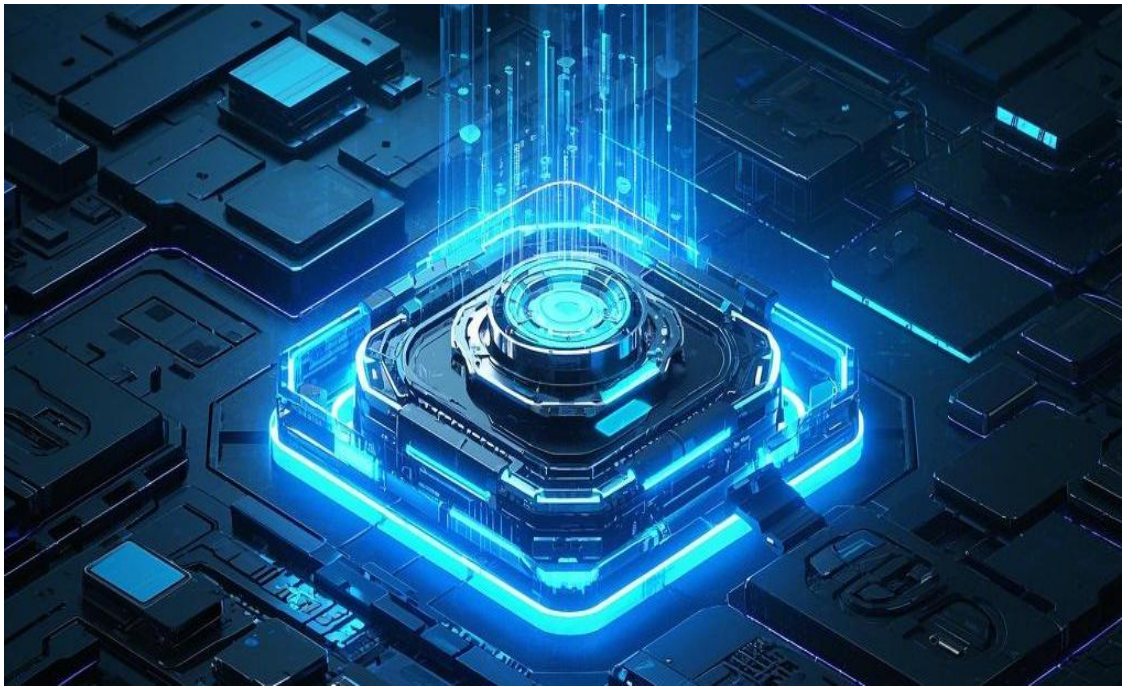
中国人民大学法学院
数字法学教研月报

2024 年第 12 期（总第 12 期）　　2024 年 12 月 20 日



本期看点

【数字法治大事件】中共中央办公厅与国务院办公厅联合发布《关于推进新型城市基础设施建设打造韧性城市的意见》，为推动新一代信息技术与城市基础设施建设深度融合作出了重要战略部署。工信部成立人工智能标准化技术委员会，标志着我国在人工智能领域的标准化建设迈出了重要一步。四部门联合发布《中小企业数字化赋能专项行动方案（2025—2027 年）》，国家数据局就《国家数据基础设施建设指引》公开征求意见，共同勾勒出我国数据经济时代的战略蓝图。

【研究动态】本期研究动态涵盖数字法学领域多个方面的问题，包括基础理论、个人信息保护、数据确权与流通、人工智能、平台治理、数字行政与司法，以及虚拟财产。学者们就数据的治理范式、平台经济下劳动者的权益保障、生成式人工智能训练语料的个人信息保护、生成式人工智能服务提供者的过错与义务等重要议题进行了讨论，对于保障公民在数字时代的合法权益具有重要意义。

【教研活动】中国人民大学未来法治研究院四位老师在“数炬计划——中国数据要素新锐学者项目”喜获殊荣；2024 年世界互联网大会乌镇峰会网络法治论坛成功召开；第七届计算法学国际会议成功举办；2024（第五届）网络法治论坛——新质生产力与人工智能法治暨 2024 北京市网络法学研究会年会在京成功举办。

【数字法评】《生成式人工智能训练语料的个人信息保护研究》，《中国法学》2024 年第 6 期，作者张新宝；《侵害企业数据权益的民事责任》，《中国法学》2024 年第 6 期，作者王叶刚。

本期目录

数字法治大事件.....3
中共中央办公厅 国务院办公厅关于推进新型城市基础设施建设打造韧性城市的意见.....3
工信部成立人工智能标准化技术委员会.....6
四部门关于发布《中小企业数字化赋能专项行动方案（2025—2027 年）》的通知.....6
关于《国家数据基础设施建设指引》公开征求意见情况的通告.....10
关于向社会公开征求《关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案》意见的公告.....15
数启未来，智领广州：《广州市公共数据授权运营管理暂行办法》深度解读与展望.....17
2024 年人民法院十大关键词之八——数字法院21
《中国-东盟人工智能发展与治理合作》报告发布.....22
研究动态.....24
基础理论.....24
个人信息保护.....26
数据确权与流通.....27
人工智能.....28
平台治理.....30
数字行政与司法.....33
虚拟财产.....33
教研活动.....35
中国人民大学未来法治研究院四位老师在“数炬计划——中国数据要素新锐学者项目”喜获殊荣.....35
2024 年世界互联网大会乌镇峰会网络法治论坛成功召开.....35
第七届计算法学国际会议成功举办.....38
2024（第五届）网络法治论坛——新质生产力与人工智能法治暨 2024 北京市网络法学研究会年会在京成功举办.....40
数字经济沙龙——“消费者认知与人工智能治理”.....43
数字法评.....46
生成式人工智能训练语料的个人信息保护研究46
侵害企业数据权益的民事责任.....63

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 敖紫辰 邓语鑫 何 芮 梁因格 李佳丽 林诗敏 麻卓妍 乔彩霞 王藜焯 王 昊 张 清 张锦涛 朱恬馨
联系方式：RUCdigitallaw@163.com

数字法治大事件

导言：在数字化浪潮的推动下，中国推进新型城市基础设施建设，为城市的可持续发展奠定坚实基础。中共中央办公厅与国务院办公厅联合发布的《关于推进新型城市基础设施建设打造韧性城市的意见》，为这一宏伟蓝图提供了政策指引。与此同时，工信部成立人工智能标准化技术委员会，不仅标志着我国在人工智能领域的标准化建设迈出了重要一步，也为技术创新与产业应用提供了规范框架。为了促进中小企业在数字化转型中的加速发展，四部门联合发布《中小企业数字化赋能专项行动方案（2025—2027 年）》，国家数据局就《国家数据基础设施建设指引》公开征求意见，共同勾勒出我国数据经济时代的战略蓝图，旨在通过数据驱动激发市场活力，推动经济高质量发展。此外，《关于完善数据流通安全治理、促进数据要素市场化价值化的实施方案》向社会公开征求意见，进一步彰显了我国在保障数据安全、促进数据流通与利用方面的积极探索。《广州市公共数据授权运营管理暂行办法》展示了地方政府在公共数据资源开发利用上的创新实践，为数据赋能城市发展树立了典范。在国际层面，《中国－东盟人工智能发展与治理合作》报告的发布，不仅加强了区域间的人工智能合作，也为全球人工智能治理贡献了中国智慧。从国家层面的政策导向到地方实践的创新探索，再到国际合作的深化拓展，中国正以数据为翼，智能为舵，全面开启数字时代的新篇章，奋力书写智慧城市与数字经济融合发展的新辉煌。

中共中央办公厅 国务院办公厅关于推进新型城市基础设施建设打造韧性城市的意见

原载：“国家数据局”微信公众号

中共中央办公厅 国务院办公厅关于推进新型城市基础设施建设打造韧性城市的意见

（2024 年 11 月 26 日）

为深化城市安全韧性提升行动，推进数字化、网络化、智能化新型城市基础设施建设，打造承受适应能力强、恢复速度快的韧性城市，增强城市风险防控和治理能力，经党中央、国务院同意，现提出如下意见。

一、总体要求

坚持以习近平新时代中国特色社会主义思想为指导，深入贯彻党的二十大和二十届二中、三中全会精神，全面落实习近平总书记关于城市工作的重要论述，坚持以人民为中心的发展思想，完整准确全面贯彻新发展理念，统筹高质量发展和高水平安全，坚持问题导向、系统观念，坚持政府引导、社会参与，坚持实事求是、因地制宜，坚持科技创新、数字赋能，推动新一代信息技术与城市基础设施建设深度融合，以信息平台建设为牵引，以智能设施建设为基础，以智慧应用场景为依托，推动城市基础设施数字化改造，构建智能高效的新型城市基础设施体系，持续提升城市设施韧性、管理韧性、空间韧性，推动城市安全发展。

主要目标是：到 2027 年，新型城市基础设施建设取得明显进展，对韧性城市建设的支撑作用不断增强，形成一批可复制可推广的经验做法。到 2030 年，新型城市基础设施建设取得显著成效，推动建成一批高水平韧性城市，城市安全韧性持续提升，城市运行更安全、更有序、更智慧、更高效。

二、重点任务

（一）实施智能化市政基础设施建设和改造。深入开展市政基础设施普查，建立设施信息动态更新机制，全面掌握现状底数和管养状况。编制智能化市政基础设施建设和改造行动计划，因地制宜对城镇供水、排水、供电、燃气、热力、消火栓（消防水鹤）、地下综合管廊等市政基础设施进行数字化改造升级和智能化管理。加快重点公共区域和道路视频监控等安防设备智能化改造。加快推进城市基础设施生命线工程建设，新建市政基础设施的物联设备应与主体设备同步设计、同步施工、同步验收、同步投入使用，老旧设施的智能化改造应区分重点、统筹推进，逐步实现对市政基础设施运行状

况的实时监测、模拟仿真、情景构建、快速评估和大数据分析，提高安全隐患及时预警和事故应急处置能力，保障市政基础设施安全运行。建立涵盖管线类别齐全、基础数据准确、数据共享安全、数据价值发挥充分的地下管网“一张图”体系，打造地下管网规划、建设、运维、管理全流程的基础数据平台，实现地下管网建设运行可视化三维立体智慧管控。强化燃气泄漏智能化监控，严格落实管道安全监管巡查责任，切实提高燃气、供热安全管理水平。落实居民加压调蓄设施防淹和安全防护措施，加强水质监测，保障供水水质安全。加强对城市桥梁、隧道等设施的安全运行监测。统筹管网与水网、防洪与排涝，健全城区排涝通道、泵站、闸门、排水管网与周边江河湖海、水库等应急洪涝联排联调机制，推动地下设施、城市轨道交通及其连接通道等重点设施排水防涝能力提升，强化地下车库等防淹、防盗、防断电功能。

(二) 推动智慧城市基础设施与智能网联汽车协同发展。以支撑智能网联汽车应用和改善城市出行为切入点，建设城市道路、建筑、公共设施融合感知体系。深入推进“第五代移动通信（5G）+车联网”发展，逐步稳妥推广应用辅助驾驶、自动驾驶，加快布设城市道路基础设施智能感知系统，提升车路协同水平。推动智能网联汽车多场景应用，满足智能交通需求。加强城市物流配送设施的规划、建设、改造，建设集约、高效、智慧的绿色配送体系。加快完善应急物流体系，规划布局城市应急物资中转设施，提升应急状况下城市物资快速保障能力。加快停车设施智能化改造和建设。聚合智能网联汽车、智能道路、城市建筑等多类城市数据，为智能交通、智能停车、城市管理等提供支撑。

(三) 发展智慧住区。支持有条件的住区结合完整社区建设，实施公共设施数字化、网络化、智能化改造与管理，提高智慧化安全防范、监测预警和应急处置能力。支持智能信包箱（快件箱）等自助服务终端在住区布局。鼓励对出入住区人员、车辆等进行智能服务和秩序维护。创新智慧物业服务模式，引导支持物业服务企业发展线上线下生活服务。实施城市社区嵌入式服务设施建设工程，提高居民服务便利性、可及性。发展智慧商圈。建立健全数字赋能、多方参与的住区安全治理体系，强化对小区电动自行车集中充电设施、住区消防车通道、安全疏散体系等隐患防治，提升城市住区韧性。

(四) 提升房屋建筑管理智慧化水平。建立房屋使用全生命周期安全管理制度。依托第一次全国自然灾害综合风险普查数据和底图，全面动态掌握房屋建筑安全隐患底数，重点排查老旧住宅电梯、老旧房屋设施抗震性能、建筑消防设施、消防登高作业面和疏散通道等安全隐患，形成房屋建筑安全隐患数字档案。建立房屋建筑信息动态更新机制，强化数据共享，在城市建设、城市更新过程中同步更新房屋建筑的基础信息与安全隐患信息，逐步建立健全覆盖全面、功能完备、信息准确的城市房屋建筑综合管理平台。健全房屋建筑安全隐患消除机制，提高房屋建筑的抗震、防雷、防火性能，坚决遏制房屋安全事故发生。

(五) 开展数字家庭建设。以住宅为载体，利用物联网、云计算、大数据、移动通信、人工智能等实现系统平台、家居产品互联互通，加快构建跨终端共享的统一操作系统生态，提升智能家居设备的适用性、安全性，满足居民用电用火用气用水安全、环境与健康监测等需求。加强智能信息综合布线，加大住宅信息基础设施规划建设投入力度，提升电力和信息网络连接能力，满足数字家庭系统需求。对新建全装修住宅，明确户内设置基本智能产品要求，鼓励预留居家异常行为监控、紧急呼叫、健康管理等智能产品的设置条件。新建住宅依照相关标准同步配建光纤到户和移动通信基础设施。鼓励既有住宅参照新建住宅设置智能产品，对传统家居产品进行电动化、数字化、网络化改造。在数字家庭建设中，要充分尊重居民个人意愿，加强数据安全和个人隐私保护。

(六) 推动智能建造与建筑工业化协同发展。培育智能建造产业集群，打造全产业链融合一体的智能建造产业体系，推动建筑业工业化、数字化、绿色化转型升级。深化应用建筑信息模型（BIM）

技术，提升建筑设计、施工、运营维护协同水平。大力发展数字设计、智能生产和智能施工，加快构建数字设计基础平台和集成系统。推动部品部件智能化生产与升级改造。推动自动化施工机械、建筑机器人、三维（3D）打印等相关设备集成与创新应用。推进智慧工地建设，强化信息技术与建筑施工管理深度融合，进一步提升安全监管效能。

（七）完善城市信息模型（CIM）平台。加强国土空间规划、城市建设、测绘遥感、城市运行管理等各有关行业、领域信息开放共享，汇聚基础地理、建筑物、基础设施等三维数据和各类城市运行管理数据，搭建城市三维空间数据模型，提高城市规划、建设、治理信息化水平。因地制宜推进城市信息模型平台应用，强化与其他基础时空平台的功能整合、协同发展，在政务服务、公共卫生、防灾减灾救灾、城市体检等领域丰富应用场景，开展城市综合风险评估，统筹利用地上地下空间，合理划定防灾避难空间，为科学确定不同风险区的发展策略和风险防控要求提供支撑，提高城市空间韧性。

（八）搭建完善城市运行管理服务平台。加强对城市运行管理服务状况的实时监测、动态分析、统筹协调、指挥监督和综合评价，推进城市运行管理服务“一网统管”。加快构建国家、省、城市三级平台体系，加强与城市智能中枢等现有平台系统的有效衔接，实现信息共享、分级监管、协同联动。完善城市运行管理工作机制，加强城市运行管理服务平台与应急管理、工业和信息化、公安、自然资源、生态环境、交通运输、水利、商务、卫生健康、市场监管、气象、数据管理、消防救援、地震等部门城市运行数据的共享，增强城市运行安全风险监测预警能力。开展城市运行管理服务常态化综合评价，实现评价结果部门间共享。

（九）强化科技引领和人才培养。组织开展新型城市基础设施建设基础理论、关键技术与装备研究，加快突破城市级海量数据处理及存储、多源传感信息融合感知、建筑信息模型三维图形引擎、建筑机器人应用等一批关键技术。建立完善信息基础数据、智能道路基础设施、智能建造等技术体系，构建新型城市基础设施标准体系。依托高等学校、科研机构、骨干企业以及重大科研项目等，加大人才培养力度，注重培养具有新一代信息技术、工程建设、城市管理、城市安全等多学科知识的复合型创新人才。

（十）创新体制机制。创新管理手段、模式和理念，探索建立新型城市基础设施建设的运作机制和商业模式。创新完善投融资机制，拓宽投融资渠道，推动建立以政府投入为引导、企业投入为主体的多元化投融资体系。通过地方政府专项债券支持符合条件的新型城市基础设施建设项目，鼓励通过以奖代补等方式强化政策引导。按照风险可控、商业自主的原则，优化金融服务产品，鼓励金融机构以市场化方式增加中长期信贷投放，支持符合条件的项目发行基础设施领域不动产投资信托基金（REITs）。创新数据要素供给方式，细化城市地下管线等数据共享规定，探索建立支撑新型城市基础设施建设的数据共享、交换、协作和开放模式。加强数据资源跨地区、跨部门、跨层级共享利用，夯实城市建设运营治理数字化底座，充分依托底座开发业务应用，防止形成数据壁垒，避免开展重复建设。鼓励先行先试，积极探索创新，及时形成可复制可推广的经验做法。

（十一）保障网络和数据安全。严格落实网络和数据安全法律法规和政策标准，强化信息基础设施、传感设备和智慧应用安全管控，推进安全可控技术和产品应用，加强对重要数据资源的安全保障。强化网络枢纽、数据中心等信息基础设施抗毁韧性，建立健全网络和数据安全应急体系，加强网络和数据安全监测、通报预警和信息共享，全面提高新型城市基础设施安全风险抵御能力。

三、加强组织领导

在党中央集中统一领导下，各地区各部门要把党的领导贯彻到推进新型城市基础设施建设、打造韧性城市工作各方面全过程，结合实际抓好本意见贯彻落实，力戒形式主义。各有关部门要主动担当作为，加强改革创新，建立健全协同机制。住房城乡建设部要牵头加强指导和总结评估，及时协调解

决突出问题。重大事项及时按程序向党中央、国务院请示报告。

工信部成立人工智能标准化技术委员会

原载:“中华人民共和国工业和信息化部”官网

中华人民共和国工业和信息化部公告

(2024 年第 35 号)

工业和信息化部决定成立部人工智能标准化技术委员会，编号为 MIIT/TC1，主要负责人工智能评估测试、运营运维、数据集、基础硬件、软件平台、大模型、应用成熟度、应用开发管理、人工智能风险等领域行业标准制修订工作。

第一届工业和信息化部人工智能标准化技术委员会由 41 名委员组成，秘书处由中国信息通信研究院承担。

特此公告。

附件: 第一届工业和信息化部人工智能标准化技术委员会委员名单

工业和信息化部

2024 年 11 月 22 日

四部门关于发布《中小企业数字化赋能专项行动方案（2025—2027 年）》的通知

原载:“中华人民共和国工业和信息化部”官网

工业和信息化部 财政部 中国人民银行 金融监管总局关于发布《中小企业数字化赋能专项行动方案（2025—2027 年）》的通知

工信部联企业〔2024〕239 号

各省、自治区、直辖市及计划单列市、新疆生产建设兵团中小企业主管部门、财政厅（局）；中国人民银行上海总部，各省、自治区、直辖市及计划单列市分行，各金融监管局:

现将《中小企业数字化赋能专项行动方案(2025—2027 年)》印发给你们，请抓好贯彻落实。

工业和信息化部

财政部

中国人民银行

金融监管总局

2024 年 12 月 12 日

中小企业数字化赋能专项行动方案（2025—2027 年)

中小企业是推动创新、促进就业、改善民生的重要力量。推进中小企业数字化转型是推进新型工业化的重要举措，建设现代化产业体系的必然要求，实现中小企业专精特新发展的关键路径。《中小企业数字化赋能专项行动方案》(工信厅企业〔2020〕10 号）印发以来，中小企业数字化进程明显加快，发展质量显著提升。为进一步贯彻党中央、国务院关于支持中小企业创新发展的决策部署，落实《制造业数字化转型行动方案》，由点及面、由表及里、体系化推进中小企业数字化转型，制定本方案。

一、总体要求

以习近平新时代中国特色社会主义思想为指导，贯彻落实习近平总书记关于加快推进新型工业化、促进中小企业专精特新发展系列重要指示精神，将推动中小企业数字化转型与开展大规模设备更新行动、实施技术改造升级工程等有机结合，以中小企业数字化转型城市试点为抓手，“点线面”结合推进数字化改造，加速人工智能创新应用和深度赋能，充分激活数据要素价值，着力提升供给质效和服务保障水平，实施中小企业数字化赋能专项行动。到 2027 年，中小企业数字化转型“百城”试点取得扎实成效，专精特新中小企业实现数字化改造应改尽改，形成一批数字化水平达到三级、四级的转型标杆；试点省级专精特新中小企业数字化水平达到二级及以上，全国规上工业中小企业关键工序数控化率达到 75%；中小企业上云率超过 40%。初步构建起部省联动、大中小企业融通、重点场景供需适配、公共服务保障有力的中小企业数字化转型生态，赋能中小企业专精特新发展。

二、重点任务

（一）深入实施“百城”试点

1.因地制宜推进中小企业数字化转型城市试点。发挥中央财政资金引导作用，分批支持 100 个

左右城市开展中小企业数字化转型试点，因地制宜探索中小企业数字化转型路径，推动 4 万家以上中小企业开展数字化转型，其中 1 万家专精特新中小企业。更新发布《中小企业数字化转型城市试点实施指南》，细化实施要求和流程规范。制定试点城市数字化转型绩效评价办法。研究探索对中小企业数字化转型城市试点服务商的服务情况进行评价，强化激励约束。（工业和信息化部牵头负责）

2.纵深推动工业大县中小企业数字化转型。面向基础较好的工业大县大范围复制推广试点城市工作经验和成果，依托县域优势产业推动人工智能、5G、区块链等新技术在重点中小企业的应用推广，打造一批数字化水平达到三级、四级的中小企业标杆。推动工业大县产业链与产业集群“链群”同转，实现县域中小企业规模化、普惠式数字化转型。（工业和信息化部牵头负责）

（二）分类梯次开展数字化改造

3.面向专精特新“小巨人”企业开展系统化集成改造。对专精特新“小巨人”企业全面“建档立卡”，“一企一策”靶向推动数字化水平系统提升。引导数字化水平二级及以下的企业加强关键业务系统部署应用与跨系统集成改造，实现数字化水平向更高层级提升跨越。支持数字化水平三级及以上企业开展高价值集成应用创新，围绕产品数字孪生、设计制造一体化、个性化定制等复杂场景开展系统化集成改造，培育一批四级标杆企业。深入实施智能制造工程，支持专精特新“小巨人”企业打造一批智能场景、智能车间、智能工厂。深入实施工业互联网创新发展工程，打造“5G+工业互联网”升级版，引导专精特新“小巨人”企业建设一批 5G 工厂。（工业和信息化部牵头负责）

4.面向省级专精特新中小企业、规上工业中小企业实施重点场景深度改造。加强中小企业数字化转型城市试点与制造业新型技术改造城市试点工作协同衔接，以“智改数转网联”为重点，优先支持数字化水平二级及以下的专精特新中小企业或规上工业中小企业实施软硬件一体化改造，打造产品工艺仿真、设备预测运维、产线智能控制等场景样本，加快行业普及推广。鼓励数字化水平三级及以上企业对标同行业标杆企业，开展更高水平改造。聚焦原材料、装备制造、消费品、电子信息等行业实施大规模设备更新，重点推动中小企业开展“哑”设备改造和关键设备更新。（工业和信息化部牵头负责）

5.面向小微企业推广普惠性“上云用数赋智”服务。加快中小企业内外网升级改造，提升数字化基础水平。完善企业级、行业级、区域级等多层次云平台布局，推动现有工业软件产品云化迁移，形成云化软件供给目录。加速关键设备、业务系统上云，推广基于云的设备运行监测、产品性能仿真以及数据存储、建模分析等普惠应用。在先进制造业集群、中小企业特色产业集群、国家高新技术产业开发区等重点集群、园区，加快新型基础设施规模化建设应用，为中小企业上云用云提供基础支撑。支持地方探索“上云券”“算力券”等优惠政策措施，为中小企业上云用算提供支持。鼓励算力中心提供“随接随用、按需付费”的云端算力服务，降低中小企业用算成本。（工业和信息化部牵头负责）

（三）推进链群融通转型

6.推广龙头企业牵引的供应链“链式”转型。支持链主企业、龙头企业开放数字系统接口，促进供应链上下游中小企业实施标准统一的数字化改造，推动中小企业主动融入大企业的供应链，强化中小企业在供应链上的配套能力。持续梳理遴选中小企业“链式”转型典型案例，编制发布案例集。（工业和信息化部牵头负责）

7.推广工业互联网平台企业驱动的产业链“链式”转型。支持细分行业工业互联网平台企业打造产业链协同能力，面向细分行业梳理数字化转型场景图谱及数据要素、知识模型、工具软件等要素清单，面向中小企业推广行业共性数字化产品及系统解决方案，提升产业链整体数字化水平。基于平台汇聚、组织制造资源，实现市场订单、研发资源、生产原料等与中小企业精准匹配，打造共享制造、个性定制、众包众创等新模式新业态，加速平台经济赋能中小企业高质量发展。（工业和信息化部牵

头负责）

8.推广以集群、园区为单位的“面状”转型。支持先进制造业集群、中小企业特色产业集群、国家高新技术产业开发区等重点集群、园区引进或建设工业互联网平台，开发标准化、模块化、解耦化的数字工具与服务，打造贯通工具链、数据链、模型链的数字底座，大力推广集采集销、中央工厂、众包众创等协同转型新模式，带动集群、园区中小企业数字化水平整体提升。探索发展跨越物理边界的“虚拟”产业园区和产业集群，推动中小企业跨地域数据互通、资源共享、业务协同，构建虚实结合的产业数字化新生态。（工业和信息化部牵头负责）

（四）推动人工智能创新赋能

9.发布中小企业人工智能应用指引。编制发布中小企业与人工智能融合应用推进指南，明确中小企业人工智能应用实施的主要模式、典型路径，为中小企业提供可落地、易操作的参考指引。鼓励各地组织开展中小企业人工智能应用案例征集遴选，培育挖掘视觉质量检测、客户画像与精准营销、财务管理自动化等一批典型场景，为中小企业提供借鉴参考。（工业和信息化部牵头负责）

10.加强中小企业人工智能应用推广。发挥中小企业数字化转型试点城市现场交流活动的平台作用，宣传推介人工智能赋能中小企业典型应用场景、解决方案，加快中小企业人工智能应用复制推广。鼓励各地参考中小企业人工智能典型应用案例、应用图谱等，推动人工智能技术在研发设计、生产制造、质量检测、运行维护、经营管理等中小企业关键业务场景应用普及。（工业和信息化部牵头负责）

11.强化中小企业人工智能应用基础。支持开放原子开源基金会等开源社区牵头成立人工智能开源社区，聚焦中小企业特色需求设立专题人工智能开源项目，提供可复制、易推广的训练框架、开发示例、测试工具和开源代码。引导中小企业积极参与开源项目，降低人工智能部署开发门槛。鼓励龙头企业、交易机构、平台企业、数据服务企业等经营主体建设公共数据集、行业数据集，为中小企业提供用于人工智能模型训练的高质量数据。建设一批适用于中小企业的垂直行业大模型，强化中小企业大模型技术产品供给。（工业和信息化部牵头负责）

（五）深度激活中小企业数据要素价值

12.提升中小企业数据管理、利用能力。鼓励各地面向中小企业加强《数据管理能力成熟度评估模型》（DCMM）标准应用推广，引导有条件的中小企业开展生产经营全过程数据采集，加快大数据系统建设部署，建立健全数据管理制度。鼓励中小企业探索数据创新应用，引导中小企业面向业务需求开展数据建模分析，实现精益生产、精细管理、精准营销等业务能力提升，推广服务型生产、增值服务、共享经济等数据驱动的新模式新业态。（工业和信息化部牵头负责）

13.加强中小企业数据资源供给与价值开发。鼓励龙头企业、平台企业向中小企业开放数据，有针对性地开展数据清洗标注、交易撮合、分析挖掘等工作，为中小企业提供专业普惠的数据服务。探索打造以可信数据空间、区块链等技术为支撑的数据流通利用基础设施，推动大中小企业间实现研发设计、设备状态、交易订单等高价值数据安全可信流通，拓宽中小企业数据获取渠道。（工业和信息化部牵头负责）支持中小企业开展数据资产价值评估，加强对中小企业数据资产依法依规入表的指导，加强数据资产管理，依法依规维护中小企业数据资产权益。（财政部牵头负责）

（六）提升数字化转型供给质效

14.供需适配发展“小快轻准”产品。围绕细分行业数字化转型场景图谱，推动龙头企业联合工业软件企业开发数字化专用工具，培育一批“小快轻准”数字化产品和解决方案，形成供需图谱。推动工业软件、工业互联网平台企业等不同厂商提供开放接口，提升“小快轻准”数字化产品和解决方案的数据互联互通与跨平台互操作能力，增强产品易用性及开发便捷性。支持地方建设“小快轻准”资源池，通过线上宣传、线下体验等方式加快产品

推广。（工业和信息化部牵头负责）

15.培育壮大数字经济领域优质企业。推动龙头企业数字化团队对外输出服务，推进现有工业互联网平台与垂直行业深度融合，培育一批在特定行业、特定领域具有较深知识积累和优质服务能力的行业型服务商、场景型服务商。以数字化培育新动能，用新动能推动新发展，推动中小企业在 5G、人工智能、工业软件、工业互联网平台等数字化领域加大创业创新力度，着力培育一批专精特新中小企业和“小巨人”企业。（工业和信息化部牵头负责）

（七）提高数字化转型公共服务能力

16.构建中小企业数字化转型标准体系。组建中小企业数字化转型标准工作组，研制一批国家标准、行业标准。更新完善中小企业数字化水平评测指标，构建细分行业中小企业数字化水平评价体系。编制细分行业中小企业数字化转型实施指南，为中小企业改造实施提供专业指导。开展中小企业数字化转型标准验证、推广，强化中小企业与龙头企业的标准适配与信息共享，推动中小企业全面融入产业链供应链。（工业和信息化部牵头负责）

17.完善中小企业数字化转型服务载体。基于优质中小企业梯度培育平台，完善全国中小企业数字化转型公共服务功能，打造满足行业共性需求和企业个性需求的工具箱、资源池、案例库。推进地方中小企业数字化转型服务平台与全国平台数据互通，提供转型咨询、诊断评估、应用推广等专业化服务。鼓励地方合规探索公益性服务和市场化运作相结合的公共服务载体运营机制。推动全国中小企业数字化转型服务平台与制造业数字化转型综合信息平台资源共享，凝聚工作合力，加强中小企业数字化转型公共服务供给。（工业和信息化部牵头负责）

18.全面增强中小企业数据与网络安全防护能力。引导中小企业建立健全网络和数据安全管理制度，促进态势感知、工业防火墙、入侵检测系统等安全产品部署应用。支持中小企业开展网络和数据安全演练，提升中小企业网络风险防御和处置能力。鼓励中小企业通过购买网络安全保险等方式降低安全风险。（工业和信息化部牵头负责）

三、保障措施

（一）强化组织保障。组织建立部省联动的中小企业数字化转型工作体系，加强横向跨部门资源调度与纵向跨层级工作协同。推动各地强化中小企业数字化转型推进力量，加强相关部门工作协同，明确重点工作组织分工，构建定期监测、指导、评估、培训、交流等长效工作机制。（工业和信息化部牵头负责）

（二）加大资金支持。深入开展“一链一策一批”中小微企业融资促进行动，按照市场化原则满足中小企业数字化转型融资需求。支持有条件的地方针对中小企业数字化转型项目提供贴息支持，分行业常态化组织投融资对接活动。鼓励金融机构推出支持中小企业数字化转型的专门信贷产品，鼓励融资担保公司提供增信支持，深入实施科技创新和技术改造再贷款政策、设备更新贷款财政贴息政策，加大对中小企业技术改造和设备更新项目，特别是数字化转型的金融支持力度。（中国人民银行、金融监管总局、财政部、工业和信息化部按职责分工负责）

（三）加强人才保障。利用中小企业服务“一张网”，面向不同行业、不同对象，分层分类提供培训课程资源，组织开展大规模数字化培训。开展数字化转型职业标准、人才标准开发与专业技术人员培养，为中小企业数字化提供专业人才支撑。依托“制造业人才支持计划”“国家卓越工程师实践基地”等加大中小企业数字化人才培育力度，壮大中小企业数字化转型人才队伍。（工业和信息化部牵头负责）

（四）促进交流互鉴。常态化举办中小企业数字化转型现场交流活动，加强沟通合作。鼓励中小企业数字化转型试点城市开展对口协作，推动转型资源共享共用与典型经验复制推广。支持开展工业互联网平台赋能中小企业数字化转型试点城市行活动，促进工业互联网平台供给与中小企业数字化转型市场需求精准对接。加大舆论宣传引导。及时

总结中小企业数字化转型工作经验，推广典型案例、典型模式、典型产品。（工业和信息化部牵头负责）

（五）深化国际合作。依托二十国集团、金砖国家等合作机制，用好亚太经合组织中小企业部长会议、中国国际中小企业博览会等平台，组织开展中小企业数字化转型国际交流合作活动，积极推动中小企业数字化转型优秀解决方案、产品服务、标准规范走出去。（工业和信息化部牵头负责）

关于《国家数据基础设施建设指引》公开征求意见情况的通告

原载：“国家数据局”微信公众号

按照有关工作安排，2024 年 11 月 22 日至 12 月 1 日，我们在国家数据局微信公众号上就《国家数据基础设施建设指引（征求意见稿）》向社会公开征求意见。征求意见期间共收集到 288 条意见，我们将认真研究，在修改完善时予以充分考虑。感谢社会各界对我们工作的关心和支持!

