则适用于电子商务平台经营者，并进一步增加了反通知规则。2020 年编撰《民法典》也增加了反通知规则，并进一步将完善后的通知删除规则上升为网络间接侵权的一般规则。在欧盟，欧盟 2000 年制定的《电子商务指令》第 14 条也引入了通知删除规则，将这一规则作为网络平台间接侵权的一般规则。[3]在全球特别是在我国，通知删除规则已经基本等同于避风港制度，成为网络平台间接侵权的核心制度。[4]

不过在制度与原理上，通知删除规则都面临一系列问题与挑战，通知删除规则存在很多不同版本，其规则存在不确定性。例如在权利人发出通知后，平台可能对疑似侵权内容进行删除，但也可能出于多种原因而不采取行动。在其他情形中，平台则可能会在删除的基础上，进一步过滤可能重复侵权的内容。其次，通知删除规则还可能存在制度冲突问题，例如我国《电子商务法》的通知删除规则就与《信息网络传播权保护条例》的通知删除规则存在差异。最后，通知删除规则常常存在对各方利益保护难以平衡的问题。一方面，有观点认为现行通知删除规则对权利人的保护不足、对平台施加责任过轻；另一方面，也有观点认为通知删除规则对权利人保护过度、对平台施加责任过重。通知删除规则常常陷于保护各方利益左右为难的境地。

本文对避风港制度面临的问题进行分析，指出问题的关键是如何理解通知删除规则。一种方式是按照传统共同侵权来理解通知删除规则，按照这种理解，权利人在发出通知后，平台即已经对第三方侵权知情，与第三方侵权者成为共同侵权方。不过本文指出，此类理解只适用于具有特定个案特征的侵权，例如平台选择将某个未获版权授权的热播电影推至主页。对于大部分典型的平台间接侵权，权利人通知并不能使平台与第三方侵权者成为共同侵权方。因为典型的平台间接侵权具有大规模治理型侵权特征，平台在接到权利人通知后不仅要预防个案侵权，同时要从整体平台治理、维护平台内多方主体的整体利益出发进行应对。基于典型平台间接侵权的这种特征，本文指出通知删除规则应被视为一种举报治理机制。从举报治理机制出发，本文对通知规则的具体制度进行全生命周期的分析，同

时对通知删除规则的平台自治与国家介入关系进行分析。从平台侵权的大规模治理特征与通知删除规则的举报治理属性出发，避风港规则面临的困境可以迎刃而解。

二、问题的展开与分析：避风港规则的困境

通知删除规则存在很多不同版本，这些不同版本的通知删除规则不仅面临制度适用冲突的问题，而且面临制度适用与权益冲突的问题。

（一）不同版本的通知删除

首先，通知删除规则对通知要求有不同规定。美国《数字千年版权法案》512 条款（c）（3）（A）规定，合格的通知必须满足六项条件：版权人的签名；被指控受到侵犯的版权作品的识别标识；被指控侵权的内容及其定位；通知者的联系方式；未获授权的善意证明；通知准确性说明以及授权证明。[5]而我国的相关法律法规则有不同规定。例如《信息网络传播权保护条例》第 16 条列举了通知的三项要求：“（一）权利人的姓名（名称）、联系方式和地址；（二）要求删除或者断开链接的侵权作品、表演、录音录像制品的名称和网络地址；（三）构成侵权的初步证明材料”，并要求“权利人应当对通知书的真实性负责”。《电子商务法》第 42 条规定，“通知应当包括构成侵权的初步证据”。2020 年《民法典》第 1195 条则规定“通知应当包括构成侵权的初步证据及权利人的真实身份信息”的要求。2020 年最高人民法院印发《关于审理涉电子商务平台知识产权民事案件的指导意见》则对《电子商务法》的通知要求进行细化规定，其第 5 条规定向电子商务平台经营者发出的通知一般包括：“知识产权权利证明及权利人的真实身份信息；能够实现准确定位的被诉侵权商品或者服务信息；构成侵权的初步证据；通知真实性的书面保证等。通知应当采取书面形式”。但其第 4 条也同时规定，电子商务平台经营者在不会“对当事人依法维护权利的行为设置不合理的条件或者障碍”的前提下，“可以根据知识产权权利类型、商品或者服务的特点等，制定平台内通知与声明机制的具体执行措施”。

其次，通知删除规则对于平台接到通知后应当采取的反通知等措施有不同规定。美国《数字千年版权法案》512 条款规定了反通知程序，即在平台接到权利人通知和将该通知转达被通知人后，被通知人可以提出抗辩，主张自己并无侵权。[6]这一规则在我国的若干法律法规中均被引入，[7]但也存在多个不同版本。[8]例如《信息网络传播权保护条例》第 16、17 条规定，被通知人在提供符合要求的反通知书面说明后，网络服务提供者应该“应当立即恢复被删除的作品、表演、录音录像制品，或者可以恢复与被断开的作品、表演、录音录像制品的链接，同时将服务对象的书面说明转送权利人”，而且“权利人不得再通知网络服务提供者删除该作品、表演、录音录像制品，或者断开与该作品、表演、录音录像制品的链接”。《电子商务法》第 43 条规定，电子商务平台经营者在接到反通知声明后，“应当将该声明转送发出通知的知识产权权利人，并告知其可以向有关主管部门投诉或者向人民法院起诉。电子商务平台经营者在转送声明到达知识产权权利人后十五日内，未收到权利人已经投诉或者起诉通知的，应当及时终止所采取的措施。”《民法典》第 1196 条则将 15 日的规定修改为“合理期限内”，《最高人民法院关于涉网络知识产权侵权纠纷几个法律适用问题的批复》（以下简称《网络知识产权批复》）则将平台采取措施的时限规定为 20 日。比较相关法律与司法政策，可以发现平台终止措施与恢复相关内容的时间越短，其对被通知方的保护越强，时间越长则对通知方的保护越强。

最后，通知删除规则对于平台最终采取的删除等必要措施有不同规定。美国《数字千年版权法案》512 条款所规定的删除，其实更为准确地表述为“移除或断开链接”（remove，or disable access），[9]本身就包含了两种不同措施。我国《信息网络传播权保护条例》采取了类似的“删除”与“断开链接”的表述。《侵权责任法》第 36 条与《民法典》第 1195、1197 条则规定了“删除、屏蔽、断开链接等必要措施”，而《电子商务法》第 42、45 条则除了规定“删除、屏蔽、断开链接”，还规定了“终

止交易和服务等必要措施”。而欧盟在 2019 年制定的《数字单一市场版权指令》（CDSM Directive）则明确了在著作权与网络传播权领域引入“通知—过滤”规则（notice-staydown），要求“在线内容共享服务提供商”（online content-sharing service providers）“在收到权利人充分证实的通知后，迅速采取行动，禁止访问或从其网站上删除所通知的作品或其他主题”，“并尽最大努力防止其未来上传”。[10]显然，不同版本的“必要措施”对于被控侵权方以及平台所施加的责任不同。如果必要措施仅仅只限于“删除”“断开链接”或单次的“终止交易和服务”，那么侵权方将仍然能够享有其他网络服务，但也可能继续上传侵权内容。相反，如果必要措施指的是通过过滤而屏蔽相关内容或主体，甚至永久性“终止交易和服务”，那么侵权方的内容将不能重复上传，但侵权方也可能同时被过滤内容，甚至被封禁账户和 IP。

（二）制度适用与权益冲突

不同版本的通知删除规则首先带来了制度适用的冲突问题。以我国《信息网络传播权保护条例》《电子商务法》《民法典》中的相关规定为例，如果采取“下位法服从上位法”的原则，则三部法律的适用性应当按照逐渐递增进行排序。但如果遵循“特殊法优先于一般法”的原则，三者又呈现逐级递减的排序。如果再考虑最高人民法院《关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》（以下简称《信息网络传播权司法解释》）、《关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》（以下简称《网络人身权益司法解释》）、《关于审理涉电子商务平台知识产权民事案件的指导意见》（以下简称《电商知识产权指导意见》）、《网络知识产权批复》的相关规定，不同版本通知删除规则的冲突问题将会更为复杂。

不同版本的通知删除规则还面临权益冲突的两难。一方面，法律对于通知要求越低、对反通知及其前后所采取措施的要求越高、对平台所采取删除等必要措施要求越严厉，通知删除规则对于权利人的权利保护水平就越高，但对其他主体的干预程度就越大。另一方面，法律对于通知要求越高，对于反通知及其前后所采取措施的要求越低、对平台所采取删除等必要措施要求越宽松，其对于权利人的权利保护水平就越低，但对其他主体的干预程度就越小。[11]就通知要求而言，有的通知可能是非权利人发出的通知，还有的通知可能仅仅是疑似侵权。当法律认定此类通知也符合通知要求，平台在删除真实侵权内容的同时，也很可能误删实际并不侵权的内容。就反通知及其前后所采取措施而言，当平台提高反通知要求，延长平台恢复被删内容的时间间隔，法律对于权利人的保护就越有利，但也可能导致并不侵权的内容无法得到及时恢复。就删除等必要措施而言，当平台采取“过滤”甚至“终止交易和服务等必要措施”等严厉要求时，其对于权利人的保护程度就更高，但此类措施也会误伤非实际侵权的用户，或者对普通侵权用户施加过重的惩罚措施。综合而言，通知删除规则常常需要平衡平台、权利人、（疑似）侵权者、普通用户之间的关系。通知删除规则甚至可能需要平衡权利人的权利保护程度问题，因为对于一些非绝对性权利，允许少量侵权可能对于权利人更为有利。例如在特定情形下，少量的著作权侵权可能会促进作品的传播和扩大作品影响力，为著作权人带来更大版权与非版权收益。

在人工智能算法执行的背景下，上述问题将更为复杂。在通知删除的各个不同环节，参与的主体都可能是机器而非人类主体。[12]就通知而言，实证研究发现，大量通知都是由权利主体或非权利主体利用机器人自动批量发出，而非由权利主体个人发出。[13]同样，平台所采取的处理措施也主要依赖于算法实施，通过技术实施避风港规则，[14]仅在少量案件中采取人工审核的方式。在通知之前，平台就可能采取“自动化内容识别系统”（automated content recognition，ACR）对平台内疑似侵权的内容进行过滤。[15]在接到通知后，平台也常常利用算法进行自动化执法，例如根据侵权内容的侵权概率保留或删除相关内容。[16]算法自动化执法可以大大

提高平台的执法效率，但其准确率却存在不同情形。在有的情形下，算法自动化执法可以比人类更准确地识别与区分侵权与非侵权内容，从而合理删除或保留相关内容。但在其他情形下，算法自动化执法可能不如人类执法准确，如大面积误删或错误保留相关内容。[17]算法在平台执法过程中如何平衡各方利益，已经成为学术界关注的焦点。[18]

三、原理分析：通知删除的两种性质

破解通知删除规则的挑战与困境，需要在原理层面对这一规则的性质进行分析。通知删除规则既可以被理解为二对一的传统共同侵权制度，也可以被理解为平台大规模治理中的举报治理制度。

（一）作为传统共同侵权的通知删除

将通知删除规则视为传统共同侵权的一部分，这意味着将平台视为与传统个案侵权中的共同侵权者相同的角色。此种观点认为，平台面对平台内海量的侵权内容与用户行为，难以对其进行一一审查与防范，平台在很多时候可能扮演消极的媒介或中介（intermediary）角色。但在通知删除规则之下，经过被侵权方的通知或提醒，平台的角色就应当不再是消极的媒介或中介，而是积极或消极参与侵权的共谋者。这就像在传统共同侵权中，间接侵权人可能以作为或不作为的方式参与侵权，例如为直接侵权人提供侵权工具，或者放任直接侵权人的侵权行为。

在此种视角下，通知删除规则可以视为传统共同侵权制度的组成部分。关于传统共同侵权，我国《民法典》第 1168 条规定：“二人以上共同实施侵权行为，造成他人损害的，应当承担连带责任”；第 1169 条规定：“教唆、帮助他人实施侵权行为的，应当与行为人承担连带责任”。第 1168 条与第 1169 条将被视为网络间接侵权的一般条款。而《民法典》第 1195 条、1196 条以及其他法律法规关于通知、反通知与必要措施的规定则可以被视为传统共同侵权下的组成部分。甚至《民法典》第 1197 条也可以视为传统共同侵权在网络领域的适用，第 1197 条规定：“网络服务提供者知道或者应当知道网络用户利用其网络服务侵害他人民事权益，未采取必要措施的，与该网络用户承担连带责任”。在传统共同侵权的视角下，第 1197 条即是第 1168 条与第 1169 条的延伸，只不过其中的共同侵权人被明确为“网络服务提供者”。域外的通知删除制度亦是如此。无论是美国《数字千年版权法案》512 条款，还是欧盟《电子商务指令》第 14 条规定，都可以被视为对传统共同侵权制度的编撰或重述。[19]

不过将通知删除视为共同侵权制度的一部分，并不符合避风港制度的初衷或原始含义。避风港制度以通知删除规则为核心进行制度设计，其核心在于免除或减少平台责任，即只要平台履行了通知删除规则下的相关义务，其侵权责任就肯定可以获得豁免。[20]平台如果接到通知后不履行相关义务，也未必会承担侵权责任，只是其无法得到避风港规则的庇护。[21]《美国千年版权法案》512 条款的原名即为《网络版权侵权责任限制法》（Online Copyright Infringement Liability Limitation Act），清晰地表明了避风港规则的意图与含义。此外，《美国千年版权法案》512 条款还明确规定，“实质上不符合版权所有者或授权代表版权所有者的人发出的通知”，不应被用于“确定服务提供商是否实际知道或意识到明显存在侵权活动的事实或情况”。[22]在普通共同侵权中，如果间接侵权人接到被侵权人的提醒，即使此类提醒在证据上并不确凿，间接侵权人也会因为提醒而处于对个案知情状态，应当承担合理的注意义务。但在避风港规则之下，平台在接到通知人的不适格通知后，其状态并未从对特定个案的不知情转化为对特定个案的知情。

只有在少量特定、孤立的侵权案件中，才可以将通知删除规则视为共同侵权制度的一部分。例如当平台与直接侵权者合谋，推送某一未获许可的版权作品，或者平台故意无视其首页所推荐的某一未获许可的热播影视，此类侵权形态具有个案性、可剥离性。当平台接到权利人通知后，平台就在个案性中扮演了直接或间接侵权的角色，应当承担较高的注意义务与预防责任。在此类案件中，平台所扮演的角色与一般共同侵权中的共同侵权人所扮演的角色具有相似性，平台所收到的通知也与传统共

同侵权中的被侵权人收到的提醒无异。当平台“知道或者应当知道”平台内存在侵权，没有及时采取必要措施，平台就应当对个案中的侵权承担连带责任。

（二）作为举报治理的通知删除

在典型的平台间接侵权中，平台在第三方侵权中所扮演的角色是大规模治理性的。首先，平台只是一般性地引起平台间接侵权案件，或一般性地与平台间接侵权案件相关。无论是平台积极作为还是消极不作为，平台间接侵权都不能拆分和剥离为一个个单独的侵权案件。这并不是说平台没有可能对每一个平台间接侵权案件进行处理，平台当然可以雇佣足够多的管理人员，在每一个间接侵权案件中尽到合理的注意义务。但这显然不符合平台的特征与一般做法。面对大规模与海量的平台侵权案件，平台不可能对每一个个案采取不同的注意义务与预防措施。即使平台采取完全人工化的审核措施，平台所采取的措施在机制上也只能是统一性，即通过对审核人员对培训而实现平台治理的标准化。在算法实施的背景下，平台所采取的措施则更具有统一性、标准化的特征。只有在上文提到的平台特定参与某个侵权案件的情形中，平台的角色才会转化为特定侵权者的角色。

其次，平台在间接侵权案件中所考虑的权益也是大规模治理性的。在平台间接侵权中，平台不仅要考虑对侵权个案中的相关主体的利益，即不仅要考虑预防侵权与维护被控侵权人的行动自由之间的平衡，而且还必须考虑其采取措施对于平台的整体性影响。例如平台为了保护著作权人免受重复侵权，引入算法过滤机制，对任何可能存在重复侵权的作品进行过滤。就预防重复侵权而言，此种措施可能在个案型侵权中具有合理性，因为平台在这类侵权中可以扮演“最小成本避免者”（least cost avoider）的角色，可以以最小的成本避免具有恶性性质的重复侵权事故发生。[23]但在平台间接侵权中，引入此类过滤机制虽然可以避免重复侵权，但也可能过滤掉大量本属于非侵权或合理使用的用户作品，对平台内很多合法合规活动产生附带伤害（collateral harm）。[24]之所以会带来此类问题，其原因在于平台所采取的措施是大规模治理性的，其采取的措施不仅涉及侵权个案中的相关主体，而且涉及平台的整体利益。

从平台间接侵权的特征出发，通知删除规则就应当被视为平台大规模治理中的一环。在典型的平台间接侵权中，平台在接到权利人通知后，其所采取的各类措施并不是针对个案的侵权预防，而是在平台整体治理原则下设置统一的程序性处理机制。[25]从性质上看，这种程序性处理机制可以类比为举报治理机制。在大规模治理中，治理者或管理者也会收到海量侵权举报，例如有的侵权举报可能会针对言论诽谤、有的侵权举报可能会针对知识产权侵权，还有的举报可能针对人身财产侵害。面对此类举报，治理者并不会在收到举报后就转变为个案中的共同侵权人角色。治理者可能介入个案，例如要求个人停止人身财产侵害。但即使治理者介入个案和采取必要措施，此时这种个案中的必要措施也是综合考虑其整体治理的必要性。例如治理者可能认为，权利人所举报的侵害较为严重、[26]其侵害行为较为容易辨别、采取必要措施并不会妨碍其他合法活动。对于权利人的举报，治理者完全可以选择不介入个案。治理者也可能认为，相关举报的真实性存疑、侵权的实际概率较低；如果治理者介入个案侵权，可能会逆向激励不实举报，威胁与妨碍大量合法活动。治理者还可能认为，被举报的侵权行为危害性不大，举报方直接对被控侵权人提起侵权诉讼更为合理；如果治理者直接处理这类举报，将会导致治理者直接用事前规制替代事后侵权救济。[27]

