

中国人民大学法学院 数字法学教研月报

2025 年第 5 期（总第 17 期）

2025 年 5 月 18 日



本期看点

【数字法治大事件】第八届数字中国建设峰会分论坛成功举办，发布“涉外法治大模型”；中央网信办等多部门积极部署数字领域工作，印发多项工作要点，涉及数字化绿色化协同转型、全民数字素养提升、数字乡村发展等方面；人工智能气象应用、终端设备直连卫星服务等领域法规政策相继出台，为新兴技术应用提供规范指引；国家数据局推动高质量数据集建设，助力 AI 发展，《数字中国建设 2025 年行动方案》印发，明确建设目标与重点任务，山东也发布数字强省建设 2025 年工作要点，积极推进地方数字建设。

【研究动态】本期研究动态聚焦数字法学多领域前沿课题。基础理论研究涵盖公司董事数据安全保障义务、大模型训练数据著作权规制等；个人信息保护领域围绕共同个人信息保护、数据处理规范依据等展开探讨；数据确权与流通研究涉及数据产权结构性分置、跨境流动规制等关键内容；人工智能

研究涵盖应用界限规制、价值链法律型塑等热点；平台治理、数字行政与司法、虚拟财产等领域也涌现诸多新成果，为数字法治建设筑牢理论根基。

【教研活动】人工智能时代的民事权益保护学术研讨会顺利召开；湖南师范大学与中国政法大学数据法治实验室开展考察交流；第二届网络与信息法学学科建设论坛聚焦学科发展；首届数字法治理论与实务对话暨《数字法治》创刊两周年座谈会深入探讨数字法治；联合国教科文组织东亚办事处启动“中日韩人工智能伦理治理项目”，促进区域研究合作。

【数字法评】

《敏感个人信息保护制度的解释性重构》，《中国法学》2025 年第 2 期，作者：丁晓东。

《智能时代的知识产权制度和理论发展》，《法制与社会发展》2025 年第 3 期，作者：张吉豫。

本期目录

数字法治大事件 3

第八届数字中国建设峰会分论坛“新一代人工智能研发与应用法治”在福州成功举办，“涉外法治大模型”正式发布 3

中央网信办等十部门印发《2025 年数字化绿色化协同转型发展工作要点》 5

中央网信办等四部门印发《2025 年提升全民数字素养与技能工作要点》 5

中央网信办等四部门印发《2025 年数字乡村发展工作要点》 6

人工智能气象应用服务办法 6

国家互联网信息办公室等七部门联合发布《终端设备直连卫星服务管理规定》 9

《终端设备直连卫星服务管理规定》答记者问 9

专家解读 | 规范终端设备直连卫星服务 完善空天信息发展治理体系 11

关于征求《全国一体化算力网 监测调度平台建设指南》标准草案意见的通知 12

国家数据局：分三类建设高质量数据集赋能 AI 发展 12

《数字中国建设 2025 年行动方案》近日印发 12

人民日报 | 《数字中国建设 2025 年行动方案》印发 不断壮大数字领域新质生产力 13

地方动态 | 山东数字强省建设领导小组办公室关于印发《数字强省建设 2025 年工作要点》

的通知 14

研究动态 19

基础理论 19

个人信息保护 23

数据确权与流通 25

人工智能 27

平台治理 30

数字行政与司法 31

虚拟财产 32

教研活动 34

会议 | 人工智能时代的民事权益保护学术研讨会顺利召开 34

湖南师范大学赴中国政法大学数据法治实验室考察交流 37

座谈交流会现场 37

第二届网络与信息法学学科建设论坛 38

首届数字法治理论与实务对话暨《数字法治》创刊两周年座谈会在沪举行 41

联合国教科文组织东亚办事处启动“中日韩人工智能伦理治理项目” 42

数字法评 44

敏感个人信息保护制度的解释性重构 44

智能时代的知识产权制度和理论发展 57

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 王黎焯 王昊 张清 张锦涛 朱恬馨

联系方式：RUCdigitallaw@163.com

本期排版：梁因格

数字法治大事件

导言：当今时代，数字技术已深度融入经济社会发展的肌理，重塑着人类的生产生活方式，在此背景下，数字法治建设成为保障数字时代有序发展的关键支柱。近期，一系列重磅政策法规接连落地，标志着我国数字法治建设进入全面深化的新阶段。第八届数字中国建设峰会分论坛成功举办，发布“涉外法治大模型”；中央网信办等十部门联合印发的《2025 年数字化绿色化协同转型发展工作要点》，锚定了经济社会发展全面绿色转型与数字技术创新应用的协同路径；四部门出台的《2025 年提升全民数字素养与技能工作要点》，致力于夯实数字社会的人才根基，推动数字红利全民共享，而《2025 年数字乡村发展工作要点》则聚焦乡村振兴，加速数字技术与农业农村的深度融合。与此同时，人工智能气象应用、终端设备直连卫星服务等新兴领域的法规政策相继出台，从顶层设计到落地细则，全方位覆盖数字法治建设的各个维度，不断完善数字领域治理体系，为数字中国建设提供坚实的法治保障，也为全球数字治理贡献中国智慧与中国方案。