国家数据局

2024 年 12 月 4 日

《国家数据基础设施建设指引(征求意见稿)》

前 言

党的十八大以来，以习近平同志为核心的党中央，敏锐把握新一轮科技革命和产业变革的新机遇，统揽中华民族伟大复兴的战略全局和世界百年未有之大变局，对发展数字经济作出重大部署，擘画了新时代数字中国建设的宏伟蓝图。

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”。各地区各部门认真贯彻落实习近平总书记重要指示精神，积极探索数据基础设施建设，为数据要素市场化配置改革、建设全国一体化数据市场奠定了良好基础。同时也要看到，数字经济蓬勃发展对数据流通利用和价值释放提出了新的更高的要求，迫切需要更好发挥有为政府和有效市场作用，构建兼顾效率和公平、适应数据要素特征、发挥数据价值效用的国家数据基础设施。

按照党中央、国务院决策部署，国家发展和改革委员会、国家数据局、工业和信息化部在充分调研的基础上，组织编制了《国家数据基础设施建设指引》，力争在当前情况下，说清楚数据基础设施的概念、发展愿景和建设目标，指导推进数据基础设施建设，推动形成横向联通、纵向贯通、协调有力的国家数据基础设施基本格局，打通数据流通动脉，畅通数据资源循环，促进数据应用开发，培育全国一体化数据市场，夯实数字经济发展基础，为数字中国建设提供有力支撑。

一、概念内涵

纵观人类经济发展史，每一轮产业变革都会孕育新的基础设施。农业经济时代，基础设施主要是农田水利设施。工业经济时代，公路、铁路、港口、机场、电力系统等成为新的基础设施。数字经济时代，网络设施、算力设施、应用设施等构建了数字基础设施。当前，数据成为关键生产要素，催生新的技术—经济范式，重塑产业发展方式，推动数字基础设施向数据基础设施延伸和拓展。建设和运营国家数据基础设施，进一步促进数据“供得出、流得动、用得好、保安全”，对于支撑数据基础制度落地、构建全国一体化数据市场、培育发展新质生产力具有重要意义。

国家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。国家数据基础设施在国家统筹下，由区域、行业、企业等各类数据基础设施共同构成。网络设施、算力设施与国家数据基础设施紧密相关，并通过迭代升级，不断支撑数据的流通和利用。

二、发展愿景

（一）主要目标

国家数据基础设施是数据基础制度和先进技术落地的重要载体。在数据流通利用方面，建成支持全国一体化数据市场、保障数据安全自由流动的流通利用设施，形成协同联动、规模流通、高效利用、规范可信的数据流通利用公共服务体系；在算

力底座方面，构建多元异构、高效调度、智能随需、绿色安全的高质量算力供给体系；在网络支撑方面，构建泛在灵活接入、高速可靠传输、动态弹性调度的数据高速传输网络；在安全方面，构建整体、动态、内生的安全防护体系；在应用方面，支持传统行业转型升级，赋能人工智能等新兴产业发展。总体实现“汇通海量数据，惠及千行百业，慧见数字未来”的美好愿景。

（二）推进路径

当前，我国数据基础设施处于起步建设阶段，围绕流通利用业务场景，各地方各行业各领域探索形成多种有针对性的技术方案和解决路径，并在不断迭代发展。在推动技术设施化过程中，要注重发挥有为政府和有效市场双重作用，坚持自上而下布局、自下而上探索双向协同，鼓励大胆创新，支持先行先试，加快技术收敛，推动技术规模化部署、系统化应用，为构建高速互联、高效调度、开放普惠、安全可靠的国家数据基础设施奠定坚实基础。

2024—2026 年，利用 2—3 年左右时间，围绕重要行业领域和典型应用场景，开展数据基础设施技术路线试点试验，支持部分地方、行业、领域先行先试，丰富解决方案供给。制定统一目录标识、统一身份登记、统一接口要求的标准规范，夯实数据基础设施互联互通技术基础。完成国家数据基础设施建设顶层设计，明确国家数据基础设施建设的技术路线和实践路径。

2027—2028 年，建成支撑数据规模化流通、互联互通的数据基础设施，数网、数算相关设施充分融合，基本形成跨层级、跨地域、跨系统、跨部门、跨业务的规模化数据可信流通利用格局，实现全国大中型城市基本覆盖。

到 2029 年，基本建成国家数据基础设施主体结构，初步形成横向联通、纵向贯通、协调有力的国家数据基础设施基本格局，构建协同联动、规模流通、高效利用、规范可信的数据公共服务体系，协同构筑数据基础设施技术和产业良好生态，国家数据基础设施建设和运营体制机制基本建立。

三、总体功能

数字中国、数字经济、数字社会建设提出了数据要素化、资源化、价值化要求，国家数据基础设施围绕打造高速互联、高效调度、可信流通、安全可靠的体系化能力，持续赋能各行业数据融合与智能化发展。

（一）数据可信流通：开放普惠的数据流通

国家数据基础设施需要打造低成本、高效率、可信赖的流通环境，便于人、物、平台、智能体等快速接入，在符合统一目录标识、统一身份登记、统一接口规范的基础上，实现数据在不同组织、行业之间安全有序流动，精准匹配数据供需关系，面向电子商务、金融支付、跨境物流、航运贸易等典型场景创新融合数据应用，同时符合相关法律法规、社会伦理、个人隐私保护等要求。

（二）高效算力供给：多元异构的算力协同

算力资源多元异构、异地分布、动态变化，给大规模计算任务的统一调度与任务协同带来挑战。面向“东数西算”等场景中对异属异构异地算力的调度需求，需要建立多元异构算力统筹调度的能力，实现算力和运力的高度融合，实现算力资源之间的无缝对接与协同计算，提高整体计算效率与资源利用率，实现算力最优配置与动态调整。

（三）数据高速传输：高效弹性的数据传输网络

高效弹性的传输网络可为数字金融、智慧医疗、交通物流、大模型训练和推理等核心场景数据传输流动提供高速稳定服务。国家数据基础设施在高效弹性传输网络的支撑下，能够显著提升数据交换性能，降低数据传输成本，为数据大规模共享流通提供高质量通道。

（四）全程安全可靠：动态全面的安全保障

数据采集、汇聚、传输、加工、流通、利用、运营等多样化活动，涉及多方主体、多个环节，需要在开放环境下对数据进行整体、动态保护。国家数据基础设施需要构建标准化、多层次、全方位的安全防护框架，推动安全防护由静态保护向动态保护、由边界安全向内生安全、由封闭环境保护向开放环境保护转变，形成贯穿数据全生命周期各环节

的动态安全防护能力，系统保障数据基础设施相关的网络、算力、数据安全。

四、总体架构

（一）技术架构

国家数据基础设施具有数据采集、汇聚、传输、加工、流通、利用、运营、安全八大能力。在数据采集方面，支持通过传感器、业务系统等手段采集相关数据。在数据汇聚方面，通过标识编码解析、数据目录等，对数据进行高效接入、合理编目，实现数据广泛汇聚、存储和发布。在数据传输方面，支持节点即时组网、数据高效传输。在数据加工方面，为参与方提供高效便捷、安全可靠的数据清洗、计算服务，建立数据质量控制和评估能力，提高数据处理环节效率。在数据流通方面，通过数据分类分级策略实现共享、交易等流通功能，为不同行业、不同地区、不同机构提供可信流通环境。在数据利用方面，为数据应用方提供数据分析、数据可视化等能力，进一步降低数据应用门槛。在数据运营方面，提供数据登记、监督管理、数据认证、合规保障等功能，有效支撑数据要素市场有序运行。在数据安全方面，提供动态全过程数据安全服务，包括防窃取、防泄露、防破坏等。在赋能方面，促进数据多场景应用、跨主体复用，赋能工业制造、现代农业、跨境数字货币、数字金融、智慧医疗、智慧交通、跨境物流、航运贸易、绿色低碳等行业领域。

其中，数据流通利用设施是国家数据基础设施的重要组成部分，为跨层级、跨地域、跨系统、跨部门、跨业务数据流通利用提供安全可信环境，包括可信数据空间、数场、数据元件、数联网、区块链网络、隐私保护计算平台等技术设施。网络设施、算力设施适应数据价值释放需要，向数据高速传输、算力高效供给方向升级发展。安全保障体系是国家数据基础设施安全可靠运行的保障，包括监测预警、信息通报、应急处置等相关制度、能力和队伍建设。

（二）主要构成

国家数据基础设施以行业、区域数据基础设施为主体，以企业数据基础设施为重要组成。企业数据基础设施是指服务企业生产、运营、管理的数据平台，包括采集、存储、处理、管理等相关硬件和软件系统，以及企业整合、协同关联数据方形成的数据服务平台。行业数据基础设施是指覆盖某一行业领域，服务行业内企业、用户及利益相关者，实现数据要素化、资源化、价值化的各类设施，包括行业数据流通交易平台、行业数据归集平台、行业数据公共服务平台等。区域数据基础设施是指覆盖本地区，服务区域内企业、用户及利益相关者，实现数据要素化、资源化、价值化的各类设施，包括数据归集平台、数据资源管理服务平台、公共数据运营平台等。国家在企业、行业、区域数据基础设施的基础上，组织建设基于统一目录标识、统一身份登记、统一接口要求的数据流通利用底座，搭建数据流通利用基础设施管理平台，以及建设数据产权登记、公共数据运营、数据资源管理、数据流通交易、算力资源监测调度等基础公共服务的平台。这些设施相互贯通、协同推进，共同促进国家数据基础设施建设发展。

五、重点方向

（一）建设数据流通利用设施底座

按照统一目录标识、统一身份登记、统一接口要求，建设数据流通利用设施底座。建立覆盖政府、行业、企业等主体及国家、省、市、县等层级的全国一体化的分布式数据目录，形成全国数据“一本账”，支撑跨层级、跨地域、跨系统、跨部门、跨业务的数据有序流通和共享应用。建立全国一体化的分布式数字身份体系，规范身份标识生成、身份注册和认证机制。建立统一的数据凭证、交易凭证结构、生成与验证机制，支持利用区块链、加密技术、智能合约等手段提高凭证的可溯性和信任性。构建标准化、规范化的交互接口，实现数据基础设施的互联互通。建设数据泛在接入体系，支持数据资源、参与主体、第三方服务更大规模接入。建立与 IPv6 等网络标识兼容的数据标识体系。建立数据目录分类分级管理机制，加强数据分类管理和分级保护。

（二）建设数据高效供给体系

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。链接各类公共数据、企业数据、个人数据以及各类高质量数据集，对社会形成统一的数据资源开放目录。研究制定高质量数据集建设相关标准，从数据生成、注释定义到数据管理的全过程，确保数据标注的准确性和数据模型的专业性。制定高质量数据标注与交付规则，提高训练数据质量。支持农业、工业、金融、自然资源、卫生健康、教育、科技、民航、气象等行业领域打造高质量数据集。因地制宜推进公共数据运营平台集约化、标准化建设，推进公共数据的规模化、常态化供给。推进数据资源管理服务平台互联互通，完善平台标准，促进平台间互操作，实现全国数据资源的跨领域、跨层级、跨区域流通利用。支持各地积极建设政务服务大模型，推动政务服务智能化。

（三）建设数据可信流通体系

建立高效便利可信的数据流通机制，促进数据大规模、低成本、安全自由流通。支持建设企业可信数据空间、行业可信数据空间，探索建设城市可信数据空间、个人可信数据空间、跨境可信数据空间。支持基础好、有条件、意愿强的行业和城市，先行先试数场建设。鼓励行业、地方积极探索建设区块链、隐私保护计算等新技术设施。支持因地制宜，探索数联网、数据元件等数据流通基础设施建设。支持建设数据流通交易公共服务平台。支持探索建设数据跨境流动基础设施。建立数据流通准入标准规则，鼓励探索数据流通安全保障技术、标准、方案。

（四）建设数据便捷交付体系

加强数据交易场所体系设计，统筹数据交易场所优化布局。支持数据交易场所创新发展，鼓励各类数据进场交易。构建集约、高效的数据交付基础设施，为场内集中交易和场外分散交易提供低成本、高效率、可信赖的数据交付环境。促进各类交易所、交易平台互联互通。推动数据价值贡献度评估、数据集推荐匹配、数据产品差异性分析等技术创新，实现供需精准匹配和便捷交付。鼓励各地提升数据加工、测试、建模验证、安全实验等社会化服务能力，打造产学研用“一公里”工作圈。

（五）建设行业数据应用体系

加强场景牵引，建设面向工业制造、现代农业、数字金融、智慧医疗、智慧交通、跨境物流、航运贸易、卫生健康、绿色低碳等重点行业领域的数据应用基础设施，促进行业数据应用创新。培育基于数据要素的新产品和新服务，促进数据多场景应用、跨主体复用，实现知识扩散、价值倍增。

六、算力底座

（一）推进算力资源科学布局

加快推动通用算力、智能算力、超级算力等多元异构算力的绿色发展、有机协同。促进各类新增算力向国家枢纽节点集聚，强化枢纽节点国家算力高地定位。建设全国一体化算力网监测调度平台。探索采用存算分离架构建设新型智算中心和新材料大数据中心。

（二）推进东中西部算力协同

加强新兴网络技术创新应用，优化网络计费方式，降低东西部数据传输成本，促进东部中高时延业务向西部转移。构建算力多级调度策略引擎，实现跨平台、跨层级、跨区域的算力资源混合部署和统一调度，促进算力资源高效对接，提升数据汇聚、处理、流通、交易效率。推动国家枢纽节点和需求地之间 400G/800G 高带宽全光连接，引导电信运营商提升“公共传输通道”效能，推进算网深度融合。

（三）推进算力与数据、算法融合创新

推动实现“瓦特”产业向“比特”产业转化，不断壮大数算产业生态体系，助力打造具有国际竞争力的数字产业集群。推动行业数据和算力协同，实现数据可信流通，提升数据处理能力和治理水平。建立健全算法开发利用机制，积极开展大模型创新算法及关键技术研究，提升数据分析能力，降低大模型计算的算力消耗水平。

（四）推进算力与绿色电力融合

强化枢纽节点与非枢纽节点的协同联动，支持绿电资源丰富的非枢纽节点融入全国一体化算力网建设。加强大型风光基地和算力枢纽节点协同联动，把绿色电力转换成绿色算力。积极推进风光绿电资源消纳，助力实现碳达峰碳中和。支持利用“源

网荷储”等新型电力系统模式。加强数据中心智慧能源管理，开展数据中心用能监测分析与负荷预测，优化数据中心电力系统整体运行效率。探索绿电直供新模式，有序开展绿电、绿证交易。

（五）推进算力发展与安全保障协同

推动建设国家算力网基础安全服务保障平台，打造一体化的安全保障服务能力。打造网络和数据安全攻防演习靶场，推动国家枢纽节点地区定期开展网络和数据安全攻防演习。建设算力网安全应用技术试验场。强化国家枢纽节点自主防护能力，统一应急处置、统一安全监测、统一运行监控，构筑全生命周期的安全管控措施。

七、网络支撑

建设高速数据传输网，实现不同终端、平台、专网之间的数据高效弹性传输和互联互通，解决数据传输能力不足、成本较高、难以互联等问题。支持基础电信运营商叠加虚拟化组网、网络协议创新和智能化任务调度等云网融合技术，形成多方快速组网和数据交换能力，支持面向数据传输任务的弹性带宽和多量纲计费。

推动传统网络设施优化升级，有序推进 5G 网络向 5G-A 升级演进，全面推进 6G 网络技术研发创新。在东中西部地区均衡布局国际通信出入口局，加快扩展国际海缆、陆缆信息通道方向。建设时延确定、带宽稳定保障、传输质量可靠的确定性网络。布局“天地一体”的卫星互联网。

八、安全防护

国家数据基础设施安全保障体系建设重点是构建多层次、全方位、立体化的国家数据基础设施安全保障框架，贯穿数据生命周期全流程，帮助各参与方提升数据安全保障能力，确保数据的可信性、完整性和安全性。

在国家数据基础设施安全保障层面，实现可信接入、安全互联、跨域管控和全栈防护等安全管理，建立网络安全风险和威胁的动态发现、实时告警、全面分析、协同处置、跨域追溯和态势掌控能力，提供芯片、软件、硬件、协议等内置后门、漏洞安全威胁的内生防护能力。加强对合作伙伴、运维人员、平台用户等数据安全内部风险的防范应对。加强对入侵渗透、拒绝服务、数据窃取、勒索投毒等外部威胁的应急响应。

在数据流通利用安全层面，综合利用隐私保护计算、区块链、数据使用控制等技术手段，保证数据的可信采集、加密传输、可靠存储、受控交换共享、销毁确认及存证溯源等，规避数据隐私泄露、违规滥用等风险。加强算法、模型、数据的安全审计，增强模型鲁棒性和安全性，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”，确保贯穿数据全生命周期各环节安全。

九、组织保障

（一）健全政策保障体系

建立健全数据基础制度体系，加快出台数据产权、流通交易、收益分配、安全治理等政策文件。在新型基础设施规划安排下，研究制定国家数据基础设施建设规划。加大中央投资对国家数据基础设施建设的支持力度。各地区、各部门要在数据基础设施规划布局、资金安排、课题研究方面给予重点支持。积极引导社会资本力量参与国家数据基础设施建设。

（二）加快技术创新探索

支持有条件的行业和地区开展先行先试探索建设数据基础设施。鼓励企业和科研机构加大研发投入，加快数据流通利用关键技术攻关和重大成果转化。通过国家重点研发项目课题立项、揭榜挂帅、数据技术创新大赛等方式推动技术创新。

（三）强化标准和人才支撑

强化标准支撑，研究制定数据基础设施相关标准规范。鼓励企业、社会团体、科研机构参与数据基础设施国际标准的制定工作。加强与 ISO、IEC、IEEE、ITU、3GPP 等国际标准化组织的合作，推动数据领域高水平专家在国际组织任职。推动人才队伍建设，建立数据人才评价标准和评选机制。

附录：

技术术语解释

（一）数据流通利用技术

在数据流通利用领域，目前常用的技术路线主

要包括隐私保护计算、区块链、数据使用控制等。

1.隐私保护计算

隐私保护计算指在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算的一类信息技术，保障数据在产生、存储、计算、应用、销毁等数据流转全过程的各个环节中“可用不可见”。隐私保护计算的常用技术方案有安全多方计算、联邦学习、可信执行环境、密态计算等；常用的底层技术有混淆电路、不经意传输、秘密分享、同态加密等。

2.区块链

区块链是分布式网络、加密技术、智能合约等多种技术集成的新型数据库软件，具有多中心化、共识可信、不可篡改、可追溯等特性，主要用于解决数据流通过程中的信任和安全问题。

3.数据使用控制

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。

（二）数据流通利用实践方案

在数据流通利用领域，目前业界的实践方案主要包括可信数据空间、数场、数联网、数据元件等。

1.可信数据空间

可信数据空间是指数据资源开放互联、可信流通的一类数据流通利用设施，其以数据使用控制为核心，以连接器为技术载体，以实现数据可信交付，保障数据流通中“可用不可见”“可控可计量”为目标，具备数据可信管控、资源交互、价值创造三大核心能力。

2.数场

数场是依托开放性网络及算力和隐私保护计算、区块链等各类关联功能设施，面向数据要素提供线上线下资源登记、供需匹配、交易流通、开发利用、存证溯源等功能，支持多场景应用的一种综合性数据流通利用设施。以高效流通、价值释放、繁荣生态为核心，实现数据可见、可达、可用、可控、可追溯，具备开放性、融合性、扩展性等特点。

数场从点、线、面、场、安全五个维度构建标准化技术框架。点是数据主体进入数场的接入点。线是数场内连接各主体、各平台的数据高速传输网，实现数场内各主体之间的互联互通。面是数场中数据主体、传输网络的集合，是实现数据大规模流通、高效安全利用的核心。由点到线、由线到面构成数场基础设施。场是基于数场基础设施构建的数据应用、场景化创新，以及相关能力、流程、规范的统称。安全是覆盖点、线、面、场的动态全流程保护措施。数场在技术架构上包括接入点、功能平台、管理平台、安全保障、网络传输等基础服务平台。

3.数联网

数联网由数据流通接入终端、数据流通网络、数据流通服务平台构成，提供一点接入、广泛连接、标准交付、安全可信、合规监管、开放兼容的数据流通服务。

4.数据元件

数据元件提供统一标准、自主可控、安全可靠、全程监管的数据存储和加工服务，支持采用标准化工序完成数据产品规模化加工、生产和再利用，适用于大规模数据加工和生产场景。数据元件作为连接数据供需两端的“中间态”，将原始数据与数据应用“解耦”，基于数据元件相关组件，实现从数据归集到数据元件加工交易全生命周期的数据要素开发和管控。

（三）数据安全技术

数据安全技术为数据收集、存储、处理、传输、共享和销毁等全生命周期提供安全保障，包括数据备份与恢复、应用数据加密、数据泄露检测、流转监测、身份认证与访问控制、数据脱敏、数据水印、数据安全态势感知等。

关于向社会公开征求《关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案》意见的公告

原载：“国家数据局”微信公众号

为贯彻党的二十届三中全会精神，落实《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》，促进数据要素合规高效流通使用，充分释放数据价值，我们会同有关部门研究起草了《关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案》，现向社会公开征求意见。

此次公开征求意见的时间是 2024 年 11 月 29 日至 12 月 6 日。欢迎社会各界人士提出意见，请通过电子邮件方式将意见发送至 gjsjjzcs@126.com。感谢您的参与和支持!

附件：关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案（征求意见稿）

国家数据局

2024 年 11 月 29 日

附件

《关于完善数据流通安全治理更好促进数据要素市场化价值化的实施方案（征求意见稿）》

数据流通安全治理规则是数据基础制度的重要组成。为贯彻落实党中央、国务院决策部署，更好统筹发展和安全，建立健全数据流通安全治理机制，提升数据安全治理能力，促进数据要素合规高效流通利用，提出如下意见。

一、总体要求

以习近平新时代中国特色社会主义思想为指导，深入落实党的二十大和二十届二中、三中全会精神，全面贯彻总体国家安全观，统筹数据发展与安全，坚持系统思维、底线思维，将安全贯穿数据供给、流通、使用全过程，落实国家数据分类分级保护制度，明确数据跨主体流通中的安全治理规则，加强数据流通安全技术应用和产业培育，完善责任界定和权益保护机制，提升安全治理能力，防范数据滥用风险，坚决维护国家安全，保护个人信息和商业秘密，以成本最小化实现安全最优化，推动数据高质量发展和高水平安全良性互动，充分释放数据价值，促进数据开发利用。

到 2027 年底，规则明晰、产业繁荣、多方协同的数据流通安全治理体系基本构建，企业数据、公共数据、个人信息合规高效流通机制更加完善，治理效能显著提升，为繁荣数据市场、释放数据价值提供坚强保障。

二、主要任务

（一）明晰企业数据流通安全规则。支持企业通过编制数据资源目录、分析流通过程安全风险、制定分类分级保护措施等方式，提升数据治理能力。鼓励企业通过多种方式加强数据开发利用。鼓励企事业单位设立首席数据官，强化数据开发利用。数据处理者应按照国家有关规定识别、申报重要数据，并依法接受监管部门的监督检查。对确认为重要数据的，相关地区、部门应当及时向数据处理者告知或公开发布。数据处理者对外提供重要数据时，应按照相关法律法规、行业主管部门要求，采取必要的安全保护措施，切实维护国家安全、经济运行、社会稳定、公共健康和安全。鼓励开展数据脱敏等技术研究，对于经脱敏等技术处理后，依据所属行业领域的分类分级标准规范重新识别为一般数据的，可按照一般数据开展流通交易。

（二）加强公共数据流通安全管理。政务数据共享过程中，供给方按照“谁主管、谁提供、谁负责”的原则，明确政务数据共享范围、用途、条件，承担数据提供前的安全管理责任，探索建立接收方数据安全管理风险评估制度，确保数据在安全前提下有序共享。接收方按照“谁经手、谁使用、谁管理、谁负责”的原则，承担数据接收后的安全管理责任。有关地方和部门开展公共数据授权运营的，应依据有关要求明确公共数据授权运营机构的安全管理责任，建立健全数据安全管理制度，采取必要安全措施，加强关联风险识别和管控，保护公共数据安全。

（三）强化个人信息流通保障。个人信息流通应当依法依规取得个人同意或经过匿名化处理，不得通过强迫、欺诈、误导等方式取得个人同意。制定个人信息匿名化相关标准规范，明确匿名化操作规范、技术指标和流通环境要求。完善个人信息权益保障机制，鼓励采用国家网络公共身份认证等多

种方式，强化个人信息保护。加强对个人信息处理活动的规范引导，健全个人信息保护投诉举报渠道

（四）完善数据流通安全责任界定机制。数据供给方应当确保数据来源合法，数据需求方应严格按照要求使用数据，防止超范围使用。鼓励供需双方在数据流通交易合同中约定各自权责范围，清晰界定权责边界。探索建立数据流通安全审计和溯源机制，完善数据流通安全治理标准，融合应用数字水印、数据指纹、区块链等技术手段，高效支撑数据流通过程中的取证和定责。支持在自由贸易试验区（港）等地方开展先行先试，围绕数据流通交易溯源机制、重点场景安全治理标准、重点场景安全责任界定机制等，探索新型治理模式，提高治理效能。

（五）加强数据流通安全技术应用。支持数据流通安全技术创新，完善数据流通安全标准，引导企业按照数据分类分级保护要求，采取不同的安全技术开展数据流通。对于不涉及风险问题的一般数据，鼓励自行采取必要安全措施进行流通利用。对于未认定为重要数据，但企业认为涉及重要经营信息的，鼓励数据供给方、需求方接入和使用数据流通利用基础设施，促进数据安全流动。对于重要数据，在保护国家安全、个人隐私和确保公共安全的前提下，鼓励通过“原始数据不出域、数据可用不可见、数据可控可计量”等方式，依法依规实现数据价值开发。

（六）丰富数据流通安全服务供给。繁荣数据安全服务业态，壮大数据安全治理服务规模，提升企业数据安全治理能力。支持数据安全服务机构加强基础理论研究、核心技术攻关和产品创新应用，向规模化、专业化、一体化方向发展，提升安全服务效能，降低应用成本。培育数据流通安全检测评估、安全审计等服务，健全有利于数据流通主体互信的市场化机制。丰富数据托管和数据保险服务供给，鼓励有条件的企业拓展面向中小企业的数据安全托管服务。

（七）防范数据滥用风险。依法严厉打击非法获取、出售或提供数据的黑灰产业，加强敏感个人信息保护，限制超出授权范围使用个人信息。依法依规惩处利用数据开展垄断、不正当竞争等行为，维护各方主体权益和市场公平竞争秩序。在国家数据安全工作协调机制统筹协调下，加强重点行业领域数据安全风险监测，持续增强风险分析、监测和处置能力，防范发生系统性、大范围数据安全风险，维护国家安全和经济社会稳定。研究完善数据流通安全事故或纠纷处置机制，提升流通风险应对能力。强化部门协同，加强数据安全、个人信息保护等方面的执法协同，推动行政执法信息共享、情况通报和协同配合，提高监管效能。组织发布数据流通安全治理典型案例，充分发挥示范作用，营造“一地创新、全国共享”“一企创新、多企复用”的创新环境，促进数据安全有序流通。

数启未来，智领广州：《广州市公共数据授权运营管理暂行办法》深度解读与展望

来源：“问道研究智库”微信公众号

广州市作为改革开放的排头兵和数据要素改革的前沿阵地，始终积极探索数据要素市场化配置的新路径，致力于释放数据价值，激发市场活力，为经济社会发展注入新动力。

2024 年 12 月，广州市政务服务和数据管理局正式发布了《广州市公共数据授权运营管理暂行办法》（以下简称《暂行办法》），为广州公共数据授权运营工作提供了制度保障，标志着广州在数据要素市场化配置改革方面迈出了重要一步，也为全国数据要素市场发展提供了宝贵的经验和借鉴。

一、内容概览

政策背景

近年来，党中央、国务院对公共数据授权运营制度体系的探索予以了高度重视。

2021 年，《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》首次提出“开展政府数据授权运营试点”。

2022 年的《“十四五”数字经济发展规划》中明确提出通过数据开放、特许开发、授权应用等方

式，鼓励社会力量进行增值开发利用。

2022 年底，中共中央、国务院发布的《关于构建数据基础制度更好发挥数据要素作用的意见》进一步推进实施公共数据确权授权机制。

2024 年 9 月，中共中央办公厅、国务院办公厅发布《关于加快公共数据资源开发利用的意见》，进一步规范公共数据授权运营行为，旨在持续扩大公共数据资源供给。

广州实践基础

广州在公共数据授权运营方面的先行探索为《暂行办法》的出台提供了坚实的实践基础。

2023 年 5 月，广州首个公共数据运营产品“企业经营健康指数”在广州数据交易所顺利完成交易，标志着广州在探索公共数据运营模式、释放公共数据潜能上迈出了新的步伐。

2024 年 8 月，广州市数据要素市场化配置改革成果发布会上，

一是广州市政务和数据局与广州数字科技集团有限公司签订相关协议，由广州数据集团有限公司承接广州市公共数据运营；

二是数字广州创新实验室揭牌、广州公共数据运营平台正式上线并发布了 37 款公共数据产品，涵盖金融、环保交通、医疗健康、商业文旅等十余个行业领域，标志着广州数据要素市场化配置改革取得了阶段性成果。

《暂行办法》核心要点

《暂行办法》共分为八章三十九条，明确了数据供给、数据商进驻、数据使用申请、数据产品开发利用、数据产品和服务交易等环节的操作流程，为公共数据授权运营提供了详细的操作指南。

数据供给：《暂行办法》要求公共数据运营机构根据公共数据授权运营目录，编制并及时更新公共数据资源供给清单，明确数据的来源、范围、格式、更新频率等关键信息，确保数据的准确性和时效性。

数据商进驻：《暂行办法》明确了数据商的条件和流程，要求数据商具备相应的数据处理能力、技术实力和信誉度，通过审核后方可进驻公共数据运营平台。这一举措有助于维护数据市场的公平竞争和健康发展。

数据使用申请：《暂行办法》规定，数据使用方需向公共数据运营机构提交数据使用申请，明确数据使用的目的、范围、期限等关键信息，并经过合规核查后方可获得数据使用权。这一流程确保了数据的合规利用和防止滥用。

数据产品开发利用：《暂行办法》鼓励数据商基于公共数据进行产品开发和创新，推动数据产品的多样化和个性化发展。同时，新规还对数据产品的开发流程、质量标准等进行了明确规定，确保数据产品的质量和安全性。

数据产品和服务交易：《暂行办法》支持公共数据产品和服务在数据交易场所进行交易，推动公共数据在二级数据要素市场的流通和增值。这一举措有助于激发市场活力，推动数据要素市场的繁荣发展。

二、亮点解读

“运商分离”模式

公共数据运营机构：负责公共数据运营平台的建设运营、服务支撑、运行维护、安全保障，以及公共数据应用场景挖掘、仿真数据生成、公共数据加工使用、公共数据需求对接、公共数据运营合规核查等相关工作。

数据商：基于应用场景需求，通过公共数据运营平台开发利用形成公共数据产品和服务，对公共数据产品和服务开展发布、承销和数据资产合规化、标准化、增值化等服务。

运商分离的核心：公共数据运营机构与数据商应当功能分离，公共数据运营机构在数据商申请使用公共数据时，不得以不正当理由拒绝申请，也不得以强行搭售数据增值服务或附加其他不合理条件等方式限制数据商申请使用公共数据。

《暂行办法》明确了公共数据运营机构与数据商功能分离的原则，即

公共数据运营机构负责搭建统一的公共数据运营平台，并提供必要的数据加工、算力支持、合规支持等服务；

数据商则基于应用场景需求，通过公共数据运营平台开发利用形成公共数据产品和服务，并进行发布、承销和数据资产合规化、标准化、增值化等服务。

这种“运商分离”模式有利于避免公共数据运营机构实施与数据商达成垄断协议或滥用市场支配地位等行为，促进公平竞争，激发市场活力，推动数据要素产业健康发展。

公共数据授权运营目录与政务信息共享目录范围趋同

数据供给：市政务大数据管理机构、市公共数据主管部门等负责统筹本市公共数据的汇聚、治理、分类分级，并向公共数据运营平台提供经授权使用的公共数据；数源部门（如公共管理和服务机构）负责编制和更新本单位公共数据授权运营目录，并向本级政务大数据中心统一汇聚公共数据。

目录管理：市政务大数据管理机构负责制定目录对接技术标准，将公共数据授权运营目录推送至公共数据运营平台；市公共数据主管部门建立公共数据授权运营目录更新机制，定期扩展公共数据授权运营目录。

《暂行办法》推动公共数据授权运营目录与政务信息共享目录范围趋同，旨在扩大公共数据资源供给。

数据商可以通过公共数据运营平台申请查阅政务信息共享目录及仿真数据，并向公共数据运营机构提出公共数据使用需求。

这不仅有效扩展了公共数据授权运营目录，而且推动了公共数据分类分级，建立了公共数据授权运营目录管理、更新机制，强化了公共数据源头治理和质量管理，从而更好地开展公共数据使用需求对接。

全流程合规机制

合规核查：公共数据运营机构应建立健全合规核查机制，对数据商进驻、公共数据使用申请、公共数据产品和服务的出域等事项在数据安全、网络安全、个人信息保护、商业秘密保护等领域展开合规核查。

申请与审核：数据商可通过公共数据运营平台申请查阅政务信息共享目录及仿真数据，并向公共数据运营机构提出公共数据使用需求。公共数据使用申请需经过“核查+审核”机制，核查机制规范了数据商申请使用公共数据时所需提供的各项材料，审核机制有效明晰了数源部门、区公共数据主管部门、市政务大数据管理机构的审核主体责任。

《暂行办法》建立了数据商进驻公共数据运营平台、公共数据使用申请、公共数据产品和服务出域的全流程合规核查机制。

通过制定公共数据使用申请核查规范、公共数据使用申请审核规范，明确了公共数据使用申请的“核查+审核”机制，规范了数据商申请使用公共数据时所需提供的各项材料，明晰了数源部门、区公共数据主管部门、市政务大数据管理机构的审核主体责任。

这一机制有效解决了公共数据开发利用中“不愿”“不敢”“不会”的难题，提升了审核效率和用数及时性，规范了数据商在公共数据运营平台的开发利用行为，保证了公共数据产品和服务出域的合规、稳定与安全，降低了数据安全风险。

建立仿真数据生成机制

仿真数据生成：公共数据运营机构在提供申请查阅政务信息共享目录信息服务的同时，基于通用人工智能大模型能力生成仿真数据。

双向机制：建立起仿真数据成果回馈和数据商查阅仿真数据的双向机制，一方面将仿真数据回馈至政务数据共享流程中，优化政务数据共享模式；另一方面提供数据商查询仿真数据的服务，提升公共数据授权运营的需求识别精准度。

通过建立仿真数据生成机制，企业和组织能够评估不同的资源配置方案，找到最优的配置方式，从而实现最大化的效益和效率。

支持公共数据产品和服务进场交易

交易原则：数据商通过公共数据运营平台开发利用形成的公共数据产品和服务用于交易时，原则上应在依法核准的数据交易场所进行。

数据交易场所：为数据产品和服务提供数据产

权登记、产品进场和挂牌交易等服务，帮助数据商实现数据资产的价值变现，并促进数据要素市场的健康发展。同时通过公共数据产品和服务为牵引，带动社会数据进场交易，进一步扩大数据要素市场规模。

这一规定推动了公共数据在二级数据要素市场的流通与增值，有利于帮助数据交易场所拓展公共数据产品和服务交易板块，进一步提升企业经营能力，以公共数据产品和服务为牵引，带动社会数据进场交易。

披露机制与运营安全监督

披露机制：市政务大数据管理机构定期向社会披露公共数据授权运营情况，公共数据运营机构定期向社会披露公共数据资源使用情况，并接受社会监督。

这种披露制度有利于市政务大数据管理机构落实运营日常管理责任，确保公共数据运营机构面向市场公平提供服务，避免产生未经授权超范围使用公共数据的行为，强化了运营安全监督，确保数据安全与合规使用。

三、影响与展望

释放数据价值

《暂行办法》的实施将促进公共数据的开发利用，提升数据资源的价值。通过数据产品和服务的创新，为经济社会发展提供新动力，推动广州经济社会高质量发展。

IDC 发布的《中国公共数据授权运营市场及技术分析，2024》报告显示，公共数据在供给、应用场景、数据安全等方面面临挑战，但也存在巨大的价值释放潜力。

2024 年 8 月发布的 37 款公共数据产品，涵盖了金融、环保交通、医疗健康、商业文旅等十余个行业领域，这些数据产品的应用场景广泛，可以为各行各业提供数据支持，推动相关产业转型升级。

例如，在金融领域，可以利用企业经营健康指数数据，开发风险控制模型，为企业提供更加精准的金融服务；在医疗健康领域，可以利用医疗数据，开发健康管理平台，为市民提供更加便捷的健康管理服务。

激发市场活力

《暂行办法》为数据要素市场发展提供了制度保障，将有效激发市场活力，推动数据要素产业的高质量发展，形成新的经济增长点。

根据《中国数据要素市场发展报告（2023）》，2023 年中国数据要素市场规模达到 3.3 万亿元，预计到 2025 年将突破 10 万亿元。

广州作为数据要素改革的前沿阵地，将抓住机遇，大力发展数据要素产业，培育新的经济增长点。

未来展望

中研普华产业院发布的《2024-2029 年中国数据治理行业发展现状分析及未来趋势预测研究报告》预计，到 2025 年，我国大数据产业测算规模突破 3 万亿元，年均复合增长率仍将保持 25%左右，这显示了我国数据治理和数据要素市场的巨大发展潜力。