从举报治理的角度看待侵权，在工业化时代的产品责任中就已经初现端倪。传统侵权法以损害、过错、因果关系为要件，以损害补偿为主要目标，其制度之所以如此设计，就是因为传统侵权主要应对一对一或小型社会的特定侵权。但在现代工业化社会，随着工业化生产所带来的产品事故等大规模侵权问题的出现，[28]产品责任等特殊侵权制度开始替代传统侵权制度，引发了传统侵权法“城堡的崩溃”（the fall of the citadel）。[29]在工业化时代的

产品责任侵权、环境侵权、食品安全侵权等侵权形态中，诉讼人的角色不仅仅是个案侵权中需要被救济的个体，而且也扮演了私人总检察长（private attorney general）的角色，承担了事故风险预防的举报角色。[30]相应的，侵权诉讼也不再仅仅具有个案救济与损害补偿的功能，而是同时发挥了社会治理功能。[31]

不过在平台间接侵权中，通知删除规则的举报治理特征更为明显。一方面，平台在间接侵权中所扮演的角色并非首要侵权者，其本身并未像产品责任侵权、环境侵权、食品安全侵权等侵权形态中的企业那样直接参与侵权。另一方面，相比产品责任侵权、环境侵权、食品安全侵权，平台对于平台内的主体又具有更强的管理能力，平台与平台内主体之间的关系更接近管理关系而非平等主体之间的关系。综合而言，平台更像是对于平台内主体之间侵权与争议的一个居中裁决者与治理者。当平台收到权利人的投诉，其采取的措施类似于大规模治理主体权衡利弊之后采取的措施。[32]

（三）小结：通知删除规则的两种性质

本节的分析表明，通知删除规则可以作两种理解。一方面，通知删除规则可以被视为传统共同侵权制度的组成部分。平台在接到通知后，就与疑似被侵权方构成共同侵权。另一方面，通知删除规则也可以被视为举报治理机制，平台在接到通知后并采取措施，类似于接到举报机制并对平台进行整体性治理。在平台间接侵权中，只有少量特定孤立型的平台间接侵权属于前者。[33]绝大部分的典型平台间接侵权则都属于后者，在此类侵权中，平台在其中扮演了大规模、整体性参与的角色，平台所参与的侵权不能被切分为独立的个体性共同侵权。[34]

四、通知删除规则的制度重构

从通知删除规则的举报治理属性出发，可以对通知删除规则进行制度重构。该部分的通知删除规则并没有标准版本，其制度设计取决于是否适合某类侵权的特性以及不同规则如何搭配。

（一）平台未获通知下的法律责任

首先需要指出，在平台没有收到权利人通知的情形中，平台也可能需要承担责任。一种情形是本文所提到的个案型侵权，例如平台首页推送未获版权授权的热映电影。在此类情形中，即使平台没有收到通知，平台也应被视为在特定侵权个案中具有故意或过失，应当对第三方侵权承担故意侵权责任。另一种情形则是本文所提到的大规模治理型侵权。如果平台在此类情形中未收到权利人通知，权利人直接向法院提起诉讼要求平台承担共同侵权责任，此时平台的责任应当视其是否尽到了大规模治理义务来判断。如果平台在治理意义上已经尽到合理注意义务，则平台可以免责。相反，如果平台在治理意义上未尽到合理注意义务，例如平台内存在大量侵权，平台本来可以很轻易地减少侵权、并且不会影响平台内正常活动，那么此时平台应当承担治理责任。[35]就治理责任的形式而言，平台应当根据其治理过错而承担相应的行政罚款数额。在平台没有受到相应行政罚款的背景下，则法律可以要求平台将其应罚款的数额分配给平台内提起或可能提起诉讼的受害主体，作为这些主体进行举报的“悬赏”（bounty）。

（二）对权利人通知的要求

对于权利人通知或举报，平台应根据平台治理特征而设定合理要求。一方面，平台对于通知或举报的真实性要求不应过低，[36]要求过低将导致平台内主体提起大量真实性存疑的通知或举报。这不仅会给平台大量的审查与辨识成本，而且会让真正受到侵权的权利人无法得到及时救济，让很多并未侵权用户以及普通用户受到错误通知或举报带来的伤害。[37]尤其在现行的通知删除规则之下，平台在接到权利人通知后常常立即采取删除等必要措施，这等于平台对于通知或举报采取了“推定真实”的立场，对被指控侵权方采取了推定过错的立场，通知常常给平台带来大量的“负外部性”。[38]从经济学的角度看，权利人的通知或举报之所以可能触发平台责任，其关键在于权利人对针对平台内侵害的通知或举报具有较强的动力和一定的信息优势，但这种责任触发也必然要求权利人发出的通知或举报是善意、高质量的。[39]

另一方面，平台对通知或举报的要求也并非越高越好，过高要求可能导致很多权利人无法进行通知或举报，从而妨碍平台治理。尤其对于一些人身和财产类的严重侵害，如果平台要求侵害必须以已经发生侵害结果为基础，那将使得很多严重侵害行为无法得到有效预防。此外，平台对于通知的要求应当与其治理需求与治理能力相匹配。当平台需要借助更多的通知或举报发现违法行为，而且平台具有较强的技术或管理能力对通知或举报进行筛查，并且可以因为其善意治理而免责，此时平台就可以降低通知要求，或者可以设计更为便捷的通知或举报入口。[40]

我国法律法规中对通知的要求也需要放置在平台治理的背景下进行理解与设计。上文已经提及，美国《数字千年版权法案》512 条款在著作权背景下对通知做出了要求，而我国的相关法律法规也对通知做出了相应规定。这里值得注意的是，不同类型的侵害具有非常不同的治理需求与治理特征。有的侵害危害性较为严重，例如人身安全侵害，这类情形具有较高的治理必要性；有的侵害可能伴随着合法目的，例如对于公众人物的批评，这类言论治理可能需要衡量不同法益；[41]有的侵害则很难辨别合法与非法，例如专利侵权是否属实，对其进行治理常常存在很高难度；[42]还有的侵害则适宜当事人直接对侵权方提起诉讼，平台很难对平台内侵权进行预防与控制。[43]就此而言，平台对于权利人的通知也应当根据不同侵害类型和不同治理特征而做不同要求。例如在专利侵权中，平台可以对《电子商务法》第 42 条中要求的“通知应当包括构成侵权的初步证据”进行严格解释，要求权利人的通知以法院判决为依据。在杭州阿里巴巴广告有限公司与深圳市朗科科技股份有限公司侵害发明专利权纠纷案中，法院认为有效通知不必以法院的判决为基础。[44]但对于判断难度大的专利侵权，此判决不合理地扩大了平台的治理义务，与其治理能力并不相符。而在人身安全类侵权中，平台则可以对《民法典》第 1195 条中规定的“侵权的初步证据”进行宽松解释，甚至不要求通知包括“权利人的真实身份信息”。正如在举报治理中，治理者可以在特殊情况下可以允许举报人进行匿名举报或对外维持匿名，平台也可以在某些严重侵权的情形中允许权利人维持匿名。[45]

（三）平台接到通知后的反通知等措施

平台在接到权利人的通知或举报后，其采取的“反通知”等措施也应当根据平台治理而设定。上文提到，我国法律法规围绕“反通知”等措施有不同规定，此处可以进一步指出，平台在接到权利人通知或举报后，其采取的措施可以有非常多的选项。对于保护权利人与保护平台内的其他主体而言，这些不同措施构成了一个光谱。采取何种选项更为合理，也完全取决于平台的治理需求与治理特征。

在保护权利人最为消极的光谱一端，平台可以在收到权利人通知或举报完全不采取任何行动。比这一措施更积极一些的则是加拿大著作权领域所采取的“通知—通知”（notice-notice）规则，即平台通知被指控的侵权人，告知权利人对其进行指控，但也同样不采取删除或断开链接等必要措施。[46]再比这措施更积极的是平台通知被指控侵权人，但并不采取措施立即删除被通知内容；平台只有在等待一段时间后没有收到反通知，才对被通知内容进行删除。[47]当然，我国目前法律所规定的通知删除规则要求都比上述做法更为积极，因为我国现有的通知删除规则要求平台在收到通知后立即删除相关内容，否则可能需要对造成的侵权承担连带责任。不过即使是要求立即删除相关内容，法律规定也有不同版本。例如保护权利人更消极的《信息网络传播权保护条例》规定，平台在接到反通知说明后立即恢复相关内容。而保护权利人更积极的《电子商务法》则在接到反通知后并不立即恢复内容，而是等待权利人向主管部门投诉或向法院起诉，只有一段时间后平台未收到投诉或起诉通知，平台才恢复内容。除此之外，在最为积极保护权利人的光谱一端，平台可以完全不适用反通知规则。平台在收到通知后，可以直接删除相关内容，不给被通知人以任何抗辩机会。如果平台采取此类措施，平台的通知删除规则将接近已经被《民法典》取代的《侵权

责任法》中的相关条款。

需要指出，上述各种措施的合理性不能一概而论。一方面，即使是光谱最极端的措施也可能具有合理性。例如当平台认为收到的通知或举报高度不可信，且通知或举报所涉及的危害轻微、对其采取措施可能带来巨大负面作用，此时平台可能认为，既不将通知转告被举报人、也不采取删除的最消极措施最具有合理性。反之，当平台认为收到的通知或举报高度可信，且通知或举报所涉及的侵权行为危害巨大、对其采取措施可能不会带来任何负面作用，此时平台可能认为，立即删除相关内容、不给通知人任何抗辩机会的最积极措施更为合理。另一方面，处于光谱中间的“通知—反通知—删除”措施也未必具有合理性。例如在著作权领域，立即删除涉嫌侵权的内容常常会对用户内容的有效传播造成严重影响。[48]有学者指出，现行的通知删除规则改变了传统知识产权中的合理使用抗辩，平台在接到通知后自动删除相关内容，这等于使得合理使用抗辩从“推定合法”变为“推定违法”。[49]

（四）平台采取的最终措施

平台采取的最终措施也可以被视为一系列光谱上的不同治理措施。在光谱最严厉的一端，平台需要在通知之前采取积极预防性措施，否则平台就需要对第三方侵权承担责任。[50]在光谱最宽松的一端，平台则不需要采取任何措施，即使平台完全消极不作为也不用承担任何责任。我国法律法规中的“删除、屏蔽、断开链接”“终止交易和服务”等必要措施则可以被视为居于光谱中间的措施。[51]

平台所采取的最终措施也同样需要根据治理需求与治理特征进行判断。首先，光谱最严格或最宽松的措施也可能具有合理性。一方面，当平台内存在大量严重侵害活动，而且预防此类活动不会对平台内的合法活动产生重大影响，那么不论平台是否收到通知或是否对具体个案知情，平台也应该采取现有可行性下最佳的人工或技术预防措施。[52]否则，平台将因为没有履行其治理义务而承担责任。另一方面，当平台内的侵害活动较为轻微，或者平台采取措施将带来较大的负面作用，或者让权利人对首要侵权方提起诉讼更有利于平台治理，则平台选择不采取措施也应当被认为具有合理性。

其次，就光谱中间的“通知—删除”与“通知—过滤”而言，二者也应适用于不同治理场景。[53]相较之下，“通知—过滤”比“通知—删除”更强化对权利人的保护，可以更有效地解决网络侵权中的重复侵权或所谓的“打地鼠”（whack-a-mole）问题，即侵权人在删除相关内容后仍然继续在其他地方上传侵权内容。不过“通知—过滤”规则在强化权利人保护的同时，也会带来很多过度审查的问题，造成治理失衡。很多研究所指出，“通知－过滤”规则的引入必然使得对特定内容或活动的“特定性审查”（specific monitor）走向“一般性审查”（general monitor），[54]因为只有一般性审查才可能实现对相关侵权内容或活动进行过滤与事前预防，而这将导致对合法活动也进行审查与过滤。[55]尤其在平台难以精确分辨侵权与活动的治理场景中，平台的一般性审查与过滤行为将会对平台的合法活动造成较大的“附带损害”（collateral damage）。[56]就此而言，“通知—过滤”应当被适用于侵害行为严重、侵害活动辨识精确度较高、过滤不会轻易影响平台合法活动的治理场景中。而在著作权侵权等活动中，由于著作权存在合理使用空间，且其侵权的辨识难度较高、过滤可能影响平台内用户的合法活动，对于在著作权等领域引入“通知—过滤”规则应当慎之又慎。[57]目前，欧盟在《数字单一市场版权指令》中引入了“通知—过滤”规则；我国则在《民法典》的网络侵权条款、《电子商务法》的知识产权侵权条款中包含了“通知—过滤”规则，而《信息网络传播权保护条例》则仅规定了“通知—删除”规则。在本文看来，平台应当在一般著作权侵权领域拒绝适用“通知—过滤”规则。[58]例如，广东省深圳市腾讯计算机系统有限公司等与北京微播视界科技有限公司等申请诉前停止侵害著作权案中，法院认为，面对平台内已知的不断上传的侵权视频，平台本身已经具备技术能力进行过滤拦截，因此应在能力范围内采取措施制止侵权行为再继续。判决书援引了抖音报告提及的

拦截违规视频数量，指出当前同等水平的科技公司具有相应的拦截能力且该种拦截过滤也并非要求100%的过滤效果，这种过滤可以更好地保护社会公共利益。[59]但该判决忽视了拦截违规视频和拦截侵犯著作权视频是两种不同情况，拦截侵犯著作权视频还需要考量合理使用以及已经获得著作权人授权等情形，因而具有更高的复杂性。只有当相关作品属于热门作品，相关侵权可能产生较大危害，且对其进行辨识具有较高精确度时，平台才应适用“通知—过滤”规则。

五、通知删除规则的自治与规制

上一部分已经阐述，通知删除规则的具体制度设计必须放置在平台治理的整体视野中进行理解。本部分从通知删除规则的平台自我规制与国家规制的角度出发，进一步指出通知删除规则应当赋予平台以较大的自治性权力，避免对通知删除规则进行过多的细节性监管。只有当平台治理与社会整体利益不一致时，国家才应当介入平台的通知删除措施，督促平台治理符合社会利益。

（一）平台自治

法律之所以应当赋予平台以较大的自治性权力，其原因在于平台本身就有较强的能力和动力设置合理的通知删除规则。平台的治理能力的优势较好理解。平台内的侵权形态纷繁复杂，包括了侮辱诽谤、著作权、商标、财产、人身安全等不同类型，不同类型侵权中的侵害程度、侵害范围、侵权方式又非常不同。[60]而且，平台内侵权的形态往往变化迅速，侵权方往往根据不同的规则而不断变化其策略。[61]面对此类复杂且多变的侵权形态，法律往往面临规制的“步调问题”（pacing problem）。[62]不仅正式法律法规难以有效应对各类平台内侵权，即使是司法解释、司法判决也常常会滞后于实践。相对而言，平台则对平台内的各类侵权掌握了第一手信息，且能够实时监控平台内的侵权形态变化。就平台的治理能力而言，由平台来自我监管和制定规则显然具有比较优势。

更具有争议性的是平台进行治理的动力或动机。有观点认为，平台虽然有通过通知删除规则进行治理的能力，但未必有治理的动力。平台为了吸引用户，往往会放任平台上的各类侵权行为与内容，对权利人造成本可以预防的侵害。例如在著作权领域，美国版权局发布了关于《数字千年版权法案》512 条款的报告，认为有关避风港规则的司法实践曲解了美国国会的立法原意，为平台提供了过多的自治空间，伤害了著作权人的相关权益。[63]欧盟的音乐产业则发布报告，指责平台企业故意放任大量盗版作品传播，平台因为大量盗版作品的传播而获益，著作权人则未从中获取任何利益，因此平台企业与著作权人之间存在“价值差”（value gap）。[64]在批评意见看来，平台总是从自身整体利益出发而进行平台治理，并不会从权利人保护或社会整体利益的角度进行治理。

对于此类质疑意见，需要指出仅仅关注权利人保护并不符合平台治理与通知删除规则的基本原理。正如安娜玛丽·布里迪（Annemarie Bridy）等学者所言，所谓的“价值差”理论主要基于具有版权的大型企业的利益考虑问题，其背后的理论假定是，版权企业应当获取平台上所有具有著作权的作品使用的利润。但事实上，这种假定忽略了平台不仅需要从权利人的角度进行治理，而且需要考虑和平衡包括普通用户在内的整体利益。[65]如果平台仅仅从预防侵权的角度对平台进行治理，平台虽然可以减少平台上的一部分侵权作品，但也同时会删除与过滤平台上大量合法作品或合理使用的作品。最终，平台的生态也会受到影响，不仅普通用户的言论与创作会大幅减少，而且版权企业也会因为用户流失、流量减少而丧失其版权利润。

从平台整体的角度看，平台有充分或充足的动力对第三方侵权进行治理。平台与其他市场中的主体一样，也面临着来自其他平台的横向竞争或面临创新性平台的颠覆性竞争。[66]其完全具有动力维持平台内的良好生态，将预防侵权与促进合法活动维持在合理程度。一方面，当平台对第三方侵权行为进行过度预防，平台会因为其治理措施过于严厉而导致用户流失。另一方面，当平台对第三方侵权过度放任，也将导致平台治理生态的恶化而丧失竞争

力。当平台内存在大范围的侵权活动，平台的生态就可能造成破坏，使得普通用户或商业用户不愿意参与该平台活动。[67]例如有关研究指出，当平台存在大量侵权行为，给外界造成一种比较“廉价”的网站印象，很多品牌为了顾及“品牌安全”（brand safety），就会不愿意在此类网站投放广告，或者不愿意支付较高的广告费用。[68]此外，一部分权利人可能就会因为侵权行为猖獗而转向其他平台，从而造成优质作品的减少和普通用户的流失。正因为如此，很多平台都自动引入了版权或优质作品的自我保护机制。例如微信公众号引入的原创保护机制，就提供了对用户原创作品的积极保护。