广州市在公共数据授权运营的未来发展中，应继续深化政府与市场机制的融合，推动全要素数据流通，构建全国乃至全球性的数据空间与数据联网，为数字经济的发展提供有力支撑。

1.由政府驱动向市场驱动转型深化

政策与市场机制的融合：广州市在公共数据授权运营的初期阶段，已采用“一局一中心一公司”模式，即由政府设立专门机构负责数据管理，同时成立数产集团进行市场化运营。未来，随着实践的深入，应进一步探索政策引导与市场机制的有效结合，确保数据流通既符合法律法规要求，又能激发市场活力。

数商生态的繁荣：随着数据要素市场的逐步成熟，广州应致力于构建多元化的数商生态体系，包括数据提供商、数据分析商、数据服务商等，形成完整的产业链。通过市场竞争和合作，促进数据产品的创新和优化，提升数据价值转化的效率和效果。

2.从公共数据到全要素数据流通的跨越

打破数据壁垒：广州市应积极推动跨部门、跨行业的数据共享与交换，打破数据孤岛现象。通过建设统一的数据平台和数据标准，实现各类数据的

互联互通，为全要素数据流通奠定基础。

促进数据资源优化配置：在全要素数据流通的背景下，广州市应加强对数据资源的统筹规划和合理配置，确保数据资源的高效利用。通过数据分析和挖掘，发现数据资源的潜在价值，推动数据资源向优势产业和区域集聚。

3.构建全国乃至全球性的数据空间与数据联网

专业领域数据空间建设：针对特定专业领域，如金融、医疗、交通等，广州市可以率先建设全国性的数据空间，进行数据资产的统一管理和备案。通过数据空间的建设，促进该领域数据的标准化、规范化和高效流通。

数据供需与开发网络的完善：广州市应积极推动数据供需双方的对接，建设广泛的数据开发网络。通过数据交易平台、数据开放平台等渠道，促进数据产品的交易和流通，满足全国乃至全球的业务数据需求。

推动大规模数据应用：在数据空间和数据联网的基础上，广州市应积极探索数据在各个领域的应用场景，推动数据与经济社会的深度融合。通过数据驱动的创新，促进经济转型升级和高质量发展。

2024 年人民法院十大关键词之八——数字法院

原载：“中国审判”微信公众号

我国正经历一场深刻的数字化转型，这一进程不仅改变了人们的生活方式和社会治理模式，也给传统司法体系带来了前所未有的机遇与挑战。

数字法院建设是适应数字中国建设进程、推动智慧法院建设迭代升级的重要举措，是数字时代推进审判工作现代化的重要引擎，是聚焦“公正与效率”、提升审判工作质效和司法公信力的有力支撑。数字法院建设前景广阔、大有可为，但不可能一蹴而就，亦没有现成的路线图可以依赖，必须始终秉持数字赋能、数字正义、以人为本的理念，在遵循司法规律的原则下不断深化完善、持续推进。

最高人民法院党组书记、院长张军在第十四届全国人民代表大会第二次会议上所作的工作报告中指出：“推进全国法院‘一张网’建设，以数字法院助力提质增效。”

2024 年，全国各地法院积极响应党中央号召，深入贯彻落实《数字中国建设整体布局规划》，在推进审判工作现代化方面取得了显著成效。这一年，是数字法院建设的关键之年。人民法院依托大数据、人工智能等前沿科技，通过场景建设和数字建模，逐步构建起覆盖立案、审判、执行等全流程的大数据平台。

目前，数字法院的框架体系、技术平台、建设路径、操作规程已初步形成。2024 年，我国数字法院建设不仅注重技术层面的应用创新，更强调理念革新和服务优化，力求以科技赋能公正高效司法。

2024 年 11 月 15 日，最高人民法院组织人民法院出版社研发并正式发布“法信法律基座大模型”这一国家级人工智能基础设施。以“法信法律基座大模型”作为底层支撑，广东省深圳市中级人民法院上线运行了人工智能辅助审判系统，将审判流程从立案到结案拆解为 85 个节点，结合法官关键工作场景，开发出立案智审、智能阅卷、智能庭审、智能文书 4 个相应的功能模块，真正实现 AI 全流程赋能，有力提升了审判工作质效。

以“法信法律基座大模型”对最高人民法院法答网、人民法院案例库数据预训练而研发的“库网融合”智能检索系统将于近期试点应用，以数字化、智能化手段促进法律适用的统一。

“数字法院建设，显著提升了司法效率与法律服务质量，让公平正义更高效更可感。”近日，全国人大代表、吉林四季盛宝纺织有限公司纺纱分厂细纱车间挡车工徐艳茹在参观吉林省珲春市人民法院时，对数字法院的显著成效给予充分肯定。

数字法院是技术的革新，是司法理念的升华，更是推动中国法治现代化不可或缺的一部分。其正以其智慧和力量，为实现公平正义注入新的活力。

专家点评

数字法院建设是司法领域的重塑性变革

上海市高级人民法院研究室主任 张果

近年来，大数据、云计算、人工智能、区块链等数字技术正在重塑人类的生产与生活方式。习近平总书记高度重视“数字中国”建设，多次作出重要部署。党的二十大报告提出，要加快建设网络强国、数字中国。2023 年 2 月，中共中央、国务院印发《数字中国建设整体布局规划》，为“数字引擎”助推中国式现代化作出了顶层设计。数字化变革深刻地影响和改变着法治的实践形态，数字法院建设应运而生。2024 年 3 月，最高人民法院党组书记、院长张军在第十四届全国人民代表大会第二次会议上明确提出，要以数字法院助力提质增效。

数字法院建设将数字技术从单纯的辅助工具演变为贯穿法院工作全流程的工作方法。数字法院通过建立覆盖立案、审判、执行、社会治理各个领域的场景模型，对海量司法大数据进行筛选、比对、碰撞，发现隐藏在案件中的问题线索，实现不间断的监督管理、辅助办案和社会治理风险预警，对内推动法院工作理念、业务流程、组织架构、治理方式再造，对外为公共决策输出数据支持和智能分析研判，辅助提升社会治理效能，以审判工作现代化支撑和服务中国式现代化。可以说，数字法院建设是司法领域实现全面数字赋能、全程预警监测、保障适法统一、提升司法质效的一场重塑性变革，有效强化了审判管理、提升了案件质效，满足了人民群众对高质量司法的新期待，开拓了司法参与社会治理的新途径。

数字法院建设不是另起炉灶，而是信息化建设、智慧法院建设的迭代升级。在数据来源上，数字法院建设所需数据绝大部分是非结构化数据，通过人工智能语义理解等技术手段实现关键数据的自动提炼，无须手动输入。在研发主体上，数字法院建设由一线法官主导，消除了业务需求与技术开发之间的隔阂。在建设模式上，在同一平台中，无论应用场景由谁负责建设，一经建成即可供其他法院共用，实现了“一地突破，全域共享”。

全国各地法院认真贯彻中央及最高人民法院的部署要求，适应数字化改革浪潮，积极探索，创造了各具特色的数字法院建设模式。以上海为例，上海法院已初步建成以“数助办案、数助监督、数助便民、数助治理、数助政务”为核心板块的数字法院建设体系，累计推广应用 852 个，嵌入系统 504 个，推送提示信息 49.2 万条，法官反馈对案件办理有帮助率达 86.9%。实践证明，数字法院建设方向是正确的，成效是显著的，前景是广阔的。

随着数字技术和人工智能的加速发展，数字法院必然会发生更加深刻的变化。持续深化数字法院建设，需要以数字化转型推动司法审判工作提质增效、推动审判监督管理现代化、驱动诉讼服务体系更加高效便捷、促推法院参与社会治理模式变革、提升司法政务高效协同水平，全面提升法院工作的现代化水平。

《中国-东盟人工智能发展与治理合作》报告发布

原载：“中国信通院 CAICT”微信公众号

2024 年 12 月 9 日，在柬埔寨举办的中国-东盟人工智能发展和治理合作论坛上，中国信息通信研究院（简称“中国信通院”）与中国国际问题研究院联合发布《中国-东盟人工智能发展与治理合作：进展观察和推进建议》报告。

报告回顾和总结了人工智能技术发展的历程、特点和相关全球治理的主要态势，深入分析当前中国人工智能技术产业蓬勃发展、加速构筑治理体系并积极参与全球治理的情况，并指出东盟的人工智能产业发展潜力巨大，起步迅速。中国与东盟是全面战略伙伴，在数字经济和智能发展领域拥有坚实的合作基础。面对人工智能的技术浪潮，中国与东盟应进一步加强合作，共同分享技术进步带来的发展红利，并尽力规避和减轻技术引发的风险挑战。

柬埔寨副首相兼内阁办公厅大臣翁赛维索、中国驻柬埔寨大使汪文斌、中国国际问题研究院院长陈波出席论坛并致开幕辞。柬埔寨国务大臣，经济、社会和文化理事会主席陈乐提，中国信通院副总工程师王爱华作主旨发言。

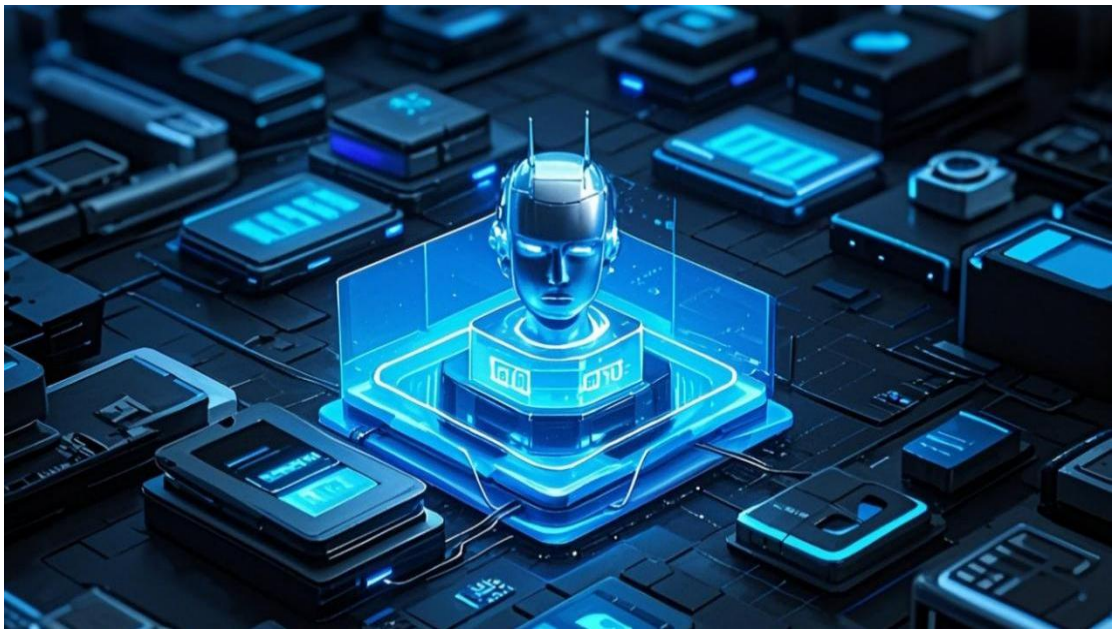
王爱华在发言中指出，当前人工智能技术正在向通用人工智能转型，带来前所未有的发展机遇。

中国积极拥抱技术创新，大力推动“人工智能+”行动，加速人工智能赋能新型工业化。与此同时，技术的快速应用也带来治理上的挑战，智能鸿沟、环境影响、劳动替代等全球共性问题也日益显著。中国信通院积极参与全球人工智能治理，承担了ITU 人工智能向善案例集编纂、中国—金砖国家人工智能发展与合作中心运作等工作，未来希望与各方进一步加强合作，共同为人工智能向善发展、造福所有人而努力。

来自中国、柬埔寨、新加坡、印度尼西亚、缅甸、马来西亚、文莱、越南、菲律宾、泰国、中国香港等十余个国家和地区的 400 位政要、学者、媒体和企业人士以及国家和国际组织驻柬代表与会。

（技术编辑：王藜焯、敖紫辰、何芮）

研究动态



基础理论

1. 神经技术时代精神隐私的保护层次及路径（陈鲁夏）

来源:《现代法学》2024 年第 6 期

精神隐私是神经技术时代隐私保护的新维度。本文旨在厘清精神隐私的不同保护层次，构建有针对性的法律保护路径。精神隐私的保护层次涉及数据层、信息层及内容层。在数据层，其所涉大脑数据是人脑结构、活动和功能相关的定量数据，其相关精神隐私风险在于大数据分析的不确定逻辑和数据安全事件可能引发的隐私问题。在信息层，精神隐私保护的对象是与个人生理、健康相关的大脑信息及精神状态信息，其相关精神隐私风险包括生物识别、个人特征预测和精神状态解码等。在内容层，精神隐私的保护对象包括命题性的精神内容和经验性的精神内容，与其相关的“读心”风险目前虽不具有技术现实性，但真实地挑战着人们的隐私感受。就保护路径而言，内容层精神隐私应纳入传统隐私权的保护范畴，信息层精神隐私可适用敏感个人信息的处理规则，数据层精神隐私存在双重保护路径。

2. 论“数字人权”的三重异化——对龚向和教授“三重否定”的回应（刘志强）

来源:《政法论坛》2024 年第 6 期

“数字人权”理论存在三重异化。一是本原异化。“数字属性”不是人之本性，脱离人的自然属性，取代人的社会属性，宰制人的精神属性，使得人权主体溢出自然人范畴，形成蔑视人性的“拜数字教”。二是形态异化。“数字形态”不是人权的道德形态，无法为社会的道德奠基；亦非人权的法定形态，欠缺民主立法和规范逻辑的承认。作为实有形态的新样貌，须接受人权伦理和法理的反思。三是概念异化。“数字权利”滥用“未列举权利”，将传统人权与民事权利混成“新”人权，泛化了人权的义务主体，不利于当代中国人权观的法治实践。“数字人权”泛化表象的根源是人权被异化，通过“否定之否定”来建构超越代际论范式的人权话语，可以促进人权对“数字化”思潮的引领作用。

3. 数字时代劳动关系概念及认定规范的中国表达（谢增毅）

来源:《中国社会科学》2024 年第 10 期

为克服现有劳动关系概念和认定规则的缺陷，应对平台用工兴起的规则需求，矫正司法实践存在

的偏差，我国有必要通过立法对劳动关系概念及其认定方法进行规定。劳动关系的本质属性依然是从属性，核心是人格从属性。从属性可从人格从属性、经济从属性和组织从属性三个角度加以考察，但三个从属性互有交叉，并非泾渭分明。劳动关系概念及其认定的规则体系建构应充分考虑数字时代的特点，规范表达应包含立法和行政意见或司法解释等不同层面的多种形式，在规则的确定性、稳定性和灵活性之间寻求平衡。在规则建构中应积极借鉴域外有益经验，并充分利用本土已有规则和实务资源。在劳动关系认定上，应把握从属性的合理程度，并对劳动者是否具有劳动自主性进行实质判断。

4. 《联合国打击网络犯罪公约》刑事定罪条款与中国刑法应对（周振杰）

来源:《中国刑事法杂志》2024 年第 5 期

在“信息和通信技术系统的使用可对刑事犯罪的规模、速度和范围产生巨大影响”与“需要加强各国之间的协调与合作”的认识下，《联合国打击网络犯罪公约》刑事定罪条款体现出了明显的预防性、灵活性、客观性、延展性与主权性特征。我国《刑法》虽然涵盖了公约刑事定罪条款的大部分内容，但是在持有儿童性虐待或儿童性剥削材料等持有型犯罪、洗钱犯罪的上游犯罪等方面还存在衔接的必要。应对公约刑事定罪条款，对于强制性规定，应坚持司法路径为主、立法路径为辅的原则，在司法解释无法解决问题之时才适当修改《刑法》以扩大处罚范围；对于任择性要求和措施，可以从前瞻性立法的角度，参考公约规定对《刑法》的相关规定进行论理与体系解释。适应人工智能、元宇宙技术的发展，应将伤害解释为包括身体伤害与精神伤害，将传播描绘儿童性行为物品的行为规定为从重情节，在认识错误场合根据主观认识对其支配下的客观行为进行定性。

5. 论信息权——知识产权、数据权益与精神性人格权的统一（李春晖）

来源:《知识产权》2024 年第 10 期

知识产权与数据权益之客体均为信息，两种权利具有高度契合性，创新性并非数据权益成为知识产权的阻碍。财产利益和精神利益是主观利益分类，可共存于任何客体上，因此精神性人格权客体并非“精神利益”，而是与人之身份有关的各种信息。精神性人格权与知识产权中的标记相关权利高度近似，并有历史渊源。同时，现有概念的知识产权和商品化权均侧重财产权益，人格权又仅仅侧重精神权益，缺乏既统一客体又统括财产权益和精神权益的概念，信息权为适宜的选择。信息权概念优于无形财产权，后者无法统括精神权益，且将知识产权与无定形客体上的物权及财产性制度建构混为一谈。信息权与物权相对，将令民法学理论和民法典之形式理性更加完善。

6. 用户账户：技术概念如何通过欧盟的 AI 法案渗透到公法中（Ida Koivisto, Riikka Koulu & Stefan Larsson）

来源：Maastricht Journal of European and Comparative Law, Vol.31, Issue 3 (2024)

本文认为，通过欧盟的技术法规，技术概念渗透到了法律语言中。这些概念可能起到移植甚至刺激的作用，造成紧张和不确定性。由于技术法规日益横向化，即对私人和公共行为者都有义务，这些新发现的法律概念仍然与既定的公法词汇及其所代表和包含的权力组合脱节。我们从公法的角度来探讨法律语言的演变，并重点关注欧盟即将出台的《人工智能法》中的“用户”和“设计者”概念。我们结合人机交互研究中有关这些概念的丰富理论来讨论这些新出现的法律概念。我们的分析表明，“用户-设计者”的法律概念和技术概念之间存在差异。我们得出三个结论。首先，数字革命发生在法律的概念语言实践中，而不仅仅是在将法律转化为代码时。其次，当外部概念被挪用到法律中时，它们会被从其既定的栖息地连根拔起，这可能会导致未来法律解释的不可预测性。第三，在公法中，采用“用户-设计者”可能会带来一些额外的挑战，因为它在公共权力和私人实体之间的关系中引入

了一个新的代理人。同时，公民似乎主要被排除在法律概念化之外，这有可能模糊传统的权力组合。

个人信息保护

1. 数据驱动型并购中个人信息竞争损害评估（杨利华）

来源:《财经法学》2024 年第 6 期

数据驱动型并购不仅会产生规模经济效应，也会增强市场集中度，易于发生单边效应，产生排除和限制竞争的影响，从而引发并购的反垄断审查。并购的竞争影响分析是作出垄断与非垄断区分的重要依据。数据驱动型并购主要是为了争夺个人信息及其生成的数据资源，反垄断审查应当重点对个人信息竞争影响进行评估。然而，数据驱动型并购对个人信息竞争的影响主要发生在非价格方面，目前反垄断执法机构还没有建立成熟的竞争影响评估方法。从市场竞争、消费者福利和创新的角度来看，数据驱动型并购导致的个人信息竞争损害都与个人信息保护有关。因而，数据驱动型并购的反垄断审查应当构建以个人信息保护为核心的非价格竞争损害理论，从个人信息保护水平、个人信息保护模式和个人信息保护的创新性三个维度进行评估。如果并购会导致个人信息保护水平降低，则表明市场中个人信息保护方面的竞争减少，市场竞争受到损害。如果并购会导致多种不同的个人信息保护模式变少或差异性变小，造成消费者的选择受限，则表明并购将减损消费者福利。如果并购会导致提供创新型个人信息保护的数字平台企业减少，使个人信息保护中的创新性经营策略消失，那么并购将导致创新损害。

2. 生成式人工智能训练语料的个人信息保护研究（张新宝）

来源:《中国法学》2024 年第 6 期

生成式人工智能训练语料的个人信息保护应当秉持鼓励和支持创新的基本立场。为确保服务提供者的个人信息利用需求能够得到满足，可以在训练端对《个人信息保护法》作适当宽松解释或例外规定。对于已公开的个人信息，可以通过宽松解释“公开目的”将其纳入可处理的范围。对于未公开的个人信息，仍需要以个人同意作为处理行为的合法性来源，但是可以通过宽松解释目的限制原则、调整“告知—同意”的相关规则，缓解服务提供者面临的困难。技术壁垒的提高加剧了信息主体的劣势地位，需要确保个人信息保护请求权的行使，以维护个人的合法权益，但是其行使不可避免受到技术现实的限制。服务提供者应严格履行包括技术措施在内的个人信息安全保护义务，尽可能降低给个人信息带来的风险。保护机制整体上应以行政监管为主导，如果侵害个人信息权益造成损害，应允许服务提供者以“符合行政监管要求”作为不存在过错的抗辩。

3. IP 地址保留和在线版权侵权的棘手问题：合议庭在“La Quadrature du Net”及类似案件中指明了道路（Daniël Jongsma）

来源：Common Market Law Review, Vol.61, Issue 6 (2024)

2024 年 4 月 30 日，欧洲法院（ECJ）组成合议庭，就为打击网络侵权而保留和访问 IP 地址的合法性作出了具有里程碑意义的判决。该判决是欧共体对其先前一些裁决的反思，在这些裁决中，法院似乎严格限制了成员国要求互联网服务提供商（ISP）保留 IP 地址的能力。保留 IP 地址通常对识别在互联网上实施刑事犯罪或承担民事责任的人的身份至关重要。《电子隐私指令》（ePrivacy Directive）是《通用数据保护条例》(GDPR)（之前为《数据保护指令》）的特别法，它禁止互联网服务提供商（ISP）存储所谓的流量数据，如 IP 地址，除非出于某些操作上的必要。不过，《电子隐私指令》也允许成员国出于某些特定目的对这一规则采取例外措施，条件是这些措施必须特别尊重欧盟的基本权利。在为保障国家安全和打击犯罪而保留数据方面，欧洲法院制定了一套详细的规则和条件，涉及保留和访问包括 IP 地址在内的流量数据的

合法性。

4. 欧盟应如何在不损害成员国的基本职能及其宪法原则的情况下保护个人数据？Österreichische Datenschutzbehörde 诉 WK（Marek Szydło）

来源：Common Market Law Review, Vol.61, Issue 5 (2024)

哪些具体的国家领域不在欧盟法律的管辖范围内？免除的领域是否包括国家议会控制行政部门的活动，尤其是当这种议会控制涉及国家安全时？欧盟机构在制定和执行欧盟次级立法的法案时，必须在多大程度上尊重各国宪法中所包含的分权原则？它们应该给予成员国多大的自由度，以使他们能够维护这一原则？这些无疑是欧盟法律的基本问题。前两个问题涉及欧盟法律的外部界限，第三个问题涉及一个重要的法律原则，它可以归类为《欧洲联盟基本条约》第 4(2)条所指的国家身份和根本宪法结构的范畴。在奥地利数据保护机构诉 WK 一案中，欧洲法院有机会在解释《通用数据保护条例》（GDPR）条款时考虑这些问题。

数据确权与流通

1. 数据知识产权登记的底层逻辑（刘建臣）

来源:《华东政法大学学报》2024 年第 6 期

我国决策层已决定通过三权分置的思路保护数据，且正在研究数据登记的新方式。在此背景下，数据知识产权登记的地方试点立法正火热开展。但立法进程的科学性依赖于两个前置性条件的成就：数据产权在立法层面将以财产权形式确立，数据知识产权在数据产权的体系中有一席之地。只有在完成双重前提论证的基础上，方可探究登记制度的具体设计。梳理试点省市立法文本可以发现，其对登记对象、审查模式和部分配套制度等重要内容均存在认识分歧。在登记对象的确定思路方面，鉴于数据知识产权可用以实现数据产品经营权的立法表达，应将其限定为合法来源、衍生数据和商业价值，并对公开数据和非公开数据均开放登记。在审查模式的选择依据维度，考虑到数据内在的高信息成本，宜仅采取版权模式下的形式审查方案。在配套制度的安排方面，立法者应当秉持与赋权模式相匹配且有助于促进数据交易流通的双重价值取向，承认独立处理例外、限定公开范围并采纳登记生效主义。

2. 论数据交易中替代交易规则的双重规范面向（林婷婷）

来源:《财经法学》2024 年第 6 期

《民法典合同编通则解释》第 60 条第 2 款确认了替代交易规则，为数据交易中违约可得利益计算提供了制度依据。不同于一般交易，数据交易的动态性和非排他性在增筑替代交易规则的优先性与确定性的同时，亦勾勒出了替代交易规则双重规范面向。在违约救济面向，替代交易规则具有对期待利益的保护功能。因此，为避免数据交易的特性对违约可得利益计算的影响，宜将“依法行使合同解除权”解释为“发出解除通知”，并将替代性要件的内涵衍化为“功能性替代”，发挥善意要件的兜底式作用。在减损措施面向，宜以替代交易规则的不真正义务属性为轴承，重塑以价格为直观指标并兼采多元化判断因素的适格性判断标准，并借助可预见性规则的损害赔偿数额限制功能，协力实现数据交易双方的利益衡平。

3. 侵害企业数据权益的民事责任（王叶刚）

来源:《中国法学》2024 年第 6 期

企业数据的来源、内容以及取得方式等具有复杂性，对行为人侵害企业数据权益民事责任的认定以及责任承担方式等有着重要影响。行为人侵害企业合法取得的数据时，企业有权依法请求行为人承担违约责任、侵权责任或者基于绝对权请求权产生的民事责任。企业对其非法取得的数据不享有数据权益，但行为人破坏企业对数据的持有状态的，企业也有权请求行为人承担停止侵害、排除妨碍、赔偿损失等责任。行为人侵害企业数据的，个人数据来源者虽不享有数据权益，但可以其个人信息权益受侵害为由请求行为人承担侵权责任或者基于人

格权请求权请求行为人承担停止侵害、排除妨碍等民事责任。行为人侵害非个人数据来源者的著作权、商业秘密等在先权利的，受害人有权依据在先权利的保护规则请求行为人承担民事责任。非个人数据来源者对企业所享有的数据查阅权、可携带权等属于相对权，原则上不受侵权法保护；但在行为人恶意侵权时，受害人也应有权请求行为人承担侵权责任。

4. 论数据治理的使用权范式（付新华）

来源:《中外法学》2024 年第 6 期

在数据治理现代化快速演进之际，“使用权范式”在诸多数据治理范式中脱颖而出，标志着数据治理理念的深刻转变。数据治理的使用权范式是近现代以来“从所有到使用”的发展趋势在数字时代的表现，其以“数据使用权”为基石范畴，以数据本质特征和数字经济基本规律为理解系统，以数据使用权的合理分配与流通利用为方法论指引，并以促进数据共享与利用为价值导向，旨在实现“数据资源”的最大化利用。使用权范式对数据基础制度的规范建构具有方法论意义，提供了跨领域和跨阶段的统一治理框架，这不仅有助于避免数据所有权模式极化可能引发的“反公地悲剧”风险，还能防止“场景理论”与“阶段理论”导致的治理碎片化，同时有助于促进数据基础制度的内部协调。故应当以使用权为中心构建数据基础制度，包括确定数据使用权的法律地位、完善数据流通机制、建立平衡收益分配制度、加强数据安全治理，以推动构建高效、公正、安全的数据治理体系。

5. 数据产权分置下反垄断规则调适与制度构建（王文君）

来源:《中外法学》2024 年第 6 期

数据产权分置下，对数据控制者赋权可能会使超大型数字平台进一步垄断数据，对数据利用者简单赋权可能会导致数据流通利用难以实现。数据垄断的应对应以生产和流通为框架，在数据控制权配置和数据利用权配置的基础上分别进行，以统筹数据有序流通的秩序目标和效率目标。数据生产环节，应强制数据控制权主体开放必需数据，拒绝开放必需数据的竞争损害评估主要围绕横向封锁、纵向封锁、创新阻塞三个维度，综合考量作为竞争维度的个人信息与隐私保护、以及作为动态效率来源的创新和投资激励这两个抗辩理由的正当性；数据流通环节，应以“资源—集合—产品”的立体化思维，将数据法人化，赋予数据集人格，构建数据法人制度，促进数字市场竞争，提高消费者福利。强制开放必需数据和构建数据法人制度时，应谨慎设置使用条件，防止规则或制度过度适用造成负面效果。

6. 数据犯罪的刑法规制：法益内涵与体系构建（吴沛泽）

来源:《中国刑事法杂志》2024 年第 5 期

围绕数据处理而形成的数据犯罪呈现出严重的社会危害性与复杂性，我国数据犯罪刑法规制体系的构建应有效回应大数据时代不断革新的外部社会事实。试图为数据犯罪设计出一套独立且周延的罪名体系的立法进路并不妥当。我国数据犯罪的规制应立足于双层法益观，阻挡层法益为数据的运行状态安全，背后层法益为数据所承载的现实具体利益。数据犯罪的双层法益观具有合理限缩数据类型、全面评价行为不法与构建罪量评价体系的功能。构建我国数据犯罪的刑法规制体系，应正确认识数据本体罪名与关联罪名的竞合情形及界限，形成开放的数据刑法体系；在刑法中贯彻数据分类分级保护理念，对数据属性及数据不法行为的法益侵害性进行具体、实质与综合的判断；调整数据罪名的体系结构，将破坏数据行为独立构罪并增加干扰数据的行为；数据犯罪司法解释应加强数据犯罪行为与后果的不法关联性，重塑数据类型与数据保护级别。

人工智能

1. 论生成式人工智能服务提供者过错的认定（沈森宏）

来源:《现代法学》2024 年第 6 期

在人工智能生成内容致人损害的情形下，过错是服务提供者承担侵权责任的归责事由。合理地认定服务提供者的过错，是有效平衡预防风险与鼓励创新双重价值目标的关键。服务提供者过错的本质是其违反了交往安全义务或注意义务。在认定标准上，应采取动态的“合理人”标准，结合技术水平、服务类型与侵权内容等维度，分析特定情境下合理的、谨慎的服务提供者应尽的注意义务。服务提供者的注意义务主要包括语料处理义务、对齐微调义务、内容审查义务、内容标识义务和用户管理义务，若服务提供者未能合理地履行这些义务，则应认定为具有过错，需对生成内容致人损害的行为承担侵权责任。服务提供者侵权责任的认定应类推适用“通知规则”，这不仅有利于实现服务提供者与权利人之间的利益平衡，还可以减轻权利人证明服务提供者过错的举证负担。

2. 机器中的作者与创作：从摄影技术到生成式人工智能（章凯业）

来源：《中外法学》2024 年第 6 期

人工智能生成内容的可版权性和归属，本质上是如何在机器创作中寻找作者和评估人的智力活动。规范意义上，作者的活动是一种与机器相分离的人类的智力活动，创作行为是由详细的构思与受控的执行两部分组成。在机器创作中，智力活动的评估对象是体现人类构思的内在表达，而不是机器执行所生成的外在表达，独创性的判断只能基于作品产生的方式，而不是机器产品的外观。作者是构思作品并控制其执行的人。对 AI 创作的分析应该首先剥离机器的部分和 AI 的贡献，随后判断人类的角色是否符合构思与执行的要求，即内容生成的准备阶段是否存在足够详细的创作计划，内中的选择能否满足独创性的要求，以及人类对 AI 的执行是否具备控制力。AI 生成内容的作者身份可能是 AI 设计者、使用者，或是没有作者，这需要在个案中，结合 AI 程序的特征、设计者和使用者各自的活动类型，并根据 AI 作品中关键的表达性元素，进行类型化分析。

3. 人工智能时代著作权的刑法保护（刘宪权）

来源：《中国刑事法杂志》2024 年第 5 期

普通人工智能时代的作品独创性完全来自于人类，人工智能只能纯粹作为人类创作的工具而无法成为作品的创作主体。弱人工智能时代的生成式人工智能已经具备“智力投入”的能力，可能成为作品的创作主体。生成式人工智能暂不具备权利主体身份而不能享有生成物的著作权，但存在著作权的转移问题。强人工智能时代的人工智能可能在独立的意识和意志支配之下完成作品的创作。根据“承认与限制”的机器人伦理基本原则，应当承认强人工智能机器人的作品创作主体乃至权利主体地位，并且应当承认其具有成为责任主体的可能性。生成式人工智能最突出的技术亮点就是“生成”，在著作权领域“生成”即为“创作”。生成式人工智能的生成物可以成为著作权法意义上的作品，其衍生权利也可以成为刑法中侵犯著作权罪的侵害法益。生成式人工智能不仅可以成为创作工具，同时也可能成为创作主体。在生成式人工智能具有法定权利主体地位之前，因其创作而产生的著作财产权应当转移给使用者所享有。使用者只享有由生成式人工智能转移而来的著作财产权，而不享有无法转移的著作人身权。侵犯相关著作财产权的行为可能构成民事侵权或者刑事犯罪。

4. 论生成式人工智能服务提供者的注意义务（林北征）

来源：《法律适用》2024 年第 10 期

生成式人工智能的技术特性使得侵权风险具有高度随机性，直接导致因果关系复杂化，增加侵权责任在司法裁判中的认定难度。生成式人工智能服务提供者在被诉侵权时，往往陷入过错抗辩难题，无法明确界定自身责任。在此背景下，得益于裁判合理性、技术兼容性及成本可控性，注意义务可改良现有“避风港”规则，指引服务提供者在合理范围内采取必要措施，降低侵权风险。注意义务既可源于公法义务的转化，也可通过服务协议加以明确。

以生成内容的标识义务、使用服务的提示义务以及侵权投诉的处理义务构建和落实注意义务体系，有利于服务提供者履行法律责任，保护服务使用者和第三方的合法权益，促进技术创新与法律规制之间的平衡。

5. 软法的实施机制——以人工智能伦理规范为例（沈岿）

来源:《财经法学》2024 年第 6 期

软法的广泛存在，并不意味着其切实地得到了遵守和执行。人工智能领域的软法——人工智能伦理规范——被证明存在“实效赤字”，其原因在于：人工智能伦理规范的非强制性，抽象性、模糊性，分散、混乱与叠床架屋，自愿遵守的动力不足，合规悖论，社会系统论困境，以及人工智能发展压倒约束的宿命论。但人工智能伦理规范因其灵活快捷性、多样适配性、合作试验性、事实压力性、跨国适用性而仍然有独特价值。经验研究表明，组织机制、合规压力机制、合规激励机制、技术方法论机制、基准机制以及软硬法互动机制，可推动软法的间接实施。价值共识与经济逻辑的结合、内在理由和外在推动的结合，是软法获得更多实效之道。

6. 算法招聘人员为何歧视：数据驱动歧视的因果挑战（Christine Carter）

来源：Maastricht Journal of European and Comparative Law, Vol.31, Issue 3 (2024)

人力资源部门通常使用自动决策系统来自动做出招聘决定。大多数自动决策系统利用机器学习来筛选、评估和推荐候选人。算法偏见和成见是这些技术常见的副作用，会导致数据驱动的歧视。然而，由于机器学习在统计上的复杂性和操作上的不透明性，往往无法证明这一点，这就影响了投诉人满足欧盟平等指令中必要的因果关系要求的能力。在直接歧视中，机器学习的使用使投诉人无法证明表面证据确凿的案件。在间接歧视中，一旦责任转移到被告身上，问题就会显现出来，而因果关系则作为一种准抗辩来运作，其参照的是与歧视无关的客观合理因素。本文认为，因果关系必须被理解为一种信息挑战，可以通过三种方式加以解决。首先，通过《欧盟基本权利宪章》的基本权利视角。第二，通过《通用数据保护条例》等数据保护措施。第三，文章还考虑了未来可能出现的法律责任，如《人工智能法》和《人工智能责任指令提案》。

平台治理

1. 必需模型反垄断法强制开放的理据与进路（许丽）

来源:《华东政法大学学报》2024 年第 6 期

基础模型具有通用性与赋能性，对下游平台提供服务、参与市场竞争具有准入上的影响，是通用人工智能时代的数字“必需设施”。通用人工智能服务提供者不仅自身提供大模型应用服务，也向下游平台企业提供预训练基础模型，下游平台企业在此基础上进行微调，研发出适用于不同场景的专业模型。由于通用基础模型具有不可或缺性、不可复制性，且开放基础模型具有可行性，在拒绝提供基础模型不具有法律上的豁免事由时，通用基础模型服务提供者具有普遍接入义务。根据“必需模型”服务提供者与拒绝交易对象之间的关系不同，拒绝提供“必需模型”行为可能构成拒绝交易、差别待遇或自我优待，从而避免了适用《反垄断法》第 22 条时须满足“支配地位之结构要件 + 消极不作为之行为要件 + 反竞争效果之效果要件”三重标准的复杂性与不可操作性。

2. 互联网平台算法推荐的版权侵权责任研究（徐俊）

来源:《政法论坛》2024 年第 6 期

尽管算法推荐技术在互联网平台得到广泛应用并受到业界普遍认同，但基于该项技术应用的版权侵权责任承担却引发了较大争议。本文提出对上述争议的解决，需要将平台责任的法律逻辑作为大前提，将算法推荐的技术逻辑和商业实践作为小前提，在场景类型化的基础上根据逻辑三段论推导得

出平台是否承担版权侵权责任的结论。算法推荐的主流技术标准客观可量化，互联网平台在算法纯粹输出场景下无需承担概括性的注意义务，同时应当在算法流量倾斜场景下承担更高的注意义务。

3. 数字市场反垄断法实施政策目标反思（叶卫平）

来源：《财经法学》2024 年第 6 期

随着数字市场经济规模扩张和市场集中度提升，差别定价、自我优待、搭售、排他性交易、扼杀式并购等垄断弊害开始凸显，强化反垄断的社会呼声渐起。为了有效回应数字市场的反垄断规制需求，我国反垄断法实施政策目标经历了从“包容审慎监管”到“强监管”再到“常态化监管”的演变。但是，过于频繁的政策目标调整，不利于市场主体形成稳定的行为预期；规制不足或者规制过度，都会减损规制的应有效果。如何在提升法律实施对经济变化的回应性的同时，避免不当实施对市场机制和经济活力的侵害，是当下反垄断法实施政策目标优化和制度建设过程中需要思考的关键问题。

4. 《数字市场法》：反垄断补救问题的部分解决方案（Friso Bostoen & David Vanwamel)

来源：Common Market Law Review, Vol.61, Issue 6 (2024)

数字市场的反垄断补救措施收效甚微。《数字市场法》（DMA）提供了部分解决方案，它建立了一个多层次的补救金字塔，解决了委员会在对反垄断侵权行为进行补救时面临的一些难题。金字塔的底层是《数字市场法》规定的义务，其中包含比反垄断补救措施更快、更规范的事前补救措施。第二层是监管对话，这是一种开放、反复的规范程序，可以减少信息不对称，并使补救措施面向未来。第三个层次是违规程序，它是对监管对话的补充。位于金字塔顶端的是系统性违规程序。它赋予欧盟委员会实施事后补救措施的权力，这些补救措施可能比欧盟竞争法的对应措施更加有力。尽管与欧盟竞争法相比，《数字市场法》加强了委员会的补救程序和权力，但委员会必须审慎行使权力。委员会的重点应放在补救金字塔的中间层，尤其是监管对话。

5. Klaudia Majcher 的《数字市场数据保护与竞争法之间的一致性》书评（Arletta Gorecka)

来源：Common Market Law Review, Vol.61, Issue 6 (2024)

在《数字市场中的数据保护与竞争法之间的一致性》一书中，Majcher 提出了一个框架，以弥合数据保护与竞争法之间的差距，倡导一种连贯的执法方法。她追溯了这两个领域的演变，强调了它们在数字市场中的共同目标和挑战。Majcher 介绍了“部门一致性”，即这些法律相互加强，促进协同而非冲突的范式。本书探讨了这种方法的概念、实践和宪法意义，强调了它在不同司法管辖区的相关性，以及它在数字时代保障民主价值和市场公平的重要性。在第 1 章中，马杰尔从欧盟的视角探讨了竞争法与数据保护之间的关系，重点是《通用数据保护条例》(GDPR）以及《欧盟运作条约》(TFEU）第 102 条和《欧盟合并条例》(Council Regulation（EC)139/2004)下滥用支配地位的情形。由于《欧盟运作条约》第 101 条与研究竞争法和数据保护之间的相互作用关系不大，因此 Majcher 将其排除在外。本章从历史角度概述了这些法律领域的演变，强调了竞争法在欧洲一体化中的作用及其不断演变的目标。Majcher 还比较了这两个法律框架的目标和价值，强调了它们的相似之处和不同之处，尤其是在数字市场方面。

6. Friso Bostoen《滥用平台权力——根据欧盟竞争法及其他法律在数字市场中的行为》书评（Sarah Legner)

来源：Common Market Law Review,Vol.61,Issue 5 (2024)

近年来，数字市场日益成为欧洲竞争法关注的焦点。这些市场通过垄断倾向挑战竞争法。在积极的间接网络效应的推动下，一些平台运营商成功地主导了整个生态系统。因此，市场竞争正在转向对市场的竞争。平台运营商通过“倾斜市场”获得的

独立行为空间使《欧盟条约》第 102 条规定的滥用禁止条款得以适用。在过去的二十年里，欧洲委员会通过各种决定试图遏制平台权力滥用，并经常处以重罚。然而出现了几个挑战。从仍为确定垄断基础的市场定义开始，必须考虑多边平台市场的性质及其单边成本结构。数字市场的独特结构以及平台作为中介的角色也意味着，传统意义上的滥用禁止理论很难直接应用于平台行为。此外，许多平台运营商与下游的商业用户竞争。在根据《欧盟条约》第 102 条评估他们的行为时，这一角色带来了进一步的挑战。

7. 平台工作与传统的员工保护： 需要替代性法律方法（Sonja Mangold）

来源：European Labour Law Journal, Vol.15, Issue 4 (2024)

通过数字平台进行的有偿工作（即所谓的众包工作和零工工作）在欧洲的重要性日益增加。平台工人常常面临较差的工作条件。大多数平台公司将众包和零工工人视为自雇或独立承包商，因此通常的劳动保护法律并不适用。作为回应，已经通过案例法和立法采取了措施，以将传统雇佣关系的范围扩展到平台工作。例如，德国联邦劳动法院（Bundesarbeitsgericht）在一些高调的裁决中重新分类并将平台工人视为雇员，这些裁决将在下文中更详细地讨论。最近通过的欧盟关于平台工作的指令确立了平台工人就业的法律推定。欧盟成员国也最近引入了法规，将平台工人纳入雇员概念之下。然而，正如本文所论述的，旨在扩大雇员身份的法律和司法举措往往由于市场动态以及平台企业使用的实际适应和规避策略而受到限制。此外，传统的劳动法律保护似乎并不总是适合解决各种类型平台的复杂性和特殊性。因此，以下论点值得讨论：1.如果将雇员身份扩展到平台工作已经在社会经济现实中得到锚定，并且在这方面能够达成社会伙伴之间的共识，那么这种做法似乎是有希望的。一个现有的例子是西班牙的骑手法，该法采取了行业性方法，不仅得到了工会组织的支持，也得到了雇主协会的支持。2.此外，应该强烈关注并从法律上推进为平台工人创造一个实质性的社会权利核心，无论其就业身份如何。关于在依赖性雇佣和自雇之间的法律灰色地带工作的替代监管方法的长期学术讨论应该被重新激活，并为数字工作平台的新现象带来成果。3.第三，应该鼓励平台公司通过自我调节的企业社会责任（CSR）倡议来改善工作条件，立法者和政策制定者应该对此给予鼓励。正如本文稍后将展示的，平台已经存在广泛的 CSR 努力。为了应对表面文章的风险，应该通过适当的配套法律措施和公众压力，使平台业务运营商自己的倡议变得有效。

8. 平台工作者的算法管理：加拿大和欧洲监管方法研究（Fife Ogunde）

来源：European Labour Law Journal, Vol.15, Issue 4 (2024)

算法管理虽然没有完全的工作自动化那么引人关注，但随着时间的推移，其影响力和力量预计会变得更大。过去十年来，算法管理的现实问题越来越受到学术界的关注，尤其是在平台经济中的雇佣关系方面。本文通过比较影响平台经济中算法管理的两项重要立法，为现有学术研究做出了贡献：Ontario 的《2022 年数字工人权利法案》和《欧洲议会和理事会关于改善平台工作条件的指令提案》。本文的主旨是，虽然该法案的总体基调表明其朝着正确的方向迈出了一步，但其对信息权的限制性方法限制了其在规范平台工人算法管理方面的整体有效性。

9. 英国的数字市场监管：CMA 新框架中比例原则的必要性（Miroslava Marinova）

来源： Journal of European Competition Law & Practice, Vol.15, Issue 7 (2024)

《数字市场、竞争和消费者法案》（DMCC）于 2024 年 5 月 24 日获得英国皇家御准通过，这是自英国竞争和市场管理局（CMA）成立以来对英国竞争和消费者保护法进行的最重大改革。DMCC

法案建立了一个新的数字市场体系，为具有“战略市场地位”（“SMS”）的公司制定了具体的行为规则，并授权英国竞争与市场管理局执行这些规则。为此，CMA 成立的数码市场组（DMU）被赋予新的工具，以调查和应对数码市场的竞争挑战。然而，对 DMCC 执行的一个主要关切来自于它赋予 CMA 在为被指定为具有 SMS（显著市场地位）的公司量身定制具体行为规则时的高度自由裁量权。虽然这种自由裁量权是有意识的选择，以允许细微差别和特定情境的监管，但不仅存在执行不一致和不可预测的风险，而且需要更好地将比例原则应用于预期选择的措施。

数字行政与司法

1. 刑事诉讼中人工智能证据的法律性质和运用规则（余鹏文）

来源:《中国刑事法杂志》2024 年第 5 期

当前由人工智能系统分析形成的证据已经出现在法庭上，对传统的刑事诉讼程序和证据制度提出了新挑战。基于生成机理和属性，人工智能证据可以被定义为历经感知、认知和决策阶段的支持事实认定的机器意见，划分为工具型人工智能证据和主体型人工智能证据。作为一种新型意见证据，人工智能证据既不同于普通证人的一般意见，也有别于专家证人意见，适用现有的法定证据种类制度以及相对应的证据审查规则并不恰当。通过比较法分析，刑事诉讼中运用人工智能证据的最佳途径是融合对抗式诉讼和审问式诉讼的证据规则，形成庭外验证评估和庭审充分质证的综合化审查机制。为有效发挥人工智能证据的证明价值，我国有必要参照综合化审查机制，以理性主义证据观为指导原则，在技术规则层面上构建人工智能主体适格验证规则，在法律规则层面上明确控方举证方式，合理强化质证对抗性，以及确立审慎的认证规则。

2. 电子数据证据“关联性”的判断逻辑研究（刘林）

来源:《法律适用》2024 年第 10 期

电子数据证据“关联性”判断应在证据“关联性”理论基础上进行考察。当前法律和司法解释对于电子数据证据“关联性”的规定较为原则，并且鉴于电子数据的专业性，在司法实践中，其“关联性”的认定呈现不同于传统证据的特点。在电子数据证据“关联性”的审查认定上，应细化为四个层次：实物关联、内容关联、法律关联、形式关联，并正确认识发挥司法论证方法在证实电子数据证据“关联性”上的作用和路径。

虚拟财产

1. 论刑事涉案虚拟货币处置（胡铭）

来源:《现代法学》2024 年第 6 期

合法、有效地处置刑事涉案虚拟货币是规范涉案财物处置的时代新课题。在涉虚拟货币犯罪高发态势下，刑事涉案虚拟货币处置已经受到理论界与实务界的共同关注。虚拟货币技术所表现的匿名性、去中心化、易跨境性等特征给公安司法机关的处置能力和传统涉案财物处置规则带来挑战。刑事涉案虚拟货币处置关乎司法公正、基本人权及信息网络犯罪综合治理成效，需要立足于虚拟货币监管政策与刑事涉案虚拟货币处置的兼容性，改革创新刑事涉案虚拟货币处置方法，将刑事涉案虚拟货币处置纳入涉案财物处置体系之中，同时强化技术手段在完善涉案虚拟货币处置制度中的作用，建立健全刑事涉案虚拟货币全过程处置程序及刑事涉案虚拟货币处置全生命周期监管链机制，保障刑事涉案虚拟货币处置的合法性。

2. 央行数字货币跨境支付的法律挑战与监管协调路径研究（范晓波）

来源:《政法论坛》2024 年第 6 期

随着央行数字货币的崛起，跨境支付领域迎来了全新的发展机遇，然而，央行数字货币跨境支付受限于技术、法律、政策等多方面因素，成为制约其广泛应用的重要瓶颈。针对央行数字货币跨境支

付监管协调的问题，金融稳定理事会提出关于加强跨境支付三个优先主题的针对性的策略建议。统一支付标准和协议、加强技术创新和优化监管框架是提升央行数字货币跨境支付的关键。同时，加强国际合作与交流、创新多央行数字货币的治理机制也具有重要意义。

（技术编辑：李佳丽、麻卓妍、艾薇）

教研活动

中国人民大学未来法治研究院四位老师在“数炬计划——中国数据要素新锐学者项目”喜获殊荣

2024 年 11 月 25 日，“数炬计划——中国数据要素新锐学者项目（Data Torch Plan - China Data Factor Emerging Scholars Program，DTP）”首期获奖名单于 2024 数据交易节上正式公布，共有 60 家单位的 99 位青年学者喜获殊荣。最终确定获特等奖 3 名、一等奖 6 名、二等奖 15 名、三等奖 45 名以及提名奖 30 名。

中国人民大学未来法治研究院共有四位老师获奖。

中国人民大学法学院教授、未来法治研究院副院长丁晓东荣获特等奖。

中国人民大学法学院教授、民商法教研室主任、未来法治研究院平台治理研究中心主任熊丙万荣获一等奖。

中国人民大学法学院副教授、未来法治研究院研究员黄尹旭荣获二等奖。

中国人民大学法学院副教授、未来法治研究院执行院长张吉豫荣获提名奖。

“数炬计划——中国数据要素新锐学者项目”是我国首个面向数据要素理论研究的青年学者奖励计划，由上海数据交易所联合大数据流通与交易技术国家工程实验室、同方知网数字出版技术股份有限公司共同发起。该项目面向 45 周岁以下青年学者，自今年 8 月正式启动，历经学者自荐、大数据筛选、专家评审等环节，吸引了社会各界的广泛关注。

学者如光，微以致远。再次祝贺研究院四位老师在“数炬计划—中国数据要素新锐学者项目”中喜获殊荣，并衷心祝愿研究院在学术领域继续耕耘取得更多成果，为推动法学院和学校的高质量发展贡献力量!

2024 年世界互联网大会乌镇峰会网络法治论坛成功召开

2024 年 11 月 21 日由中国人民大学主办的 2024 年世界互联网大会乌镇峰会网络法治论坛顺利召开。网络法治论坛以“人工智能时代的网络法治”为主题，设置“中国网络法治三十年与世界网

络法治前瞻”“人工智能时代的法治挑战与数据保护”“全球人工智能监管规则”等议题。论坛由中国人民大学主办，中国人民大学法学院、京东集团协办，中国人民大学未来法治研究院、中国人民大学涉外法治研究院、中国人民大学法学院数字法学教研中心、国际数字法学协会支持。来自国内外政府部门、高校和研究机构的专家学者、互联网企业代表、媒体记者等各界嘉宾参加论坛。

2024 年世界互联网大会乌镇峰会网络法治论坛会场

在中国人民大学中华法治文明高等研究院院长、《中国法学》总编辑黄文艺的主持下，本次论坛的开幕式顺利进行。

中国人民大学中华法治文明高等研究院院长、
《中国法学》总编辑
黄文艺主持开幕式

国家互联网信息办公室副主任杨建文、浙江省人民政府副省长胡伟、中国人民大学校长林尚立参加开幕式致辞。中国法学会党组书记，全国人大常委会委员、宪法和法律委员会副主任委员王洪祥在开幕式中发表主旨演讲。

浙江省人民政府副省长胡伟开幕式致辞

中国法学会党组书记、
全国人大常委会委员、
宪法和法律委员会副主任委员
王洪祥发表主旨演讲

中国人民大学校长林尚立发表致辞。林尚立校长在致辞中表示，网络法治是信息革命发展的时代需求，是网络强国建设的重要保障。本次论坛聚焦人工智能时代的网络法治，对于提高人工智能安全治理水平，引导人工智能向善而行，确保人工智能发展安全可控具有重要意义。推动人工智能与网络法治双向赋能应以“良法”促“善智”，首要在夯实法治基石；以“良法”促“善智”，关键在加强学科建设；以“良法”促“善智”，基础在培养高素质法治人才；以“良法”促“善智”，动力在增进国际交流合作。中国人民大学将为人工智能法治领域的理论创新和实践发展、携手构建网络空间命运共同体贡献智慧和力量。

中国人民大学校长林尚立开幕式致辞

中国网络法治三十年与世界网络法治前瞻

本议题由中国人民大学法学院副教授、未来法治研究院执行院长张吉豫主持。

中国法学会副会长，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、上海市高级人民法院院长贾宇、美国乔治城大学法学院教授阿努帕姆·钱德、英国伦敦政治经济学院媒体与传播学系资深政策研究员达米安·坦比尼、京东集团副总裁胡焕刚就“中国网络法治三十年与世界网络法治前瞻”这一议题进行了交流研讨。

人工智能时代的法治挑战与数据保护

本议题由中国人民大学法学院教授、未来法治研究院副院长丁晓东主持。

美国信息产业机构(USITO)总裁缪万德、西南政法大学校长林维、波兰华沙经济学院研究员马里厄斯·克里奇托斯弗克、澳门大学法学院副教授亚历山大·斯维特里奇尼、携程集团副总裁王欣就“人工智能时代的法治挑战与数据保护”这一议题进行了交流研讨。

全球人工智能监管规则

本议题由中国人民大学法学院教授、未来法治研究院副院长丁晓东主持。

中国社会科学院法学研究所副所长周汉华、中国人民大学法学院教授张新宝、中欧数字协会首席专家欧恺安、挪威卑尔根大学教授比约纳尔·鲍维克、英国杜伦大学法学院教授威廉·鲁西就“全球人工智能监管规则”这一议题进行了交流研讨。

闭幕式

在论坛的闭幕式致辞中，黄文艺院长总结了本次论坛的四个鲜明特色：一是体现了理论与实践相结合，二是体现了产学研融合，三是体现了理论研究、人才培养和宣传教育三位一体，四是体现了高层次的国际学术对话和交流。

中国人民大学中华法治文明高等研究院院长、《中国法学》总编辑黄文艺发表总结致辞

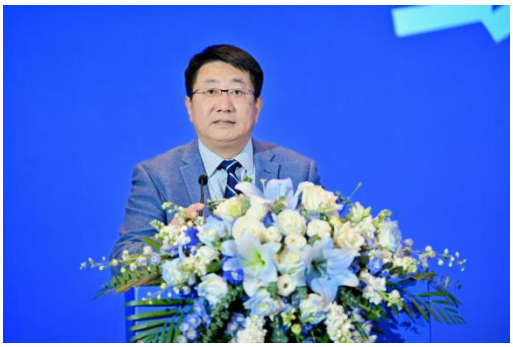
此次网络法治论坛的成功举办，为人工智能时代网络法治建设提供了宝贵的交流平台与发展思路。各界代表的积极参与和深入研讨，展现了共同应对网络法治挑战的决心。相信在各方的努力下，网络法治建设将不断完善，推动网络空间朝着更加有序、健康、创新的方向发展，为全球互联网治理注入新的活力，助力构建更加美好的网络空间命运共同体，在数字时代的浪潮中书写网络法治建设的新篇章。

2024 年世界互联网大会乌镇峰会

网络论坛圆满结束

第七届计算法学国际会议会场

在中国海洋大学法学院党委书记刘健的主持下，本次论坛的开幕式顺利进行，开启了第七届计算法学国际会议的议程。



清华大学人工智能国际治理研究院人工智能法律法规方向首席专家、

中国法学会民法学研究会常务理事、

北京市法学会物权法研究会副会长、

中国卫生法学会副会长

申卫星在开幕式致辞

第七届计算法学国际会议成功举办

2024 年 11 月 29 日至 11 月 30 日，由清华大学主办，中国法学会网络与信息法学研究会和中国计算机学会计算法学分会指导，清华大学法学院、清华大学智能法治研究院和中国海洋大学法学院承办的第七届计算法学国际会议成功召开。本次会议，共有来自全国知名高校、科研机构、律师事务所、行业顶尖企业以及来自英国、美国、奥地利、印度尼西亚、巴西和国际统一私法协会的专家共计 50 余位嘉宾出席。

本论坛的开幕式由由中国海洋大学法学院党委书记刘健主持，申卫星、周汉华、刘大川、李岩分别致辞。

本次会议设立了三个分论坛和一个圆桌讨论环节，分别是“数据产权与数据流通交易”“计算法学的全球视野”“人工智能立法：国际经验与中国立场”“数据与人工智能的产业实践”。来自英国、美国、奥地利、印度尼西亚、巴西等国家和地区的五十余位专家学者参与了各个单元的讨论。为期两天的会议为跨学科交流提供了宝贵的平台，与会嘉宾围绕数据产权、数据交易、人工智能立法和人工智能司法应用等话题，从学术和实践的双重视角进行了深入交流和热烈讨论，充分地辩明争议、凝聚共识。

清华大学人工智能国际治理研究院人工智能法律法规方向首席专家、中国法学会民法学研究会常务理事、北京市法学会物权法研究会副会长、中国卫生法学会副会长申卫星发表致辞。申卫星代表会议主办方对与会中外专家学者和各界嘉宾的到来表示热烈欢迎，对中国海洋大学在会议筹办上的鼎力支持以及全体会务人员的辛勤付出表示诚挚感谢。他回顾了计算法学国际会议的发展历程，指出会议已成为法学与信息技术交叉领域的重要学术平台。他表示，本次会议主题鲜明，设置了涵盖数据产权、人工智能国际经验与中国立场、产业界与学术界圆桌讨论等环节，体现了国际视野与本土实践的结合。他强调，在数据与计算交织的时代，

法学界需要守正创新，积极吸纳现代科学方法和技术手段，希望通过此次论坛，各方能打破学科壁垒，推动计算法学的发展。

中国社会科学院法学研究所研究员、
中国社会科学院研究生院教授、
周汉华在开幕式致辞

中国社会科学院法学研究所研究员、中国社会科学院研究生院教授、周汉华发表致辞。周汉华表示，计算法学作为多学科交叉的新兴领域，不仅关系到法学研究的前沿化，法律实践的现代化，也关系到社会治理的智能化和法治化。本次会议聚焦数据产权制度构建、数据流通与人工智能立法的核心问题，具有重要的理论价值和现实意义。他强调，习近平总书记提出的“构建数据基础制度体系”和“保障人工智能健康发展”的重要指示，为相关研究与实践提供了方向指引。计算法学的未来需要全球学者共同努力，推动科技与法治的良性互动，促进更高水平的数字正义。

青岛市工业和信息化局党组书记、局长
刘大川在开幕式致辞

青岛市工业和信息化局党组书记、局长刘大川发表致辞。刘大川书记介绍了青岛市在人工智能和数据治理领域的布局与成果。他指出，青岛市正快速发展成为人工智能产业高地，聚焦算力提升、行业大模型构建、场景应用拓展及生态建设，打造全国领先的人工智能产业链和数字治理体系。他表示，人工智能治理是全球性课题，青岛市将继续加强与科研院所及专业机构的合作，推动数据治理和人工智能产业高质量发展。

中国海洋大学校长助理李岩在开幕式致辞

中国海洋大学校长助理李岩发表致辞。李岩助理指出，本次大会契合数字中国建设的战略需求，为促进人工智能和数据治理领域的立法研究提供了重要平台。学校将以此次会议为契机，深入参与计算法学建设，培养高素质的交叉学科人才，提升在人工智能和数据治理领域的学术贡献与社会影响力。

论坛一“数据产权与数据流通交易”

论坛一上半场由中国海洋大学法学院院长李晟教授主持。

中国电子数据产业集团首席科学家、CCF 数据治理发展委员会执委国丽，中国政法大学李爱君教授，四川大学法学院王竹教授，中国人民大学法学院熊丙万教授发表了主题报告。山东大学法学院张平华教授对四位报告人的报告内容进行了深入评议。

论坛一下半场由《比较法研究》副主编丁洁琳主持。

中国政法大学的金晶副教授，印度尼西亚立诚律所的 Daruma Daishi 博士，对外经济贸易大学的许可副教授，上海交通大学的沈健州副教授发表了主题报告。青岛大学蔡颖雯教授作为与谈人，对各位嘉宾的报告进行了精彩点评。

论坛二 “计算法学的全球视野”

论坛二由金巧明律师事务所（Goldpoly Chambers）的香港执业大律师洪羽婕和清华大学法学院助理研究员靳雨露主持。

清华大学法学院申卫星教授为本场论坛致辞。牛津大学的 Philip Howard 教授，维也纳大学的 Christiane Wenderhorst 教授，美国密歇根大学的 Salom é Viljoen 副教授，香港中文大学 Eliza Mik 副教授，国际统一私法协会（UNIDROIT）的法律顾问 Theodora Kostoula，对外经济贸易大学的张欣教授，巴西热图利奥·瓦加斯基金会的 Luca Belli 教授，英国布里斯托大学的 V á clav Janeček 教授发表了主题报告。中国人民大学的熊丙万教授，中国政法大学的金晶副教授发表了与谈意见。

论坛三 “人工智能立法：国际经验与中国立场”

论坛三上半场由山东大学法学院王芳教授主持。

中国社科院法学研究所周汉华研究员，华东政法大学马长山教授，中国政法大学张凌寒教授，欧盟《人工智能法》的主要起草人加布里埃尔·马志尼（Gabriele Mazzini）博士，中国海洋大学章凯业副教授发表了主题报告，国际关系学院副院长许可教授发表了与谈意见。

论坛三下半场由《中国法律评论》副编审万颖主持。

东南大学法学院王禄生教授，中国人民大学法学院张吉豫副教授，奇安信科技集团股份有限公司首席法律顾问马兰，北京德和衡（深圳）律师事务所合伙人辛小天，深圳大学区域国别与国际传播研究院曾建知副研究员发表了演讲，北京世辉律师事务所管理合伙人王新锐发表了与谈意见。

圆桌讨论 “数据与人工智能的产业实践”

圆桌讨论由北京德和衡律师事务所副总裁陆阳律师主持。

华为技术有限公司法务部总裁**张健**，阿里巴巴集团法务总监**王莹**，蚂蚁集团法务及合规部资深专家、隐私保护研究中心主任**李海英**，百融云创科技股份有限公司总法律顾问**颜欣**，奇安信科技集团股份有限公司首席法律顾问**马兰**及山东德衡律师事务所权益合伙人**韩云龙**等专家，通过案例分析，分享企业和律所在数据管理、人工智能应用及合规运营中的经验与挑战，为学术研究提供实践反馈，为产业界提供法律与政策上的启示和建议，推动学术界与产业界的协同发展。

为期两天的会议为跨学科交流提供了宝贵的平台，与会嘉宾围绕数据产权、数据交易、人工智能立法和人工智能司法应用等话题，从学术和实践的双重视角进行了深入交流和热烈讨论，充分地辩明争议、凝聚共识。会议的圆满召开，不仅体现了计算法学这一新兴交叉领域蓬勃发展的态势，也为未来该领域的研究与实践指明了方向。在各方的共同努力下，计算法学必将迎来更加辉煌的明天，为数字中国建设的法治保障贡献智慧与力量。

第七届计算法学国际会议圆满落幕

2024（第五届）网络法治论坛——新质生产力与人工智能法治暨 2024 北京市网络法学研究会年会在京成功举办

2024 年 12 月 7 日，第五届网络法治论坛暨北京市网络法学研究会 2024 年年会、新质生产力与人工智能法治公益大讲堂在中国政法大学学院路

校区综合科研楼二楼学术报告厅隆重召开。本次论坛由北京市法学会指导、北京市网络法学研究会主办，中国政法大学互联网金融法律研究院、中国政法大学数字经济与法治研究中心、北京邮电大学互联网治理与法律研究中心共同承办。

本次论坛以“新质生产力与人工智能法治”为主题，来自高校、科研机构、公检法、政府机关、企业等专家学者和青年学子共 42 人就本次论坛主题发表真知灼见，并集中围绕“人工智能法治”、“数据法治”、“数字金融法治”三大议题深入研讨，分享前沿研究成果与创新思路，为与会者带来一场学术盛宴。

本论坛的开幕式由中国人民大学法学院副教授、未来法治研究院执行院长**张吉豫**主持，中国法学会副会长、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**，玉环市委副书记、政法委书记**应曙华**，北京师范大学刑事法律科学研究院副院长、教授、G20 反腐败追逃追赃研究中心主任、高铭暄学术馆馆长**王秀梅**和中国人民大学法学院教授**黄文艺**在开幕式中发表致辞。

北京市网络法学研究会副会长、中国矿业大学（北京）矿业法研究中心执行主任殷召良主持会议开幕式

北京市网络法学研究会副会长、中国矿业大学（北京）矿业法研究中心执行主任殷召良主持会议开幕式。殷召良副会长首先介绍了与会嘉宾并对与会嘉宾表示热烈欢迎，随后简要介绍了本次会议的主题内容。

北京市法学会联络部副主任程露茜女士致开幕辞

北京市法学会联络部副主任程露茜女士致开幕辞。程露茜副主任介绍了北京市法学会近年来落实决策部署、加强政治引领、繁荣网络法学领域相关问题研究、服务法治实践等方面的重要工作内容。

指出本次论坛的主题选择与组织研讨充分体现了研究会积极服务国家、首都高质量发展，为推动人工智能产业政策和治理体系建设，赋能新质生产力发展贡献智力支持和法治保障的勇于担当精神、积极作为态度和求真务实行动。为助力研究会建设发展提出了强化研究会政治性、先进性和自身建设三点建议，希望各位法律工作者共同努力，为繁荣法治研究、服务法治实践、建设法治中国作出应有的贡献。

李爱君教授代表全体会员作 2024 年研究会工作报告

随后北京市网络法学研究会会长李爱君教授代表全体会员作 2024 年研究会工作报告并组织会员对年度工作报告审议表决通过。

周长玲教授宣读了增补常务理事、理事共 6 人，全体会员一致表决通过。

接下来，由北京市网络法学研究会常务理事、中国政法大学周长玲教授宣读了增补常务理事、理事共 6 人，全体会员一致表决通过。

主题发言

主题发言环节由北京市网络法学研究会常务理事、中国政法大学财税金融法研究所所长、博士生导师翁武耀教授的主持。

北京市网络法学研究会副会长、中国社会科学院法学研究所研究员、博士生导师席月民，北京市网络法学研究会副会长、人类命运共同体研究院副院长、中国传媒大学王四新教授，北京市网络法学研究会副会长、北京航空航天大学法学院副院长、博士生导师周学峰教授，陕西省法学会人工智能与大数据法学研究会会长、西北工业大学张敏教授，北京市网络法学研究会副会长、北方工业大学文法学院王斐民教授，北京市网络法学研究会副会长兼秘书长、北京邮电大学互联网治理与法律研究中心主任谢永江教授进行了主题发言。

议题一“人工智能法治”

议题一由北京市网络法学研究会副会长兼秘书长、北京邮电大学互联网治理与法律研究中心主任谢永江教授主持。

北京市网络法学研究会常务理事、中央财经大学法学院副院长、博士生导师、中央财经大学数字经济与法治研究中心执行主任刘权教授，北京市网络法学研究会常务理事、中国政法大学财税金融法研究所所长、博士生导师翁武耀教授，工信部国际经济技术合作中心经贸法律研究所所长郭成龙研究员，北京市网络法学研究会常务理事、中国社会经济系统研究会新质生产力专委会杨煜东副主任，北京市网络法学研究会副会长谭俊，北京市网络法学研究会理事、北方工业大学文法学院教师尚志红发表了主题演讲。北京市网络法学研究会副会长、北京航空航天大学法学院副院长、博士生导师周学峰教授和北京市网络法学研究会常务理事、中国政法大学法治与可持续发展中心执行主任郝作成就议题及发言人的发言内容发表了与谈意见。

议题二“数字法治”

议题二由北京市网络法学研究会副会长、北方工业大学王斐民教授主持。

北京市网络法学研究会常务理事、中国政法大学法律硕士学院副院长刘智慧教授，中国人民大学法学院熊丙万教授，北京市网络法学研究会理事、中国信息通信研究院安全所副所长、正高级工程师刘越，北京市网络法学研究会理事、北方工业大学文法学院副研究员陈兰兰，北京市网络法学研究会常务理事、北京化工大学廉政研究中心常务副主任金鸿浩副教授，中国政法大学民商经济法学院民法研究所金晶副教授，北京环球律师事务所合伙人、武汉仲裁委员会仲裁员王艺，北京市网络法学研究会理事、北京市金杜律师事务所顾问方禹，发表了主题演讲。清华大学智库中心助理研究员刘云和中国科学院科技战略咨询研究院大数据战略研究中心博士后夏菲就议题及发言人的发言内容发表了与谈意见。

议题三“数字金融法治”

议题三由中国政法大学民商经济法学院周昀教授主持。

北京市网络法学研究会理事、北京金融法院审判员耿瑗，北京市网络法学研究会常务理事、中国

社会科学院法学研究所副研究员、创新工程执行研究员肖京，北京市网络法学研究会理事、北京信息科技大学梁力军副教授，北京市炜衡（重庆）律师事务所合伙人、党委委员温灏洁发表了主题演讲。北京市网络法学研究会副会长、北方工业大学王斐民教授就议题及发言人的发言内容发表了与谈意见。

学生交流

本次论坛还设置了青年学子发展论坛，来自北京大学、清华大学、中国政法大学、中国社会科学院大学、中央财经大学、北京理工大学、北京邮电大学、中国海洋大学等各大高校的博士、硕士研究生共 15 人围绕论坛主题各抒己见，分享交流研究成果。

本届论坛经过精彩的研讨与交流，最终在热烈的氛围中顺利闭幕。

北京市网络法学研究会副会长、
中国社会科学院法学研究所研究员、
博士生导师
席月民总结发言

闭幕式上，北京市网络法学研究会副会长、中国社会科学院法学研究所研究员、博士生导师席月民总结发言，指出本次年会主题非常鲜明、讨论非常深入，充分彰显了网络法学研究会的特色，研究会的吸引力、影响力和组织力正逐年增强，此次论坛不仅加强了网络与数据法学领域的学术交流与合作，也成为展示相关研究成果和人才培养的重要平台，对于推动我国网络法治建设发展具有重要意义。

数字经济沙龙——“消费者认知与人工智能治理”

2024 年 11 月 15 日，中国人民大学社会科学高等研究院（深圳）数字经济研究中心与对外经贸大学数字经济与法律创新研究中心联合举办了题为“消费者认知与人工智能治理”的数字经济沙龙。沙龙探讨了近日中央网信办、工信部等机构发布的“关于开展‘清朗·网络平台算法典型问题治理‘专项行动的通知“中关注的信息茧房、信息操纵、算法向善等问题。沙龙围绕四大核心议题展开了深入探讨：消费者认知水平对算法和 AI 大模型应用的影响、消费者认知“鸿沟”及态度分化对人工智能应用的影响、公众的期待和担忧如何影响人工智能政策与监管，以及人工智能治理如何实现“以人为本”。