（二）规制下的自治

平台自治并不总是带来合理的通知删除规则。首先，平台整体利益与社会利益可能未必完全一致，即使平台采取了有利于平台整体利益的通知删除规则，这种规则也可能未必有利于社会。[69]例如有的小型平台可能故意放任平台内存在大量盗版内容或假冒产品，此类盗版内容或假冒产品虽然可能有利于平台上的商户和普通用户，但却可能伤害社会整体利益，把负外部性转移给社会。其次，市场竞争也可能无法迫使平台将此类外部性内部化。[70]例如在上述例子中，小型平台可能仅仅在乎一小部分用户的评价，对于社会整体评价并不在意。即使小型平台受到优质用户与权利人的抵制，小型平台也可能置之不理。[71]最后，平台还可能犯错，即使平台的整体利益与社会利益具有一致性，平台的通知删除规则也可能不合理。平台可能过快回应权利人的通知或通知，对平台的治理过于严厉，从而带来假阳性（false positive）的问题。平台也可能对通知或通知反应不足，对平台的治理过于消极，也能带来假阴性（false negative）问题。[72]因此，法律在赋予平台自治权力的同时，也应当对其进行规制。

在我国，有关通知删除规则的法律法规也同时包含了平台自治性规定与强制性规定。一方面，司法实践要求从整体上判断平台是否履行了通知删除义务。例如《网络人身权益司法解释》第四条规定，“人民法院适用民法典第一千一百九十五条第二款的规定，认定网络服务提供者采取的删除、屏蔽、断开链接等必要措施是否及时，应当根据网络服务的类型和性质、有效通知的形式和准确程度、网络信息侵害权益的类型和程度等因素综合判断”。最高人民法院发布的《电商知识产权指导意见》则进一步赋予平台的自治性权力，其第四条规定，对于《电子商务法》第 41 至 43 条所规定的通知删除规则，“电子商务平台经营者可以根据知识产权权利类型、商品或者服务的特点等，制定平台内通知与声明机制的具体执行措施”。另一方面，从《信息网络传播权保护条例》到《电子商务法》到相关法律法规的司法解释，相关条款对通知删除规则作出了事无巨细的规定。这些规定不仅涉及通知删除规则的“全生命周期”，而且涉及各个不同领域，既包括人身财产侵权、知识产权侵权，也包括一般性的网络侵权。综合本文对于平台自治与规制的分析，我国对于通知删除规则的法律适用也应遵循相关原理。即法律应当从整体上判断通知删除规则的合理性，避免对平台所设定的通知删除规则做过于细节性的判断。

具体而言，平台的自治与规制应首先区分平台的恶意治理与善意治理。[73]对于平台故意放任大量侵权内容、把问题留给社会的恶意治理，法律应当介入此类平台的通知删除实践，确保平台利益与社会利益对齐。其次，对于不存在重大过失的善意治理，应允许平台对通知删除规则进行自治，免除平台治理中对第三方侵权的责任。[74]这一点在现行的通知删除规则下尤其重要。因为现行的通知删除规则仍然以“知情”作为平台是否应当承担责任的重要标准，平台在很多场景下常常会因为“治理越多”而“知道越多”，从而越可能承担责任。[75]最后，对于存在重大过失的善意治理，法律也可以建立督促机制，对平台采取约谈、指导等方式进行矫正。不过此处需要再次强调，平台的治理错误既可能是对权利人保护与预防侵权不足，也可能是预防过度和过度遏制合法活动。整体而言，后者的情况更为普遍、而且常常被忽略，更需要平台在通知删除规则的设定中加以重视。

结语

作为避风港制度的核心，通知删除规则在美国《数字千年版权法案》被引入，其制度的关键目的是为了在著作权间接侵权中给平台提供合规免责的“避风港”。[76]这一制度随后在我国与欧盟等国家与地区成为适用不同领域的一般性网络侵权制度。不过对这一制度进行仔细分析，就会发现通知删除规则并不像想象的那样确定。从通知要求到反通知到删除与过滤，通知删除制度都存在众多版本，而且不同的版本都存在制度适用冲突与各方权益平衡的难题。如何理解避风港制度、对通知删除的具体制度进行设计，都需要从法律原理与法律制度层面进行重思与重构。

破解通知删除规则难题的关键在于理解典型的平台间接侵权具有大规模治理型侵权的特征。在典型的平台间接侵权中，平台并不特定参与某个侵权个案，而是一般性地引起了大规模侵权；同时，平台所需要考虑的是平台的整体治理效果，而非个案中的事故预防。因此，典型的平台间接侵权与传统共同侵权具有本质性区别。只有在极少量的特定个案型平台间接侵权中，例如平台将未获版权授权的某热门作品在主页上进行推送，此时平台才扮演了传统的共同侵权人角色。基于典型平台间接侵权的大规模治理型侵权特征，[77]本文指出，避风港制度下的通知删除规则更接近于举报治理机制，即平台在接到权利人的通知或举报后，从平台整体利益出发采取相应的治理措施。

通过将通知删除规则视为举报治理，避风港制度可以进行重构。首先通知删除规则应当根据平台治理的需求与治理特征进行设计。无论是通知要求、反通知等平台接到通知后的措施，还是平台最终采取的删除、过滤等措施，都没有绝对的优劣之分。整体而言，当平台间接侵权的侵害性越严重、平台间接侵权活动同时带来的正面作用越小、分辨平台合法与非法活动越容易、直接侵权制度越失灵，平台所采取的措施就应当越严厉。反之，平台所采取的措施就应当越克制，以免造成过度审查与过滤，伤害平台内的合法活动与整体利益。[78]此外，法律还应当给予平台较大的通知删除自治权，避免对通知删除规则进行过多和过细的强制性干预；当法律介入与规制平台自治性规则时，其干预应当使平台利益与社会利益对齐。从举报治理的角度看待通知删除规则，避风港制度的难题与挑战可以得到有效破解与回应。

数据权益之权能体系的再思考

此处删除了原文脚注，全文请参见《法学评论》2025 年第 2 期，转载或引用请注明出处。

作者：阮神裕

摘要：在数据权益的建构性讨论中，存在一种通过界定和描述积极权能的方式进行确权的偏好。但是，积极权能在实践推理中不具有规范性，既不是权利主体的行动理由，也不是其他主体的行动理由。积极权能应当被看作财产权的目的，消极权能则是财产权目的实现的手段。消极权能在实践推理中具有规范性，一方面作为排他性理由直接指导不特定陌生人的行动，另一方面作为权利主体享有的权力或法律意志的作用对象，使权利主体按照自己的意愿改变数据所涉法律关系。数据权益的积极权能兼具竞争性利益和非竞争性利益，因此从根本上不同于所有权或者知识产权。数据权益的消极权能既要服务于竞争性利益，即禁止他人破坏数据完整性，也要服务于非竞争性利益，即以数据在虚拟层面的可访问性为标准，区分公开数据权益和非公开数据权益，前者原则上允许他人访问、复制或者使用，除非他人的利用行为构成不正当竞争；后者原则上禁止他人访问、复制或者使用，除非他人的利用行为构成合理使用。一旦确立消极权能，数据权益的静态结构就能得到确定，数据确权的难题将会转向数据权益的权利变动。

2022 年 12 月 2 日，中共中央、国务院印发的《关于建构数据基础制度更好发挥数据要素作用的意见》（“《数据二十条》”）提出了“探索建立数据产权制度”的政策目标。国家数据局颁布的《关于促进企业数据资源开发利用的意见》提出从“完善企业数据权益形成机制、完善企业数据权益保护机制和健全企业数据收益分配机制”三个方面“健全企业数据权益实现机制”。为此，在理论上需要说明的是，所谓的数据产权或者数据权益的具体内容究竟为何？按照传统民法的话语体系，数据权益的内容就是指其积极权能与消极权能。在数据确权的现有讨论中，大多数观点尝试通过积极权能的列举与描述的方式界定数据权益，而对数据权益的消极权能着墨不多。事实上，自《民法通则》以来，立法者对所有权的界定始终关注占有、使用、收益和处分的积极权能，而不关注所有权的消极权能。似乎只要说明清楚积极权能的具体内容，就可以完成数据确权的工作。然而经验和直觉表明，即便数据没有得到确权，企业也可以按照自己的意愿持有、加工使用或者经营数据；假设数据得到确权了，企业利用数据的权能也不会发生根本性改变。如此一来，数据确权的意义似乎不大。这不免引发一个疑问：所谓的“数据确权”，究竟是要确立什么？

为此，本文将以数据确权的讨论为契机，从实践哲学的行动理由的理论出发，对财产权利中的积极权能和消极权能进行反思性讨论，为数据权益之权能体系的建构提供更加清晰的基础概念。本文将重点回答以下四个子问题：第一，为什么在数据确权中存在积极权能偏好？第二，积极权能对于数据权益而言发挥何种作用？第三，数据确权为什么应当更加关注消极权能？第四，数据权益的消极权能应当如何表达？

一、数据确权中的积极权能偏好

在数据确权的众多讨论中，始终存在一种“积极权能偏好”，也就是大多数观点尝试通过界定和描述积极权能的方式确立数据权益，至于数据权益的消极权能往往只是被附带提及，没有得到充分的讨论。这一积极权能偏好不仅体现在政策文件、地方性法规中，也体现在关于数据应当如何确权的学说中。具体而言：

首先，《数据二十条》以及相关政策文件提出数据权益结构性分置制度时，强调的是权利主体对数据进行利用的积极权能。例如《数据二十条》提出了“建立数据资源持有权、数据加工使用权、数据产品经营权等分置的产权运行机制”，其中三种权利强调的是权利主体对数据的持有、加工使用和经营的利用可能性。又如对于不涉及个人信息和公共利益的企业数据而言，“市场主体享有依法依规持有、使用、获取收益的权益”。再如“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”“承认和保护依照法律规定和合同约定获取的数据加工使用权”或者“充分保障数据处理者使用数据和获得收益的权利”。又如国家数据局颁布的《关于促进企业数据资源开发利用的意见》明确提出“保护企业对其合法持有数据的开发利用、经营收益、流通交易等合法权益。企业有权依法或依合同约定，自主或委托他人基于其合法持有数据开发数据产品或提供数据服务。”这些表达方式充分说明《数据二十条》以及相关政策文件强调的是权利主体如何利用数据，体现了对积极权能的明显偏好。相比之下，以上政策文件基本没有提及数据持有者在何种情况下以及在多大程度上可以禁止他人对数据的利用（即消极权能）。

《数据二十条》以及相关政策文件强调权利主体对数据享有的积极权能，而不对消极权能作出具体规定，是可以理解的。这是因为政策文件的重点在于提出构建数据基础制度所要实现的经济目标和政策目标，而不是对数据权益制度提出具体的法律方案。可以说，数据资源持有权、数据加工使用权和数据产品经营权只是经济上的权利，还不是法律上的权利。这些经济上的权利的性质和具体内容仍然存在诸多模糊之处。对于法学界和立法机关而言，必须解决数据权益究竟是一个权利还是数个权利，每个权利的内容和效力如何等具体问题。[1]因此，《数据二十条》以及相关政策文件从积极权能的角度提出的三权分置方案，还没有满足法律权利的要求。

其次，地方性法规对数据的规定，也呈现出积极权能偏好。例如，一些地方性法规借鉴《数据二十条》的表述方式，规定了数据资源持有权、数据加工使用权和数据产品经营权：《吉林省大数据条例》第 22 条第 1 款、《厦门经济特区数据条例》第 37 条第 1 款以及《汕头经济特区数字经济促进条例》第 14 条第 1 款均规定了“建立数据资源持有权、数据加工使用权、数据产品经营权等分置的产权运行机制”。又如，一些地方性法规没有明确界定“数据××权”，而是正面规定民事主体可以对数据实施哪些利用行为：《四川省数据条例》第 38 条第 1 款规定：“自然人、法人和非法人组织可以依法使用、加工合法取得的数据；对依法加工形成的数据产品和服务，可以依法获取收益”；《苏州市数据条例》第 30 条第 1 款规定：“支持自然人、法人和非法人组织通过合法、正当的方式加工和利用数据”；《广西壮族自治区大数据发展条例》第 44 条第 1 款规定：“自然人、法人和非法人组织对其合法取得的数据，可以依法使用、加工”。以上规定均从积极权能的角度规定数据权益的具体内容。

最后，理论学说在界定数据权益的具体内容时，不管采取何种方法或者范式，最终总是通过积极权能界定数据权益的内容。例如，有的观点主张采用权利束范式界定数据权益，但是谈到数据权益的具体内容时，仍然借鉴所有权的权能体系，将数据权益的法律权能界定为持有、使用、收益和处分的权能。[2]有的学者主张通过建构新型财产权的方式进行确权，其提出的数据财产权的主要权能包括利用权能、收益权能、占有（持有）权能和处分权能。[3]有的学者主张将数据涵摄于“所有权－用益权”的框架中，其提出的数据用益权的积极权能包括数据控制权、数据开发权、数据许可权和数据转让权。[4]有的学者主张数据权益的积极权能应当包括访问权、复制权、使用权和处分权。[5]等等，诸如此类的观点不胜枚举。[6]以上观点的共同特征在于，研究者对积极权能予以较大篇幅的讨论和建构，尝试最为全面地描述和概括权利主体对数据的任何利用可能性，但是对于权利主体可以禁止他人实施哪些行为，即数据权益给不特定陌生人施加了哪些义务，则简要略过。

以上例证说明了，不管是在政策文件、地方性法规还是理论学说中，存在着通过积极权能进行数据确权的偏好。事实上，积极权能偏好并非新鲜事物，这一观念由来已久。只要稍微考察一下法律法规和法律理论对所有权、知识产权等法定财产权的定义和说明，就可以发现，在财产理论中始终存在着通过积极权能定义财产权的偏好。具体而言：

其一，我国法律法规习惯性地通过积极权能定义或者命名一项财产权。以所有权为例，《民法通则》第 71 条规定：“财产所有权是指所有人依法对自己的财产享有占有、使用、收益和处分的权利”。《物权法》《民法总则》以及《民法典》延续了这一规定方式，《民法典》第 240 条将所有权定义为“所有权人对自己的不动产或者动产，依法享有占有、使用、收益和处分的权利。”尽管理论上通常承认所有权具有“排除他人一切干涉”的消极权能，但是立法机关对所有权的规定始终只提及积极权能。同样，尽管不少知识产权学者主张知识产权不是自用权，而是排他权，[7]但是《著作权法》的条文表述在很大程度上包含了著作权人的自用权的意思，例如发表权是“决定作品是否公之于众的权利”，复制权是“以印刷等方式将作品制作一份或者多份的权利”，展览权是“公开陈列美术作品、摄影作品的原件或者复制件的权利”。

其二，传统民法学说在阐释所有权时往往更加重视积极权能。早在萨维尼的时代，物权就被看作是权利主体的意志施加于“不自由的自然”的权利。[8]根据这一观念，所有权人享有的积极权能决定了所有权的本质。[9]当然，现在通常认为，所有权的法律权能既包括积极权能，也包括消极权能，其中积极权能是指依法享有占有、使用、收益和处分的权利。[10]但是，在定义消极权能时，我国民法学说通常将其定义为排除他人对积极权能进行侵扰的权利。例如有的观点认为：“所有权是对物为全面支配的权利，而所有权人在行使占有、使用、收益和处分权能时，均有可能受到来自他人的不当侵扰。为贯彻上述积极权能，需要所有权产生出排斥他人不当干预的力量。”[11]又如“所有权之此种权能仅于所有权之积极权能受他人不法干涉时，始能表现，否则隐而不彰，故称为消极权能。”[12]这些观点的内在逻辑是，先有所有权的积极权能，再依积极权能定义其消极权能；反过来说，若是积极权能没有得到清楚的界定，那么其消极权能的含义将是不清楚的。故此，消极权能的内容直接依附于积极权能的内容。这些观点有意或无意地表明，积极权能的重要性显著高于消极权能。

其三，在英美法中，权利束理论也强调，财产权乃是权利主体享有的多种利用权能的总和。例如奥诺尔教授（A.M.Honoré）认为，所有权的标准要素（standard incidents）包括占有权、使用权、管理权、对事物收入的权利、资本的权利、安全权、可转让和无期限的权利或要素、禁止有害使用、执行责任以及剩余索取权。[13]这些要素均是从权利主体对财产享有的利用权能角度加以定义的。奥诺尔的分析为权利束范式的发展奠定了基础，在很长的一段时间里，财产权被英美的法学家和制度经济学家理解为权利主体对财产的多种利用权能之束集。[14]正如科斯所述：“人们通常认为，商人得到和使用的是实物（一亩土地或一吨化肥），而不是行使一定（实在）行为的权利。我们会说某人拥有土地，并把它当做生产要素，但土地所有者实际上拥有的是实施一定行为的权利。”[15]

通过以上简要回顾，可以发现数据确权中的积极权能偏好并非新鲜事物，而是存在一定的理论传统。事实上，通过积极权能定义财产权利具有一定的合理之处。一方面，通过积极权能定义财产权具有一定的哲学基础。在康德看来，一个主体的意志选择的对象可以是外在之物、他人行为或者他人所处的状态，当个人意志独立支配的领域是外在之物时，就形成了“所有权”的法权。[16]根据这一观念，所有权的本质应当是权利主体按照自己的意志实施行动的自由。另一方面，通过积极权能定义财产权符合人们日常生活的体验。当有人想要实施一定的行动，尤其是在这个行动可能受到他人（其他民事主体或者国家机关）的阻碍时，只要声称自己享有采取这一行动的权利，那么这个行动将获得正当性，他人似乎就没有理由再加阻碍。因此，人们渴望法律赋予他们这样的“权利”，让他们在日常生活中可以按照自己的意愿实施行动，例如任意地装修自己的房屋的权利，或者开发利用数据的权利。