中国信息通讯研究院人工智能研究中心高级业务主管**呼娜英**，腾讯研究院高级研究员**彭云**，蚂蚁集团研究院研究总监**王培成**，对外经贸大学数字经济与法律创新研究中心主任**许可**，中国人民大学经济学院副院长及数字经济研究中心研究员**李三希**，中国人民大学社会科学高等研究院（深圳）数字经济研究中心主任**程华**，中国人民大学法学院副教授、未来法治研究院执行院长**张吉豫**以及中国人民大学法学院副教授**黄尹旭**参加了研讨会。

首先，中国人民大学社会科学高等研究院（深圳）数字经济研究中心主任**程华**介绍了《算法与 AI 大模型的用户认知调研报告（2024）》的内容。报告基于 8030 份消费者问卷数据，对用户关于大模型和算法的认知、使用情况、算法与人工智能治理、自身权益保护等问题进行了分析。

中国人民大学社会科学高等研究院（深圳）数字经济研究中心主任程华

在听完整体报告介绍后，中国信息通讯研究院人工智能研究中心高级业务主管呼娜英分享了她的观点：首先，从算法到大模型，人工智能时代的到来势不可挡。消费者的认知是从下往上非常重要的一环，因此，深入理解消费者的看法具有重大意义。其次，消费者对大模型风险的担忧，这包括失业、欺诈和失控等，显示出了从自身安全到衍生安全、从最小的单元再到宏观安全性的思考。最后，过去几年政产学研普遍强调数字素养的重要性，并展开了各项推广教育工作，这显著提升了消费者对大模型的认知水平。尽管安全问题是全球关注的焦点，但社会整体对大模型的发展保持着积极乐观的态度。

中国信息通讯研究院人工智能研究中心高级业务主管呼娜英

中国人民大学法学院副教授黄尹旭表示，人工智能是一项重要的全球性议题，就目前情况来看，中国的大模型生态系统尤为丰富，技术处于相对领先的地位。从公众的角度审视人工智能显得尤为关键，因为公众的需求在很大程度上是由其认知水平决定的。对比今年发布的报告与 2022 年的报告，可以观察到，随着算法技术的不断进步和大型模型技术的兴起，公众的看法在哪些方面发生了变化。通过分析这些变化，我们或许能够揭示出一些新的制度需求和政策建议，促进人工智能的技术向善。

中国人民大学法学院副教授黄尹旭

中国人民大学经济学院副院长、数字经济研究中心主任李三希在讨论中强调了消费者认知与技术扩散之间的互动关系，认为消费者对 AI 的态度会影响其在各行业的应用和扩散，同时，AI 技术的影响与行业特性有关，正面和负面影响取决于行业对 AI 技术的依赖程度，不同行业对 AI 的感知存在差异，如翻译和设计行业的变化。李三希认为需要通过更细致的行业数据分析，了解 AI 技术的影响，探讨 AI 技术的使能性和替代性对人们态度的影响。他还强调了 AI 教育和培训的重要性，认为这是提高公众对 AI 认知的关键，并建议利用大数据和媒体分析来更准确地捕捉公众对技术的真实态度。

中国人民大学经济学院副院长、数字经济研究中心主任李三希

腾讯研究院高级研究员彭云分享了腾讯研究院关于人工智能技术社会影响的调查结果，调研显示，人工智能生成内容（AIGC）的使用率显著提升，但城乡使用率差距扩大；公众关注的焦点集中在数据安全与隐私风险；对于青年群体，数字鸿沟虽有

所缩小，但失业替代压力成为他们的主要顾虑，尤其是在校生对就业问题的关注度最高。同时，社会对 AI 的理性认知在增强，部分人开始通过学习新技能适应技术带来的变革，但学习意愿与资源分配不均的问题仍然突出。最后，她强调数字素养的提升是治理的重要因素，并提出需要对 AI 发展中的数据隐私保护和中小企业利益保障给予深度关注。

腾讯研究院高级研究员彭云

中国人民大学法学院副教授、未来法治研究院执行院长张吉豫表示，虚假信息可能是监管层更加关注的，但消费者更加关注的是隐私和个人数据安全问题，当设计相关审查程序时也应当考虑在内。

张老师认为无论是联合国方面还是本调查的统计，都体现出人们对 AI 的态度非常积极。过去大家更多从政策角度出发，这是一种发展导向的治理。但实际上，从很多人的切身体会来看，大家表现出较为积极的态度，AI 创新带来的便利、效率有很好的期待，这为如何平衡安全和发展提供了很好的佐证。另一方面，消费者对 AI 的担心也是相关领域发展的重要障碍，尤其是对个人数据安全的担心，当涉及 AI 相关产品审查程序时也需要考虑消费者的主观感受。

中国人民大学法学院副教授、

未来法治研究院执行院长张吉豫

最后，对外经贸大学数字经济与法律创新研究中心主任许可对研讨会进行了总结。许可老师认为社会治理无论是继续发展还是解决原来的问题，核心在于民众认知。因为目前不同群体的认知之间存在大量的断裂，尤其是与社会公众之间的断裂。这里面既有对消费者和用户培育数据素养的问题，也有数字监管的关切与公众认知之间存在断裂的问题。民众大量关注的是失业或者其他风险，而非虚假信息。

许可认为应当首先关心的是眼前的问题，即就业相关的问题，而虚假信息和产权保护问题虽然重要，但是它带来的影响需要更加长远地看待。第二，目前还需要做的工作是相关议题的跨国比较，在中国的语境下提出与全球治理不一样的思路。中国以发展为基础的人工智能导向非常有潜力，应当让 AI 的应用继续落地，实现为个人赋能。第三，在研究方法上，许可建议在更具代表性和典型性的平台上进行新一轮的问卷投放，以保障研究结果更加接近真实情况。

对外经贸大学数字经济与法律创新研究中心主任许可

（技术编辑：张锦涛、林诗敏）

数字法评

生成式人工智能训练语料的个人信息保护研究

原载：《中国法学》2024 年第 6 期，第 2-23 页

作者：张新宝

摘要：生成式人工智能训练语料的个人信息保护应当秉持鼓励和支持创新的基本立场。为确保服务提供者的个人信息利用需求能够得到满足，可以在训练端对《个人信息保护法》作适当宽松解释或例外规定。对于已公开的个人信息，可以通过宽松解释“公开目的”将其纳入可处理的范围。对于未公开的个人信息，仍需要以个人同意作为处理行为的合法性来源，但是可以通过宽松解释目的限制原则、调整“告知—同意”的相关规则，缓解服务提供者面临的困难。技术壁垒的提高加剧了信息主体的劣势地位，需要确保个人信息保护请求权的行使，以维护个人的合法权益，但是其行使不可避免受到技术现实的限制。服务提供者应严格履行包括技术措施在内的个人信息安全保护义务，尽可能降低给个人信息带来的风险。保护机制整体上应以行政监管为主导，如果侵害个人信息权益造成损害，应允许服务提供者以“符合行政监管要求”作为不存在过错的抗辩。

一、问题的提出

生成式人工智能的应用市场正在不断扩大，中美等科技强国纷纷布局生成式人工智能，争取在新一轮的科技革命中抢占先机。训练生成式人工智能需要海量的高质量语料作为支撑，而个人信息数据具有真实性、多样性、连贯性以及大规模等特征，恰好可以满足生成式人工智能研发对高质量训练语料的需求。然而，其合法性界限尚未得到明确。一方面，将个人信息数据用作训练语料会带来一定风险；另一方面，生成式人工智能研发需要处理尽可能多的高质量数据，因此在适用《个人信息保护法》时面临着困境，若严格地适用《个人信息保护法》，可能会加剧训练语料的短缺。

（一）语料短缺与个人信息保护之间的矛盾

我国当前面临训练语料尤其是高质量中文语料不足的困境，限制了生成式人工智能技术的发展。全球通用的 50 亿大模型数据训练集里，中文语料占比仅为 1.3%。[1] 虽然我国数据资源丰富，但是尚未得到充分挖掘，而且数据权属不清，导致数据流通不足。个人信息语料被限制使用意味着服务提供者需要在数据预处理阶段将个人信息数据剔除，这不仅会恶化我国语料短缺的局面，而且会给服务提供者造成较重的数据处理负担。从我国数字经济发展的角度考虑，应当允许将更多个人信息数据用作训练语料，以缓解当前语料不足的困境。作为重要的生产要素，数据（包括个人信息数据）对于经济社会的重要价值已经愈发显现。习近平总书记强调，发挥数据的基础资源作用和创新引擎作用，加快形成以创新为主要引领和支撑的数字经济。[2]数据的充分利用是数字经济高质量发展的重要前提，促进个人信息数据的流通和利用，对于“做大做强数字经济，增强经济发展新动能，构筑国家竞争新优势”具有重要意义。

生成式人工智能目前仍然处在早期阶段，存在安全方面的不足和个人信息泄露风险。相较于过去的人工智能技术，生成式人工智能可以输出特定内容，输出端的个人信息风险是其特殊性之所在。模型通常只有在出现过拟合等情况下才会记忆训练数据，但有研究表明，模型可能在没有过拟合的情况下无意中记忆训练数据中的个人信息。[3]有研究显示，可以通过让 ChatGPT 重复“诗歌”“公司”“发送”“制造”和“部分”等词语来喷出其记忆的部分训练数据。[4]OpenAI 表示，GPT-4 可能了解那些在公共互联网上有重要影响力的人，比如名人和公众人物，而且还可以综合多种不同的信息类型，并在特定的输出中执行多个推理步骤；可以完成多个可能与个人和地理信息相关的基本任务，例如确定与电话号码相关的地理位置或者回答教育机构位于何处，而无需浏览互联网。[5]可见，即便

泄露用户个人信息的概率非常小，但如果刻意加以引导和提示，仍可能用来生成包含个人信息内容的回答。[6]此外，不法分子可能会对生成式人工智能实施攻击以获取训练语料中的个人信息，包括成员推理攻击、模型萃取攻击、模型逆向攻击等；或者利用 API 的安全漏洞，微调模型以降其安全性，进而获取个人信息。[7]

（二）个人信息作为训练数据的制度困境

若严格适用“告知—同意”和相关的配套规则，服务提供者在获取个人信息语料时需要频繁地取得个人的同意，可能导致服务提供者无法获取必要的个人信息语料。利用未公开个人信息训练生成式人工智能的行为通常不属于《个人信息保护法》第 13 条第 1 款第 2—7 项的情形，所以服务提供者只有根据第 1 项的规定取得个人同意，处理才具备合法性。“告知—同意”规则一直发挥着平衡个人信息利用与保护的制度功能，个人有权决定其个人信息是否以及如何被处理。对于未公开的个人信息而言，除非出现必须处理的特殊情况或者为了更高位阶的利益而对其自主决定的权利进行合理限制，否则 “个人同意”都承担着规范处理者行为的阀门作用。只有在生成式人工智能研发是为了维护公共利益或者是为了维护该自然人的合法权益的情形，才可以不适用“告知—同意”规则。目前生成式人工智能主要由互联网企业进行研发，往往以营利为主要目的，并非是为了维护公共利益或者该自然人的合法权益，因此，难以将“告知—同意”之外的规定作为一般情况下的合法性依据。利用已公开的个人信息虽然不需要以个人同意作为处理的合法性基础，但是若超出合理范围以至于对个人权益有重大影响，则需要取得个人同意。然而，语料所涉及的信息主体并非都是服务提供者的用户，可能缺少取得个人同意的有效方式和渠道，适用“告知—同意”规则会给服务提供者带来难以克服的阻碍。此外，对于信息主体而言，频繁接收个人信息处理者的告知，久而久之也会不堪其扰。

生成式人工智能的发展当然不能以威胁甚至侵害个人信息权益为代价，个人信息的安全和自然人享有的个人信息权益即构成训练行为的合法性边界。近期，我国先后发布了《生成式人工智能服务管理暂行办法》（以下简称《暂行办法》）和《生成式人工智能服务安全基本要求》（以下简称《基本要求》），以回应生成式人工智能的治理需求；针对训练数据的安全问题，专门发布了《网络安全技术 生成式人工智能预训练和优化训练数据安全规范（征求意见稿）》（以下简称《安全规范》）。这些文件对生成式人工智能服务、服务提供者、训练语料等概念以及服务安全、训练数据的安全等问题进行了规定，但是对训练语料的个人信息保护问题回答得过于笼统，仅仅作了原则性的规定，不足以指导和规范实践。我国人工智能立法工作已经正式启动，[8]为此，本文将从训练语料个人信息保护的基本立场与指导思想出发展开讨论，希望通过分析，提出一个合理的个人信息保护方案，服务于我国人工智能法的制定。

二、个人信息语料获取困境的解决

（一）以“数据二十条”为指导平衡产业发展与个人信息保护

“数据二十条”的核心思想在于促进数据合规高效流通使用、赋能实体经济，充分实现数据要素价值，促进全体人民共享数字经济发展红利。鉴于生成式人工智能高度关系到国家、社会和个人的利益，应当坚持支持创新的基本立场，顺应加快构建数据基础制度、激活数据要素潜能的政策导向，尽可能在满足产业对个人信息利用需求的前提之下保护个人信息的安全，最大限度地协调生成式人工智能产业的发展和个人信息的保护。

1.支持生成式人工智能创新的基本立场

中国参与签署的《布莱切利宣言》指出：“人工智能为全球带来巨大的机会，具备改变和提高人类的福祉、和平和繁荣的潜力。”强人工智能已经成为国家间竞争的前沿阵地。[9]未来，人工智能或许会承担起科技基础设施的角色，开发“主权人工智能”有助于捍卫本国的数据主权，避免数字殖民。生成式人工智能不仅具备巨大的经济潜力，[10]还可

以带动各行各业的转型，目前已经应用于国防、金融、医疗等重要领域。国防方面，人工智能不仅可以作为实现致命性自主武器系统的关键技术大幅提高系统作战能力并扩大其对敌威慑程度，[11]而且在情报分析、决策制定、网络安全维护等方面都有用武之地。金融方面，人工智能正被应用于股票交易执行以及计算保单赔付，还推动了为投资和贷款决策寻找替代数据的趋势，催生了“所有数据都是信贷数据”的口号。[12]医疗方面，人工智能可以发挥疾病预测和治疗、药物研发等功能，如 DeepMind 公司开发的人工智能模型 AlphaFold 可以预测蛋白质结构。[13]此外，生成式人工智能在司法、教育、制造、城市建设等领域同样拥有广阔的应用空间和巨大的应用潜力。

党和国家高度重视人工智能研发的“头雁”效应，全面部署了相关工作：2017 年，国务院颁布《新一代人工智能发展规划》，指出人工智能是国际竞争的新焦点、经济发展的新引擎；2018 年 10 月 31 日，习近平总书记在中共中央政治局第九次集体学习上强调，加快发展新一代人工智能是我们赢得全球科技竞争主动权的重要战略抓手，是推动我国科技跨越发展、产业优化升级、生产力整体跃升的重要战略资源；[14] 2022 年，科技部等六部门颁布《关于加快场景创新以人工智能高水平应用促进经济高质量发展的指导意见》，着力解决人工智能重大应用和产业化问题；2024 年 3 月 5 日，《2023 年国民经济和社会发展计划执行情况与 2024 年国民经济和社会发展计划草案》提请十四届全国人大二次会议审查，提出“人工智能 +”行动，即推动人工智能技术与经济社会各领域深度融合，支撑各行业应用创新，赋能百业智能化转型升级，提高生产效率，激发创新活力，重塑产业生态，培育经济发展新动能，形成更广泛的以人工智能为创新要素的经济社会发展新形态。地方也积极响应党中央部署，全力推进人工智能的创新与应用，北京、上海、深圳等多地都制定了相关地方性法规和规章。总之，生成式人工智能研发是建设数字中国、推进中国式现代化的关键步骤，我们应从国家发展全局的视角出发来思考其治理问题，将支持和鼓励创新作为当前生成式人工智能个人信息风险治理的重要考虑因素。

2. 平衡产业发展与个人信息保护的基本思路

面对训练语料的个人信息保护问题，应当充分考虑生成式人工智能技术发展对国家、社会、个人的重要意义。个人信息保护制度的根本目的在于将风险控制在合理范围内，实现个人信息利用与安全之间的平衡。禁止或过度限制使用个人信息作为训练语料，或者让《个人信息保护法》为生成式人工智能的研发“开绿灯”，显然都不足为取。鉴于生成人工智能的重要意义，训练语料的个人信息风险治理不应成为技术发展的阻碍，虽然需要未雨绸缪，但是整体上应持有包容审慎的态度，鼓励和支持生成式人工智能的发展。作为解决生成式人工智能训练语料个人信息保护问题的基本思路，可以在训练端适当放松而相应地在其他环节收紧：原则上允许使用个人信息数据作为训练语料，并结合生成式人工智能的技术特征来解释《个人信息保护法》的规定，必要时可以作出例外规定，以实现个人信息（尤其是一般个人信息）的最大化利用，满足生成式人工智能研发对个人信息的利用需求；同时，应当确保个人信息保护请求权的行使，要求服务提供者尽到严格的个人信息安全保护义务，尽最大努力消除生成式人工智能研发给个人信息（尤其是敏感个人信息）带来的风险。如此，可以最大程度地兼顾生成式人工智能技术的发展和个人信息权益的保护，实现两者的平衡。

生成式人工智能虽然会给个人信息带来一定的安全隐患，但是风险可控可化解。限制将个人信息作为训练语料无非是出于风险预防的考虑，但是应仔细考量风险的大小以及采取预防的必要性。新型技术的出现向来都会带来一定的风险，但是牺牲创新从来也都不是化解技术风险的一个可行方案。侵害的高度可能性是风险预防的基本前提——如果风险只是存在，但发生概率及严重程度尚不清楚，那么风险就只是可能的、抽象的风险，然而风险预防需要付出的是具体的成本，如产业的发展受到一

定程度的限制，此时，风险预防的正当性就有所减弱。事实上，生成式人工智能并不像公众所担忧的那样会造成不合理的个人信息风险。虽然域外发生了一些泄露个人信息的安全事件，但我国暂且没有类似的情况发生。另外，生成式人工智能会在何种程度上输出个人信息也尚未可知。既然目前风险尚未成为现实，就没有理由过度强调预防而限制对个人信息的处理，可以等到相应的问题实际发生后再作出应对和调整。退而言之，即使生成式人工智能的研发会给个人信息带来不合理风险，但也会为国家和个人带来不可估量的福利，因此，为了更高的利益目标而对个人信息权益作一定的限制亦具有合理性。此外，技术领域同样在寻求解决方案，未来完全可能通过技术手段来化解生成式人工智能带来的个人信息风险。

(二) 基于平衡理念对个人信息保护法的调适

基于兼顾产业发展与个人信息保护的考虑，应当对《个人信息保护法》的规定作出有利于生成式人工智能发展的解释，以满足生成式人工智能训练对个人信息数据的利用需求，并在必要时作出例外规定。生成式人工智能训练语料的个人信息保护，本质上仍然是个人信息的利用与保护如何协调的问题。应当继续坚持“两头强化，三方平衡”的基本立场，[15]强化一般个人信息在生成式人工智能研发中的利用和敏感个人信息的保护。

1.已公开个人信息的处理

互联网上的公开数据是生成式人工智能的主要语料来源，[16]其中包括了已公开的个人信息数据。是否可以收集已经公开的个人信息作为训练语料，高度关系到生成式人工智能产业的发展。

(1) 理论层面的考量

数据的公开可访问性并不意味着可以被“不分青红皂白”地收集或使用，[17]个人信息已经公开也不意味着可被任意地用于生成式人工智能的训练。我国《个人信息保护法》对已公开个人信息采取了弱保护的模式，力度低于未公开的个人信息，但并不是放弃保护。根据《个人信息保护法》第 27 条的规定，可以利用已公开的个人信息用于生成式人工智能训练，但不得超过合理范围，如果对个人权益有重大影响，应当取得个人同意。事实上，“合理的范围”和“对个人权益有重大影响”的判断是同一个过程的两个侧面：如果是在合理的范围内处理，则不会对个人权益有重大影响；如果对个人权益有重大影响，则超出了合理的范围。而且第 27 条采取了比较模糊的表述，导致已公开个人信息处理的合法性判断存在较大解释空间。

一般认为，处理个人自愿公开的个人信息以推定同意为合法性基础；处理依法强制公开的个人信息以目的一致为合法性基础。

就个人自愿公开的个人信息而言，自愿公开行为可以被推定为同意（默示的同意），代表个人已经同意他人在可预期的风险之内处理个人信息——自然人既然自愿将其个人信息公开，就应当清楚其个人信息可能会被他人处理，且可能带来一定的权益侵害风险，因此无需再次取得同意。而且，虽然整体来看，当前社会公众对生成式人工智能缺乏足够的信任，接受程度尚且不高，通常不会希望自己公开的个人信息被用作训练语料，但事实上，个人权益被侵害的风险并不会因为用作训练语料而增加。通常认为，“公开”本身即为高风险的个人信息处理行为，使得个人信息处在一个无法完全受个人控制、随时可能被他人获取的状态，作为理性的自然人，应当清楚公开个人信息可能带来的风险以及后果，并且谨慎实施公开行为。换言之，自愿公开即意味着主动将其个人信息暴露在较高的风险之中。因此，只要没有给个人造成更高的风险，便可以直接处理该已公开的个人信息，以实现“个人信息权益保护与合理行为自由维护之间的协调与平衡”[18]。而生成式人工智能训练中对个人信息的学习不同于将生成式人工智能作为个人信息处理的工具，其目的不在于获取特定的信息，而在于学习其中的规律，更不会利用个人信息挖掘潜在联系。[19]机器学习过程给个人信息带来的风险主要是泄露，但已公开个人信息已经处在可以被不特定第三人接触的状态，即便发生泄露也不会给个人带来更高风险。况且，只要服务提供者能够严格尽到安

全保护义务，便可以避免信息泄露。因此，可以认为使用自愿公开的个人信息训练生成式人工智能属于合理范围之内的处理行为。

就依法强制公开的个人信息而言，强制公开行为反映了个人信息权益与公共利益之间的平衡——为了公共利益目的之实现而对个人信息权益作出合理的限制。后续的处理行为需要具备和公开目的一致的处理目的，才能延续强制公开的合法性。换言之，判断是否可将依法强制公开的个人信息用作训练语料的关键在于处理目的与公开目的是否一致。[20]如作严格解释，利用依法强制公开的个人信息作为训练语料似乎违背了公开目的，因而合法性存疑，但如果从促进产业发展的角度对处理目的作宽松解释，“用作训练语料”亦可属依法强制公开的目的范围之内。例如，司法公开的目的在于“保障人民群众知情权、参与权、表达权和监督权，促进提升司法为民、公正司法能力”，[21]如作严格解释，生成式人工智能训练的直接目的在于技术研发而非保障人民群众的知情权、参与权等，但生成式人工智能作为重要的技术工具已经运用于司法，不仅如此，最高人民法院还颁布了《关于规范和加强人工智能司法应用的意见》，以推动人工智能同司法工作深度融合。可见，虽然生成式人工智能训练本身并不直接促进司法公开，但其最终成果可以作为促进司法公开的手段，间接地对司法公开产生推动作用。按照这个思路，基础大模型几乎可以服务于任何公共目标，利用依法强制公开的个人信息用作训练语料间接地契合了个人信息公开的目的，可被归为合理范围之内的处理行为。而训练运用于特定领域的垂直大模型虽然无法按照该思路使用依法强制公开的个人信息作为训练语料，但通常只需要借助特定类型的数据微调基础大模型，借助未公开的个人信息即可满足需求。

（2）国际竞争与产业发展层面的考量

美国采取的是排除保护已公开个人信息的模式，[22]因此已公开个人信息并不会对其生成式人工智能研发造成限制。根据欧盟《通用数据保护条例》（GDPR）第 6（1）（f）条的规定，如果处理对于控制者或第三方所追求的正当利益具有必要性，则处理行为合法。欧盟《人工智能法案》第 59 条允许在人工智能监管沙盒中出于公共利益处理为其他目的合法收集的个人信息数据，以支持人工智能创新。英国信息专员办公室也认为，“合法利益”可以作为网络抓取训练生成式人工智能的合法基础，但是需要进行三项合法性测试：一是处理目的具有合法性；二是处理的必要性；三是受损害的个人利益范围不得超过开发者的合法利益。[23]可见，美国、欧盟和英国的个人信息保护制度在生成式人工智能训练语料的获取方面具有一定“优势”。站在国际竞争的角度考虑，我国应当允许将已公开个人信息用作训练语料，以避免陷入被动局面。

而从产业发展来看，如果人工智能企业面临过高的个人信息合规难度，不仅无法有效化解个人信息风险，反而可能会使制度目的落空。公开数据中的部分个人信息数据是生成式人工智能训练的客观需要，部分则是因为混杂在其他数据中而被收集。如果认为使用已公开个人信息数据训练会对个人权益造成重大影响，将导致服务提供者面临两难困境：完全剔除或取得个人的同意都难以实现。对于前者而言，虽然数据投入训练之前会经过相当复杂的数据清洗过程，包括剔除多余数据、补充缺失数据、修正、错误、数据等。但是，能否对所有的个人信息数据都作出实质性的判断，存在一定的可行性疑问，而且投入的成本也是不得不考虑的因素。对于后者而言，已公开个人信息具有非接触性特征，服务提供者难以与个人取得联系。在既难以取得信息主体的同意又难以将其中的个人信息完全剔除的情形下，服务提供者可能会不得已选择以违法的方式处理已公开个人信息。作为缓和，可以宽松解释《个人信息保护法》第 27 条的规定，相应地要求服务提供者严格地履行个人信息安全保护义务，尽可能降低给个人信息造成的风险。

2. 未公开个人信息的处理

（1）已收集的信息：宽松适用目的限制原则

判断可否将已收集的未公开个人信息用作训练语料，关键看其是否超出了初始的处理目的。《个

人信息保护法》第 6 条规定了目的限制原则，要求信息处理者在收集个人信息时应有明确、合理的目的，且在后续的处理过程中不偏离此目的。根据《个人信息保护法》第 14 条第 2 款，如果用于生成式人工智能训练超出了初始的处理目的，服务提供者只有重新取得个人同意才能处理该个人信息。但时间因素对于科技竞争至关重要，虽然数据在以极快的速度产生，[24]但数据的积累毕竟需要一个过程，短时间内可能会对技术研发产生较大影响。我国本身就面临严峻的语料不足问题，若已经收集的个人信息数据无法得到充分利用，可能会进一步加剧我国在生成式人工智能发展上的劣势。因此，可以在今后收集个人信息时告知个人用于生成式人工智能训练的目的并取得同意。

鉴于产业发展的客观需求，可以认为将已经收集的未公开个人信息用于生成式人工智能训练没有超出初始的处理目的，无需重新取得个人同意。数字技术发展迅速，个人信息的利用需求愈加广泛，处理者收集个人信息时无法完全预见未来是否可能出现新的处理目的。在进行语料训练时，处理者可能已经不再具备信息收集时的条件，难以重新获得信息主体的同意，否则需要付出不成比例的努力。[25]甚至，处理者已经和个人失去了直接联系，事实上不具有重新取得同意的可行性。如果要求后续的使用严格符合初始目的，难免会制约个人信息的利用。因此，“不宜片面强调信息处理对于初始目的的严格遵循，而应要求信息处理者将信息处理可能引发的风险控制在合理范围之内，以符合大数据时代信息多元利用的趋势”[26]。可供参照的是，GDPR 采取了一种“窄进宽出”的模式，[27]虽然要求处理目的应具体、明确、合法，但是根据第 6（4）条，并不完全禁止初始目的之外的处理，不过需要考虑初始目的与进一步处理目的之间的关联性、进一步处理可能造成的结果等因素。《个人信息保护法》虽然没有作出类似的规定，但笔者认为，应当综合考虑处理的性质、风险等因素来判定是否超出了初始目的。

事实上，训练人工智能的过程本质上是“学习数据”，而非“分析数据”或“记忆数据”，一般情况下不会直接反映出数据中的内容，将已经收集的个人信息数据用作训练语料并不会给个人带来更高的风险。利用个人信息进行数据分析对个人信息的利用具有直接性，通常是通过挖掘数据中的内容得出结论（如通过用户的浏览数据分析其偏好），其过程是将分布在海量数据中的零散信息集中起来，通过统计分析等方法挖掘其中的有效信息。而生成式人工智能训练完全不同，其对个人信息的使用具有明显的间接性。“学习”是深度学习技术的核心与本质所在，“训练”实际上是一个让机器发现和学习规律的过程。生成式人工智能的功能和水平由庞大规模的参数决定，代表了其“知识储备”。未经训练之前，各个参数都处在未知状态，通过海量数据的训练，参数的值（映射规则）得以确定下来，生成式人工智能便获得了回答人类提问的能力。可见，生成式人工智能的输出过程并不是对训练数据的重新组合或者直接调取，而是通过复杂的映射规则来处理用户的提问，然后将得到的内容反馈给用户。除非出现过拟合等特殊情况，或者受到外部攻击，否则不会直接记忆并输出个人信息。

此外，正如上文所述，生成式人工智能具有重要的科技战略价值，关系到国防、经济、医疗、教育等诸多关键领域的发展。尤其是，基础大模型未来可能会承担起科技基础设施的角色，为此，可以允许服务提供者直接使用已经收集的未公开个人信息作为训练语料，不用取得个人同意。虽然过去在医疗、金融等领域也会涉及个人信息的处理，但是其目的往往在于提供和优化某种特定服务。生成式人工智能的意义远不局限于此，作为一种技术工具，其对于社会的影响具有革命性。GDPR 第 5（1）（b）条规定，因为公共利益、科学或历史研究或统计目的而进一步处理数据，不视为违反初始目的。而且 GDPR 序言第 159 条指出：“以科学研究为目的的个人数据处理应以广泛的方式解释，包括例如技术开发和示范、基础研究、应用研究和私人资助的研究。”这些相关内容可以为我国目的

限制原则的理解提供借鉴。当然，目前生成式人工智能的研发主要由互联网企业开展，将其解释为纯粹的科学研究难免有些牵强，但生成式人工智能训练具有较高的科学研究属性不可否认，可以作为宽松适用目的限制原则的依据。

(2) 未收集的信息：集中取得个人同意

鉴于生成式人工智能研发的特殊性，应当在适用“告知—同意”及相关规则的时候作出符合技术特征的调整。随着生成式人工智能的发展和普及，个人信息处理者完全能够意识到自己收集的个人信息可能会用于生成式人工智能研发，因此属于可以预见的处理目的和处理方式，可以在收集个人信息时一并告知可能会用于生成式人工智能训练并取得同意，便于日后将收集的个人信息用作训练语料。

难点在于，根据《个人信息保护法》第 23 条的规定，个人信息处理者向第三方提供其处理的个人信息时，需要取得个人的单独同意，并向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类等信息。不同于过去的个人信息处理场景，生成式人工智能训练需要借助各种途径获得高质量的训练数据，商业数据即是一种重要来源，这意味着个人信息数据会在不同的主体之间流通，而且可以预见，随着数据权属问题得到明确，个人信息数据的流通将会变得更加频繁。如果每次将个人信息提供给第三方都需要作出告知并取得个人的单独同意，无疑会极大地影响数据的使用效率，甚至可能会阻碍行业的创新，不符合当前鼓励人工智能发展的政策导向。[28]笔者认为，考虑到训练语料的流通需求，可以允许个人信息处理者集中地取得向不同人工智能企业提供个人信息的同意，缓和“告知—同意”规则给生成式人工智能研发造成的限制，以促进训练语料的流转。如此一来，个人信息处理者无需在向第三方流转个人信息时频繁地征求个人的单独同意，只需集中地告知个人并取得概括的同意之后，便可以直接将收集的个人信息流转给不同的人工智能企业；服务提供者与其他个人信息处理者通过交易获取个人信息语料时也无需取得个人同意。由此，语料获取的难度得到极大的降低，从而满足生成式人工智能研发对个人信息的利用需求。集中告知应涵盖处理的目的、方式，且表明可能向第三方提供并应作出例外规定，如果第三方的姓名、联系方式、保存期限等信息尚不能确定，可以暂时不予告知，但是应充分告知可能对个人产生的影响以及相关权利的行使方式和程序等内容。这种集中取得同意的方式只是针对性地在告知的内容和方式上作出了调整，并不会对个人造成明显的不利影响，个人仍然可以自主决定其个人信息是否可被用作训练语料、是否可被提供给第三人。不可否认，集中告知增加了后续处理的不确定性，由于没有充分告知情况，可能会增加个人信息被不当处理的风险，但这些风险完全可通过强化个人信息安全保护义务、规范服务提供者的处理行为来化解。

除非有充分的必要性，应当避免将敏感个人信息数据用作训练语料，尤其是用于基础大模型的训练。但在确实需要使用敏感个人信息训练生成式人工智能时，同样可采取上述集中取得个人同意的方式。《基本要求》规定：“使用包含敏感个人信息的语料前，应取得对应个人单独同意或者符合法律、行政法规规定的其他情形。”《安全规范》也作出了类似的规定。鉴于敏感个人信息高度关系到人格尊严、人身和财产安全，确有必要对敏感个人信息的处理作出必要的限制。《个人信息保护法》第 28 条第 2 款规定：“只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。”问题的关键在于，用于生成式人工智能的训练是否属于“具有特定的目的和充分的必要性”。笔者认为，对此应区分不同模型进行判断。对于基础大模型而言，没必要用包含敏感个人信息的数据来训练，因为这对提升其功能水平的作用有限（自然人的生物识别、特定身份、医疗健康等信息可能并不会对特定功能的取得产生实质作用），但是会增加泄露风险，难谓具备充分的必要性。虽然基础大模型需要学习海量的数据来提高泛化能力，但是个人信息数据在训练

数据中的比重相对较小，敏感个人信息数据更是如此，因此敏感个人信息在其中的作用可能微乎其微。而敏感个人信息作为高度关系到自然人的人格尊严、人身和财产安全的个人信息类型，风险系数相对较高，因此保护优先于利用。当然，无需完全禁止将敏感个人信息用作训练语料，只是如果使用敏感个人信息训练基础大模型，服务提供者应对必要性（例如，可以显著提高基础大模型的水平）进行详细说明，并且应当评估相关风险，同时做好充分的安全保护措施。而对垂直领域的人工智能模型的训练而言，因为需要应用于特殊和敏感的行业或领域（包括医疗、金融、人脸识别等），则更需要敏感个人信息作为训练语料，可以认为具有充分的必要性。但不管是哪种大模型训练，未成年人的个人信息都应重点予以限制。

(3) 不宜普遍认定为合理使用

处理个人信息符合个人信息合理使用情形的，无需取得个人同意。问题在于，是否需要将获取未公开个人信息语料纳入合理使用的适用范围？纳入显然更有利于服务提供者获得充足的训练语料、提高我国生成式人工智能研发的竞争优势。但笔者认为，不宜普遍地将使用未公开个人信息数据作为训练语料的行为认定为合理使用，原因主要在于：首先，通过宽松解释目的限制原则和调整“告知—同意”的相关规则基本已经可以解决未公开个人信息语料的获取难题。即使普遍引入合理使用，由于个人信息往往是在使用网络产品和接受网络服务的过程中产生，服务提供者仍然需要从其他个人信息处理者处取得未公开个人信息语料。如果可以宽松解释《个人信息保护法》中的相关规定或者作出有针对性的例外规定，使得个人信息处理者将其收集的个人信息流转用作训练语料时不用再取得个人同意，其实最终的效果与引入合理使用无异，因此需要斟酌引入合理使用制度的必要性。其次，虽然集中取得个人同意会给服务提供者带来一定的成本，但是这对于服务提供者而言是应当支出的合理成本。通过适当的宽松解释和调整，服务提供者已经可以直接使用已公开的个人信息作为训练语料，获取未公开的个人信息也只需要与特定的个人信息处理者进行磋商和交易，并不会给其造成难以克服的困难。再次，部分情况下个人信息数据并非必要的训练语料。通常而言，个人信息包含的内容较短，模型不易从中学习到语言的一般规律。相较于使用较高风险的个人信息数据，服务提供者可能有更好的选择。对于非必要的个人信息数据，如果允许服务提供者受到合理使用制度的庇护，只会徒增个人信息风险。最后，对于敏感个人信息而言，更不宜通过合理使用进行使用。除非有充分的必要性，应当限制将敏感个人信息作为训练语料。如果允许其受到合理使用的庇护而无需取得个人的单独同意，带给个人的损害可能会远大于服务提供者节省的成本，难以认为具有合理性。