但是，问题在于积极权能真的如此重要吗？所谓的“数据确权”想要确立的是数据持有者对数据进行复制、使用、加工、分析或挖掘的积极权能

吗？笔者对此表示怀疑。仅仅通过一些日常经验和直觉认识，就可以初步发现，积极权能在数据确权中没有想象中那么重要。一方面，目前数据还没有得到确权，但是企业有权并且实际上已经按照自己的意愿利用数据。企业对数据的利用不需要数据确权就已经存在了，那么在数据确权中进一步列举、说明和描述积极权能的意义何在？另一方面，一些学者提出的数据确权方案落实到具体内容时，强调的均是数据持有者对数据进行占有（持有）、使用、收益和处分的积极权能，[17]这一表述方式与《民法典》第 240 条的规定高度相似，这是否意味着由此形成的数据权益是数据所有权？如果不是的话，它们的积极权能何以如此相似？故此，无法简单地通过界定和描述积极权能的方式对数据进行确权。

二、积极权能真的重要吗？

在数据权益以及其他财产权中，积极权能是否真的如此重要？其究竟处于何种地位？要对此作出最终回答，需要将财产权的积极权能置于实践推理的框架中加以分析。

（一）财产权与行动理由

通常认为，财产权具有调整权利人与不特定陌生人之间法律关系的功能。财产权之所以具有调整功能，是因为财产权作为对世权，指导着不特定陌生人的行为。若进一步追问财产权何以指导行动，就不得不引入“行动理由”的概念。

在哈特（H．L．A．Hart）看来，作为社会控制的方法，法律的主要功能在于，以各种方式被用来控制、引导以及计划我们的生活。[18]为了实现这一功能，法律应当成为我们采取特定行动的依据，并且在面对反对意见时，法律将充当辩护的基础。如此一来，法律就扮演着“行动理由”的角色。只不过哈特最初并未明确使用“行动理由”的概念，而是运用“规则”这个概念进行阐释的。[19]同样，想要理解财产权何以发挥调整功能和指导功能，就不得不使用“行动理由”的概念。

拉兹（Joseph Raz）进一步引入“行动理由”（reasons for action）的概念对规范在实践推理中的功能进行了分析。首先，实践推理（practical reasoning）是实践哲学的一个分支，旨在解释我们在日常生活中决定行动的方式。实践推理不关心行动的最终理由，比如道义论或功利主义；而是关注日常决策和行动层面中的推理结构。其次，行动理由大体是指行为人做出行动的依据。在日常生活中，我们经常为自己的行动寻找理由。可以说，当且仅当一个行动获得理由的支持时，这个行动才被称为是理性化的。例如，“电影很精彩”可能是一个人去看电影的理由，“论文没写完”可能是这个人不去看电影的理由。几经权衡之后，这个人可能作出不去看电影的行动。当有人问他为什么不去看电影时，他可能会用“论文没写完”的理由来说明并且正当化自己的行动。再次，拉兹引入了二阶理由（尤其是排他性理由）的概念，以解释行动理由在不同层次上的运作。[20]通常情况下，一个人根据理由的强弱决定如何行动。但是，倘若存在排他性理由，那么原本用于权衡的某个一阶理由将被排除不予考虑，从而作出不同的行动。例如，即便“论文没写完”的理由胜过了“电影很精彩”的理由，但是由于已经答应了他的妻子“今晚去看电影”，那么这个承诺将会排除已经胜出的“论文没写完”的理由。这是因为，作出承诺就像事先作出了一个具有约束力的决定，在作出该决定时，诸如“电影很精彩”“论文没写完”等一阶理由已经被考虑过了，承诺排除了基于这些理由行动的可能性。在电影即将开始之际，这个人不应该再对一阶理由进行权衡。[21]最后，拉兹认为，规范不仅仅是特别强势的行动理由，而且是排他性理由（exclusionary reason）。[22]对于一个规范要求的行动，一个人可能既有理由作出、也有理由不作出该行动，但是规范的存在意味着，这个人应该排除后一理由。换句话说，规范将考虑所有因素转变为直接遵守既定标准来实现秩序。

这里无法再对规范与实践推理的关系进行深入讨论，以上论证的目的在于初步说明什么是行动理由，即那些足以说明、指导和评价一个人的行动的理由。厘清了这些概念之后，下文就可以论证积极权能为什么没有想象中那么重要了。

（二）积极权能不是行动理由

1. 积极权能不指导权利主体的行动

当法律体系赋予权利主体一项积极权能时，似乎表明了权利主体因此享有某种自由。例如《民法典》第 240 条规定，所有权人对自己的不动产或者动产，依法享有占有、使用、收益和处分的自由。《数据二十条》提出的“市场主体享有依法依规持有、使用、获取收益的权益”，也表明了市场主体享有持有、使用和获取收益的自由。但是，积极权能所蕴含的自由不能指导权利主体的行动。这是因为：

其一，积极权能蕴含的自由，乃是与生俱来的，而非法律体系赋予的。当《数据二十条》提出数据资源持有权、数据加工使用权和数据产品经营权时，目的不是赋予数据处理者进行持有、加工使用和经营的自由。事实上，在《数据二十条》发布之前，数据处理者已经开展了大量的数据经营活动，无需政策文件或者法律法规的许可，数据处理者就享有这些自由；在《数据二十条》或者将来的数据权益立法颁布之后，数据处理者仍然享有这些自由。数据处理者对数据的处理自由，不是法律体系授权的结果，而是市场主体经营自由的应有之义。当然，法律体系可以对数据处理者的自由施加限制，例如个人信息权益限制数据处理者向他人提供数据的自由，国家利益限制数据处理者跨境传输数据的自由。不过，这些限制是针对积极权能的，而非积极权能本身。[23]

其二，积极权能蕴含的自由，不是权利主体的行动理由。积极权能蕴含的自由可能具有两种不同的理解方式：一是法律不予规范的自由，二是法律授予许可的自由。这两种意义上的自由均不是权利主体的行动理由。

一方面，法律不予规范的自由是指法律既不要求权利主体实施某一行为，也不禁止其实施这一行为。权利主体是否实施这个行为，可以取决于他的爱好、欲望或者利益。当《民法典》第 240 条规定，所有权人享有使用动产或者不动产的自由时，意味着所有权人可以积极投入生产赚取利润，也可以消极怠工荒废资源。对于所有权人的选择，法律不加干涉。拉兹将法律不予规范的自由称为“弱许可”，弱许可意味着“理由之阙如”，表明了法律体系对所有权人的选择没有规定相反的理由。在这个意义上，作为弱许可的积极权能对于实践推理毫无贡献。[24]

可能会有论者提出，诸如《民法典》第 240 条规定占有、使用、收益和处分的积极权能的言下之意是，法律体系保障积极权能的实现。由于积极权能受到法律的保障，将会在一定程度上改变权利主体的行动。例如，倘若没有法律提供的保护，那么一块土地的所有权人将会建造围墙或者其他防御措施，以便通过自助行为抵御陌生人可能实施的侵害行为。但是，由于法律保护土地所有权，可以想象，陌生人实施侵害行为的可能性要小得多，因此所有权人通常不会建造防御措施。在这个意义上，积极权能的确影响了权利主体的行动。但是积极权能仍然不是权利主体的行动理由，而是因为法律保障改变了权利主体作出行动的环境，从而间接地影响了权利主体的行动。[25]

另一方面，所谓法律授予许可的自由，是指在法律禁止实施一定行为的背景下，授予权利主体实施该行为的许可。这个意义上的许可，并非“弱许可”，而是“强许可”。强许可意味着强制之豁免。拉兹将此称为“排他性许可”，其具有抵消理由的力量。尽管它们并不直接指导行为，因而不是行动理由，但是它们具有一种规范的力量。[26]例如，《民法典》第 344 条规定：“建设用地使用权人依法对国家所有的土地享有占有、使用和收益的权利，有权利用该土地建造建筑物、构筑物及其附属设施。”尽管这一条款也规定了占有、使用和收益的积极权能，但是其中蕴含的自由，不同于《民法典》第 240 条的自由。这是因为，取得建设用地使用权的主体，原本受到国家所有权相关的指向性义务的拘束，但是从其取得建设用地使用权的那一刻起，其就获得了一项排除该指向性义务的许可（排他性许可）。也就是说，尽管国家所有权要求某一主体不要使用国家所有的土地，但是这一主体取得建设用地使用

权时，他就取消了国家所有权施加的义务。国家所有权施加的义务本来是这一主体作出行动的决定性理由，但是建设用地使用权作为排他性许可抵消了这一决定性理由，因此这一主体可以自主决定是否进行占有、使用和收益。故此，尽管《民法典》第 344 条和第 240 条均使用了“占有、使用和收益”的表述，但是它们在实践推理中具有截然不同的意义。

然而需要注意的是，尽管法律授予许可的自由在实践推理中发挥了规范力，但是其仍然不是权利主体的行动理由。建设用地使用权人根据其获得的排他性许可，可以忽略国家所有权施加的义务，但是在决定是否以及采取何种方式对土地进行实际的占有、使用和收益时，建设用地使用权的存在，如同所有权的存在一样，不是权利主体实施具体经营活动的行动理由。

2. 积极权能不直接指导其他主体的行动

尽管积极权能不是权利主体的行动理由，但是积极权能能否成为其他主体的行动理由呢？这个问题的答案可以在传统民法对所有权妨害的定义中找到线索。通常认为，妨害是指权利主体不能行使或者不能正常行使权利。[27]其中的行使权利一般被理解为行使积极权能。例如某甲欲在家中从事论文写作，但是邻居的装修噪声使其无法静心研究，邻居的行为很有可能构成权利妨害。这一观念似乎表明，倘若权利主体享有某一积极权能，那么其他主体就负有不得阻碍这一积极权能实现的义务，在这个意义上，积极权能似乎可以成为其他主体的行动理由。

然而，日常生活中的例子足以说明，权利主体享有的积极权能不一定总是给其他主体施加义务。例如，某甲拥有汽车所有权意味着其享有按照自己的意愿驾驶汽车的自由，但是当某甲的汽车被堵在路上时，堵在前面的某乙虽然阻碍了某甲的积极权能，但是没有义务为某甲让行。又如，某一建筑公司的挖掘机在作业时挖断了电缆，导致某一工厂无法正常生产，也阻碍了该工厂的积极权能的实现，但该建筑公司通常无需对此承担责任。[28]因此，权利主体享有的积极权能并不总是给其他主体施加相关义务（correlative duty）。

事实上，霍菲尔德（WesleyN．Hohfeld）的权利分析以简单明了的方式说明了权利主体的积极权能和其他主体承担的相关义务之间没有逻辑相关性。在霍菲尔德看来，权利的概念存在模糊之处。为了克服这一模糊性，霍菲尔德提出了权利分析的八个构件，即要求权与义务、特权与无权利、权力与责任以及豁免与无能力。其中，要求权（claim）与义务（duty）之间具有逻辑上的相关性。所谓逻辑上的相关性，是指若是存在一项要求权，那么在逻辑上必然存在与之相关的、由其他主体承担的义务。倘若缺少了这样的义务，那么也就不可能存在一项要求权。换句话说，要求权的存在必然蕴含着义务的存在，要求权这个概念以义务的概念为前提条件。[29]在民法中，债权请求权是典型的要求权，一个人若是想要成为债权人，那么至少要有一个债务人。

但是，在霍菲尔德的概念矩阵中，特权（privilege）与义务之间却没有逻辑上的相关性。笼统而言，这里的“特权”等同于“自由”或者“积极权能”。[30]与“特权”具有逻辑上相关性的，乃是其他主体的“无权利”（no-right）。当且仅当其他主体没有要求权给某甲施加某种义务时，某甲才享有特权、自由或者积极权能。上文对“弱许可”和“强许可”的讨论与此有关：在弱许可的情况下，由于法律体系没有通过赋予他人权利的方式给某甲施加义务，因此某甲享有特权；而在强许可的情况下，由于该排他性许可取消了法律体系本来施加的义务，因此某甲也享有特权。但是，在权利主体的特权和其他主体的义务之间，无论如何也没有逻辑上的相关性。然而，这并不意味着法律体系不可以通过给其他主体施加义务的方式保障权利主体享有的积极权能。只不过在这么做的时候，应当注意到其中存在着实质性的理由。也就是说，当一个法律体系规定权利主体享有做某件事的自由，同时规定其他主体负有不得阻碍的义务时，其中必然隐藏着一个实质性的理由。[31]

以上论证表明，积极权能不仅不是权利主体的行动理由，也不是其他主体的行动理由。法律体系可能基于某种实质性理由，要求其他主体承担某些义务，从而有利于权利主体实现其积极权能。但是，此时成为其他主体行动理由的，乃是法律体系特别施加的义务，而非权利主体的积极权能本身。

（三）积极权能作为财产权的目的

既然财产权的积极权能既不是权利主体的行动理由，也不是其他主体的行动理由，那么积极权能对于财产权来讲还有什么意义呢？有的理论家甚至进一步主张，主观权利应当化约为针对他人的命令或禁令，主观权利只是次级防御（eine sekundäre Negation）的单纯反射。[32]按照这一观点，诸如财产权中所包含的积极权能似乎更加无关紧要了。如此一来，我国民法学说缘何如此重视财产权的积极权能？

笔者认为，尽管积极权能不直接发挥规范力，也不直接调整权利主体与其他主体的法律关系。但是，积极权能在财产权的法律构造中仍然发挥着不可磨灭的重要功能，是财产权不可忽视的必要构件。积极权能的功能在于决定财产权的目的。具体而言：首先，法律体系在规定一项财产权的积极权能时，实际上尝试描述和说明权利主体可以从财产中获得的经济利益。《民法典》第 240 条规定所有权人可以对动产或者不动产进行占有、使用、收益或者处分，从而获得经济利益。《数据二十条》尝试通过描述数据处理者对数据的持有、加工使用和经营，明确数据处理者针对数据享有哪些经济利益。就此而言，积极权能的观念是对权利主体应当享有的利益的具体呈现，积极权能彰显了财产权的目的。其次，为了实现权利主体应当享有的利益，法律体系还进一步规定了一项财产权的消极权能，即施加给不特定陌生人的相关义务。此时，权利主体的利益成为给他人施加义务的理由。拉兹的权利理论主张，当且仅当义务被赋予以服务或保护某人的利益时，这个人才是权利的承担者。因此，利益是产生义务的理由。权利是对权利主体来说足够重要的利益，足以作为指导他人行动的排他性理由，因此他人被施加了若干义务。[33]故此，消极权能是实现积极权能界定的经济利益的手段。最后，在积极权能和消极权能之间存在“目的与手段”的关系。以所有权为例，其积极权能是所有权人可以按照自己的意愿处置其物，包括但不限于占有、使用、收益和处分；其消极权能是排除他人一切干涉。积极权能与消极权能通常被并列看待。但在笔者看来，积极权能是所有权的目的，而消极权能则是实现目的的手段，即所有权的效力或作用。正是因为所有权所要实现的目的是赋予所有权人按照自己的意愿处置其物，各个法律体系才规定所有权人可以排除他人一切干涉。

将积极权能看作所有权的目的，将消极权能看作实现目的的手段，最大的理论意义在于：若是所有权（或者其他财产权）给不特定陌生人施加的相关义务存在争议时，法律适用者可以一再地回到所有权的积极权能中，探究某一存在争议的相关义务是否属于实现所有权的积极权能所必需的。倘若这一相关义务所要实现的利益超越了所有权的积极权能的边界，那么法律适用者就不能将该相关义务认定为所有权的消极权能，否则将会过度干涉社会公众的行动自由。兹以所有权为例进行说明：德国学者泽熙教授（Herbert Zech）在讨论所有权的边界时，将所有权的积极权能限定为竞争性利用，并且据此厘清了所有权人施加给他人的不得干涉之义务的边界。具体而言：首先，尽管《德国民法典》第 903 条的规定赋予所有权人按照自己的意愿处置其物，似乎是将对物之全面支配分配给了所有权人，也就是说所有潜在的对物进行利用的方式均由所有权人独占享有，但是在信息社会中，所有权人的积极权能并非全面的，而是基于特定目的而产生，因此是存在其边界的。其次，泽熙教授进一步指出，所有权之积极权能的边界在于竞争性。易言之，竞争性乃是对物支配定义中的隐藏标准。只有那些涉及对物的利用行为具有竞争性的积极权能，才是所有权所要追求的目的。再次，只要他人实施的行为会影响所有权人对物的竞争性利用，那么这些行为就构成对所有权的妨害。相反，倘若他人实施的行

为并不涉及对物的竞争性利用，那么这些行为就不构成对所有权的妨害。在这个意义上，他人未经房屋所有权人同意而对房屋外景进行拍摄的行为，并不构成对所有权的妨害。尽管拍摄行为看起来未经同意而对房屋外景实施了利用行为，但是拍摄行为并不属于竞争性利用，因此不落入所有权效力的范围中。[34]这一论证表明，在分析一项诸如所有权的复杂权利时，应当先明确所有权所要实现的目的是什么，再据以判断所有权的效力边界，即所有权给不特定第三人施加的义务之边界。

综上，尽管财产权中的积极权能不直接调整权利主体与其他主体之间的关系，不具有规范力，但是积极权能并非毫无必要。积极权能和消极权能并不属于同一范畴，前者乃是目的，后者则是手段。积极权能往往涉及权利主体可以实施的行为类型，体现了权利主体可以获取的利益，彰显了权利的目的。而实现这些目的的手段，则是真正调整人与人之间法律关系的规范性要素，即财产权的消极权能。反过来，一项权利在多大程度上给哪些义务主体施加何种义务，则取决于权利的目的。因此，积极权能与消极权能既不会排斥彼此，也非简单并列，而是存在“目的与手段”的关系。在积极权能与消极权能之间，存在着合目的性与合比例性等方面的考量标准。

三、认真对待消极权能

在数据确权的讨论中存在着一种积极权能偏好，理论家要么只讨论积极权能而完全没有提及消极权能，要么只是在界定积极权能之后，将消极权能界定为不得干涉、阻碍该积极权能的义务，消极权能似乎只是积极权能的附带产物。然而，在实践推理中真正发挥指导行动之功能者，恰恰不是积极权能，而是消极权能。因此，在数据确权中，应当认真对待消极权能。