虽然通过合理使用制度解决作品语料获取的困境得到了比较广泛的认可，[29]但是个人信息语料与作品语料存在如下差异：第一，个人信息的产生和收集往往存在一个“中心点”——网络平台等个人信息处理者，个人信息较为集中地处在个人信息处理者的控制之下，尤其是大型的个人信息处理者掌握了海量主体的个人信息；而作品语料极其分散，虽然我国成立了文字作品等集体管理组织，但是大量作品仍在集体管理组织的管理之外。第二，使用作品语料主要涉及的是权利人的著作财产权，而使用个人信息语料关系到权利人的人格权益，因此考虑个人信息的语料获取问题，应更加重视权利人的保护。第三，作品是生成式人工智能学习的关键内容，对于提高学习效果有重要作用；而个人信息数据在许多情况下不具有必要性，因为我们“希望模型能了解世界，而非个人”[30]。第四，服务提供者基于“告知—同意”规则获取个人信息不需要向个人支付费用，但是基于授权许可获取作品需要向著作权人支付报酬，后者可能会给服务提供者带来超过收益的成本，但是前者并不会带来过高的经济负担。综合以上原因，对作品语料和个人信息语料的获取不能作简单的等同处理，对于后者，应当重视对“告知—同意”及相关规则的调适，而慎重考虑普遍地认定为合理使用。

笔者认为，可以在总结实践经验的基础之上，尝试将确实存在使用需求又难以通过集中取得个人同意来获取充足语料的情形认定为合理使用，但是应确保个人的合法权益不会受到严重损害。未经个人同意处理个人信息的“合理性”来源无非两种：其一，为了维护公共利益而对个人的合法权益进行一定程度的限制；其二，为了实现权利主体的优先利益而对劣后的利益进行限制——这正是《民法典》第 1036 条第 3 项所规定的两种情形。若是为了维护公共利益而处理个人信息，应当确保对个人的影响轻微。如果在维护公共利益的同时严重损害了个人的合法权益，同样不宜认为是合理使用。虽然生成式人工智能研发高度关系到国家、社会、个人的利益，但是很多情况下难以认为研发活动纯粹是为了维护公共利益或维护信息主体的合法权益。不过，部分情况下仍然存在《民法典》第 1036 条第 3 项的适用空间，例如训练征信等需要涵盖全国人民相关个人信息的生成式人工智能模型。此时，一方面，服务提供者难以通过集中取得个人同意来满足对个人信息的处理需求；另一方面，训练此种模型具有突出的公共利益属性，同时也是为了维护信息主体的合法权益，因此存在适用合理使用的正当性和必要性。

三、个人信息权益的实现与保障

（一）个人信息保护请求权的行使

语料获取的适当放宽会给个人信息造成一定的风险，需要在研发的其他环节及使用阶段尽可能降低风险，以实现个人信息利用与安全的平衡。生成式人工智能技术壁垒的提高加剧了个人的劣势地位，而个人信息保护请求权的行使可以推动权益保护的实现。《暂行办法》第 11 条第 2 款规定：“提供者应当依法及时受理和处理个人关于查阅、复制、更正、补充、删除其个人信息等的请求。”服务提供者应当依法处理个人的权利请求并尽可能予以满足，但是个人信息保护请求权的实现不可避免地受到技术现实的限制。囿于篇幅，下文仅通过对查阅复制权、删除请求权和解释说明权的分析来说明个人如何向服务提供者行使权利，以及技术特征可能对权利行使产生的影响。

1.个人查阅、复制权的行使

查阅、复制权是为了满足作为实体权益的知情权而设置的个人信息保护请求权。[31]根据《个人信息保护法》第 45 条第 2 款，权利人可以随时向个人信息处理者请求提供其个人信息。法律不应对其行使设置要件，个人只需证明自己是信息主体，而无需证明存在其他正当利益。[32]但是，如何向服务提供者行使查阅、复制权，需要结合数据存储和查阅的技术能力和行使成本等因素进行分析，并且受到上述因素的合理限制。

首先，需考虑服务提供者是否有能力满足查阅和复制请求。受技术水平限制，服务提供者可能无法准确地从数据库中查阅到特定的个人信息。模型训练对数据规模的要求极高，如 GPT-4 的训练需要大概 4 万亿至 8 万亿个单词。[33]要在如此大规模的数据集中精准、高效地查阅到特定信息，无疑对数据存储和查阅技术提出了挑战。随着数据库技术的发展，目前已有很多数据库可以满足生成式人工智能训练对非结构化数据的存储、查阅等需求，如 NoSQL 数据库、时序数据库、向量数据库等。服务提供者收到查阅、复制的请求后，可从数据库中调取个人信息数据，满足个人的权利请求。例如，向量数据库在人工智能研发中发挥着不可替代的作用，通常需要通过“词嵌入”（embedding）把文本、图片、视频等训练数据转化为机器更容易理解的数学向量，以提高数据的存储和检索能力，并更好地解决训练数据更新的问题。如果采用向量数据库，在个人提出查阅、复制的请求之后，服务提供者可从数据库中查询向量，然后通过逆向映射得到个人信息。

其次，需考虑查阅、复制的范围和成本的问题。虽然数据库技术可以帮助服务提供者实现在海量数据中的查阅，但若允许个人不受限制地行使查阅、复制权，难免会给服务提供者带来不合理的负担。虽然行使查阅、复制权可能会给处理者带来一定的成本，但为了保障权利的顺利行使，《个人信息保

护法》并没有收取费用的规定。当然，行使个人信息保护请求权的成本不应完全由个人承担，否则无疑违背了权利设置的初衷。但是，任由个人行使查阅、复制权，忽略可能给服务提供者带来的负面影响，同样也不可取。笔者认为，查阅、复制权的行使应以服务提供者的客观技术能力和合理成本为限，若个人的查阅、复制请求超出了技术可行范围，则应当受到限制；若个人的请求超出了合理限度，服务提供者也可拒绝或收取相应费用。可行的解决方案是，服务提供者应免费满足个人合理频次（如一年一次或两次）的查阅、复制请求；如果超出合理频次则可要求个人说明正当理由，否则可以按成本收取费用；如果存在反复请求甚至恶意请求的情况，由于其违背了诚实信用原则，服务提供者可以拒绝请求或者收取更高费用。

2.个人解释说明请求权的行使

生成式人工智能至今仍然是一个“黑箱”，令人难以理解其运行机制和工作原理。可解释性难题使得信息主体不可避免地对生成式人工智能产生不信任，担心可能会输出其个人信息。《个人信息保护法》第 48 条规定了解释说明请求权，依此，如果权利人提出请求，服务提供者应充分告知利用其个人信息的有关情况，这在一定程度上可以帮助个人了解生成式人工智能训练对个人信息的处理机制，缓解对模型安全性的担忧。然而，解释说明请求权的实现同样不得不受到技术现状的制约。生成式人工智能借助了深度神经网络技术，具有极其复杂的结构。基础大模型的参数已经达到千亿级别，它们共同决定生成式人工智能的功能，导致输入到输出之间的逻辑不够清晰，难以清楚地观察和解释模型为何会输出特定回答。要求人工智能模型实现算法透明在客观上相当困难，且强制透明化可能会阻碍神经网络技术的应用。[34]因此，服务提供者可能难以解释个人信息如何被学习和对模型产生影响，导致解释说明权无法得到完全行使。

“通常情况下，开发者没有义务对外披露人工智能的研发过程，包括研发中使用的训练数据。这不仅是开发者保有其技术秘密的正当性使然，而且是科学技术研究自由的内在要求。”[35]但是，服务提供者应尽可能帮助个人理解生成式人工智能学习个人信息数据的整个过程。首先，应公开训练语料中个人信息数据的来源等信息。其次，个人提出算法解释要求时，服务提供者应当以清晰易懂的语言向个人解释生成式人工智能训练的基本原理，包括学习数据的过程、是否可能输出其个人信息等，换言之，算法解释的方式应当符合信息主体的知识水平。需要注意的是，算法解释的目的是解释输出结果的逻辑和机制，而非算法本身。即使算法完全透明化，用户或公众也未必能理解。[36]目前，技术领域正致力于提高生成式人工智能的可解释性，如可视化技术、可解释性模型、对抗性样本等。麻省理工学院科学家的研究简报《人工智能和工作的未来》指出，人工智能模型可以通过一些实践变得更加透明，例如构建更可解释的模型、开发可用于探索不同模型如何工作的算法等。[37]随着生成式人工智能可解释性水平的提高，服务提供者应当提供更为详细的解释，以充分满足个人的权利请求。

3.个人删除请求权的行使

如果信息主体明确拒绝利用其已公开个人信息训练人工智能，或者撤回对未公开个人信息的同意，根据《个人信息保护法》第 47 条第 1 款的规定，个人可以行使删除请求权。然而，个人信息数据可能已经通过训练过程对参数的确定发挥了作用，个人行使删除请求权之后，服务提供者是否需要对模型重新训练，以达到让模型“遗忘”该个人信息数据的效果，恢复到没有学习该个人信息数据的状态？如果这样可能破坏数据库或者模型的功能，是否还应当满足信息主体的请求？

删除请求权的行使在生成式人工智能场景下有一定的特殊性，彻底删除特定个人信息数据不仅可能存在技术上的障碍，而且可能对数据库或者模型功能产生破坏性影响。即便服务提供者尽可能采用行业内认可的先进数据库，但客观上仍然可能出现无法删除的技术障碍。大型数据库中往往具有大量内置机制和故障安全措施，如自动备份、恢复到以前版本等避免数据丢失和损坏的措施。实践中，

数据经常存储在多个地方，可能很难识别和删除所有的“副本”；而且删除一个文件时，即便清空了保存该文件的空间，也仍然没有真正地将其从数据库中删除，只有当它被一个新的文件覆盖时，数据才真正消失。[38]此外，通过识别数据所存储的所有空间并及时用新的信息覆盖来实现彻底的删除，还可能会严重危害数据库的一致性、稳定性，甚至会破坏系统安全性，以致损毁数据库。[39]而且，缺少部分训练数据还可能会影响其功能的正常实现。[40]如此一来，权利人要求服务提供者删除其个人信息，就可能要以破坏数据库或者模型的功能作为代价。因此，如果受到客观技术能力的限制，服务提供者可以不予删除，但是应当停止除存储和采取必要的安全保护措施之外的处理。

更复杂之处还在于，经过机器学习过程，被请求的个人信息数据可能已经对模型参数的确定产生了影响，训练数据集改变之后，可能需要重新训练，参数才能改变。如果想要实现彻底删除的效果，需要实施机器反学习，模型才能达到彻底“遗忘”该数据的状态。实现机器反学习的方法包括彻底的机器反学习和不彻底的机器反学习，前者是指通过重新训练模型消除特定数据对模型的影响，后者是指借助重新训练之外的方法实现机器反学习，如直接修改部分参数。直接修改参数虽然便捷，但是较为粗略，所以效果有限，可能无法实现彻底删除。而且，生成式人工智能模型中存在明显的“核心区域”，某个关键参数发生变化就可能会对模型的整体功能产生“致命”影响。[41]因此，如果想要确保将模型恢复到没有学习该个人信息的状态，唯一理想的解决办法就是重新训练。但是以重新训练作为实现删除请求的方式并不可取，原因显而易见——这需要耗费大量的时间和经济成本。虽然借助 SISA （Sharded, Isolated, Sliced, and Aggregated training）等方法可以较为高效地实现重新训练，但是也存在降低模型准确率等缺点。[42]

综上，删除请求权的行使应当受到一定的限制：首先，受到技术发展现状的限制。由于物理上彻底删除难以实现，只要个人信息数据达到无法被利用并且安全的状态，即可认为实现了删除。如果技术上无法删除或者实现删除将带来不合理的成本，服务提供者可以《个人信息保护法》第 47 条第 2 款作为抗辩。不过，“所谓技术上难以实现，应当从客观标准进行理解，即结合当前的技术条件是否可删除进行判断，否则将导致信息处理者寻找各种理由和借口不予删除，实质上架空删除权的实效性”[43]。服务提供者应当提供详细的说明，避免以技术不可行为借口推脱责任。其次，受到服务提供者利益的限制。若生成式人工智能已经得到充分的学习，缺少特定数据不会对其产生实质的影响，个人可以请求删除；但若缺失对应数据会对数据库或者模型产生实质影响，破坏其完整性，甚至影响其功能的实现，则应当对权利的行使进行限制。此时，服务提供者同样可以《个人信息保护法》第 47 条第 2 款作为抗辩，或者证明此时删除请求权的行使不符合诚实信用原则的要求，属于权利的滥用。再次，受到生成式人工智能原理的限制。个人无权要求服务提供者重新训练模型，只能请求将其个人信息从数据库中删除，并在下次重新训练时使用不包含该个人信息数据的语料。如果服务提供者可以判断被请求的个人信息对哪些参数产生了影响，并且修改参数的成本在合理范围之内，则应在不损坏模型功能的前提下通过修改参数实现机器反学习。最后，删除请求权的行使如果超过了合理频次且没有正当理由，服务提供者可以拒绝或者收取相应的费用。

（二）个人信息安全保护义务与侵权责任

作为在语料获取问题上作宽松处理的“对价”，服务提供者应尽到严格的个人信息安全保护义务，以最大程度地降低个人信息风险。具体而言，服务提供者应当采取与信息敏感性相称的措施，保护在生成人工智能的整个生命周期中收集或使用的任何个人信息，并且持续关注可能出现的威胁，[44] 例如，采取关键词过滤等措施避免模型输出个人信息，采用隐私计算等技术防止未经授权的访问以及个人信息的泄露、篡改、丢失等。此外，服务提供者需要进行详细的个人信息保护评估，确保其训练行

为符合《个人信息保护法》等规定，以及提供的产品和服务具备较高的安全性。

1.隐私计算、过滤等措施

生成式人工智能训练给个人信息带来的风险很大程度上是因为技术发展不充分，对此，技术领域积极探索了相应的解决方案，因此服务提供者可以采用多种技术手段来降低个人信息风险，具体包括：

（1）隐私计算技术

隐私计算技术（又称“隐私增强技术”）可减轻生成式人工智能研发带来的个人信息和隐私风险，实现保护隐私的机器学习，如多方安全计算、同态加密、差分隐私，[45]以及分布式、去中心化的机器学习模型训练方案——群体学习（Swarm Learning）。[46]

隐私计算技术可以通过避免数据传输、建立安全计算环境，以及使数据处于加密状态等方式确保个人信息的安全。《人工智能白皮书（2022 年）》指出：“AI 结合隐私计算技术，可从数据源端确保原始数据真实可信。利用隐私计算技术，数据‘可用不可见’，形成物理分散的多元数据的逻辑集中视图，可以保证 AI 模型有充足的、可信的数据可供利用。”近年来，隐私计算等技术已经得到快速发展：多方安全计算、联邦学习、可信执行环境等技术不断迭代优化，单点层面技术能力得到上限提升，技术间的内部融合趋势得到增强，通过优势互补突破应用瓶颈，差分隐私、区块链等技术被应用于辅助隐私计算，实现了外部的融合，数据保护能力也进一步增强。[47]目前，隐私计算技术目前已在金融、医疗等行业的生成式人工智能训练中得到应用，极大地降低了个人信息泄露风险。服务提供者应当在模型训练过程中充分结合隐私计算技术，并尽可能采用最有效的技术方案。

（2）过滤及其他措施

服务提供者应采用关键词过滤等技术对侵害个人信息权益的内容进行屏蔽。一方面，要过滤用户的输入，避免用户引导模型生成侵害他人个人信息权益的内容；另一方面，要过滤模型的输出，避免模型在过拟合等情形下意外输出用户的未公开个人信息甚至是敏感个人信息。服务提供者可以在用户协议中对使用规范和相应的后果进行说明。如果用户企图利用模型获取他人的个人信息，服务提供者应当及时提醒、纠正，对达到严重程度者应禁止其使用。[48]《基本要求》指出，应采取关键词、分类模型等方式对使用者输入信息进行检测，使用者连续三次或一天内累计五次输入违法不良信息或明显诱导生成违法不良信息的，应依法依约采取暂停提供服务等处置措施。此外，服务提供者还可通过微调模型来拒绝用户对个人信息的请求，[49]借助多种途径规范用户的使用行为。

服务提供者还应积极采用其他可以降低个人信息风险的措施，包括使用合成数据、抵御外部攻击等。使用合成数据可在实现预期模型功能的前提下有效降低个人信息风险，例如，合成数据组成的真实医疗记录集不包含任何个人信息，但仍对医学研究有应用价值。[50]如果使用合成数据可以达到相同或近似的效果，则应使用合成数据替代个人信息数据。实践中，模型可能会受到的攻击包括成员推理攻击、模型逆向攻击、模型提取攻击等，服务提供者应采取有效的抵御措施，提高数据库和模型的安全水平，防止个人信息因受到外部攻击而泄露。以成员推理攻击[51]为例，虽然研究表明，即使采取了联邦学习等隐私计算技术仍可能遭受成员推理攻击，[52]但目前技术领域已提出借助差分隐私、知识蒸馏等方式来抵御模型推理攻击，[53]服务提供者有义务采取一种或多种上述措施。此外，《安全规范》还提出了采取身份鉴别、访问控制等技术措施对训练数据进行安全保护。

2.个人信息保护评估

个人信息保护评估不仅包括事前的影响评估，还包括后续的合规审计。个人信息保护评估对于个人信息权益的保护具有重要意义。原因在于，生成式人工智能训练的技术门槛比过去的个人信息处理场景更高，难以从外部准确地评判其风险，因此需要服务提供者从内部开展评估。评估的重点在于将个人信息用作训练语料的必要性，以及模型在避

免个人信息泄露方面的安全性。对于评估结果，应当形成书面的评估报告，便于相关部门进行指导与监督。

（1）必要性评估

必要性评估是指服务提供者应评估其利用某种类型个人信息训练生成式人工智能是否具有必要性，确保将个人信息语料的数量控制在实现模型功能所需的最小范围之内。超过必要范围处理个人信息的行为违反了必要原则和最小化原则的要求，可能会给个人带来不合理的风险。根据《个人信息保护法》第 6 条第 2 款的规定，个人信息收集应当限于实现处理目的的最小范围。虽然生成式人工智能研发需要海量的训练数据，但仍应受到最小化原则的限制，在确保模型功能的前提之下尽可能减少个人信息的处理。不过，应当灵活解释最小化原则，以避免对生成式人工智能训练造成限制。[54]个人信息语料的数量越多，生成式人工智能泄露个人信息的可能性也就越高。任由服务提供者利用个人信息进行训练而不受必要原则的限制，显然不可取。而且，并非所有的个人信息数据都是实现模型功能所必要（例如，并非所有财务信息和人口特征都有助于预测信用风险），[55]如果将非必要的个人信息数据用作训练语料，只会徒增个人信息风险而不会产生任何效益。因此，服务提供者需要判断个人信息处理与其欲达到的目的之间是否具有相关性，明确其使用的个人信息数据是否必要、是否存在过度收集的情况。服务提供者应在构建模型或者算法的时候就考虑选择使用对个人信息数据依赖性更小的方式，并在开展训练之前判断某种类型的个人信息数据是否会对模型功能的实现发挥实质作用。如果对模型功能的贡献甚微，应当尽量避免将其作为训练语料。

（2）安全性评估

安全性评估是指服务提供者应评估其模型是否可以较大程度地避免输出侵害个人信息权益的内容，以及是否可以有效抵御外部的攻击。绝对的安全固然无法实现，但是服务提供者仍应在评估风险的基础之上判断是否采取了充分的安全保护措施，并及时作出相应的调整和优化。

安全性评估应当覆盖生成式人工智能从训练到投入使用的全过程。一方面，生成式人工智能的技术特征可能导致其会输出个人信息；另一方面，生成式人工智能可能不可避免地成为网络攻击者的目标，导致安全漏洞的出现。[56]《基本要求》对人工智能生成内容的安全评估作出了规定：服务提供者应当分别采取人工抽检、关键词抽检、分类模型抽检的方式，借助测试题库对生成内容的合格率进行评估。但是，从《基本要求》中生成内容测试题库涵盖的三十余种安全风险来看，似乎无法通过生成内容测试题库评估出侵害个人信息内容的输出概率。笔者认为，应当针对生成内容的个人信息合规概率进行专门的评估，并且设置较高的合格标准。若合格率不达标，就应及时采取措施对生成内容进行更深度的过滤。另外，《基本要求》对问题拒答评估也作出了规定，但是并没有要求应拒答测试题库必须涵盖侵害他人个人信息权益的风险。对于诱导输出他人未公开个人信息尤其是敏感信息、私密信息的问题，模型应当拒绝回答，服务提供者应当评估模型是否可以准确识别相关问题并作出正确的应对。此外，服务提供者还须评估模型抵御外部攻击的能力，及时检测和修补安全漏洞，持续关注可能遭受的攻击并且采取有效的预防措施。根据《基本要求》的规定，服务提供者应当将训练环境与推理环境隔离，避免数据泄露和不当访问；持续监测模型的输入内容，防范恶意输入攻击；定期对所使用的开发框架、代码等进行安全审计，关注开源框架安全及漏洞相关问题，识别和修复潜在的安全漏洞。通过对模型安全性的评估，及时发现和应对可能存在的个人信息风险。

此外，服务提供者还需要尽到《个人信息保护法》以及《基本要求》《安全规范》等文件规定的其他个人信息安全保护义务，包括制定并组织实施个人信息安全事件应急预案、实行训练数据的分类分级管理、建立完整的个人信息处理活动记录等。

3.服务提供者的过错推定责任与行政合规抗辩

严格的监管措施可能会对产业的发展造成制约，但是不可以忽略生成式人工智能的责任问题，否则可能会导致产业的无序发展，甚至使人工智能成为像空壳公司一样的转移责任的工具。[57]处理未公开个人信息需要基于个人的明确同意，因此社会公众对生成式人工智能的信任显得至关重要。而在生成式人工智能造成损害的情况下，获得赔偿的可能性不仅决定了社会公众的信任和接受程度，还决定了购买或使用生成式人工智能产品和服务的可能性。[58]所以，明确服务提供者侵害个人信息权益的民事责任，可以提高公众对生成式人工智能技术的信任，进而使其获得更充足的个人信息语料。

作为专门的保护性法律，《个人信息保护法》对个人信息处理者的行为标准和应尽义务作了全面的规定，其中第 69 条规定了个人信息处理者的过错推定责任，但可能会给服务提供者带来较重的负担。根据第 69 条的规定，如果“处理个人信息侵害个人信息权益造成损害”，可以推定处理行为违反了《个人信息保护法》的规定（行为具有违法性），进而可以推定处理者主观上存在过错。质言之，个人信息处理者没有履行保护性法律规定的作为义务，就表明处理者没有达到应有的注意程度，至少存在过失；反之，如果没有违反《个人信息保护法》的规定，处理者便不存在过错。基于该认识，个人信息处理者的过错体现在三个方面：一是没有按照《个人信息保护法》的要求处理个人信息；二是没有依法处理行使个人信息保护请求权的请求；三是没有尽到个人信息安全保护义务。个人信息处理者可以通过证明处理行为符合《个人信息保护法》的规定来证明无过错。然而，生成式人工智能训练相较于其他个人信息处理过程更加复杂，服务提供者难以进行清晰的“复盘”，以证明处理过程完全符合《个人信息保护法》的要求。例如，必要性原则要求服务提供者在确保实现目标模型功能的前提下尽可能减少个人信息的处理，但是，要求服务提供者回溯到训练之前，证明某种类型的个人信息是在必要范围之内，可能会相当困难。如此一来，过错推定责任可能会事实上发展为无过错责任。即使处理过程完全符合《个人信息保护法》的规定，大模型仍可能会在特殊情况下输出侵害个人信息权益的内容。可见，推定过错的合理性存疑。

笔者认为，生成式人工智能发展初期的个人信息保护机制应当以行政监管为主导，并且重指导轻处罚，以促进生成式人工智能的健康稳定发展。可以允许服务提供者以“符合行政监管要求”作为不存在过错的抗辩，原因主要有以下几点：首先，可以缓解过错推定责任给服务提供者带来的证明负担，避免因过重的责任阻碍技术创新；其次，行政监管可以为服务提供者提供一个可预期的合法合规标准，利于个人信息保护合规工作的开展；最后，服务提供者无需在多个诉讼中重复证明其处理行为符合《个人信息保护法》的规定，利于加快纠纷解决，节省诉讼资源。总之，行政合规抗辩应是考虑到现有技术水平所作出的合理制度安排。[59]目前生成式人工智能的发展程度有限，相较于以往的个人信息处理法律关系，需要重新平衡个人与服务提供者之间的利益。相关部门应详细指导并监督服务提供者开展个人信息合法合规工作。相关合法合规工作主要包括三个方面：一是训练语料的处理符合《个人信息保护法》等规定，包括处理的范围符合最小化原则的要求等；二是依法满足个人的查阅、复制、删除、解释说明等请求；三是采取充分的个人信息安全保护义务，包括进行关键词过滤、采取有效措施应对可能存在的风险等。

值得注意的是，欧盟委员会于 2022 年通过了修订《产品责任指令》的提案，拟通过产品责任来解决人工智能的责任问题。但笔者认为，生成式人工智能输出侵害个人信息的内容是技术发展不充分的结果，除非是安全性明显低于一般技术水平的情况，否则不能一概将其视为“缺陷”所致并对其适用产品责任。而且，生成式人工智能主要提供一般性的信息服务，不会像自动驾驶汽车等因为固有缺陷而威胁他人的生命、健康、财产等权益，因此不应适用产品责任。[60]即使是从保护受害人的角度

考虑，产品责任也不一定是更有利的选择。表面上看，适用产品责任无需考虑服务提供者的过错，似乎更容易成立侵权。但适用产品责任也增加了受害人的举证负担——受害人需要证明生成式人工智能产品存在缺陷，而人工智能的高技术壁垒会使其面临举证上的困难。[61]作为配套制度，就只能在缺陷的证明责任上进行缓和，[62]但其效果与适用过错推定责任相差不大。

综上，应根据《个人信息保护法》第 69 条而非产品责任的有关规定追究服务提供者的个人信息侵权责任，并且允许以“符合行政监管要求”作为不存在过错的抗辩。这样不仅可以在一定程度上避免服务提供者因难以证明无过错而承担过重的责任，阻碍产业的健康发展，而且可有效缓解受害人面临的举证困难，给予受害人较为充分的保护。

四、结　语

生成式人工智能技术迎来了爆发式发展，已经对国家、社会和个人产生了广泛的影响，然而技术的复杂性导致其治理面临诸多挑战，其中之一便是训练语料的个人信息保护问题。本文从基本立场和指导思想出发，分析了如何在生成式人工智能场景下适用和调整《个人信息保护法》的有关规定，以兼顾个人信息的利用和保护。一方面，应当以平衡原则为指引宽松解释《个人信息保护法》，并在必要时作出例外规定，缓解服务提供者在获取个人信息语料时面临的困难；另一方面，应当确保个人信息保护请求权的行使、要求服务提供者尽到严格的个人信息安全保护义务，充分保障个人信息权益。总之，我国在制定人工智能法的时候，应当结合生成式人工智能的技术特征和产业需求作出相应的规定，构建符合生成式人工智能客观发展规律的个人信息保护制度。

参考文献

[1] 参见罗云鹏：《大模型发展亟需高质量“教材”相伴》，载《科技日报》2024 年 1 月 15 日，第 6 版。

[2] 参见《习近平在中共中央政治局第二次集体学习时强调 审时度势精心谋划超前布局力争主动 实施国家大数据战略 加快建设数字中国》，载《人民日报》2017 年 12 月 10 日，第 1 版。

[3] See Nicholas Carlini, Evaluating and Testing Unintended Memorization in Neural Networks, at https://bair.berkeley.edu/blog/2019/08/13/memorization/ (Last visited on April 9, 2024).

[4] See Jai Vijayan, Simple Hacking Technique Can Extract ChatGPT Training Data, at https://www.darkreading.com/cyber-risk/researchers-simple-technique-extract-chatgpt-training-data (Last visited on April 9, 2024).

[5] See OpenAI, GPT-4 Technical Report, at https://arxiv.org/pdf/2303.08774.pdf (Last visited on April 9, 2024).

[6] 参见孙祁：《规范生成式人工智能产品提供者的法律问题研究》，载《政治与法律》2023 年第 7 期，第 165 页。

[7] See Kellin Pelrine et al., We Found Exploits in GPT-4’s Fine-tuning & Assistants APIs, at https://far.ai/post/2023-12-exploiting-gpt4-api/ (Last visited on April 9, 2024)

[8] 《国务院 2023 年度立法工作计划》和《国务院 2024 年度立法工作计划》均将“人工智能法草案”列入预备提请全国人大常委会审议项目。参见《国务院办公厅关于印发〈国务院 2023 年度立法工作计划〉的通知》（国办发〔2023〕18 号）；《国务院办公厅关于印发〈国务院 2024 年度立法工作计划〉的通知》（国办发〔2024〕23 号）。

[9] See Matthew R. Gaske, Regulation Priorities for Artificial Intelligence Foundation Models, Vanderbilt Journal of Entertainment and Technology Law, Vol.26:1, p.7-8 (2023).

[10] 麦肯锡指出，生成式人工智能的跨行业应用预计每年可提供 2.6 万亿美元至 4.4 万亿美元的经济效益。 See Michael Chui et al., The Economic Potential of Generative AI: The Next Productivity

Frontier, at https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/the%20economic%20potential%20of%20generative%20ai%20the%20next%20productivity%20frontier/the-economic-potential-of-generative-ai-the-next-productivityfrontier.pdf (Last visited on April 9, 2024).

[11] 参见齐亚双等：《人工智能国防战略的目标、愿景与实施路径：国际经验与启示》，载《情报杂志》2024 年第 3 期，第 55 页。

[12] See Ross P Buckley et al., Regulating Artificial Intelligence in Finance: Putting the Human in the Loop, Sydney Law Review, Vol.43:43, p.48 (2021).

[13] See John Jumper et al., Highly Accurate Protein Structure Prediction with AlphaFold, Nature, Vol.596:583 (2021).

[14] 参见《习近平在中共中央政治局第九次集体学习时强调 加强领导做好规划明确任务夯实基础 推动我国新一代人工智能健康发展》，载《人民日报》2018 年 11 月 1 日，第 1 版。

[15] 参见张新宝：《从隐私到个人信息：利益再衡量的理论与制度安排》，载《中国法学》2015 年第 3 期，第 49-52 页；张新宝：《论作为新型财产权的数据财产权》，载《中国社会科学》2023 年第 4 期，第 156-159 页。

[16] 例如，通过借助 Common Crawl 等开放的网络爬虫数据库，ChatGPT 等大语言模型可以收集并使用互联网上任何没有被特别保护的内容进行训练。See Benjamin Fabre, Generative AI Is Scraping Your Data. So, Now What?, at https://www.darkreading.com/vulnerabilities-threats/generative-ai-is-scraping-your-data-so-now-what (Last visited on April 9, 2024).

[17] See Office of the Privacy Commisioner of Canada, Principles for Responsible, Trustworthy and Privacy-protective Generative AI Technologies, at https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/ (Last visited on April 9, 2024).

[18] 程啸：《论公开的个人信息处理的法律规制》，载《中国法学》2022 年第 3 期，第 92 页。

[19] See Karl Manheim & Lyric Kaplan, Artificial Intelligence: Risks to Privacy and Democracy, The Yale Journal of Law & Technology, Vol.21:106, p.120-121 (2019).

[20] 参见张新宝、昌雨莎：《已公开裁判文书中个人信息的保护与合理利用》，载《华东政法大学学报》2022 年第 3 期，第 14-16 页；前注 [18]，程啸文，第 98-101 页。

[21] 参见《最高人民法院关于进一步深化司法公开的意见》（法发〔2018〕20 号）。

[22] 参见丁晓东：《公开个人信息法律保护的中国方案》，载《法学》2024 年第 3 期，第 5-6 页。

[23] See Information Commissioner's Office, Generative AI First Call for Evidence: The Lawful Basis for Web Scraping to Train Generative AI Models, at https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/generative-ai-firstcall-for-evidence/ (Last visited on April 9, 2024).

[24] IDC 最新发布的 Global DataSphere 2024 报告显示，中国的数据量预计将从 2023 年的 30.96ZB 激增至 2028 年的 97.06ZB，5 年复合增长率 CAGR 高达 25.7%。参见《合规场景双引擎驱动——2023 年中国数据库审计市场份额报告发布》，载微信公众号"IDC 咨询"，2024 年 7 月 19 日上传。

[25] See János Mészáros & Chih-Hsing Ho, Big Data and Scientific Research: The Secondary Use of Personal Data under the Research Exemption in the GDPR, Hungarian Journal of Legal Studies, Vol.59:403, p.404 (2018).

[26] 朱荣荣：《个人信息保护"目的限制原则"的反思与重构——以〈个人信息保护法〉第 6 条为中心》，载《财经法学》2022 年第 1 期，第 30 页。

[27] 参见梁泽宇：《个人信息保护中目的限制原则

的解释与适用》, 载《比较法研究》2018 年第 5 期, 第 20-24 页。

[28] 参见毕文轩:《生成式人工智能的风险规制困境及其化解:以 ChatGPT 的规制为视角》, 载《比较法研究》 2023 年第 3 期, 第 164 页。

[29] 参见林秀芹:《人工智能时代著作权合理使用制度的重塑》, 载《法学研究》 2021 年第 6 期;焦和平:《人工智能创作中数据获取与利用的著作权风险及化解路径》, 载《当代法学》 2022 年第 4 期。

[30] Open AI, Our Approach to AI Safety, at https://openai.com/blog/our-approach-to-ai-safety (Last visited on April 9, 2024).

[31] 参见张新宝:《论个人信息保护请求权的行使》, 载《政法论坛》 2023 年第 2 期, 第 27-28 页。

[32] 参见程啸、王苑:《论我国个人信息保护法中的查阅复制权》, 载《法律适用》2021 年第 12 期, 第 25 页。

[33] 参见前注 [1], 罗云鹏文。

[34] 参见商建刚:《生成式人工智能风险治理元规则研究》, 载《东方法学》 2023 年第 3 期, 第 14 页。

[35] 刘文杰:《何以透明, 以何透明: 人工智能法透明度规则之构建》, 载《比较法研究》 2024 年第 2 期, 第 126 页。

[36] 参见周尚君、罗有成:《数字正义论: 理论内涵与实践机制》, 载《社会科学》 2022 年第 6 期, 第 168 页。

[37] See Tsedal Neeley, 8 Questions about Using AI Responsibly, Answered, at https://hbr.org/2023/05/8-questions-about-using-airesponsibly-answered (Last visited on April 9, 2024).

[38] See Tiago Sérgio Cabral, Forgetful Al: Al and the Right to Erasure under the GDPR, European Data Protection Law Review, Vol.6:378, p.383-384 (2020).

[39] 参见翟凯:《论人工智能领域被遗忘权的保护:困局与破壁》, 载《法学论坛》 2021 年第 5 期, 第 145 页。

[40] See Tiago Sérgio Cabral, supra note 38, 388.