（一）消极权能的概念分析

消极权能这一概念存在两种不同的理解方式。一种观点将消极权能定义为绝对权请求权。例如“消极权能就是指所有权在受到侵害以后所产生的物权请求权，它是指所有权在遭受损害的情况下，权利人对所有权进行保护的权利。”[35]根据这一观点，所有权的消极权能就是物权请求权。另一种观点认为，消极权能是指绝对权施加给他人的相关义务（或称指向性义务）。例如《德国民法典》第 903 条的条旨为“所有权的权能”（Befugnis des Eigentums），明确规定了所有权人按照自己的意愿处置其物，并且排除他人一切干涉。其中，“排除他人一切干涉”不是请求权基础规范，该条没有规定用以实现所有权人之法律权能的请求权。[36]按照本文的术语，《德国民法典》第 903 条只是规定了所有权施加给不特定陌生人的相关义务，但是没有赋予所有权人诸如返还原物、排除妨害或者消除危险请求权，这些请求权被规定在《德国民法典》的第 985 条和第 1004 条。因此消极权能是一回事，而用于实现消极权能的绝对权请求权则是另一回事。

问题在于，应当在哪一种意义上使用消极权能这一概念呢？笔者倾向于在第二种意义上使用消极权能这一概念。这是因为：消极权能通常被认为是所有权的内容（Inhalt）。[37]这意味着，只要存在一个所有权，那么在逻辑上就必然同时存在作为所有权内容的消极权能。例如，当我享有一辆汽车的所有权时，他人就对我负有不得干涉我的汽车的相关义务。但是，存在一个所有权，并不必然同时存在一个排除妨害请求权。排除妨害请求权至少应当包含两个构成要件：一是我拥有一个所有权，二是存在所有权妨害的事实。[38]据此可知，即便我享有一辆汽车的所有权，若非存在妨害事实，我将不实际享有一个排除妨害请求权；当且仅当存在妨害事实时，我才享有一个排除妨害请求权。因此，排除妨害请求权在概念上不可能是所有权的内容。在逻辑上不可能出现“集合存在、但是集合中的元素不存在”的局面。排除妨害请求权只能是所有权遭受妨害之后产生的救济性请求权，而非所有权的内容，亦非所有权的消极权能。

事实上，王利明教授在阐释数据权益的消极权能时，区分了“静态层面”和“动态层面”，具体而言：“持有权是静态层面的权利，其重点在于要

求不特定第三人不得随意利用归属于数据处理者的数据，而不是数据处理者提出具体的权利主张。停止侵害、排除妨碍和消除危险请求权则是动态层面的权利，即在数据财产权遭受侵害或者妨碍这一新的法律事实发生后，数据处理者针对特定的加害人或者妨害人提出的停止侵害或者排除妨碍的请求权。”[39]这一区分可资赞同。数据权益的静态层面仅指一项法律地位给不特定第三人施加的相关义务，而动态层面则是该项义务遭到违反之后，权利主体享有的用于执行该项义务的请求权。在讨论数据确权时，首先应当明确的是数据权益给不特定第三人施加的相关义务，然后才能讨论第三人违反该义务之后，权利主体享有何种请求权。故此，本文所称消极权能是指一项绝对权施加给不特定陌生人的相关义务。

（二）消极权能的规范性

消极权能之所以应当受到认真对待，是因为消极权能在两个层次上发挥着规范性。在一阶权利的意义上，由于消极权能是指一项绝对权施加的相关义务，因此消极权能本身就是其他主体的行动理由。在二阶权利的意义上，消极权能则是权利主体享有的改变法律关系的权力的出发点。具体而言：

1. 消极权能是其他主体的行动理由

绝对权在实践推理中的规范性作用，是通过其消极权能而非积极权能实现的。上文指出，积极权能既不是权利主体的行动理由，也不是其他主体的行动理由，尤其是弱许可意义上的积极权能对于实践推理几乎没有贡献。但是，一个绝对权的消极权能意味着给不特定陌生人施加了相关义务，该相关义务对陌生人在日常生活中的行动产生了拘束，因此绝对权的消极权能就是不特定陌生人的行动理由。例如，不动产所有权给陌生人施加了不得随意进入的相关义务，任何人在面对该不动产时，该相关义务均是其不进入不动产的行动理由。

绝对权施加的义务不仅仅是陌生人权衡的一阶理由，而且还是二阶理由，或者准确地说是排他性理由。通常情况下，一个人是根据一阶理由的权衡决定如何行动的。一个人在决定是否进入一块不属于自己的土地时，节省时间是支持进入的理由，可能遭受攻击的危险是反对进入的理由，这个人将权衡两个理由最终做出行动。但是，排他性理由与此不同。排他性理由通过排除特定一阶理由，从而改变了人们的行动。由于土地所有权给不特定陌生人施加了不得进入的义务，这一义务排除了行动者节省时间的理由；这一义务还改变了作出行动的权衡方式，即将通过一阶理由的权衡来作出行动转变为了直接遵守既定的行为准则来作出行动。[40]在一个没有法律的原始社会，一个人可能在权衡了一阶理由之后，因节省时间的理由胜过了可能遭受攻击之危险的理由而进入一块土地。但是在一个法治社会中，这个人的理由权衡发生了变化，土地所有权施加的不得进入的义务作为排他性理由，排除了一阶理由的权衡。在日常生活中，人们面对不属于自己的土地时，往往不需要权衡，就下意识地作出不穿行于该土地的行动。这是因为，土地所有权施加的义务已经成为一个成熟法治社会中每个人作出行动时的排他性理由。

正是由于绝对权的消极权能（施加的相关义务）是实践推理中的排他性理由，绝对权才能发挥调整权利主体与不特定陌生人之间法律关系的功能。倘若绝对权的消极权能只是一阶理由，因而可能被其他理由所胜过，那么在每一个陌生人的理由权衡中，可能得出不同的决策。可能对有的人来讲，绝对权施加的义务作为行动理由仍然会胜过其他一切理由；但是，对有的人来讲，节省时间的理由将会胜过绝对权施加的义务，那么他将枉顾绝对权的存在而穿行于他人土地。在这样的社会中，绝对权及其消极权能的存在无法发挥调整权利主体与不特定陌生人之间法律关系的功能。在这个意义上，有的学者，主张财产权（作为一种绝对权）之所以可以产生对世效力，不只是因为法律的制裁和权利主体的自助行为，而是因为财产权通过简单信号形成了稳固的“不得干涉”的道德观念。[41]

以上论证旨在说明，绝对权之所以可以发挥调整权利主体与不特定陌生人的法律关系的功能，是因为绝对权的消极权能乃是陌生人的排他性理由，

指导着陌生人在日常生活中的行动。故此，在确立一个诸如数据权益的绝对权时明确它的消极权能举足轻重。

2. 消极权能是法律权力的作用对象

可能会有论者主张，数据确权不仅仅是为了调整权利主体与不特定陌生人之间的法律关系，也是为了调整因权利主体让渡数据权益（包括转让和许可使用）而产生的法律关系。《数据二十条》第 5 条提出“鼓励探索企业数据授权使用新模式”；并且第 4 条中的“建立数据资源持有权、数据加工使用权、数据产品经营权等分置的产权运行机制”通常被理解为数据流通阶段数据权益的“权利分置”或者“权能分离”的结果。[42]循此观点，在数据流通阶段更加重要的似乎是积极权能，而非消极权能。尤其是“权能分离”理论主张，当且仅当数据所有权人享有持有权、加工使用权和经营权的积极权能时，该所有权人才能将这些积极权能分离出去，交由数据用益权人享有。[43]在数据权益的让渡中，数据权益的消极权能似乎不是那么重要了。本文尝试论证的是，消极权能不仅仅是其他主体的行动理由，还是权利主体享有的、改变其与其他主体之法律关系的权力（power）的出发点。故此，即便是在数据权益的让渡中，消极权能也值得认真对待。

权能分离理论来源于传统物权法。该理论主张，定限物权乃是所有权的占有、使用、收益和处分权能发生分离的结果。定限物权与所有权之间的关系，恰似子权与母权之间的关系：定限物权派生于所有权，所有权是定限物权的母权，定限物权是所有权的子权。母权必须蕴含子权的基因，母权的权能要遗传给子权。[44]德国学者也主张，所有权人有可能为了他人的利益，自其完全权利中“分离”出去一部分权能，并且这种分离可以采取使该他人取得一项物权性权利的方式实现。[45]根据权能分离理论，当且仅当所有权人享有特定的积极权能时，该所有权人才能将积极权能分离出去授予他人，后者由此取得用益物权。这是一幅非常符合日常经验的图景，权利人如同让渡一个苹果一样让渡积极权能。

然而，英美法的财产理论提供了另一幅图景：财产的许可使用或者转让的逻辑起点，不是积极权能，而是消极权能。由于财产权的消极权能给不特定陌生人施加了不得干涉的义务，因此当陌生人想要利用该项财产时，其首先需要克服的，乃是财产权施加的义务。在一个以私法自治为基本原则的社会中，权利主体不仅可以通过排除他人干涉而独自享受利用财产的经济利益，还可以通过有选择地不排除他人（免除他人不得干涉的义务），从而实现财产的社会性利用。也就是说，权利主体有权通过改变财产权施加的相关义务，从而允许某些人利用财产。在这个意义上，“财产权就像一道门而不是一堵墙”。[46]财产权的享有者如同“守门人”（gatekeeper）一般，有权决定谁在何种条件下可以使用财产。[47]这一比喻具备法理上的正当性基础。在哈特的权利理论中，一个人若是拥有权利，那么其就对他人承担的相关义务享有广泛的控制权，其如同一个小型的主权者一般控制着他人承担的义务：首先，权利持有者可以放弃或撤销义务，也可以让其处于存续状态；其次，在义务遭受违反或者即将遭受违反之际，权利持有者可以通过赔偿之诉或者禁令之诉执行该项义务，也可以不予执行；最后，权利持有者还可以放弃因义务遭受违反产生的赔偿之责。[48]由此可见，若以消极权能为出发点，并且承认权利主体具有改变消极权能的法律权力，就可以演绎出财产权的让渡规则。

事实上，德国学者的晚近研究表明，定限物权的设定也是以消极权能为出发点的，即所谓的权能分离理论中首先蕴含着权利主体对其消极权能的改变。例如欧利教授（Ansgar Ohly）对私法中的“同意”的研究表明，在“同意”这一概念之下存在多个层级的同意类型，包括移转性权利转让、构成性权利转让、债权合同许可、不可撤回的同意以及可撤回的单方同意。它们的共同特征是：免除了行为人本来应当承担的某项义务，从而使得行为人实施的行为不具有违法性。[49]例如，诸如设定用益物权等“构成性权利转让”与可撤回的单方同意在免除义务的方面是一致的，即行为人本来不能进入某一土地，但是因其获得用益物权或者可撤回的单方

同意，就可以进入这一土地。这些不同层级的同意的差异只是表现在行为人的行动在多大程度上受到法律的保护。用益物权一经设定，所有权人就没有办法随意加以废除；但是，所有权人授予的单方同意是可以随意撤回的。然而，不管是用益物权的设定，还是可撤回的单方同意，它们的逻辑起点均是诸如所有权在内的财产权的消极权能。

以上论证的目的不是为了讨论权能分离理论是否正确，而是旨在说明，不管采取何种理论解释财产权的让渡问题，均以财产权的消极权能为起点。换句话说，财产权人享有的改变其法律关系的法律权力，其作用对象总是不可避免地作用于财产权的消极权能。故此，在确立一个新型财产权如数据权益的过程中，界定财产权的消极权能是不容忽略的。

（三）消极权能的界定方式

财产权的消极权能是指财产权施加给不特定陌生人的相关义务，即他人未经同意不得擅自利用财产。消极权能作为实践推理中的排他性理由，发挥着调整权利主体与不特定陌生人之间法律关系的功能，从而实现社会的协调运作。由此产生的下一个问题是，财产权的消极权能如何界定？

在理论上，财产权可以通过两种策略界定其消极权能，即不特定陌生人所负的相关义务，一是通过物理边界确定义务，二是通过行为规制确定义务。[50]具体而言：

其一，通过外在客体的物理边界界定义务。财产权承载着对外在客体进行分配的功能，并且调整人与人之间如何利用外在客体的法律关系。鉴于财产权所要调整的法律关系不是某些少数主体之间的法律关系，而是权利主体与众多的、不特定的陌生人之间的法律关系，财产权应当以一种简单明确的方式向社会公众说明他们负有何种义务，即通过“简单信号”说明财产权的存在及其边界。唯有如此，才能最大限度地减少人们在社会交往中的信息成本。[51]动产与不动产的物理边界，恰恰是这样的简单信号。这是因为，动产与不动产的“有体性”（tangibility）及其在现实空间中的物理边界（即架构），使得不特定的义务主体显著感知到行动自由的界限。所有权乃是通过物理边界界定相关义务的典范。所有权的权利边界原则上是由动产或者不动产的物理边界确定的。未经所有权人的同意，他人原则上不得干涉所有权人之物，[52]否则就构成妨害。此时，场域（Ortung）、权利和秩序实现了统一。[53]故此，界定消极权能的策略之一，就是利用外在客体的物理边界。

其二，通过涉及外在客体的行为规范界定义务。通过物理边界界定义务的前提，乃是外在客体的物理边界是清晰和显著的，以至于不特定陌生人可以轻易认识到财产权的存在及其边界。但是，诸如信息等无形财产的物理边界，恐怕就没有那么明显了。于此场景，财产权须通过涉及无形财产的行为规范加以一一界定。著作权乃是通过行为规范界定相关义务的典范。《著作权法》第 3 条规定了作品作为权利客体，第 10 条列举式地规定了他人未经许可不得实施的针对作品的利用方式。[54]由此可见，不同于动产或者不动产，信息作为权利客体的特殊之处在于：后者的物理边界无法像前者一样传递有关权利边界的信号。因此，以信息为客体的财产权，往往需要辅之以行为规范才能确定其消极权能。

当然，现行法中的各类财产权综合运用这两种方法共同确定义务。有的论者将客体的物理边界称为“垂直边界”，垂直边界使得一项客体不同于另一项客体；将涉及客体利用的行为规范称为“水平边界”，水平边界决定了哪些行为专属于权利人，哪些行为则由社会公众共同享有。[55]与此相似，亦有美国学者主张结合“排他策略”和“治理策略”界定财产权，排他策略划下了财产分配的“第一刀”（a rough first cut），用来解决广泛的、不特定的、开放的如何利用财产的分配问题；治理策略则是对重要的边际问题提供更加细致的方案。[56]例如，尽管所有权总体上是以物理边界界定其消极权能的，但是在相邻关系的场景中，现行法通过涉及不动产的行为规范进行更加细致的调整（《民法典》第 288 条至第 296 条）。

需要说明的是，强调财产权的消极权能，尽管对他人的相关义务有所侧重，但是不能简单等同于

行为规制模式。笔者认为，财产权模式与行为规制模式是渐进过度，而非截然二分的。首先，财产权模式本质上也包含对行为的规制，即通过施加相关义务的方式，一般性地要求他人不得实施特定行为。最为典型的财产权，如物之所有权，通过其物理边界界定他人的相关义务，即他人未经同意不得干涉所有权人之物。其次，诸如著作权等知识产权，乃是通过物理边界与行为规范相结合的方式规定他人的相关义务。因而有的学者主张知识产权是混杂行为主义规制要素的财产权；[57]有的学者甚至认为，知识产权本质上是一种行为规制。[58]最后，最为典型的行为规制，则通过纯粹的行为规范界定他人的相关义务，如《反不正当竞争法》第 11 条规定，经营者不得编造、传播虚假信息或者误导性信息，损害竞争对手的商业信誉、商品声誉。因此，包括数据权益在内的法益究竟采取何种法律保护模式，是财产权模式，还是行为规制模式，应当考察该种法律保护模式在多大程度上依赖于外在客体的物理边界。[59]下文将会说明，数据权益的消极权能在很大程度上可以通过数据的物理边界进行界定，因此数据权益更加靠近财产权模式，而非行为规制模式。

四、数据权益的权能体系

积极权能是财产权的目的，消极权能是财产权的手段。想要理解一个财产权的全部特征，就要同时检讨其目的和手段，探究其积极权能和消极权能。数据权益亦是如此。《关于促进企业数据资源开发利用的意见》提出通过“保护企业对其合法持有数据的开发利用、经营收益、流通交易等合法权益”的方式“完善企业数据权益保护机制”，其中企业对其数据的开发利用、经营收益、流通交易属于积极权能的范畴，唯有疑问的是，为了实现这些积极权能，数据权益的消极权能应当如何型构，政策文件似乎没有提及，因而有待理论上的澄清。

（一）数据权益的积极权能

数据权益的积极权能彰显的是数据确权的目的，即数据确权究竟想要保护的是何种利益。毫无疑问，数据权益的积极权能仅涉及数据的经济利益，而非人格利益，即“人财两分”。[60]唯须进一步讨论的是，数据权益所要实现的经济利益究竟为何？一种常见的思路是一一列举权利主体对数据的占有（持有）、使用、收益和处分（类似于《民法典》第 240 条）。本文第一部分已经论证了这一思路意义有限，并且容易挂一漏万。由此可能产生另外一种思路，即一般性地规定权利主体享有按照自己的意愿处置数据的权利（类似于《德国民法典》第 903 条）。然而如此界定数据权益的积极权能，将会掩盖数据权益所要实现的经济利益所具有的特殊之处，即数据权益所要实现的经济利益，不仅包括竞争性利益，也包括非竞争性利益。正是这一特殊之处，使得数据权益从根本上不同于所有权，也不同于知识产权。具体而言：