[41] 参见张奇:《只修改一个关键参数, 就会毁了整个百亿参数大模型? 》, 载微信公众号“CSDN”, 2024 年 2 月 18 日上传。

[42] See Bjørn Aslak Juliussen, Jon Petter Rui & Dag Johansen, Algorithms that Forget: Machine Unlearning and the Right to Erasure, Computer Law & Security Review, Vol.51:1, p.8-9 (2023).

[43] 王利明:《论个人信息删除权》, 载《东方法学》2022 年第 1 期, 第 44-45 页。

[44] See Office of the Privacy Commisioner of Canada, supra note 17.

[45] See Barnabás SZÉKELY, Mitigating the Privacy Risks of AI through Privacy-Enhancing Technologies, Acta Universitatis Sapientiae: Legal Studies, Vol.11:35, p.48-57 (2022).

[46] See Stefanie Warnat-Herresthal et al., Swarm Learning for Decentralized and Confidential Clinical Machine Learning, Nature, Vol.594:265 (2021).

[47] 参见隐私计算联盟:《隐私计算白皮书(2022 年)》(2022 年 12 月发布), 第 5-13 页。

[48] OpenAI 已经采取拒绝回答类似请求、监控用户行为等方式来降低个人信息风险。 See OpenAI, supra note 5.

[49] See OpenAI, supra note 30.

[50] See Adam J. Andreotta, Nin Kirkham & Marco Rizzi, AI, Big Data, and the Future of Consent, AI & Society Vol.37:1715, p.1719 (2022).

[51] 机器学习中的成员推理攻击(Membership Inference Attacks)通过推测一个数据样本是否被用来训练目标机器学习模型来获取个人信息或者隐私。参见牛俊等:《机器学习中成员推理攻击和防御研究综述》, 载《信息安全学报》2022 年第 6 期, 第 4 页。

[52] 参见张佳乐等:《基于 GAN 的联邦学习成员推理攻击与防御方法》, 载《通信学报》 2023 年第 5 期, 第 195-198 页。

[53] 参见前注 [51], 牛俊等文, 第 15-18 页。

[54] 参见斜晓东：《风险与控制：论生成式人工智能应用的个人信息保护》，载《政法论丛》2023 年第 4 期，第 64-65 页。

[55] See Information Commissioner’s Office, How Should We Assess Security and Data Minimisation in AI?, at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-should-weassess-security-and-data-minimisation-in-ai/#whatdataminimisation (Last visited on April 9, 2024).

[56] See Elizabeth Montalbano, Generative AI Projects Pose Major Cybersecurity Risk to Enterprises, at https://www.darkreading.com/vulnerabilities-threats/generative-ai-projects-cybersecurity-risks-enterprises (Last visited on April 9, 2024).

[57] See Frank Pasquale, Data-informed Duties in AI Development, Columbia Law Review, Vol.119:1917, p.1918 (2019).

[58] See Teresa Rodríguez de las Heras Ballell, The Revision of the Product Liability Directive: A Key Piece in the Artificial Intelligence Liability Puzzle, ERA Forum, Vol.24:247, p.248-249 (2023).

[59] 参见王若冰：《论生成式人工智能侵权中服务提供者过错的认定——以“现有技术水平”为标准》，载《比较法研究》2023 年第 5 期，第 20-25 页。

[60] 参见王利明：《生成式人工智能侵权的法律应对》，载《中国应用法学》2023 年第 5 期，第 33 页。

[61] 参见周学峰：《生成式人工智能侵权责任探析》，载《比较法研究》2023 年第 4 期，第 122-124 页。

[62] 参见杨立新：《人工智能产品责任的功能及规则调整》，载《数字法治》2023 年第 4 期，第 38 页。

侵害企业数据权益的民事责任

原载：《中国法学》2024 年第 6 期，第 127-147 页

作者：王叶刚

摘要：企业数据的来源、内容以及取得方式等具有复杂性，对行为人侵害企业数据权益民事责任的认定以及责任承担方式等有着重要影响。行为人侵害企业合法取得的数据时，企业有权依法请求行为人承担违约责任、侵权责任或者基于绝对权请求权产生的民事责任。企业对其非法取得的数据不享有数据权益，但行为人破坏企业对数据的持有状态的，企业也有权请求行为人承担停止侵害、排除妨碍、赔偿损失等责任。行为人侵害企业数据的，个人数据来源者虽不享有数据权益，但可以其个人信息权益受侵害为由请求行为人承担侵权责任或者基于人格权请求权请求行为人承担停止侵害、排除妨碍等民事责任。行为人侵害非个人数据来源者的著作权、商业秘密等在先权利的，受害人有权依据在先权利的保护规则请求行为人承担民事责任。非个人数据来源者对企业所享有的数据查阅权、可携带权等属于相对权，原则上不受侵权法保护；但在行为人恶意侵权时，受害人也应有权请求行为人承担侵权责任。

一、问题的提出

企业数据是企业取得并维持其竞争优势的重要条件。甚至可以说，谁掌握了数据，谁就获得了市场先机。[1]这大抵也是侵害企业数据权益[2]行为频频发生的重要原因。例如，在近年来常见的侵害数据权益诉讼案件中，行为人通常是为了获得竞争优势或出于“搭便车”的心态，利用网络爬虫等技术手段爬取其他企业的数据。[3]从受害企业数据来源上看，行为人侵害的既可能是企业在日常生产、经营过程中附带生成的数据，[4]也可能是企业从其他主体处取得的数据[5]。从受害企业取得数据的方式上看，行为人侵害的可能是企业合法取得的数据，[6]也可能是其非法取得的数据[7]。而从受害企业所持数据的信息内容上看，行为人侵害的可能是有关

自然人信息的数据（简称“个人数据”），[8]也可能是与非自然人主体的信息有关的数据（简称“非个人数据”）[9]。

在当前纠纷的处理中，人民法院总体上倾向于在竞争法的框架下来评判当事人的利益诉求，即先强调数据是一种重要的企业经营资源，承认企业对数据享有竞争性利益，再评价行为人获取企业数据的行为是否构成不正当竞争，然后依据竞争法规则确定行为人的法律责任。在我国现行立法尚未完成对数据予以确权的背景下，通过此种方式解决纠纷的确可以回避数据权益权利属性认定这一难题。但此种做法的问题也比较明显：一方面，此种做法仅能解决行为人构成不正当竞争情形下企业数据权益的救济问题。但在许多情形下，行为人与受害企业之间并没有竞争关系，[10]即便存在竞争关系，行为人侵害企业数据权益的行为也可能不构成对受害企业的市场替代，并不当然构成不正当竞争。[11]如此一来，受害企业在这些情形下的损害救济就会被概括性排除。另一方面，竞争法规则旨在解决经营者之间因竞争关系产生的权益纠纷问题，难以为数据来源者的权益救济提供规则基础。事实上，企业数据之上同时承载着企业数据权益与数据来源者的权益，[12]且两者密切关联，要准确认定行为人侵害企业数据权益的民事责任，就需要厘清企业与数据来源者对企业数据所享有权利的边界与范围，并在此基础上明确行为人对数据来源者的民事责任。例如，在行为人侵害企业数据权益构成不正当竞争的情形下，依据《反不正当竞争法》第 17 条第 3 款规定，如果企业的损失难以确定，则其有权主张按照行为人的侵权获利赔偿。此时，如果承认数据来源者也对企业数据享有数据权益，则数据来源者也应有权主张分享行为人的侵权获利。

目前学理上关于是否应当通过产权路径保护企业数据，存在不同的观点。持反对观点的学者主张，不宜对数据进行确权，否则会造成“反公地悲剧”，影响数据要素的流通和利用。[13]另有观点主张，数据的财产权属性取决于其所包含的信息内容而非其本身，数据必须依赖于一定的载体，否则其本身无法单独发挥作用，数据本身也不具备独立的经济价值，因此不能成为民事权利的客体，其保护问题应当由代码规则等技术手段予以解决。[14]笔者认为，依赖载体的特点并不足以成为否定企业数据为民事权利客体的理由。因为随着社会的发展，各种无形财产的价值日益凸显，并逐渐成为民事权利客体，是否具有有形性、是否依赖于一定的载体并非成为民事权利客体的必要条件。同时，承认企业数据为民事权利客体，既是培育数据要素市场、完善数据产权制度的基本要求，也是保障数据处理者依法获得收益、实现数据要素供给激励的重要途径。更多的学者对企业数据的产权保护路径持肯定立场，但就企业数据的产权保护而言，既有文献侧重关注企业数据的产权保护路径[15]、企业数据产权保护的样态[16]、企业数据权益的内容[17]、企业数据的流通与交易规则[18]等问题，而对侵害企业数据权益的民事责任问题着墨不多。即便新近的文献注意到了这方面的问题（如有的学者从宏观上探讨了通过公法规则配合侵权法规则保护企业数据权益的必要性，[19]或者从微观上探讨侵害企业数据权益的损害赔偿责任这一具体问题[20]），也还是缺乏对侵害企业数据权益民事责任的系统研究。诸如行为人侵害企业自产数据与侵害企业从其他主体处取得的数据时，其民事责任的认定与承担有何区别；是否需要区分企业取得数据方式的合法与非法，分别认定行为人的民事责任；行为人侵害企业数据中的个人数据与非个人数据对其民事责任的认定又有何种影响等许多问题，都是企业数据权益保护所面临的重大理论和实践难题，亟需展开深入研究。

我国现阶段数据立法及相关数据保护政策主要聚焦于数据确权与数据流通问题，也没有过多关注企业数据权益遭受侵害后的民事责任认定问题。《民法典》第 127 条虽然对数据权益保护作出了宣示性规定，[21]但尚未提供关于数据权益保护的具体规则，难以为企业数据权益的保护提供有效的实定法依据。对于直接受害企业以外的其他受害主体，虽然《民法典》和《个人信息保护法》对个人信息的保护规则已作较为系统的规定，但其调整对象限

于个人数据，难以为非个人数据来源者等主体提供权益保护依据。即便就个人数据而言，《民法典》和《个人信息保护法》也难以解决相关的企业数据权益纠纷。例如，在包含个人数据的企业数据遭受侵害时，个人虽然可以其个人信息权益受侵害为由要求行为人承担民事责任，但其能否对企业数据主张数据权益，并以数据权益受侵害为由请求行为人承担民事责任？再如，如果企业受侵害的数据是其通过非法处理个人信息而取得的，其能否以数据权益受侵害为由请求行为人承担民事责任？针对上述问题，《民法典》与《个人信息保护法》难以提供明确的法律依据。《数据安全法》虽然也规定了数据保护规则，但该法的核心立法目的在于保障数据安全，而非在于数据确权以及调整侵害数据权益的民事责任。虽然该法第 32、51 条规定了数据的收集应当采用合法、正当的方式，不得窃取或以其他非法方式获取数据，但就行为人侵害他人数据权益应当承担何种民事责任，该法并未作出明确规定。《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”)也对数据保护问题作出了规定，但其旨在确立数据产权保护的基本框架、促进数据流通，相关数据确权规定仍不够具体，也难以为侵害企业数据权益民事责任的认定提供具体指引。

鉴于企业数据来源与内容的复杂性，本文拟从企业数据来源、数据内容以及企业取得数据的方式三个层面对企业数据的类型进行区分，并在此基础上分别探讨行为人对受害企业以及数据来源者的民事责任，以求为我国相应数据立法规则的设计提供理论参考，并为法官在审判实践中裁判企业数据侵权纠纷案件提供理论指引。

二、企业数据的基本类型区分

关于企业数据的类型区分，我国现行立法并未作出明确规定。“数据二十条”第 2 条将数据区分为公共数据、企业数据与个人数据，但此种分类之下的三类数据之间可能存在一定的交叉关系，欠缺周延性。尤其是，“个人数据”是从数据所包含的信息内容层面来构建的概念，对应的概念应当是非个人数据；而“企业数据”强调的是企业生产或者享有的数据，旨在表明此类数据的产生主体和归属；“公共数据”强调的是相关数据资源的公共性，当然，公共数据中的特定类型如政务类数据应由国家享有，也强调了此类数据的归属问题。[22]二者与“个人数据”并非同一层次的概念。事实上，无论是企业数据，还是公共数据，都可能包含个人数据，即以个人信息为内容的数据。清晰明确的“企业数据”概念界定是认定侵害企业数据权益的民事责任的基础，而此种对数据类型的不周延区分显然难以帮助精准界定企业数据。考虑到企业数据的复杂性，更好的办法是从实际出发，依据具体的标准对企业数据进行更为周延和精准的区分。

从实践来看，企业数据的构成较为复杂，其来源具有多样性，内容具有复杂性，企业取得数据的方式也有合法与非法之分，因而有必要从数据来源、数据内容以及企业取得数据的方式三个层面区分企业数据，从而更为准确地认定行为人的民事责任。首先，从数据来源层面区分企业数据，有助于厘清行为人侵害的权益类型。与企业自产数据不同，在企业从其他主体处取得数据时，可能出现数据的双重或者多重持有状态，[23]即两个或者两个以上的数据处理者均持有相关的数据，并享有数据权益[24]。此时，行为人侵害企业数据不仅会侵害受害企业的数据权益，还可能侵害其他主体的数据权益。其次，从数据内容层面区分企业数据，有助于明确不同数据来源者请求行为人承担民事责任的依据。个人数据来源者有权依据个人信息保护的规则主张民事责任；而对非个人数据来源者而言，由于其并不享有个人信息权益，因而只能以在先权利等受侵害为由提出请求。最后，从企业取得数据的方式层面区分企业数据，则有利于对受害企业的权益提供不同强度的保护。对企业合法取得数据，应当通过数据产权保护规则对企业提供保护；而在企业非法取得数据的情形下，其不应当享有数据权益，只能通过类似于占有保护的规则对其持有数据的状态予以保护。

（一）企业自产数据与企业从其他主体处取得的数据

从数据来源上看，企业既可通过采集自身生产、经营过程中附带生成的数据或者用户数据等方式取得数据，也可通过合同等方式从其他主体处取得数据。依此，可以按照来源不同，将企业数据区分为企业自产数据与企业从其他主体处取得的数据。

企业自产数据由企业在自身生产、经营过程中通过数据采集行为所取得。企业数据采集是企业从数据源处收集、识别和选取数据的过程。[25]企业采集数据的方式多种多样，既可以借助相关的自动化工具进行数据的自动化采集（如通过网络爬虫等自动化技术采集），[26]也可以通过人工录入等方式进行手动数据采集。企业取得自产数据主要有如下三种途径：一是企业采集自身生产、经营过程中附带生成的数据。企业在生产、经营过程中可能附带产生大量的数据，这些数据只有被采集才能产生相应的利用价值。企业在生产、经营过程中产生的数据之价值经常取决于可以从中提取的知识而非数据本身，而此种价值的产生离不开数据采集行为。[27]因此，企业通过实施数据采集行为，对自身生产、经营过程中附带生成的数据进行识别和选取，本身也是对数据进行“赋值”的过程。对于由此取得的数据，企业应当享有产权内容较为完整的数据权益，[28]即企业应当享有数据持有权、数据使用权与数据经营权[29]。二是企业采集用户的个人数据。依据《民法典》第 1035 条与《个人信息保护法》第 13 条规定，在取得个人同意或符合其他法定条件时，个人信息处理者可以依法处理用户的个人信息，企业据此在处理用户个人信息过程中所采集的用户个人数据也属于企业自产数据。例如，在取得用户同意后，企业在其运营过程中采集的用户姓名、IP 地址、网络浏览记录等用户个人数据即属于此类企业自产数据。[30]三是企业采集非自然人主体的数据。例如，平台经营者经与平台内的商户约定而采集取得的该商户的相关营销数据，即为企业从非自然人主体处取得的自产数据。在我国司法实践中，有的法院也承认企业从非自然人主体处取得数据行为的合法性。[31]在后两种情形下，企业取得数据权益的原因并不在于个人同意或者相关数据中财产价值的让渡，因为无论是企业采集用户的个人数据还是非自然人主体的数据，当事人之间既没有转让相关数据中财产价值的意愿，也没有转让该财产价值的合意，企业取得数据权益源于其依法处理数据的行为，此种情形与财产权的原始取得类似。

除自产数据外，企业还可能从其他主体处取得数据。企业通常是通过合同的方式从其他主体处取得数据。当事人之间流转数据的合同类型具有多样性，既可能是数据转让合同，也可能是数据许可使用合同或者其他类型的合同。例如，实践中，企业可以将包括后端数据在内的企业数据整合成一系列计算机易识别的应用编程接口开放出去，供第三方开发者使用。[32]第三方开发者在访问相关的企业数据时，通常需要向企业支付一定费用（可一次性支付相关的数据访问费用，也可在每次访问企业数据时单独支付访问费用）。[33]当然，为了规范第三方从开放平台调取数据的行为，同时也为了保护个人信息和企业数据安全，企业通常会与第三方签订开放平台开发者服务协议，约定包括第三方在开放平台内调取数据的权限以及用途等内容。[34]除合同方式外，企业还可能通过取得授权或者爬取等方式从其他主体处取得数据。前者如企业通过取得有关机关授权的方式取得相关的公共数据。例如，全国企业信用查询系统“企查查”平台通过取得授权的方式，取得了相关的裁判文书司法数据。后者如企业通过数据爬取等方式，在未经其他主体同意的情形下，取得相关的数据。与企业自产数据不同，企业从其他主体处所取得的数据通常是其他主体已经实施了一定数据处理行为而形成的具有一定价值的数据集合。

将企业数据区分为企业自产数据与企业从其他主体处取得的数据，对于认定行为人侵害企业数据权益的民事责任具有重要意义。行为人侵害企业自产数据与侵害企业从其他主体处取得的数据，其所侵害的权益存在一定的区别，这也会影响行为人所需承担民事责任的类型与责任范围。就企业自产

数据而言，仅企业享有数据权益，数据来源者并不享有数据权益，用户个人与其他非自然人数据来源者虽然也可能依法享有数据查阅权、可携带权等权利，[35]但其属于数据来源者对数据处理者所享有的权利，本身并非数据产权意义上的数据权益。因此，在行为人侵害企业自产数据的情形下，仅需考虑受害企业的数据权益与数据来源者在先权利的保护问题，而无须考虑数据来源者数据权益的救济问题。而在企业从其他主体处取得数据的情形下，可能出现数据的多重持有现象，多个主体均可能对相关数据享有数据权益。在此情形下，行为人的行为可能同时侵害多个主体的数据权益，并因此需要对多个主体承担侵害数据权益的民事责任。例如，在甲公司许可乙公司复制并使用其数据开放平台的数据之情形中即存在数据的双重持有，如果丙擅自从乙公司处窃取相关的数据，则该行为不仅侵害了乙公司的数据权益，也可能构成对甲公司数据权益的侵害。当然，与企业自产数据类似，行为人侵害企业从其他主体处取得的数据时，也存在数据来源者在先权利的保护问题，行为人侵害企业数据权益同时侵害数据来源者在先权利的，数据来源者也有权就其在先权利的损害请求行为人承担停止侵害、赔偿损失等民事责任。

（二）个人数据与非个人数据

从企业数据的内容上看，其可能是有关自然人个人信息的数据，即个人数据；也可能是与非自然人主体信息有关的数据，即非个人数据。

无论是企业自产数据，还是企业从其他主体处取得的数据，都可能包含个人数据与非个人数据。就企业自产数据而言，例如，企业在取得用户同意的情形下处理用户的个人信息，并据此所取得的个人数据，即属于企业自产数据中的个人数据；而企业通过采集自身在生产、经营过程中产生的营销数据、存货数据等，即属于数据企业自产数据中的非个人数据。就企业从其他主体处取得的数据而言，例如，在企业通过数据共享的方式从供电企业、供水企业处取得数据的情形下，企业作为接受数据共享的一方所取得的数据既可能是个人数据，也可能是非个人数据。前者如特定用电用户的用电数据和用水数据；后者如区域用电数据、区域用水数据等。

需要指出的是，无论是企业自产数据中的个人数据，还是企业从其他主体处取得的个人数据，其本质上都属于个人数据，企业在处理此类数据时，都应当满足依法处理个人信息的要求。[36]而企业数据中的非个人数据则存在较大的区别，如就企业自身在生产、经营过程中附带生成的非个人数据而言，其数据权益主体通常限于企业自身，一般不涉及其他主体；而就企业从其他主体处取得的数据而言，其可能存在数据的多重持有现象，在遭受侵害时就可能涉及多个主体的数据权益保护问题。因此，当行为人侵害企业数据中的个人数据或非个人数据时，其民事责任的认定与承担会有所不同，具体体现在行为人对数据来源者的责任方面。在责任认定方面，当行为人侵害个人数据时，个人数据来源者可依据《个人信息保护法》第 69 条请求行为人承担损害赔偿责任，此时适用过错推定原则；个人数据来源者也可基于人格权请求权请求行为人承担民事责任，此时，行为人民事责任的成立既不需要过错，也不需要受害人遭受一定的损害，而且个人的请求权不受诉讼时效的限制。而当行为人侵害非个人数据时，除有特别规定外，非个人数据来源者请求行为人承担侵权损害赔偿责任应适用《民法典》第 1165 条第 1 款，原则上适用过错责任原则。在责任承担方面，在个人数据遭受侵害时，由于个人信息涉及人格利益，个人数据来源者有权基于人格权请求权请求行为人承担停止侵害、排除妨碍、消除危险等民事责任；如果行为人侵害个人数据造成个人数据来源者财产损害或严重精神损害的，受害人有权依法请求行为人承担财产损害赔偿和精神损害赔偿。[37]而行为人侵害非个人数据通常是侵害非个人数据来源者的特定在先权利，此时需要依据该在先权利的保护规则认定行为人的民事责任。例如，在行为人侵害非个人数据来源者的著作权时，该非个人数据来源者有权依据《著作权法》第 52 条请求行为人承担停止侵害、消除影响、赔礼道歉等责任。此外，由于非个人数据来源者的在先权利

通常是财产权，在遭受损害后，受害人通常无权请求行为人承担精神损害赔偿责任。

（三）企业合法取得的数据与企业非法取得的数据

1.企业合法取得的数据

无论是企业取得自产数据，还是企业从其他主体处取得数据，均存在合法取得与非法取得的问题。企业在采集自身生产、经营过程中附带产生的数据时通常不涉及他人在先权利的保护，因此一般不存在非法采集的问题。但企业采集用户个人数据的行为应当符合《民法典》《个人信息保护法》等法律规定的处理个人信息的条件。具体而言，企业可以通过取得用户同意的方式（如签订用户协议）取得处理用户个人信息的权利，据此实施个人信息处理行为并取得个人数据；除个人同意外，在符合法律规定的情形下，企业也可以不经个人同意而处理其个人信息，并据此取得相关的数据。例如，企业在依据《个人信息保护法》第 13、27 条处理已公开的个人信息时，也可以合法取得相关的个人数据。企业采集非自然人主体的数据也应当严格按照当事人的约定进行，如果其中涉及个人信息的采集，企业采集相关数据还应当符合依法处理个人信息的要求。

企业从其他主体处合法取得数据的主要方式是合同。企业与其他主体可以就数据的提供与利用等作出约定，如约定数据提供的范围、方式、期限等内容。当然，当事人有关提供数据的约定不得侵害他人的在先权利。例如，就个人数据共享而言，依据《个人信息保护法》第 23 条的规定，个人信息处理者在向他人提供个人信息时，应当符合法律规定的条件，并取得个人的单独同意。据此，在其他数据处理者向企业提供的数据中包含个人信息时，此种数据共享行为也应当符合上述规定。问题在于，在企业与其他主体订立数据共享等协议的情形中，如果相对人实际不具有共享相关数据的权利但伪造了其已经取得共享数据的授权等证明文件，而企业对此并不知情时，企业能否合法取得相关的数据？有观点认为，在相对人并不具有共享个人数据的权利时，其共享数据的行为构成数据财产权的“无权处分”，如果符合善意取得的构成要件，则企业仍可合法取得数据。[38]此种观点具有合理性。与有体财产的交易类似，数据财产权的交易同样存在交易安全的保护问题，需要通过善意取得等制度保护当事人的合理信赖。当然，与有形财产的善意取得不同，数据财产权善意取得的成立具有一定的特殊性：一是权利外观的特殊性。就有体物的善意取得而言，通常是相关的动产由无权处分人占有，或者不动产登记在无权处分人名下，无权处分人因而可以对有体物进行直接控制和处分，从而形成无处分权人享有处分权的权利外观。而在数据财产权的善意取得情形中，无处分权人的权利外观通常体现为其持有相关的数据，[39]但对数据的持有不同于对有体物的物理控制，更多地体现为依托相关的技术手段对他人查阅或者使用数据的权限进行控制。二是相对人善意认定的特殊性。以个人数据为例，在涉及个人数据的交易时，由于我国《民法典》与《个人信息保护法》原则上要求个人信息的共享应当取得个人的单独同意，因此，企业在与相对人订立数据共享协议时，不能仅从相对人持有相关数据的外观而当然认定其对相关的数据具有处分权，而应当依据法律规定进一步核实其是否有共享个人数据的权利（如已经取得个人单独同意等），否则难以认定企业为善意。三是权利变动方式的特殊性。我国现行立法尚未对数据财产权变动的公示方式作出明确规定，一般而言，如果相对人已经通过查阅、复制等方式从无权处分人处“取得”数据，或者完成数据产权变动的登记，即可认定当事人已经完成了数据财产权变动的公示。

此外，企业还可以通过合法的数据爬取行为从其他主体处合法取得数据。我国现行立法并未对合法的数据爬取规则作出规定，已有的司法实践一般认为，企业对其数据享有合法权益，行为人未经许可不得随意爬取他人的数据，否则将构成对他人合法权益的侵害，甚至构成不正当竞争。[40]有观点主张，为了满足消除数据孤岛现象、增强数据供给以及保障人工智能等新兴产业发展的需要，应允许数

据处理者实施合法的数据爬取行为。[41]在国家数据主管部门牵头起草的数据产权文件的讨论中，也有观点主张，为了促进公开数据的复用，数据处理者在不影响网络服务正常运行和服务、不破坏有效技术措施、不违反法律法规的前提下，应当有权合法爬取相关的公开数据。在合法爬取数据的情形下，企业取得相关数据虽然并未取得其他数据处理者的同意，但也构成合法取得企业数据。

2.企业非法取得的数据

企业非法取得的自产数据包括用户个人数据以及非个人数据。例如，企业借助 cookie 等技术手段，在用户不知情的情况下收集其个人信息甚至隐私信息，[42]在不具备其他法定事由的情形下，企业即构成非法取得用户个人数据。再如，企业违反与平台内商户的约定，超出约定范围采集商户营销数据的，即构成非法取得非个人数据。

企业也可能从其他主体处非法取得数据。除法律另有规定外，企业从其他主体处取得数据原则上应当通过合同的方式，如果企业通过窃取等非法方式从其他主体处取得数据，即构成非法取得数据。[43]与个人数据类似，企业从无权利人处取得非个人数据如果不构成善意取得，同样构成非法取得数据。例如，企业从其他主体处取得非个人数据时，如果该其他主体对其所持有的数据不享有数据经营权，其向企业提供数据的行为即构成无权处分，如果不符合善意取得的构成要件，则企业也构成非法取得非个人数据。

因为企业取得数据方式的合法性将直接影响其能否对相关数据取得数据权益以及取得数据权益的范围，行为人侵害企业合法取得的数据与侵害企业非法取得数据所要承担的民事责任存在一定的区别。进一步而言，在企业合法取得数据的情形下，企业通常可以取得相应的数据权益，例如，企业合法采集自产数据的，通常可以取得完整的数据产权；在企业从其他主体处合法取得数据的情形，其也可以基于当事人的约定取得相应的数据权益。行为人侵害企业合法取得的数据时，企业有权以其数据权益受侵害为由请求行为人承担民事责任。而在企业非法取得数据的情形下，企业不仅不享有数据权益，其对非法取得的数据还应负有删除义务。例如，依据《个人信息保护法》第 47 条，在企业非法处理个人信息的情形下，其负有删除相关个人数据的义务。行为人侵害企业非法取得的数据时，企业无权以其数据权益受侵害为由请求行为人承担侵权责任，而只能考虑通过设置类似于占有保护请求权的规则对企业持有数据的状态提供保护。可见，对企业非法取得的数据的保护力度要小于企业合法取得的数据，行为人侵害企业非法取得数据的民事责任的认定更为严格。

三、行为人侵害企业数据权益时对企业的民事责任

在行为人侵害企业数据时，认定行为人对企业的民事责任，首先需要明确行为人侵害了企业的何种民事权益。如前所述，企业取得数据的方式有合法与非法之分，且企业取得数据的方式合法与否将直接决定其能否取得数据权益以及取得数据权益的类型。因此，认定行为人对企业的民事责任，需要区分企业合法取得数据与非法取得数据两种情形，分别予以认定。

(一)行为人侵害企业合法取得的数据的民事责任

1.企业对合法取得数据的权益界定

认定行为人的民事责任，首先需要确定企业对相关数据所享有的民事权益的范围。在合法取得数据的情形下，企业对相关数据通常享有完整的数据权益，即享有数据持有权、数据使用权以及数据经营权。当然，在特殊情形下，企业对其合法取得的数据所享有的权益也可能受到一定的限制，此种限制主要来自两个方面：一是当事人约定的限制。在企业通过合同方式从其他主体处取得数据时，当事人可能会在合同中约定企业对数据所享有的权益的范围。例如，企业在通过合同方式从其他数据处理者处取得数据时，如果当事人约定企业对相关数据仅享有数据持有权与数据使用权，而不享有数据经营权，则企业无权随意将相关数据转让给其他主

体。二是法律法规的限制。法律也可能就企业对其合法取得的数据所享有的权益进行一定的限制。例如，在国家数据主管部门牵头起草的数据产权文件的讨论中，一种较有影响力的观点认为，企业对其合法爬取的公开数据原则上仅享有数据持有权与数据使用权，其数据经营权应当受到严格限制。如果将来立法采纳了此种观点，此种情形即构成对企业数据权益的法定限制。笔者认为，在企业合法爬取公开数据的情形下，为了更好地发挥公开数据的经济效用，不应当一概排除企业的数据经营权，但企业应当在保护国家安全且不实质性替代被爬取方产品和服务的前提下行使数据经营权。

当企业对合法取得的数据享有完整的数据权益时，企业可以获得更高强度的保护。在行为人的行为影响企业数据持有权、数据使用权或者数据经营权的实现时，企业均可请求行为人承担民事责任。而在企业对合法取得的数据所享有的权益受到一定限制时，判断企业能否请求行为人承担民事责任以及行为人应承担何种民事责任，首先需要确定企业对相关的数据享有何种民事权益。例如，在企业通过数据开放平台从其他主体处取得数据的情形下，当事人约定企业对其所取得的数据仅享有数据持有权与数据使用权，如果行为人从企业处窃取相关的数据并用于经营活动，由于企业并不享有数据经营权，其无权主张行为人侵害了其数据经营权。在此情形下，只能由开放数据的数据处理者请求行为人承担侵害其数据经营权的民事责任。当然，如果行为人的行为构成不正当竞争，企业也有权依据竞争法规则请求行为人承担民事责任。

2. 行为人侵害企业合法取得数据民事责任的具体认定

在行为人侵害企业数据权益的情形下，针对企业可以请求行为人承担哪些民事责任，需要依据当事人之间不同的基础关系分别予以认定，具体而言：

一是违约责任。如果企业与行为人之间存在合同关系，则行为人侵害企业数据权益的行为可能构成违约，企业有权依法请求行为人承担违约责任。按照私法自治原则，当事人原则上可以在合同中约定相对人使用企业数据的时间、范围以及使用方式等内容，相对人超出约定范围使用相关企业数据的，构成违约，企业有权依法请求相对人承担违约责任。例如，在“深圳市腾讯计算机系统有限公司、腾讯科技（深圳）有限公司、腾讯数码（天津）有限公司诉北京微播视界科技有限公司、北京拍拍看看科技有限公司不正当竞争纠纷案”中，当事人订立协议，约定腾讯公司通过数据开放平台向抖音产品开放微信/QQ 数据，帮助抖音授权用户使用微信/QQ 头像、昵称等信息实现抖音登录。抖音产品仅能为实现上述授权登录目的而使用相关数据，后抖音超出授权范围，将隐私设置中的“把我推荐给好友”选项默认为开启状态，并在推荐好友时向其他用户显示该用户头像、昵称。法院认为，该行为构成对来源于开放平台的相关数据的再次使用，显然已超出授权登录的使用目的和使用范围。[44]在该案中，相对人超出数据许可使用协议使用企业数据，构成对企业数据权益的侵害，企业应当有权依法请求相对人承担违约责任。

二是侵权责任。企业数据权益作为一种民事权益，应当受到侵权法规则的保护，行为人侵害企业数据权益的，企业有权依法请求行为人承担侵权责任。我国《民法典》侵权责任编同时规定了损害赔偿责任与停止侵害、排除妨碍、消除危险等预防性的侵权责任承担方式，这些责任承担方式都可以用于企业数据权益保护。例如，针对行为人正在实施的非法窃取、篡改、泄露或破坏企业数据的行为，企业有权依法请求行为人承担停止侵害、排除妨碍等侵权责任。行为人侵害企业数据权益造成企业损害的，企业有权依法请求行为人承担侵权损害赔偿责任。需要指出的是，企业数据权益在性质上属于财产权益而非人身权益，即便企业数据中包含个人数据，企业也仅对其享有财产权益而非人身权益。[45]因此，在具体计算企业数据权益遭受侵害后的财产损害数额时，应当依据《民法典》第 1184 条关于侵害财产权益的损害赔偿规则确定赔偿数额，即具体按照损失发生时的市场价格或者其他合理方式计算财产损失数额，而不能依据《民法典》第

1182 条关于侵害人身权益的财产损失赔偿规则进行计算。[46]

三是基于绝对权请求权产生的民事责任。关于数据权益是否为绝对权，企业对其持有的数据是否享有绝对权请求权，学理上存在不同的主张。有观点认为，数据权益作为一种新型的财产权，其在性质上应当属于绝对权。在数据权益遭受侵害时，权利人有权基于绝对权请求权请求行为人承担停止侵害、排除妨碍、消除危险等民事责任。[47]有观点则主张，对数据进行确权时，应当考虑促进数据的流通与共享，不应当确认相关主体对数据享有绝对性与排他性的权利，而应当根据个案提供场景化的保护。[48]还有学者则采折中的立场，主张为了使企业获得对抗特定类别主体和特定类别的行为，应当在数据之上创建具有有限排他性的准财产权，即数据控制者所享有的数据财产权仅能对抗与其具有竞争关系的行为人，且仅能排除行为人以自动化技术等方式过度获取数据的行为。[49]笔者认为，对数据进行确权的确应当考虑促进数据的流通与共享，这也是推动数据产业发展的基本要求，但这并不影响将数据权益界定为一项绝对权。[50]由于企业数据是企业的重要经营资源，是企业取得和维持其竞争优势的重要条件。因此，为了保护企业的竞争利益，允许其对所持有的数据进行相对“垄断性”的控制和支配是必要的，这也是数据产权保护途径的应有之义，如果否定数据权益的排他性，放任侵害数据权益的行为，可能使企业丧失“人无我有”的竞争优势，并在一定程度上架空企业持有数据的价值。[51] 即便在数据多重持有的情形下，也应当承认各个数据处理者数据权益的绝对权属性，各数据处理者可据此排除第三人的不法侵害行为。承认企业数据权益的绝对权属性，并不当然影响数据的流通与利用。正如有观点所指出的，在基于合同约定流通数据的情形下，承认数据权益的排他性，并在此基础上建立相对明确的数据财产权利体系，有利于降低当事人在数据交易中的信息获取成本，这不仅不会阻碍基于合同约定而发生的数据流通，反而有利于促进数据的流通。[52]据此，在行为人侵害企业数据的情形下，企业应当有权基于绝对权请求权请求行为人承担停止侵害、排除妨碍、消除危险等民事责任。当然，由于我国现阶段数据立法尚不完善，企业的绝对权请求权还有待于法律的确认。此外，在承认企业数据权益绝对权属性的同时，有必要通过确立数据查阅权[53]、数据合理使用制度以及合法爬取数据的规则等方式，缓解可能产生的数据垄断，以促进数据的流通与利用。

（二）行为人侵害企业非法取得的数据的民事责任

在企业非法取得数据的情形下，判断行为人是否需要承担民事责任，首先需要明确企业对非法取得的数据是否享有数据权益或其他民事权益。依据《民法典》第 1037 条第 2 款、《网络安全法》第 43 条以及《个人信息保护法》第 47 条第 1 款第 4 项规定，如果个人信息处理者违反法律、行政法规或者违反约定处理个人信息，其负有删除相关个人信息的义务。因此，不宜承认企业对其非法取得个人数据享有数据权益，否则不仅与企业依法负有的删除义务相冲突，也可能变相鼓励企业非法处理个人信息。就企业非法取得非个人数据（如企业违反其与平台内商户的约定、非法采集商户营销数据）时是否负有删除义务，我国现行立法尚无明文规定。笔者认为，为了遏制企业实施非法取得非个人数据的行为，应当采取与前述企业非法取得个人数据相同的立场，即不宜承认企业对其非法取得的非个人数据享有数据权益，企业对相关数据也应当负有删除义务。据此，在行为人侵害企业非法取得的数据时，企业不得以其数据持有权、数据使用权、数据经营权等企业数据权益受侵害为由请求行为人承担民事责任。

问题在于，企业对其非法取得的数据不享有数据权益是否意味着，行为人可以随意侵害企业非法取得的数据？笔者认为，此处需要区分数据权益中的数据持有权与数据持有状态：数据持有权在性质上属于独立的民事权利，企业享有数据持有权应当以其合法取得数据为前提；数据持有状态则是企业客观上持有数据的一种状态，而无论该相关数据是

企业合法取得抑或非法取得。在企业非法取得数据的情形下，其持有数据的状态与无权占有人占有财产的状态类似，应受到类似的保护。依据《民法典》第 462 条规定，行为人非法侵害占有人对物的占有状态的，占有人有权依法主张占有保护请求权，请求行为人承担返还原物、排除妨害或消除危险等民事责任。《民法典》之所以保护没有权源基础的占有状态，是为了维护已经成立的占有事实状态，通过排除非法侵害的方式维护相关的财产秩序。[54]企业非法取得数据所形成的对相关数据的“持有”状态，与有体物的占有状态类似，同样形成了一定的财产秩序，他人也应负有不得非法破坏企业持有数据状态的义务。尤其是企业已经对其非法取得的数据进行了一定的加工，或者将其用于自身的生产、经营活动时，该财产秩序更应受到法律的保护。因此，即便企业是非法取得相关的数据，其持有数据的状态也应受到法律保护。行为人侵害企业数据、破坏企业持有数据的状态的，企业有权请求行为人承担民事责任。例如，在行为人以篡改、破坏等方式实施侵害行为时，企业有权请求行为人停止实施相关行为；而在行为人窃取企业数据的情形下，企业有权请求行为人返还数据或者删除数据。

需要指出的是，与侵害有体物的占有不同，行为人侵害企业非法持有的数据时，并不当然会破坏企业持有数据的状态，企业能否请求行为人承担民事责任，需要区分行为人不同的侵害方式及其对企业持有数据状态的影响，分别予以认定：在行为人通过泄露、非法访问等方式侵害相关数据时，该行为并不会对企业持有数据的状态产生不当影响，不宜承认企业的停止侵害、排除妨碍等请求权；而在行为人以窃取、篡改、破坏等方式实施侵害行为时，由于该行为可能破坏企业持有数据的状态，应当承认企业有权请求行为人承担停止侵害、排除妨碍、赔偿损失等民事责任。

四、行为人侵害企业数据权益时对数据来源者的民事责任

行为人侵害企业数据权益不仅会造成受害企业的损害，也可能侵害数据来源者的民事权益。个人数据来源者对个人数据享有个人信息权益，非个人数据来源者对非个人数据主要享有著作权、商业秘密等在先权利，由于个人信息与著作权、商业秘密等在先权利的性质不同，其保护规则也存在差别。例如，个人信息属于人格利益，可依《民法典》与《个人信息保护法》的个人信息权益保护规则受到保护；而非个人数据来源者的在先权利主要是财产权，主要受《著作权法》及商业秘密等在先权利保护规则的保护。因此，有必要区分个人数据来源者与非个人数据来源者，分别认定行为人对数据来源者的民事责任。

（一）行为人对个人数据来源者的民事责任

1.个人数据来源者对企业数据所享有的权利

在行为人侵害企业数据权益的情形下，确定行为人对个人数据来源者应当承担的民事责任，首先需要明确个人数据来源者就企业数据享有何种权利。

企业数据中的个人数据虽然是企业数据的组成部分，但其并不因此丧失个人信息的属性。而个人信息在性质上属于人格利益，具有人身专属性，因此个人数据来源者对企业数据中的个人数据仍应享有个人信息权益。无论是企业在生产、经营过程中采集的个人数据，还是从其他主体处取得的个人数据，本质上都属于个人信息，即便企业对相关的个人信息进行了一定的处理，除匿名化处理外，也不会改变其个人信息属性。例如，企业在基于个人同意而采集其个人信息时，当事人之间应当成立个人信息许可使用关系[55]而非个人信息转让的关系，企业对相关的个人信息享有的只是一种利用权，[56]个人仍然是个人信息主体。《民法典》与《个人信息保护法》对个人在个人信息处理活动中的权利作出的规定，也当然适用于企业处理个人数据的情形。例如，依据《个人信息保护法》第 45 条第 3 款，个人对其个人信息享有可携带权，即便相关个人信息已成为企业数据的组成部分，个人也有权依法请求将其相关个人信息转移至其指定的个人信

息处理者。无论企业是基于合法原因取得个人数据，还是非法取得个人数据，均不影响个人的信息主体地位。例如，即便企业所持有的个人数据是从其他数据处理者处窃取的，该部分个人信息的信息主体也仍然是个人，其仍可依据个人信息保护的相关规则主张个人信息权益。

针对企业数据中包含的个人数据，由于个人数据只是企业数据的组成部分，个人应当仅对自己的个人数据而非整个企业数据享有权利，否则会不当扩张个人对其个人数据所享有的权利范围。但问题在于，既然个人数据是企业数据的组成部分，个人能否主张与企业分享数据权益？例如，在企业通过使用或者经营企业数据而获利时，个人能否主张分享该获利？再如，在行为人侵害企业数据权益的情形下，企业在请求行为人承担责任并获得损害赔偿后，个人能否主张分享该损害赔偿金？对此，有观点认为，无论是企业还是个人，对数据价值的形成都有一定的贡献，应当根据各自贡献程度的不同赋予其数据权益。[57]此种观点值得商榷，因为如果赋予个人对企业数据享有数据权益，为了便于企业数据的利用，就需要进一步衡量个人在企业数据中的贡献度，进而确定企业与个人对企业数据享有权利的比例，但企业数据中往往包含海量用户的个人数据，就单个用户的个人数据在企业数据价值形成过程中究竟有多大影响、应当赋予个人享有多大比例的数据权益，几乎难以确定。[58]这不仅会导致企业数据之上存在大量的数据权益主体，也将不可避免地影响企业数据的有效利用。[59]从“数据二十条”的规定来看，其所规定的数据确权也主要是对数据处理者数据财产权的确权，而非对个人数据来源者数据财产权的确权，此种做法值得赞同。

2.行为人对个人数据来源者民事责任的具体认定

如前所述，在企业数据中包含个人数据的情形下，个人数据来源者仅对相关的个人数据享有个人信息权益，而不享有数据权益。在行为人侵害企业数据权益的同时也侵害了个人数据来源者的个人信息权益时，个人仅能以其个人信息受侵害为由请求行为人承担民事责任，[60]而不得以数据权益受侵害为由主张民事责任。从《民法典》与《个人信息保护法》的规定来看，行为人对个人数据来源者所需要承担的民事责任主要是基于人格权请求权产生的责任与侵权责任。

《民法典》第 995 条对人格权请求权规则作出了规定，但从该条的文义来看，其保护对象限于“人格权”，而不包括个人信息等人格利益。[61]那么，在行为人侵害企业数据权益同时侵害个人数据来源者个人信息的情形下，个人数据来源者能否依据人格权请求权请求行为人承担停止侵害、排除妨碍、消除危险等责任？笔者认为，个人信息等人格利益在客观上也有受人格权请求权保护的必要，当行为人实施侵害个人信息的行为时，应当允许个人基于人格权请求权请求行为人停止侵害、排除妨碍、消除危险等民事责任，以防止损害的发生或者扩大。从人格利益保护的价值基础来看，与姓名、肖像等人格利益相比，个人信息等人格利益同样与个人的人格尊严存在密切关联，[62]也有受到人格权请求权保护的必要。因此，《民法典》第 995 条将人格权请求权的保护范围限定为“人格权”而不包括个人信息等人格利益，存在法律漏洞，有必要通过目的性扩张解释的方式，将个人信息等人格利益纳入保护范围。据此，当行为人侵害企业数据同时构成非法处理个人信息时，个人数据来源者应当有权基于人格权请求权请求行为人承担停止侵害、排除妨碍、消除危险等民事责任。而且，个人数据来源者在依据《民法典》第 995 条规定主张人格权请求权时，并不需要证明自身遭受了现实损害，也不需要证明行为人具有过错，该请求权的行使也不受诉讼时效的限制。

当个人信息遭受侵害时，个人数据来源者同样有权请求行为人承担侵权责任。个人数据来源者在依据《民法典》第 1167 条请求行为人承担停止侵害、排除妨碍、消除危险等预防性的侵权责任时，既不需要证明行为人具有过错，也不需要证明其遭受了现实损害。例如，在行为人擅自向他人提供个人数据时，个人有权请求行为人停止数据共享行为，

并消除潜在的个人数据泄露风险。而依据《个人信息保护法》第 69 条第 1 款规定，个人数据来源者请求行为人承担侵权损害赔偿责任时，则采过错推定原则，即个人无需证明行为人具有过错，而推定行为人具有过错，由其举证证明自身没有过错。在损害的证明方面，由于个人信息等人格权益的客体具有无形性，在遭受侵害后，受害人往往难以证明其客观上遭受了何种损失，许多情况下，个人甚至并不知道其个人信息受到了侵害。[63]因此，为了降低受害人的举证负担，可以借鉴规范损害说，即只要行为人实施了侵害他人个人信息的行为，就可认定受害人遭受了一定的损害。[64]在损害赔偿额的计算方面，依据《民法典》第 1182 条与《个人信息保护法》第 69 条第 2 款规定，具体可以按照受害人的实际损失或者行为人的获利赔偿，或者由法院酌定赔偿数额。受害人在请求行为人按照实际损失赔偿或者按照行为人的获利赔偿时，应当证明自身实际损失数额或者行为人获利数额，否则将难以获得救济。但是，如前文所述，在个人信息遭受侵害时，受害人往往难以证明自身遭受了何种损害，且单个受害人的个人信息在行为人获利中的比例通常也难以确定。因此，这两种损害赔偿数额计算方式在实践中往往难以适用。此时，受害人可以请求法院酌定赔偿数额，或者由法院依职权酌定赔偿数额。[65]

值得探讨的是，如果行为人对受害企业的民事责任成立，能否当然认定其对个人数据来源者的民事责任成立？笔者认为，个人数据来源者的权益与企业数据权益虽然都属于企业数据之上所承载的民事权益，但二者属于相互独立的民事权益，在民事责任的认定上也应当相互独立。在企业数据中包含个人数据时，即便认定行为人侵害了企业数据权益，也不宜当然认定其构成对个人信息权益的侵害，反之亦然。例如，在当事人共享包含个人数据的企业数据时，如果提供企业数据的一方并未取得个人数据来源者的同意，则接受共享数据的一方在利用企业数据时可能仅构成对个人数据来源者个人信息权益的侵害，而不构成对共享数据一方企业数据权益的侵害。相反，当接受共享的一方超出约定的范围使用个人数据但其取得了用户个人的同意的，则其仅构成对提供企业数据的一方数据权益的侵害，但并不构成对用户个人信息权益的侵害。[66]

(二) 行为人对非个人数据来源者的民事责任

与行为人对个人数据来源者的民事责任类似，在行为人侵害企业数据权益的情形中，确定行为人需要对非个人数据来源者承担哪些民事责任，同样需要首先明确行为人侵害了非个人数据来源者的何种民事权益。一般而言，数据来源者的权利包括在先权利及其对数据处理者所享有的权利两类。[67]在行为人侵害企业数据权益时，非个人数据来源者的上述两类权利均可能受到侵害，需要分别认定行为人的民事责任。

1.行为人侵害非个人数据来源者在先权利的民事责任

行为人侵害企业数据权益的，也可能侵害非个人数据来源者的著作权、商业秘密等相关在先权利。例如，当企业数据中包含非个人数据来源者的商业秘密时，如果行为人窃取数据或者泄露数据，可能导致非个人数据来源者的商业秘密受到侵害，此时，受害人有权依法请求行为人承担侵权责任。[68]非个人数据来源者的在先权利通常都是立法明确规定的民事权利，事实上，行为人侵害企业数据不过是其侵害非个人数据来源者在先权利的一种方式而已，此时仍应依据侵权责任的一般规则或者在先权利保护的规则来认定行为人的民事责任。

在企业从其他主体处取得数据的情形下，非个人数据来源者同时也可能是数据处理者，其也可能依法享有数据持有权、数据使用权以及数据经营权，此时构成企业数据的双重或者多重持有，行为人侵害企业数据可能构成对多个数据处理者数据权益的侵害，应当依法对多个数据处理者承担民事责任。例如，网店许可平台经营者持有并使用其营销数据，如果行为人从平台经营者处窃取该数据并用于经营，则该行为不仅侵害了平台经营者的数据权益，也构成对网店数据权益的侵害，网店也有权请求行为人承担民事责任。

2.行为人侵害非个人数据来源者对企业所享有权利的民事责任

在企业从非个人数据来源者处取得数据的情形下，非个人数据来源者就数据的利用等也对企业享有一定的权利。我国《民法典》与《个人信息保护法》仅对个人信息处理活动中个人对个人信息处理者所享有的权利作出了规定，[69]而没有规定非个人数据来源者对数据处理者所享有的权利。有观点认为，为了促进数据的有效利用，打破数据孤岛，有必要承认非个人数据来源者对数据处理者享有公平访问权（即查阅权）、合理利用权等权利。[70]此种观点值得赞同。“数据二十条”在规定数据来源者权益保护时，也明确规定，“保障数据来源者享有获取或复制转移由其促成产生数据的权益”，这实际上也承认了数据来源者的数据查阅权、复制权与可携带权。但问题在于，非个人数据来源者对企业所享有的数据查阅权、数据复制权以及数据可携带权等权利在性质上是何种权利？其能否成为民事责任的救济对象？

对此，有观点主张，非个人数据来源者对数据处理者所享有的权利在性质上属于一种程序性、非绝对性、举报建议性权利，其并非一种实体性、绝对性和可诉性的权利。[71]按照此种观点，在行为人侵害非个人数据来源者的上述权利时，非个人数据来源者无权请求行为人承担民事责任。另一种观点则认为，非个人数据来源者对数据处理者所享有的数据查阅权、复制权、可携带权等权利在性质上属于实体性权利，而且作为相对权，此类权利的实现需要数据处理者提供便利，只有数据处理者未提供便利或者拒绝数据来源者行使权利时，数据来源者才能依法请求数据处理者承担民事责任，其不能对第三人产生绝对、排他的效力，在遭受侵害时，数据来源者无权请求第三人承担侵权责任。[72]

笔者认为，非个人数据来源者的数据查阅权、复制权、可携带权等权利在性质上应当属于实体性权利，此类权利的行使虽然涉及相关的程序，但其权利基础应当源于实体法的规定，是保障非个人数据来源者权益的重要实体性权利。与个人在个人信息处理活动中的权利类似，非个人数据来源者所享有的查阅权、复制权、可携带权等权利也仅能向数据处理者主张，其应当属于相对权。问题在于，在行为人侵害企业数据，并因此影响非个人数据来源者对企业行使相关上述权利时，非个人数据来源者能否请求行为人承担侵权责任？例如，行为人破坏企业从非个人数据来源者处取得的数据，导致非个人数据来源者无法访问相关的数据，此时非个人数据处理者能否请求行为人承担侵权责任？按照前述观点，在上述权利遭受侵害时，非个人数据来源者无权请求行为人承担侵权责任。此种观点具有其合理性，因为企业所持有的数据来源具有复杂性，非个人数据来源者对企业所享有的权利作为相对权，在客观上缺乏有效的公示方式，非个人数据来源者与企业之外的第三人既难以判断相关非个人数据的来源，也难以判断是否存在数据来源者以及数据来源者享有何种权利。当行为人侵害企业数据进而影响非个人数据来源者行使数据查阅权、复制权等权利时，如果课以其对非个人数据来源主体承担侵权责任，会过分加重行为人责任，从而可能导致不当限制个人的行为自由，有违侵权责任法的立法目的。但完全将非个人数据来源者的上述权利排除在侵权法的保护范围之外，也存在一定的问题，因为《民法典》侵权责任编保护的权益范围具有开放性，不仅包括绝对权，还包括相对权及各种民事利益。[73]非个人数据来源者的上述权利作为一种合法权益，也应当受到侵权法的保护。而且，非个人数据来源者的上述权利虽然具有相对性，但在特殊情形下，行为人在侵害企业数据时也可能知晓非个人数据来源者享有相关权利，甚至可能出于不正当竞争等目的恶意侵害非个人数据来源者的上述权利。此时，对行为人行为自由的保护应让位于非个人数据来源者权益的保护，非个人数据来源者应当有权依法请求行为人承担侵权责任。

五、余　论

自“数据二十条”颁布后，学术界就数据确权问题、数据流通与交易等问题展开了广泛研究，并

就企业数据应受法律保护以及企业数据的产权保护路径等问题达成了初步共识。在判定侵害企业数据权益民事责任时，通过对企业数据的来源、企业数据的内容以及企业取得数据的方式等方面的区分，可以帮助我们抓住认定侵害企业数据权益民事责任的要点，从而更为准确地认定行为人侵害企业数据权益的民事责任。

将来围绕侵害企业数据权益民事责任的研究仍需要重点解决如下两方面的问题：一是行为人侵害企业数据权益民事责任的具体承担问题。数据权益的保护是互联网、大数据时代的新问题，传统的民事责任承担方式在适用于企业数据权益保护时，可能需要进行一定的变通。例如，在企业数据权益遭受侵害后，行为人究竟应当以何种方式停止侵害、排除妨碍、消除危险等，需要进一步研究。二是行为人侵害企业数据权益民事责任与行政规制方式之间关系衔接的问题。企业数据权益的保护既需要考虑对相关主体进行赋权，也需要发挥行政规制手段的作用，双管齐下，构建企业数据权益保护的系统解决方案，这就需要协调侵害企业数据权益民事责任与行政监管方式之间的关系。例如，在确定行为人侵害企业数据权益损害赔偿的数额时，可能需要将对行为人进行行政处罚的数额纳入考量。再如，在行为人侵害非个人数据来源者的查阅权、复制权、可携带权等权利时，受害人既有权依法请求行为人承担侵权责任，也有权依法向行政机关进行投诉或者举报建议，这同样涉及民事责任与行政监管关系的协调。关于民事权益保护与行政监管之间的关系，《民法典》施行以来的司法实践已经进行了有益探索。在企业数据权益保护方面，也可以考虑借鉴这一司法实践经验，但在行为人侵害企业数据权益的情形下如何实现民事责任与行政监管的有效衔接，值得进一步研究。

参考文献

[1] See Tabrez Y. Ebrahim, Algorithms in Business, Merchant-Consumer Interactions, & Regulation, West Virginia Law Review, Vol.123:873, p.873-906 (2021).

[2] 需要说明的是，由于数据之上可能承载多项民事权益，“数据权益”本身也因此有广义与狭义之分。广义上，数据之上承载的各种民事权益如数据处理者的数据产权、个人数据来源者的个人信息权益、隐私权等，均可以称为“数据权益”；而狭义上的“数据权益”仅指数据产权。本文均在狭义上即数据产权意义上使用“数据权益”的概念。

[3] See Zachary Gold & Mark Latonero, Robots Welcome: Ethical and Legal Considerations for Web Crawling and Scraping, Washington Journal of Law, Technology & Arts, Vol.13:275, p.280-281 (2018).

[4] 参见“北京爱奇艺科技有限公司、随州市飞流网络科技有限公司诉上海七牛信息技术有限公司不正当竞争纠纷案”，江苏省高级人民法院（2019）苏民终 778 号民事判决书。在该案中，飞流公司利用其柠檬挂机软件所具备的技术手段，对爱奇艺公司网站所提供的视频进行所谓“刷量”，反复、机械地制造相关视频的点播量，即侵害了视频访问数据这一企业自产数据。

[5] 例如，行为人所侵害的企业数据是企业基于数据开放协议从其他企业的数据开放平台所取得的数据。

[6] 例如，在“绍兴衡某科技有限公司等诉浙江天某技术有限公司等不正当竞争纠纷案”中，法院认为，数据的原始生成主体主要为商家，平台系经过原始商品数据生成主体授权，实施涉案商品数据的采集和储存，属于合法取得非个人数据。参见浙江省高级人民法院（2023）浙民终 1126 号民事判决书。

[7] 参见“深圳爱拼信息科技有限公司等诉北京市海淀区学而思培训学校等不正当竞争纠纷案”，北京市海淀区人民法院（2017）京 0108 民初 51904 号民事判决书。

[8] 参见“北京微梦创科网络技术有限公司诉北京淘友天下技术有限公司、北京淘友天下科技发展有限公司不正当竞争纠纷案”，北京知识产权法院

（2016）京 73 民终 588 号民事判决书。在该案中，被告非法爬取新浪微博中用户的职业信息、教育信息等个人数据，并非法获取用户通讯录联系人与新浪微博中相关用户的对应关系，其侵害的就是企业数据中的个人数据。

[9] 例如，在“北京百度网讯科技有限公司诉上海汉涛信息咨询有限公司不正当竞争纠纷案”中，大众点评网平台内的数据就同时包含了消费者的个人数据以及平台内商户的数据等非个人数据。百度公司未经许可大量使用相关的数据，就涉及对非个人数据的侵害。参见上海知识产权法院（2016）沪 73 民终 242 号民事判决书。

[10] 例如，行为人的经营范围、对相关数据的利用目的可能完全不同于受害人，甚至不存在相关性。See Jennie E. Christensen, The Demise of the CFAA in Data Scraping Cases, Notre Dame Journal of Law, Ethics & Public Policy, Vol.34(2):529, p.531(2020).

[11] 参见蔡川子：《数据抓取行为的竞争法规制》，载《比较法研究》2021 年第 4 期，第 183-184 页。

[12] 参见王利明：《论数据权益：以“权利束”为视角》，载《政治与法律》2022 年第 7 期，第 99 页。

[13] 参见周汉华：《数据确权的误区》，载《法学研究》2023 年第 2 期，第 10-14 页。

[14] 参见梅夏英：《数据的法律属性及其民法定位》，载《中国社会科学》2016 年第 9 期，第 178 页。

[15] 参见崔国斌：《新酒入旧瓶：企业数据保护的商业秘密路径》，载《政治与法律》2023 年第 11 期，第 2-23 页；刘鑫：《企业数据知识产权保护的理论证立与规范构造》，载《中国法律评论》2023 年第 2 期，第 38-50 页。

[16] 参见孙莹：《企业数据确权与授权机制研究》，载《比较法研究》2023 年第 3 期，第 56-73 页；房绍坤、周秀娟：《企业数据“三权分置”的法律构造》，载《社会科学战线》2023 年第 9 期，第 226-238 页；付新华：《企业数据财产权保护论批判——从数据财产权到数据使用权》，载《东方法学》2022 年第 2 期，第 132-143 页。

[17] 参见程啸：《企业数据权益论》，载《中国海商法研究》2024 年第 1 期，第 50-62 页；姚佳：《企业数据权益：控制、排他性与可转让性》，载《法学评论》2023 年第 4 期，第 149-159 页；黄细江：《企业数据经营权的多层用益权构造方案》，载《法学》2022 年第 10 期，第 96-111 页。

[18] 参见李依怡：《论企业数据流通制度的体系构建》，载《环球法律评论》2023 年第 2 期，第 146-158 页；张艳：《企业数据交易模式的构建》，载《法商研究》2024 年第 2 期，第 72-86 页；苏宇、程子洳：《数据财产法益保护的行为规制模式》，载《郑州大学学报（哲学社会科学版）》2023 年第 6 期，第 52 页。

[19] 参见梅夏英：《企业数据权益原论：从财产到控制》，载《中外法学》2021 年第 5 期，第 1203 页。

[20] 参见潘重阳：《解释论视角下的侵害企业数据权益损害赔偿》，载《比较法研究》2022 年第 4 期，第 45-56 页。

[21] 参见黄薇主编：《中华人民共和国民法典总则编解读》，中国法制出版社 2020 年版，第 407 页。

[22] 公共数据是各级党政机关、企事业单位依法履职或者提供公共服务过程中收集、产生的涉及公共利益的数据，其类型较为复杂，既包括政务类数据，也包括事业单位的数据、公共服务型企业的数据、经营性国有企业等所产生的具有公共性的数据，以及其他涉及公共利益的数据。公共数据的类型不同，其公共性程度存在一定的差别，这也会影响公共数据的产权归属界定：对于政务类公共数据而言，认定其由国家享有并不存在大的争议，但对于其他类型的公共数据，尤其是经营性国有企业等产生的公共数据，是否一概需要进行国有化，值得进一步研究。

[23] 参见熊丙万、何娟：《数据确权：理路、方法与经济意义》，载《法学研究》2023 年第 3 期，第 65 页。

[24] 此处数据的双重持有或者多重持有并不包括数据的委托持有，在数据委托持有的情形下，受托

人虽然客观上持有数据，但并不享有数据权益。在行为人侵害企业数据时，受托人也无权以其数据权益受侵害为由请求行为人承担民事责任。

[25] See Gautier Duflos & David Viros, The Collection, Storage and Processing of Data and Its Implications for Competition Law: Something Old, Something New, Competition Law & Policy Debate, Vol.2(4):21, p.22 (2016).

[26] See Eleni Kosta, Peeking into the Cookie Jar: The European Approach towards the Regulation of Cookies, International Journal of Law and Information Technology, Vol.21:380, p.381 (2013).

[27] See Gautier Duflos & David Viros, supra note 25, 32.

[28] 参见程啸：《论数据权益》，载《国家检察官学院学报》 2023 年第 5 期，第 85 页。

[29] 关于数据权益的内容或者权能，我国现行立法并未作出明确规定，“数据二十条”将其规定为“数据资源持有权”“数据加工使用权”与“数据产品经营权”。有观点认为，这三项权利中的描述性前缀在财产法层面并无必要，可以直接理解为“数据持有权”“数据使用权”与“数据经营权”。参见夏庆锋：《个人数据交易的私法制度构造研究》，载《中国法学》 2024 年第 5 期，第 155-156 页；熊丙万、何娟:《论数据要素市场的基础制度体系》，载《学术月刊》 2024 年第 1 期，第 104 页。此种观点值得赞同，本文在阐释数据权益的内容时也采用“数据持有权”“数据使用权”与“数据经营权”的表述。

[30] 有观点认为，个人同意是个人信息中财产利益实现的基础，依此，企业在基于个人同意处理其个人信息时，有权保留相关个人数据中的财产性利益。参见姜程潇：《论从无权利人处取得数据财产权》，载《国家检察官学院学报》 2024 年第 2 期，第 165-166 页。

[31] 参见前注 [6]，浙江省高级人民法院（2023）浙民终 1126 号民事判决书。

[32] 参见刘建臣：《企业数据赋权保护的反思与求解》，载《南大法学》 2021 年第 6 期，第 6-7 页。

[33] See Heleen Janssen, Jennifer Cobbe, Chris Norval & Jatinder Singh, Decentralized Data Processing: Personal Data Stores and the GDPR, International Data Privacy Law, Vol.10(4):356, p.368 (2020).

[34] 除当事人之间的协议约定外，当事人还可能对特定的数据或者数据集合采取文件加密等方式，以限制他人的访问。See Daniel L. Rubinfeld & Michal S. Gal, Access Barriers to Big Data, Arizona Law Review, Vol.59(2):339, p.362-363 (2017).

[35] 个人数据来源者可以基于个人信息保护规则对企业主张查阅权、复制权、可携带权等权利；而非自然人数据来源者究竟对企业享有哪些权利，我国现行立法尚未作出明确规定。有观点主张其对相关数据应当享有公平访问权、合理利用权、可携带权等权利。参见王利明：《论数据来源者权利》，载《法制与社会发展》 2023 年第 6 期，第 46-51 页。此处的公平访问权与我国《个人信息保护法》所规定的查阅权类似，因此笔者使用“查阅权”的概念。

[36] 参见王叶刚：《企业数据权益与个人信息保护关系论纲》，载《比较法研究》 2022 年第 4 期，第 39-40 页。

[37] 参见李东宇：《论侵害个人信息权益的精神损害赔偿》，载《财经法学》 2023 年第 4 期，第 140-143 页。

[38] 参见前注 [30]，姜程潇文，第 172-175 页。

[39] “数据二十条”提出“研究数据产权登记新方式”，在将来立法规定数据登记方式之后，无权处分人享有处分权的权利外观还可能体现为相关数据权益登记在其名下。

[40] 参见前注 [8]，北京知识产权法院（2016）京 73 民终 588 号民事判决书；“安徽美景信息科技有限公司诉淘宝（中国）软件有限公司不正当竞争纠纷案”，浙江省杭州市中级人民法院（2018）浙 01 民终 7312 号民事判决书。

[41] 参见许可：《数据爬取的正当性及其边界》，载《中国法学》 2021 年第 2 期，第 172 页。

[42] See Robert Slattery & Marilyn Krawitz, Mark Zuckerberg, the Cookie Monster - Australian Privacy Law and Internet Cookies, Flinders Law Journal, Vol.16:1, p.8 (2014).

[43] 如果权利人已经对自身持有的数据采取技术保护措施，行为人通过破坏相关技术措施取得数据的，即构成非法取得数据。参见“深圳市谷米科技有限公司诉武汉元光科技有限公司等不正当竞争纠纷案”，广东省深圳市中级人民法院（2017）粤 03 民初 822 号民事判决书。

[44] 参见天津市滨海新区人民法院（2019）津 0116 民初 2091 号民事裁定书。

[45] 参见程啸：《论个人数据经济利益的归属与法律保护》，载《中国法学》 2024 年第 3 期，第 60 页。

[46] 需要指出的是，在行为人侵害企业数据权益构成不正当竞争的情形下，依据《反不正当竞争法》第 17 条第 3 款规定，因不正当竞争行为受到损害的经营者可以主张的赔偿数额，首先按照其所遭受的实际损失确定，如果其实际损失难以确定，则按照侵权人的侵权获利予以确定；同时，行为人的赔偿数额还应当包括经营者为制止侵权行为所支付的合理开支。如果企业依据竞争法规则请求行为人承担损害赔偿责任，则应当依据上述规则确定行为人的赔偿数额。

[47] 参见程啸：《论大数据时代的个人数据权利》，载《中国社会科学》2018 年第 3 期，第 102、118 页。

[48] 参见丁晓东：《数据到底属于谁？——从网络爬虫看平台数据权属与数据保护》，载《华东政法大学学报》 2019 年第 5 期，第 69 页。

[49] 参见杨翱宇：《数据财产权益的私法规范路径》，载《法律科学》 2020 年第 2 期，第 75-77 页。

[50] 关于企业数据权利绝对性与数据流通、共享的关系，参见前注 [36]，王叶刚文，第 33-44 页。

[51] 参见沈健州：《数据财产的排他性：误解与澄清》，载《中外法学》 2023 年第 5 期，第 1169 页。

[52] 参见前注 [51]，沈健州文，第 1175 页。

[53] 参见前注 [19]，梅夏英文，第 1203 页。有观点认为，部分企业对用户数据的控制权对竞争构成了威胁，而企业对其他数据处理者数据访问能力的限制，对竞争构成了更为严重的威胁，有必要承认其他数据处理者对企业数据的访问权。See Ioannis Drivas, Liability for Data Scraping Prohibitions under the Refusal to Deal Doctrine: An Incremental Step toward More Robust Sherman Act Enforcement, The University of Chicago Law Review, Vol.86:1901, p.1913 (2019).

[54] 参见黄薇主编：《中华人民共和国民法典物权编解读》，中国法制出版社 2020 年版，第 846 页。

[55] 参见程威：《破产程序中数据权益之保护——以信义义务为视角》，载《财经法学》 2022 年第 4 期，第 121 页。

[56] See Benjamin L. W. Sobel, A New Common Law of Web Scraping, Lewis & Clark Law Review, Vol.25:147, p.175 (2021).

[57] 参见申卫星、李夏旭：《个人数据所有权的赋权逻辑与制度展开》，载《法学评论》 2023 年第 5 期，第 115-122 页；季卫东、翁壮壮：《个人数据财产权的证立及诠释》，载《法制与社会发展》2024 年第 4 期， 169-180 页。

[58] 参见前注 [35]，王利明文，第 53 页。

[59] 在企业数据的利用过程中，相关的个人数据可能会发生一定的改变，其既可能是数量上的变化，也可能是数据内容的变化。如果承认个人作为数据来源者可以对企业数据享有数据权益，将导致个人数据权益可能处于持续变动之中，这也给确定个人数据权利的内容、范围等带来极大的困难。See Ivan Stepanov, Introducing a Property Right over Data in the EU: The Data Producer ’ s Right - An Evaluation, International Review of Law, Computers & Technology, Vol.34:65, p.79-80 (2020).

[60] 当然，行为人在侵害包含个人信息的企业数据时，也可能侵害个人的隐私权以及其他民事权益，本文此处仅从个人信息保护的角度探讨行为人对个人数据来源者的民事责任。

[61] 参见王利明：《论个人信息删除权》，载《东方法学》 2022 年第 1 期，第 41 页。

[62] See Edward J. Eberle, The Right to Information Self-Determination, Utah Law Review, Vol.2001(4):965, p.968 (2001).

[63] 例如，在企业收集大量用户个人数据的情形下，用户个人往往并不知道企业具体使用了其何种数据以及使用数据的具体方式，即便用户数据被泄露，用户通常也难以知道其数据被泄露的事实。 See Joanna Kessler, Data Protection in the Wake of the GDPR: California’ s Solution for Protecting “the World’ s Most Valuable Resource” , Southern California Law Review, Vol.93:99, p.100 (2019).

[64] 参见徐建刚：《〈民法典〉背景下损害概念渊流论》，载《财经法学》 2021 年第 2 期，第 38-41 页。

[65] 参见王叶刚：《论侵害人格权益财产损失赔偿中的法院酌定》，载《法学家》 2021 年第 3 期，第 109-111 页。

[66] 参见前注 [44]，天津市滨海新区人民法院（2019）津 0116 民初 2091 号民事裁定书。

[67] 参见前注 [35]，王利明文，第 56 页。

[68] 参见前注 [15]，崔国斌文，第 2 页。

[69] 参见《民法典》第 1037 条、《个人信息保护法》第四章。

[70] See Ivan Stepanov, supra note 59, 75.

[71] 参见丁晓东：《论数据来源者权利》，载《比较法研究》 2023 年第 3 期，第 25 页。

[72] 参见前注 [35]，王利明文，第 56 页。

[73] 参见黄薇主编：《中华人民共和国民法典侵权责任编解读》，中国法制出版社 2020 年版，第 3-4 页。

（技术编辑：张清）