一方面，数据权益应当保障竞争性利益。这里所称的竞争性利益，是指当财产被人以某种方式使用时，其他人无法以相同的方式进行使用；[61]相反，非竞争性则是指财产可以被数人以相同方式加以使用。根据这一标准，所有权保护的是竞争性利益，而知识产权保护的是非竞争性利益。有的论者主张数据具有非竞争性，因而不应该进行数据确权。[62]这一论点忽视了数据具有竞争性的一面：数据的更改与删除是竞争性的，针对一个特定的数据副本，一人实施更改或删除的处理行为后，他人无法实施相同的处理行为。就此而言，数据的更改与删除和动产或者不动产的事实性处分十分相似。正是基于这一相似性，德国学者尝试通过数据载体的所有权实现数据权益的保护，即未经同意更改或者删除数据的行为，可以被评价为《德国民法典》第 823 条第 1 款意义上的所有权侵害。[63]这是因为：如果数据载体被损坏、破坏或其性质发生改变，就无疑构成了对物之所有权的侵犯。因此，当存储介质的磁化状态被更改、存储在这些介质上的信息被更改或删除时，这构成了所有权侵害。

另一方面，数据权益还应当保障非竞争性利益。通过数据载体所有权保护数据的观点，忽视了数据承载的非竞争性利益。例如，当他人未经同意复制数据时，不会改变数据载体的电磁结构或者电荷状态，因此并不构成所有权侵害。综上，数据的复制，

以及建立在复制基础上的后续利用行为通常是非竞争性的，这些非竞争性利益同样应当受到法律保护。

故此，数据权益的积极权能兼具竞争性利益与非竞争性利益，这使得数据权益完全不同于只保护竞争性利益的所有权和只保护非竞争性利益的知识产权，可以说数据权益兼具所有权和知识产权的部分特征。

（二）数据权益的消极权能

阐释数据权益的积极权能只是“描述”了数据确权的目的，还没有真正“规定”数据权益的规范构造，不足以作为实践推理中的行动理由调整数据权益主体与不特定陌生人的法律关系。数据确权还需要进一步确定数据权益的消极权能。一旦数据权益的消极权能得到明确，不特定陌生人的行为自由将会发生实质性改变。

1. 旨在保护数据竞争性利益的消极权能

数据权益所要保护的竞争性利益决定了，他人未经同意不得删除、篡改或者增加数据，即未经同意不得破坏数据的完整性。此乃数据确权工作应当予以确立的首要消极权能。

需要进一步讨论的是，现行法是否已经对数据中的竞争性利益给予了充分的保护，以至于无需进一步确立该消极权能？一方面，德国学说表明数据载体的所有权可以用于保护数据免受他人删除和更改，我国《民法典》第 240 条规定的所有权亦可实现同一功能。另一方面，《刑法》第 286 条第 2 款规定：“违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。”这一条款比较明确地给不特定第三人施加了一项关于数据的义务，即不得对计算机信息系统中存储、处理或者传输的数据进行删除、修改或者增加。不特定第三人若是违反这一义务，不仅可能面临刑事责任，还可能因违反保护性规范给权利人造成损害而承担侵权责任。笔者认为，尽管现行法可以对数据的竞争性利益提供一定的保护，但是在解释上可能面临一些难题。一方面，《民法典》第 240 条只有在数据持有者与数据载体所有权人是同一主体时才能发挥作用。在云存储的场景中，他人删除、篡改或者增加数据时，由于数据持有者不是数据载体的所有权人，因此其难以依据《民法典》第 240 条主张防御性请求权或者损害赔偿请求权，此时数据持有者的竞争性利益无法得到保护。另一方面，尽管《刑法》第 286 条第 2 款在理论上可以通过“保护性法律”转介到侵权法中，但是我国《民法典》实际上没有如同《德国民法典》第 823 条第 2 款一样明文规定，违反以保护他人为目的之法律者需要承担侵权责任。因此《刑法》第 286 条第 2 款在实践中可以在多大程度上转介到侵权法中，仍然存有疑问。相比之下，通过数据确权的方式，规定他人未经同意不得破坏数据完整性的消极权能，更具清晰性和明确性。

2. 旨在保护数据非竞争性利益的消极权能

数据权益所要保护的非竞争性利益决定了，数据持有者还应当享有禁止他人访问、复制或者使用数据的消极权能。笔者认为，在界定这一消极权能时，应当以数据的物理边界为中心，明确他人未经同意不得访问、复制或者使用数据。在这个意义上，尽管本文强调了数据确权中的消极权能，但是数据权益的法律保护应当更加靠近财产权模式，而非行为规制模式。具体而言：

第一，数据权益的消极权能首先应当借助数据的物理边界进行界定，而非一一列举他人不得实施的具体行为。数据权益如同其他财产权一样，在日常生活中发挥着指导海量不特定陌生人行动的功能，因此数据权益的法律构造应当具有一般性，而不应该过分复杂，以免造成大量的信息成本。在数据确权的一般化方案中，数据权益的消极权能应当通过数据的物理边界进行界定。存在疑问的是，数据是否存在物理边界？如果存在的话，应当如何描述？对此问题，笔者主张在虚拟层面上通过可访问性界定数据的物理边界。具体而言，在纯粹物理意义上，数据乃是数据载体中的电磁结构，因此难谓存在显著的物理边界。但是，数据不是通过其电磁结构参与人们的日常生活的，而是通过其在操作系

统和应用程序呈现的虚拟形式呈现在人类社会中的。在虚拟层面上，数据具有较为清晰的物理边界。数据的物理边界是通过其可访问性决定的。不管是普通用户浏览网页，还是数据处理者处理个人信息，数据的可访问性决定了人们的行为边界（如《个人信息保护法》第 27 条）。因此，数据的可访问性界定了一条非常明确的物理边界，为数据确权奠定了基础。数据权益的消极权能应当借助数据的可访问性进行界定。[64]

第二，访问是一切数据利用行为的起点，诸如复制、分析、挖掘或者公开数据，甚至是破坏数据完整性，均以访问数据为出发点。有的学者甚至认为，对信息的访问，在功能上类似于对动产或者不动产的占有。对信息的处理行为中，最简单的方式就是对信息的访问。[65]在技术上，任何对数据的利用行为均建立在数据访问的基础上。消费者对文本、图片或者视频等非结构性数据的利用，以访问数据为前提条件。对于消费者没有购买访问权限的数据，消费者没有访问可能性，因此也就无法利用数据进行娱乐。经营者对其他经营者的业务数据的利用，也以访问数据为前提条件。甚至可以说，恶意第三人想要攻击一个计算机系统，对该系统中的数据进行删除、修改或者增加，也是以访问该数据为前提条件的。故此，一个数据驱动的业务模式和经济模型，主要不是取决于一个企业通过占有载体实际控制的数据的大小，而是取决于该企业可以访问的数据的多少。[66]

数据访问与数据的后续使用之间难以得到有效界分，控制数据的访问等同于控制数据的利用。倘若某一主体可以访问数据，那么其就可能实施其他使用行为。数据持有者很难在允许他人访问数据的同时禁止他人使用数据。数据持有者若要独占数据，只能通过禁止他人访问的方式实现。在这个意义上，数据的可访问性是决定不特定陌生人如何对待数据的关键信号。相反，数据持有者若是想要赋予他人使用数据的权利，首先应当赋予他人访问数据的权利。为了应对市场失灵、克服数据垄断，立法者应当赋予他人的，也是访问数据的权利。例如，欧盟委员会的数据确权方案经历了从“产权化”到“去产权化”的变化，放弃了赋予数据生产者数据财产权，提出了更具针对性的数据访问权。[67]所谓数据访问权，是指在一定条件下赋予对数据访问具有利益的企业与消费者访问、使用数据的权利，也即在法律上要求数据持有者承担允许他人访问数据的义务。[68]由此可见，数据的访问权是数据权益的消极权能的核心。

第三，就非竞争性利益的保护而言，应当区分公开数据与非公开数据，分别界定数据权益的消极权能。就数据权益的竞争性利益而言，不管是公开数据还是非公开数据，数据持有者均享有禁止他人破坏数据完整性的消极权能。存在疑问的是，就数据权益的非竞争性利益而言，是否需要区分公开数据和非公开数据？有的学者主张通过创设高度标准化的“数据一般财产权”进行数据确权，这一权利的标准化程度如此之高，以至于公开数据和非公开数据的差异无关紧要，即应当赋予二者同一“数据一般财产权”。这一观点似乎主张，公开数据持有者也可以禁止他人访问、复制或者使用数据，但是这不会影响数据的非合意流通，这是因为公开数据持有者虽然“有权”禁止他人访问、复制或者使用数据，但是不会真的“执行”这一权利。[69]笔者认为这一观点值得商榷，这是因为：这一确权方案先是规定公开数据持有者具有禁止他人访问、复制和使用的权能，再将是否行使权能的选择交给公开数据持有者。该持有者可能在多数时候不行使权能，然而将在其认为有利可图的时候提起诉讼行使权能，从而给数据需求方造成极大的不确定性，终将限制公开数据的非合意流通。还有的学者主张先对数据进行统一确权，再通过法律推定的技术免除陌生人应当承担的相关义务。例如“将数据加以公开，本身向外界传递了可以自由访问和复制的意思，或者说，他人有权作此理解”。[70]又如“数据控制者自主公开数据的，应推定含有允许他人访问、获取和利用数据的意思”。[71]循此观点，公开数据权益先给陌生人施加了不得访问、复制或者使用的义务，但是因其具有公开性，因此应当推定公开数据持有

者又通过意思表示或者其他方式免除了陌生人的义务。这一权利构造未免叠床架屋。笔者认为，更加简明的确权方案应该是，区分公开数据与非公开数据，其中公开数据原则上允许他人访问、复制或者使用，除非他人的利用行为构成不正当竞争；非公开数据原则上禁止他人访问、复制或者使用，并且可以在此原则基础上明确若干他人可以访问数据的情形。当然，不管是公开数据还是非公开数据，均给不特定陌生人施加了不得破坏数据完整性的义务。

最后需要说明的是，界定数据权益的消极权能只是数据确权的起点。确定数据权益的消极权能之后，数据权益的静态结构就已经得到了确立。当且仅当法律明确数据权益将给他人施加禁止访问、使用或者破坏数据的义务，诸如数据资源持有权、数据加工使用权和数据产品经营权作为对该禁止性规定的“强许可”，才有规范性意义。《数据二十条》提出的数据资源持有权与数据加工使用权、数据产品经营权虽然均是从积极权能的角度命名的，但是它们可以在两种不同的层次上进行理解：一是在“弱许可”的意义上理解，即法律不予干涉的自由，不过上文已经论证，这不是数据确权的关键。二是在“强许可”的意义上理解，即通过授予许可使他人实施原本应被禁止的行为，正是在这个意义上，数据确权具有实益。详言之，数据加工使用权与数据产品经营权不应当被看作初始的数据资源持有者享有的法律权能，而应当被看作初始的数据资源持有者许可他人使用数据产生的权利。在这个意义上，《数据二十条》提出的数据加工使用权与数据产品经营权应当作为“强许可”加以理解。正是由于数据资源持有权人享有禁止他人访问与使用的消极权能，给不特定陌生人施加了一个抽象的、一般性的禁止性规定，才需要通过数据确权明确其他市场主体在何种情况下可以突破该禁止性规定，获得加工使用数据或者经营数据产品的积极权能。如此一来，数据确权的难题就是动态的权利让渡，即数据流通环节中各方主体之间的权利义务关系，包括数据提供方和数据接收方之间的权利义务关系、当数据接收方将其得到的数据再次提供给其他主体产生的法律关系、数据需求方是否享有某种权利强制获取数据、个人数据的信息主体在多大程度上可以携带数据等等问题。

结语

本文的目标不在于提出一套数据权益的全新方案，理论家与实务家已经提出了足够丰富繁杂的确权方案。本文的目标在于反思诸多数据确权方案中的概念工具，即基于实践哲学的行动理由，对财产权利中的积极权能和消极权能进行反思性讨论。在本文看来，如同任何一项财产权一样，数据确权的重点不应该是积极权能，而是消极权能。积极权能与消极权能不是简单的并列，而是目的与手段的关系。积极权能是财产权的终极目的，消极权能则是实现终极目的的具体手段。唯有消极权能能够直接调整财产权人与陌生人之间的法律关系，因此数据确权的重点在于确立其消极权能。

数据权益兼具竞争性利益与非竞争性利益，因此从根本上不同于所有权或者知识产权。为了保护数据的竞争性利益，数据确权应当赋予数据持有者禁止他人破坏数据完整性的消极权能；为了保护数据的非竞争性利益，还应当赋予数据持有者禁止他人访问、复制或者使用数据的消极权能。至此，数据权益的静态结构已经得到了较为充分的阐释。然而，这只是数据确权工作的起点，《数据二十条》提出的数据加工使用权与数据产品经营权不宜作为静态结构进行理解，否则其意义十分有限；而是应当作为“强许可”进行理解，即数据流通环节中各方主体享有的权利。它们是否应当如同物权法定原则一样定型化，还是遵循合同自由原则？这些问题仍需进一步的研究。

数据可以占有吗？——兼论数据持有的法律构造

此处删除了原文脚注，全文请参见《华东政法大学学报》2025 年第 2 期，转载或引用请注明出处。

作者：阮神裕

摘要：数据占有论将数据持有视为物之占有，通过直接适用或者类推适用占有制度解决数据利用引发的纠纷，从而在不创设新型权利的前提下对数据提供较为全面的法律保护。然而，占有保护、占有的权利推定效力和善意取得以及多层次的占有关系无法准确适用于数据场景。数据占有论忽视了占有制度只能用于保护竞争性利益的隐藏条件。数据兼具竞争性利益和非竞争性利益，其中非竞争性利益无法通过占有制度得到调整。数据持有的法律构造应当具备二元结构：一方面，数据的竞争性利益可以通过类推适用占有制度加以调整；另一方面，数据的非竞争性利益则应当通过建构以数据访问权为核心的法律制度加以调整。

一、问题的提出

2022 年 12 月 2 日，《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》）提出了“建立数据资源持有权、数据加工使用权、数据产品经营权等分置的产权运行机制”，国家数据局等部门《关于促进企业数据资源开发利用的意见》将其简化为“数据持有权、使用权、经营权”。其中，“数据持有”是基础性概念，被用来指称各类主体与数据之间的静态关系。一些域外的法律法规或政策文件亦使用了“数据持有者”（data holder）的概念。[1]然而，现行法还没有确立绝对权意义上的数据产权，“数据持有”充其量只能作为事实受到法律保护。“数据持有”容易让人联想到民法中的占有制度。倘若数据可以成立占有，那么即便不对数据进行确权，因数据利用引发的冲突亦可直接适用或者类推适用占有制度，从而在现行法中找到一个系统性的解决方案。但问题在于，数据真的可以被占有吗？占有的客体通常是动产或者不动产，作品、专利或者商标等无形财产不能成立占有，但是液体、气体或者土地上的空间等又可成立占有，并且不以物之支配为前提的财产权（如债权）亦有准用占有制度之可能。可见，数据是否可以成立占有仍有争辩空间。对此问题的讨论，显然不能停留于概念之争，而应当深究占有制度所要保护的利益类型为何，以及数据之上承载哪些需要保护的利益类型，方可辨明数据是否可以被占有。

进一步的问题是，倘若数据无法成立占有，那么数据持有意味着什么？在数据是否应当确权仍有争议的背景下，“数据持有”为数据进入法律领域提供了多种可能性：进可确立“数据持有权”作为基础性的数据产权，从中衍生“数据使用权”“数据经营权”等其他数据权益，最终形成数据权益体系；退可将“数据持有”作为受法律保护的事实状态，借鉴占有制度或者商业秘密保护等类似制度，在数据不确权的背景下对数据持有者提供法律保护。可以说，数据持有的法律构造意义十分重大。问题在于，数据持有究竟意味着什么？同样，对此问题的讨论也诉诸数据之上承载的利益类型。

为使数据持有的法律构造得到具体呈现，本文拟围绕现实场景展开讨论：一是数人分别或者共同持有同一数据的场景，如数人共同维护某一数据库的数据池、数据的许可使用、委托处理或者云存储等；二是数据来源不合法的场景。以上两种场景不仅在数据处理实践中较为常见，而且与占有制度密切相关。本文将会一再回到以上场景，讨论数据究竟是否可以被占有，以及数据持有的法律构造应当为何。本文尝试论证，数据之上既有竞争性利益又有非竞争性利益，[2]因此“数据持有”从根本不同于旨在保护竞争性利益的占有制度，亦从根本上不同于旨在保护非竞争性利益的知识产权制度。数据持有的法律构造具有双重属性，兼具占有或其他物权制度和知识产权制度的部分特征。

二、数据占有论及其缺陷

鉴于现行法还没有对数据进行确权，而数据持有者对数据的事实控制在一定程度上受到法律保护，[3]将数据持有等同于或者类比于物之占有的观

点就不足为奇。数据占有论的实益在于，其可以在不创设新型财产权利的情况下，通过直接适用或者类推适用占有制度，对数据提供较为全面的法律保护。然而，数据持有与物之占有“似是而非”，将占有制度用于数据场景，将在一定程度上扭曲占有制度。

（一）数据占有论及其理由

在数据确权的讨论中，有一种观点主张数据可以成立占有，因数据使用产生的冲突可以适用《民法典》第 458 条以下的占有制度。[4]这种观点的主要理由是：占有乃一种民事主体对客体的事实管领关系，而数据持有者通过占有数据载体或密钥等方式实际控制数据，数据持有在本质上等同于物之占有。还有一些论者在阐释数据产权时，承认数据的占有权能或者与占有权能高度相似的持有权能，即数据持有者可以对数据进行实际管领，并且排除他人的非法侵入、干扰、盗窃或者破坏。[5]在刑法领域，有的学者主张财产犯罪中的占有概念应当得到重塑，从而将他人非法获取数据的行为认定为刑法上以“非法占有”为要件的财产犯罪。[6]

数据占有论可能面临的一个难题是，占有的客体通常为动产或者不动产，只在少数情况下适用于液体、气体或者土地上的空间以及无线电频谱等无体物。[7]而数据通常被归为无形财产，其能否成为占有的客体，不无疑问。[8]为此，有的论者退而求其次，主张数据可以成立“准占有”。准占有是指民事主体对财产权（如债权）的事实支配关系。该事实支配关系虽然不是占有，但是可以准用占有之规定。故此，尽管数据不是有体物，而是数字空间的无形财产，但是数据可以成为准占有的客体。[9]

以上观点均在一定程度上将数据持有等同于物之占有，可统称为“数据占有论”。数据占有论的实益在于，通过直接适用或者类推适用《民法典》第 458 条以下的占有制度，解决数据使用引发的冲突，从而在不创设新型权利的前提下对数据提供较为全面的法律保护。具体包括以下三个方面：第一，《民法典》赋予占有人的自力防御权和防御性请求权可以适用于数据。诸如“侵夺”“拷贝”数据，或者“非法接入接口”访问数据的行为，类似占有侵夺或占有妨害，数据持有者可以对此主张占有保护。[10]第二，数据持有可以适用占有的权利推定效力，即通过证明“事实上的控制”来推定数据持有者享有合法的数据产权，从而减轻数据持有者的举证责任。[11]有的论者进一步主张数据占有可以产生公信力，相对人因为信赖行为人对数据占有的外观可以善意取得数据。[12]第三，数据产权的归属难题可以通过多层次的占有关系得到化解。例如：数据处理者将其收集的个人信息委托给受托人进行处理，数据处理者与受托人分别成立间接占有和直接占有；在云存储的场景中，云服务提供商为直接占有，用户则为间接占有。[13]

（二）数据占有论的缺陷

数据占有论似乎为数据保护和数据交易提供了全面的解决方案，然而若对占有制度进行细致考察就可发现，该制度无法完全适用于数据场景。占有制度在数据场景中的适用均在一定程度上扭曲了占有制度。

1.占有保护无法完全适用于数据

占有保护主要包括两类：一是占有人的自力防御权；二是基于占有的防御性请求权和损害赔偿请求权。数据占有论者主张，以上两种占有保护均可被适用于数据场景。然而，实际情况并非如此。

一方面，在数据场景中承认占有人的自力防御权似有不妥。就占有防卫权而言，即便没有适用占有制度，数据持有者既有权利也有义务使用技术措施保障数据安全（《数据安全法》第 32 条），从而实现占有防卫的功能。因此承认数据可以被占有，没有对数据安全保障提供更多的规范。就占有取回权而言，值得讨论的是，数据持有者是否可以使用强力取回或者删除他人非法复制的数据？美国 2017 年的《积极网络防御确定性法案》（ACDC）曾经提出赋予网络攻击的受害者以“积极反击权”，即允许网络被攻击的受害者采取诸如进入攻击者的系统以收集证据、识别攻击源及删除非法获取的数据等积极网络防御措施。[14]不过该法案没有得到通过。有的论者认为，赋予遭受网络攻击的受害者

以积极反击权，将会违背国家暴力垄断的原则。[15]笔者认为，对于积极反击权的正当性问题，存在进一步讨论的空间。然而，可以明确的是，不能仅仅因为数据持有的事实状态类似物之占有，就将占有取回权直接适用于数据场景。这是因为，占有的初衷在于保障现有的事实管领力，维护社会和平（即和平功能），并维持对物的持续占有（即维持功能）。占有取回权的功能在于，占有人可以在不能获得国家机关保护的情况下立即采取合理措施取回占有。在数据被他人非法复制的场景中，数据持有者本人对数据的持续控制其实没有遭到破坏，故此没有必要赋予数据持有者取回数据的积极反击权；相反，若赋予其积极反击权，可能引发网络空间的相互攻击，反而加剧网络秩序的破坏。

另一方面，将基于占有的防御性请求权适用于数据场景，可能面临另一个困难：非法复制数据的行为既不侵夺也不妨碍数据持有者对数据的事实管领，因此无法构成“占有侵夺”或“占有妨害”。为了弥补这一偏差，有的论者将非法复制产生的新数据视作原数据的孳息，原数据持有者可以基于孳息返还规则要求行为人返还或者删除数据。[16]这一观点值得商榷。其一，通过复制行为产生的新数据不符合“孳息”的定义。物的孳息是指该物的出产物和依该物的用法而从该物中取得的其他收获物，如奶牛的奶或幼崽、绵羊的毛、树木的果实等。物的孳息在与该物分离后，是不同于原物的新物。然而，非法复制形成的新数据与原数据在内容层面没有实质差异，难谓不同于原数据的“新物”。其二，即使认为未经同意复制的新数据与原数据在符号层面有所不同，从而认定其为孳息，但孳息返还规则本质上是被用来保护本权的权利人的，而非仅仅保护占有人。《民法典》第 460 条规定，不动产或者动产被占有人占有的，权利人可以请求返还原物及其孳息。据此，只有数据持有者享有主观权利时，其才享有孳息返还请求权；而数据持有的事实状态则无此项请求权。

2.占有的权利推定效力或善意取得无法适用于数据

数据占有论者将占有的权利推定效力适用于数据，可能产生两个方面的实益：一方面，在数据交易的场景中，若要求数据持有者一一证明其合法有效地取得数据产权，将会产生较高的交易成本，而数据占有的权利推定效力可以免去数据持有者的证明成本，促进数据流通。另一方面，在数据保护的场景中，数据持有者主张防御性请求权或者损害赔偿请求权时，亦可适用占有的权利推定效力，即数据持有者只需证明其事实上控制数据，无须证明其数据来源的合法性，就可以主张防御性请求权或者损害赔偿请求权。

本文认为，将占有的权利推定效力以及善意取得制度适用于数据有所不妥，理由如下：首先，占有产生权利推定效力的前提之一，是动产物权的转让原则上以现实交付（占有转移）为必要，只有在少数情况下进行观念交付，故此占有状态与真实权利关系相吻合的可能性极大。[17]然而数据交易恰恰相反。一则数据副本的事实移转并不一定伴随着数据产权的转让。例如，在数据的许可使用中，持有数据副本的被许可人不一定享有转让或者再次许可使用的权能。又如，在云存储中，持有数据副本的云服务提供商亦不享有数据产权。二则数据产权的转让不一定伴随着数据副本的事实移转。例如，在数据持有者将其数据存储在第三方服务器时，其可以在不移转数据的情况下转让数据产权。其次，占有的权利推定效力意味着，不论占有人是有权占有还是无权占有，均可推定其享有真实权利，交易相对人只要信赖占有的事实状态即可，不必追问占有人的权利来源。[18]然而数据交易与此不同。至少在个人数据交易中，数据交易的双方当事人均应当审查个人数据来源的合法性，其中数据提供者还负有确保个人数据合法性的结果性义务。交易相对人不能简单根据数据持有的事实状态，就信赖数据提供者享有合法的数据产权。再次，占有的权利推定效力往往是在诉讼程序中发挥作用的，即占有人可能无法证明其占有从何而来，或真实权利人可能难以证明其占有因何丧失，而法官不得不在事实真伪不明的状态下作出判决，故此法律特别规定占有之

权利推定效力，减轻占有人之举证责任。[19]然而数据的特征决定了，数据持有者可以简单地通过其网络日志、系统日志或者应用日志等技术手段证明其数据来源。这意味着，若数据持有者无法证明其数据来源，则不应当推定其数据来源为合法，反而应该推定为非法才更加符合数据的技术特征。最后，既然数据持有不能产生占有之权利推定效力，无法形成权利外观，那么基于权利外观的信赖而产生的善意取得也就不能轻易适用于数据场景。

3.多层次的占有关系无法适用于数据

数据占有论者还主张将直接占有与间接占有等多层次的占有关系适用于数据，然而数据的技术特征决定了多层次的占有关系无法适用于数据。

间接占有这一概念的功能在于，除对物的事实支配以外，另外承认间接的对物关系，形成多层次的占有关系，赋予间接占有人以占有的全部功能。[20]由于数据可能被数人分别或者共同持有，因此可以通过类推适用间接占有和直接占有规则，赋予数据持有者全面的法律保护。例如，甲将其数据委托乙进行分析处理，丙非法复制乙持有的该数据时，甲为间接占有人，乙为直接占有人，不管是甲还是乙均可主张基于占有的防御性请求权。[21]间接占有这一概念之所以必要，是因为间接占有人尽管失去了对物的事实支配，但仍有对物的利益，如针对第三人行使基于占有的防御性请求权，以免因直接占有人怠于行使这些请求权而终局性地失去占有物。

然而，“数据的间接占有”似无必要。在数据场景中更加常见的情况是，数据持有者共享数据时不丧失自己持有的数据原件，而是创建更多的数据副本，各个数据持有者独立控制数据副本。例如，甲将其数据委托乙进行分析处理时，甲没有必要将数据原件移转给乙，而是只提供数据副本，或者允许乙访问甲的数据库即可。于此场景，甲没有失去对数据的事实控制。即便第三人从乙处非法复制了甲的数据，甲也不会面临如同间接占有人可能终局性地丧失占有物的危险。因此，甲不符合间接占有人的定义，也不需要间接占有制度进行保护。有论者进一步指出，同一数据的多个副本可能被多个数据持有者控制，倘若承认数据的间接占有，这些数据持有者一方面直接持有自己的数据，另一方面间接持有他人的数据，间接占有人与直接占有人的数量将以辐射状激增，反而不利于澄清主体间的权利义务。[22]故此，将间接占有和直接占有的概念套用于数据场景有所不妥。

综上，尽管数据持有是一个受法律保护的事实状态，但以上论证表明数据持有总是在一定程度上偏离了物之占有。事实上，只要进一步考察占有概念本身就会发现，这种偏离不是“偶然性”的，而是“根本性”的。

三、占有的边界与数据的利益类型

占有制度无法完全适用于数据场景，究其根本，是因为占有的概念及其相关规则的适用存在一个隐藏条件，即占有制度只能被用于保护竞争性利益。而数据之上承载的利益不仅仅是竞争性利益，还包括非竞争性利益。对于数据的非竞争性利益，占有制度没有适用空间。需说明的是，本文所称“竞争性”或者“非竞争性”是指，当某一客体被人以某种方式使用时，其他人是否可以按照相同的方式进行使用，而非经营者在市场中相对于其他竞争对手享有的利益，因此不同于司法实践中认定网络运营者针对其竞争对手享有的“竞争性财产权益”的概念。[23]

（一）占有制度只能被用于保护竞争性利益

数据占有论的主要理由是数据持有的事实状态类似物之占有。在论及占有的前提条件时，民法学说通常要求民事主体对物具备事实管领力。[24]至于何为事实管领力，存在两个标准：一是人对物的影响可能性（Einwirkungsmöglichkeit），即人是否可以某种物理方式触碰物，从而对物施加影响。当然，这一标准也非绝对，例如尽管一个人可以通过触碰甚至损毁的方式对停放在停车场的汽车施加影响，但是不足以构成占有。二是排除他人干涉的防御可能性（Abwehrmöglichkeit），即当一个人能够排除他人对物施加的影响时，就存在事实管领力。当然，现在更加常见的标准是综合二者，即对物支配是人对物具备影响可能性和防御可能性的事实

状态。[25]萨维尼在《论占有》一书中写到，人们通常认为，占有某物的状态，不仅仅是在物理上可以自己对物施加影响，而且可以阻止他人施加影响。[26]至于在具体场景中，人对物是否具备影响可能性或防御可能性，则须依社会观念，参酌空间关系、时间关系甚或法律关系一一进行判断。

然而，以上标准所要回答的问题是：一个民事主体需对动产或者不动产实现多大程度的事实控制，才能满足“事实上的管领力”要求，从而成立物之占有？因此，在界定占有的概念时，常见的例子均是民事主体对动产或者不动产的控制关系，如居住于房屋、耕作于田间、身着西装等等。这些例子假定了客体是动产或者不动产，讨论的是主体对客体的控制程度。问题在于，倘若客体不是动产或者不动产，以上标准是否仍然适用？

对此问题，知识产权学者提供了一个较为清晰的答案：即便知识产权的权利人可以对知识产品施加影响，如修改作品、改进发明等，并且借助法律手段禁止他人复制作品、实施专利或者使用商标，表面上符合影响可能性与防御可能性的定义，但是作品、专利或者商标等无法成立占有，权利人不能像占有动产或者不动产一样占有无形财产。[27]由此可见，将占有概念置于作品、专利或者商标以及本文讨论的数据等无形财产的场景中时，影响可能性和防御可能性两个标准是不充分的。在占有概念及其相关规则中，仍然存在一个隐藏的标准，界定了占有制度的边界。

笔者认为，占有概念及其相关规则中的隐藏标准，乃民事主体对客体施加的影响必须是竞争性的。换句话说，占有制度只能用于保护竞争性利益。这一隐藏标准决定了占有制度的边界。具体理由如下：

首先，占有概念自始就以民事主体对客体的控制具有竞争性为前提。萨维尼认为，占有的概念及其应用都存在一个规则，这个规则具有非常普遍的性质，影响到占有理论的所有部分，这个规则就是：“所有占有都是排他的（ausschließend）。”即便是共同占有的概念，也没有违背这一规则。这是因为多人对一物进行同时占有时，他们的占有受到相互限制，他们只是表面上看起来共同占有一物，但实际上只占有物的一部分，而没有占有物的其余部分。[28]这里的“排他”就是占有的竞争性，即一方的占有将会干涉他方的占有，二者不可兼容。

其次，不仅仅是占有概念，整个占有制度均隐含着竞争性标准。第一，基于占有的自力防御权和防御性请求权所针对的占有侵夺和占有妨害，均具有竞争性。一旦他人侵夺了占有，占有人将失去其占有，占有的和平功能与维持功能均遭破坏；一旦他人妨害占有，占有人就无法按照自己的意愿支配占有物。他人的侵夺或者妨害或多或少排斥了占有人的物之支配，这种排斥就是竞争性标准的具体表现。第二，占有的权利推定效力之前提，乃一物要么为甲占有，要么为乙占有，不可能同时为二人或多人各自占有，因此他人可以信赖占有人享有其所行使的权利。善意取得之所以必要，是因为一物的所有权要么归属于所有权人，要么归属于受让人，法律必须作出决断，没有其他方式可以折中。第三，间接占有的概念具有实益，亦是因为物之占有具有竞争性，无法为数人同时进行全面的事实支配，法律不得不创设以媒介关系为基础的间接占有概念。

最后，占有的扩张适用或者类推适用亦以所要保护的利益乃竞争性利益为前提条件。具体而言：一方面，诸如液体、气体或者地上空间可以适用占有制度，关键不在于这些客体具备了有体物的某些特征，而是因为民事主体对这些客体的使用是竞争性的。谢在全先生认为，不论是气体、液体或者是土地上的空间，均属于人力可以排他支配的对象，因而可以被占有。[29]该标准可能存在模糊之嫌。根据该标准，诸如作品、专利或者商标等信息亦可成立占有，这不符合上文提到的知识产权学界的主流观点。更加合适的标准应该是，气体、液体或者土地上的空间可以成立占有，是因为民事主体对这些客体的使用是竞争性的。一方主体占据土地上的空间后，他方主体再也无法以相同方式使用同一空间。尽管气体、液体或者土地上的空间不是严格意义上的动产或者不动产，但是民事主体对其进行使用产生的利益冲突与动产或者不动产无异，因此可以适

用占有规则。另一方面，准占有的概念成为可能，同样是因为不以物之支配为内容的财产权的行使具有竞争性。准占有的典型事例，乃债权准占有，即债权的准占有人行使债权请求权，或者受领债务人的给付时，因具有事实上支配债权的外观，而准用占有的权利推定效力，发生清偿效果。例如，某人利用伪造的银行卡提取原告存在被告银行处的存款，原告诉请被告银行赔偿损失。一、二审法院均驳回了该诉讼请求，其主要理由是，伪造银行卡的人可以构成债权准占有人，被告银行尽了形式审查义务后向债权准占有人提供给付，应当发生清偿效果。[30]债权可以成立准占有，是因为债权请求权的行使是竞争性的——债务人只需提供一次给付，该给付要么被真实债权人受领，要么被债权准占有人受领，从而发生清偿效果。正是因为真实权利人和债权准占有人之间的利益关系类似真实权利人和占有人之间的利益关系，即二者对同一利益具有竞争性关系，因此在债务人因信赖债权准占有的外观而提供给付时，才有准用占有的权利推定效力的余地。

由此可见，占有制度只能被用来保护竞争性利益，而数据的特殊之处恰恰在于其具有非竞争性。一人对数据的使用，通常不会影响他人对数据的使用。因此，数据占有论失败（至少是不完整的）的根本原因在于忽视了数据上的非竞争性利益与占有制度无法契合。

（二）数据兼具竞争性利益与非竞争性利益

数据占有论的问题在于，其忽视了数据上的非竞争性利益。与此相反，一些主张数据应该成为知识产权的客体的观点，[31]虽然正确地强调了数据所涉利益的非竞争性，但同样是片面的，忽视了数据上的竞争性利益。事实上，数据的特殊之处在于，其承载着两种不同的利益类型：一是竞争性利益，二是非竞争性利益。[32]

一方面，数据之上承载着竞争性利益，主要表现为禁止他人更改、删除或者增加数据的利益，可以简称为“数据的完整性利益”。对数据进行更改、删除或者增加的行为是竞争性的，针对一个特定的数据副本，一人实施更改、删除或者增加的处理行为后，他人无法实施相同的处理行为。尤其是一人对数据进行永久性破坏后，他人将无法使用数据。就此而言，数据的更改、删除或者增加与动产或者不动产的事实性处分十分相似。尽管数据被更改、删除或者增加后可以复原，但是这一特征不影响这些行为的竞争性，正如动产或者不动产的事实性处分亦可恢复原状。正是基于这一相似性，德国学者尝试通过数据载体的所有权实现数据产权的保护，即未经同意更改、删除或者增加数据的行为，实际上属于未经同意行使了竞争性权能，因而可以被评价为《德国民法典》第 823 条第 1 款意义上的所有权侵害。[33]也正是基于这一相似性，数据占有论具有部分的正确性。[34]

另一方面，数据之上同时承载着非竞争性利益，主要表现为禁止他人进行访问、复制或者传播等数据使用行为的利益。如同作品或者其他信息产品，对信息进行访问、复制或者传播的行为是非竞争性的。[35]通常认为，数据作为新型财产，最为重要特征即非竞争性。那些主张数据上不应该确立私人的财产权利，而应当将其作为公共产品进行法律规制的观点，其主要理由就是数据的使用具有非竞争性。[36]而主张数据应当确权者，亦同意数据具有非竞争性，且恰恰是因为数据具有非竞争性，其法律保护才必须通过确权等法律手段进行，否则很难保护相关主体的数据产权。[37]有的论者基于数据的非竞争性与知识产权客体的属性高度相似，进一步主张数据应当成立知识产权。[38]可以明确的是，数据的使用行为通常具有非竞争性，此与知识产权十分相似，但数据的更改、删除或者增加则是竞争性的。完全忽视数据的竞争性利益，将数据纳入知识产权体系，恐怕有所不妥。尽管如此，用于调整非竞争性利益的知识产权的相关规则，可以为数据持有的法律构造提供一定的启示（详见下文）。

综上，数据的特殊之处在于，其不仅承载着竞争性利益，还承载着非竞争性利益。这使得数据不同于有体物，也不同于作品、专利或者商标等其他无形财产。虽然数据和作品、专利或者商标均是无

形财产，但数据既是具体的又是抽象的——作为具体的无形财产，数据可能被破坏，数据的使用可能被妨碍，数据呈现出类似有体物的特征；作为抽象的无形财产，同一数据可以同时存在于数个载体之上，因此呈现出类似作品、专利或者商标等知识产品的特征。相比之下，知识产品只有抽象的一面，知识产权提供的法律保护只在禁止他人未经同意使用知识产品，但是几乎不曾担心知识产品遭到破坏，亦不担心他人妨碍权利人行使知识产权。在这个意义上，数据的确是一种新型财产，数据持有或数据持有权的法律构造从根本上既不同于保护竞争性利益的占有或者物权，也不同于保护非竞争性利益的知识产权。

四、数据持有的二元结构

既然数据之上既有竞争性利益又有非竞争性利益，那么数据持有的法律构造就应当具有二元结构：一部分用于调整数据的竞争性利益引发的法律问题，另一部分用于调整数据的非竞争性利益引发的法律问题。[39]前者可以有限地类推适用占有制度，后者则需要创设数据访问权的概念，借鉴知识产权领域的相关规则对数据访问权的保护和交易制度进行建构。

（一）数据的竞争性利益与占有保护

数据持有的法律构造应当对数据上的竞争性利益提供保护，在此限度内，数据持有可以类推适用占有制度。当他人实施更改、删除或者增加数据等侵害数据完整性的行为时，由于这些行为侵害的是数据上的竞争性利益，数据持有者可以主张占有保护：一方面，数据持有者有权采取适当的技术措施防止他人侵害数据完整性。数据持有者享有的自力防御权应当仅限于占有防卫，即采取一定的技术措施防止他人破坏数据完整性。对于他人实施的非法复制行为，数据持有者是否可以采取技术手段进行防御甚至反击的问题，不应当诉诸占有制度，而应当使用数据访问权的概念建构基于非竞争性利益的法律规则。另一方面，数据持有者基于持有数据的事实状态享有停止侵害、排除妨害等防御性请求权。对于数据持有者的防御性请求权，应当结合数据持有的特定场景展开讨论，详述如下：

第一，数据持有者的防御性请求权建立在数据持有的事实状态基础上，在数人分别或者共同持有同一数据的场景中亦是如此。（1）在数据的共同持有（数据池）中，每个持有者实际上均事实持有数据，因而均可主张防御性请求权。（2）在云存储中，不管是云服务提供商还是用户，均可针对他人侵害数据完整性的行为主张防御性请求权。（3）在数据的许可使用中，若许可人与被许可人同时持有同一数据的不同副本，二者仅对其实际持有的数据副本享有防御性请求权。被许可人持有的数据副本遭到破坏时，没有理由赋予许可人防御性请求权；反之亦然。但若被许可人没有取得独立的数据副本，而是通过 API 接口实时访问许可人的数据，则只有许可人对其事实上持有的数据享有防御性请求权。（4）在数据的委托处理中，若委托人与受托人同时持有数据副本，那么二者同样仅对其实际持有的数据副本享有占有保护；若委托人将其数据提供给受托人，委托人不再实际控制数据，则针对他人实施侵害数据完整性的行为，受托人可以基于数据持有的事实状态主张防御性请求权，而委托人基于其享有的数据产权（本权）享有防御性请求权，二者有所不同。

第二，数据的占有保护不以数据持有者享有合法的数据产权为必要。值得讨论的是，数据持有者非法获取数据时，是否可以主张防御性请求权？例如，甲非法收集个人信息形成数据集合，乙植入的病毒软件导致甲无法访问该数据集合，乙的行为妨害了甲的数据处理，于此情形，甲是否可以主张排除妨害请求权？由于乙的行为侵害了甲的竞争性利益，因此存在类推适用占有制度的空间。《民法典》第 462 条规定了基于占有的排除妨害请求权，该项请求权不以有权占有为前提，即便是恶意的无权占有人亦受保护。[40]根据这一规定，尽管甲的数据来源不具合法性，其亦应当享有基于数据持有的排除妨害请求权。因为基于占有的排除妨害请求权是基于纯粹的占有事实（possessorisch），而非基于本权（petitorisch）产生的防御性请求权，其功能在于维护社会和平。这一理由同样适用于数据持有。

为数据持有的秩序和平考虑，数据的占有保护应当建立在数据持有的事实状态基础上，不问数据持有的合法性来源。当然，若乙是被非法收集个人信息的信息主体，其为保护个人信息安全而在甲的系统中植入病毒，则乙可以基于个人信息权益提起反诉，要求甲删除个人信息。

（二）数据的非竞争性利益与数据访问权

数据持有的法律构造还应当调整数据的非竞争性利益引发的法律问题，上文表明占有制度无法用于保护这些非竞争性利益，为此应当引入数据访问权等概念。

1.数据访问权的概念

数据访问权是指，数据持有者享有的在一定条件下禁止他人访问数据的权利。数据持有者固然享有访问数据的积极权能，但是这种积极权能无须法律赋予，即便没有数据确权的法律或政策，数据持有者也可以访问其收集的数据，因而积极权能不是数据确权的重点。数据访问权的规范重心是其消极权能，即禁止他人访问、复制、传播等使用数据的消极权能。可以说，数据访问权是“排他权”，而非“自用权”，与知识产权具有相似性。

对于数据访问权的性质及其效力，需要说明的是：

第一，数据访问权是数据非竞争性利益的典型表现。除了数据访问权，数据持有者还享有禁止他人复制、分析、挖掘、传播或者公开数据的权利（权能）。这些权利均建立在数据访问的基础上：一方面，在技术上，任何对数据的复制、分析、挖掘、传播或者公开等利用行为，均建立在数据访问的基础上。有的德国学者甚至认为，对信息的访问，在功能上类似对动产或者不动产的占有。对数据产权的法律权能进行分配时，首先需要考虑的就是访问权能。[41]另一方面，数据访问与数据的后续使用之间难以得到有效界分，控制数据的访问等同于控制数据的利用。倘若某一主体可以访问数据，那么其就可能实施其他使用行为。数据持有者很难在允许他人访问数据的同时禁止他人使用数据。数据持有者若要独占数据，只能通过禁止他人访问的方式实现。故此，数据访问权是调整非竞争性利益的核心概念。

第二，数据访问权应当是数据持有者享有的数据产权的法律权能，而不仅仅是用户或者第三人在特定场景中享有的请求权。数据访问权的概念可能存在两种含义：一是数据产权的法律权能。例如，有的学者主张，对信息进行法律权能的分配，首先应当考虑的是信息访问权，即谁有权访问信息，并且控制他人对信息的访问。[42]二是用户或者第三人访问数据的权利。欧盟的数据立法经历了从“产权化”到“去产权化”的变化，最终颁布的《数据法》创设了数据访问和使用权，这些权利旨在赋予用户或第三人访问数据的权利。[43]我国亦有学者主张数据访问权是享有合法利益的第三人访问数据持有者实际控制之数据集合的权利。[44]以上两种含义并不冲突。正是由于数据持有者对其实际控制的数据享有控制他人访问的权利，因此才有必要通过法律规定赋予用户或者其他第三人访问数据的权利。在著作权法领域亦有类似的构造，著作权人享有的复制权是禁止他人复制的权利，而他人基于合理使用复制作品的权利亦可称为复制权。

尽管如此，在数据确权的讨论中，更加重要的是将数据访问权界定为数据产权的法律权能。欧盟数据立法中赋予用户或者第三人的数据访问权，只能调整数据持有者与用户之间的权利分配。至于数据持有者究竟享有何种法律地位，欧盟的数据立法目前还没有给出答案。相比之下，我国《数据二十条》等文件的思路和欧洲立法有所不同。《数据二十条》提出：“根据数据来源和数据生成特征，分别界定数据生产、流通、使用过程中各参与方享有的合法权利，建立数据资源持有权、数据加工使用权、数据产品经营权等分置的产权运行机制。”该文件的目标不是仅调整数据持有者与用户之间的法律关系，而是探索建立全面的数据产权制度，赋予市场主体一般性的数据产权。[45]故此，数据访问权的概念不仅是指用户或者第三方在某些场景下请求访问数据的权利，而且是数据持有者享有的数据产权的法律权能。

第三，数据确权的难题在于，何种情况下应当赋予数据持有者全面的数据访问权（即完全排除他人访问数据的权利），而在何种情况下只能赋予数据持有者有限的数据访问权。笔者主张区分公开数据和非公开数据分别界权。若数据是可访问的或者公开的，他人原则上应当可以自由访问、复制或者使用数据，只要这些利用行为不构成不正当竞争即可。相反，若数据是不可访问的或者非公开的，那么他人负有未经同意不得访问、复制或者使用数据的义务。[46]之所以作此区分，主要是基于信息成本的考虑。在操作系统和应用程序呈现的虚拟界面上，数据的物理边界是由其可访问性决定的。正如动产或者不动产的物理边界决定了不特定陌生人的行为边界一样，[47]数据的可访问性也决定了其他主体是否可以使用数据的边界。倘若一个网站一方面允许人们访问数据，另一方面又禁止复制或使用数据，那么就会引发数据持有者进行加密、其他主体采取各种手段进行解锁的拉锯战，影响普通用户访问数据的流畅度，最终阻碍信息流通。因此，不妨以数据的可访问性为标准进行界权，可访问的数据通常也是可以自由使用的，而不可访问的数据通常就是不可使用的。

2.数据访问权的保护

数据访问权旨在保障数据持有者对数据享有的非竞争性利益，数据访问权与知识产权更有相似性，其法律构造应当参考知识产权，而非占有制度。

首先，在判断他人使用数据的行为是否构成对数据访问权的侵害时，应当考察该行为是否落入数据持有者享有的专有权利领域。例如，他人未经同意访问、复制或者使用非公开数据的，通常应当被认定为侵害了数据访问权，除非他人可以证明其行为属于合理使用的范畴。相反，对公开数据的使用原则上不应当被认定为侵害数据访问权。若他人实施的行为属于数据持有者的专有权利，数据持有者享有停止侵害、排除妨碍或者消除危险等防御性请求权；行为人造成损害的，数据持有者可以依法主张损害赔偿请求权。[48]

其次，在数人分别或者共同持有同一数据的场景中，针对他人实施的非法访问行为，只有数据持有者享有数据产权时，其才享有防御性请求权或者损害赔偿请求权。（1）在数据的共同持有中，因各个持有者共同享有数据产权，故均可主张数据访问权保护。（2）在云存储中，尽管云服务提供商和用户均持有数据，但是只有用户享有数据产权，因而只有用户可以主张数据访问权保护（不同于上文提到的数据的占有保护）。(3)在数据的许可使用中，被许可人是否可以主张数据访问权保护的问题，与知识产权的被许可人是否享有防御性请求权的问题具有相似性，即他人未经同意利用数据时，并不妨碍被许可人自身对数据的利用，只不过是在市场关系中获取了本来可能由被许可人取得的经济利益。在知识产权法领域，法律并未赋予所有的被许可人防御性请求权。例如，《最高人民法院关于审理商标民事纠纷案件适用法律若干问题的解释》第 4 条根据被许可人取得的使用许可的类型分别进行了规定，其中普通使用许可合同的被许可人需要商标注册人的明确授权才能提起诉讼。在数据的许可使用中，被许可人的数据访问权的法律保护亦可借鉴知识产权领域的规则，区分使用许可的类型分别规定。（4）在数据的委托处理中，由于受托人对其处理的数据不享有自主的数据产权，因此其不享有数据访问权的法律保护。

最后，数据访问权的实质是赋予数据持有者对数据访问的专有权利，故数据访问权应当以数据具备合法性为前提。就此而言，数据访问权不同于物之占有，后者不问占有人是否享有正当权源。例如，甲非法收集了大量个人信息，乙未经同意访问并且爬取了个人信息，甲在向乙主张返还数据请求权或者删除数据的请求权时，甲是否需要证明其数据来源的合法性，或者乙可否以甲的收集行为违法为由进行抗辩？一种观点主张准用占有规则，不论甲持有的数据是否合法，均应赋予甲向乙主张返还或者删除数据的请求权。[49]笔者认为，这一观点值得商榷。因为这一主张赋予非法的数据持有者防御性请求权的主要理由是外部的，即不是考虑非法的数据持有者的自身利益，而是为了保护被非法收集了个

人信息的信息主体的利益——通过赋予非法的数据持有者防御性请求权，避免个人信息进一步泄露。故此，该数据持有者行使防御性请求权的规范基础，不应该是占有制度，而是《个人信息保护法》第 57 条第 1 款所要求的“发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施”，其中“补救措施”应当包括行使返还或者删除数据的请求权等法律手段。由此可以进一步推论，倘若甲非法获取的数据不涉及个人信息，那么其就不应当享有返还或者删除数据的请求权。上文提到，若乙通过植入病毒软件等手段限制甲访问其已经收集的数据，则甲可以基于数据持有的纯粹事实状态要求排除妨害。但是，当乙非法获取数据时，甲不得主张返还或者删除数据。这种差别对待的正当性在于，两项规则保护的法益存在差异。针对破坏数据完整性的防御性请求权，如同针对法律所禁止之私力的占有保护一样，旨在维持和平秩序，因此不问数据持有者是否享有正当权源。与此相反，针对爬取数据的返还或者删除数据请求权，其功能在于保障数据持有者对数据的独占经济地位，应当以该数据持有者享有合法的权源为必要。

3.数据访问权的交易

数据访问权不仅应当服务于静态保护，还应当服务于动态交易，调整数据持有者与潜在交易者之间的法律关系。中国信息通信研究院牵头起草的《数据交易合同（示范文本）》第 1.1 条指出，数据交易存在数据转让和数据共享两种模式。但在实践中，数据交易通常表现为许可使用。[50]数据交易涉及的法律问题纷繁复杂，这里无法作出全面讨论，只能对数据占有论引发的几个问题展开讨论。

第一，在数人分别或者共同持有同一数据的场景中，只有依据合同约定或者法律规定享有自主的数据访问权的主体有权转让或者许可他人使用数据。故此，云服务提供商和数据委托处理中的受托人不享有流通数据的权利；数据的被许可人是否享有进一步许可他人使用的权利，则取决于数据许可使用合同的约定。在数据共同持有的场景中，各持有者是否可以单独许可或转让其持有份额，也是一个关键问题。由于数据使用通常为非竞争性使用，类似知识产权中的合作作品关系，应类比适用相关规则。《德国著作权法》第 8 条第 2 款较为严格地限制合作作品作者的权利行使，要求全体合作作者同意；[51]美国版权法则允许任何一方自行使用作品或许可他人使用作品。[52]在数据持有的场景下，由于不存在精神性利益的考虑，类似我国《著作权法实施条例》第 9 条的折中立场，原则上允许数据持有者自行使用数据或许可他人使用，而无须其他共同持有者同意，只需合理分配收益。

第二，在共同或分别持有同一数据的情形下，某些主体拥有数据的转让权，而其他主体虽然持有数据但不具备转让权限。这可能导致数据无权处分的情况，尤其是在数据持有者非法取得数据时，可能出现无权处分的现象。在这种情况下，若交易相对人是善意的，如何保护其信赖就成为关键问题。笔者认为，由于数据持有的事实状态不能直接形成权利外观，也不具备权利推定效力，因此在现行法律框架下不适用善意取得。但善意取得制度并不排斥无形财产，前提是无形财产具备公示方法和公信力。未来若建立数据产权登记制度，并且登记簿能够与真实的权利状况一致，则可赋予数据产权推定效力和公信力，进而可能实现数据的善意取得。[53]目前，数据交易中的善意相对人只能通过合同法手段得到保护，而非财产法。若数据提供者未取得合法数据产权，导致相对人无法获得数据访问权，相对人可以根据《民法典》第 597 条解除合同并要求违约赔偿；若交易合同被撤销或无效，数据提供者需根据《民法典》第 157 条和第 500 条承担民事责任，包括信赖利益的损害赔偿。

五、结语

不论立法者将来是否在法律层面确立绝对权意义上的数据产权，“数据持有”均是数据保护与数据交易的基础性概念。数据占有论将数据持有等同于物之占有，忽视了数据持有中的非竞争性利益，因此无法完整地呈现数据持有的应然构造。数据之上同时承载着竞争性利益与非竞争性利益，与此相应，数据持有的法律构造应当具有二元结构，一则

用来保护竞争性利益，二则用来保护非竞争性利益。数据产权和数据交易制度的建构应当一再地回到数据持有的二元结构，方可创设出既适合数据特征又契合法律原理的数据基础制度。

（技术编辑：艾薇）