第八届数字中国建设峰会分论坛

“新一代人工智能研发与应用法治”在福州成功举办，“涉外法治大模型”正式发布

4月30日，由中国人民大学主办，中国人民大学法学院、吉林大学法学院、京东集团承办的“新一代人工智能研发与应用法治分论坛”在福州海峡国际会展中心403会议室成功举办，并在论坛中发布了中国人民大学研发的“涉外法治大模型”。中国人民大学福州研究院、中国人民大学未来法治研究院、教育部哲学社会科学创新团队“新科技革命与未来法治创新团队”、吉林大学司法数据应用研究中心、教育部哲学社会科学创新团队“中国式现代化的法治轨道研究创新团队”作为支持单位为论坛提供支持。本论坛是数字中国建设峰会中唯一由法学学科承办的法治分论坛，体现了中国人民大学服务国家建设的责任担当。



第八届数字中国建设峰会分论坛现场

在中国人民大学法学院党委书记、副院长杜焕芳的主持下，本次论坛的开幕式顺利进行。中国人民大学党委常委、副校长支晓强，国家数据局副局长余英，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，福建省委常委、政法委书记石好勇在开幕式上致辞。



中国人民大学法学院党委书记、副院长杜焕芳

在成果发布环节，中国人民大学党委常委、副校长支晓强介绍了中国人民大学自主研发的“涉外法治大模型”，“涉外法治大模型”依托中国人民大学法学院和高瓴人工智能学院，组建跨学科研发团队，联合北京智源人工智能研究院进行研发。自2024年12月29日项目启动以来，法学院组织了14个部门法师生团队开展研究及数据标注，项目目前共收集了3万多部法律法规、超过4810亿词的法律类文本数据、30万条法律类指令数据，覆盖24个国家，并使用约1090亿词的数据进行了训练。涉外法治大模型深度融合法学理论与前沿技术，构建政产学研用协同创新生态，形成多语言、多法域、高可信的大模型架构，全面服务国家涉外法治重大战略。



中国人民大学党委常委、副校长支晓强

在以“新一代人工智能治理范式、理论与实践”为议题的主旨演讲环节，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**主持了该议题下的交流研讨。吉林大学哲学社会科学资深教授、中国法学会法学教育研究会会长、教育部社会科学委员会法学学部召集人**张文显**，中国人民大学法学院教授、中国法学会网络与信息法学研究会副会长、学术委员会主任**张新宝**，吉林大学党委常委、常务副校长、“中国式现代化的法治轨道研究创新团队”首席专家、中国法学会副会长**蔡立东**，全国政协委员、新大陆科技集团 CEO **王晶**，京东集团副总裁**胡焕刚**，中国移动集团有限公司法律监督事务部总经理、中国法学会网络与信息法学研究会副会长**于莽**，围绕这一议题发表主旨演讲。



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

在以“全球人工智能与数据治理及合作”为议题的主旨演讲环节，中国人民大学法学院教授、未来法治研究院副院长**王莹**主持了该议题下的交流研讨。中国人民大学法学院教授、未来法治研究院副院长**丁晓东**，上海交通大学区块链研究中心首

席科学家、中原工学院学术副校长、中国计算机学会区块链专委会荣誉主任、福州市区块链首席专家**斯雪明**，中国传媒大学计算机与网络空间安全学院院长**林卫国**，北京航空航天大学法学院副教授、北京航空航天大学网络空间国际治理研究基地副主任**赵精武**，吉林大学法学院副教授**齐英程**，南方电网能源发展研究院有限责任公司党委委员、总会计师、工会主席、总法律顾问、合规官**林志文**，抖音集团法律研究与合作负责人**丁道勤**，蚂蚁集团法务总监、中国法学会网络与信息法学研究会常务理事**李海英**，奇安信科技集团首席法律顾问**马兰**，围绕这一议题发表主旨演讲。



中国人民大学法学院教授、
未来法治研究院副院长 王莹

在“圆桌对话：人工智能应用及法治前瞻”环节，中国人民大学法学院教授、未来法治研究院副院长**丁晓东**主持了该议题下的交流研讨。中国人民大学法学院教授、未来法治研究院副院长**王莹**，中国人民大学法学院副教授**黄尹旭**，腾讯国内数据隐私合规负责人**张亚男**，美团数据法务总监、中国法学会网络与信息法学研究会理事**田喜清**，长春吉大正元信息技术股份有限公司副总裁**田景成**，万法智能 CEO **周正**，长春嘉诚信息技术股份有限公司副总裁**崔放**，北京盈科律师事务所福建区管委会主任**施鲜锋**，聚法科技（长春）有限公司总经理**侯德斌**，围绕多个问题进行了交流研讨。



圆桌对话现场

随着各个单元会议讨论的圆满落幕，本次论坛也缓缓步入了尾声。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对本次论坛进行了总结，并感谢大家的到来，期待下次再会。

中央网信办等十部门印发《2025年数字化绿色化协同转型发展工作要点》

原载：“网信中国”微信公众号

近日，中央网信办、国家发展改革委、工业和信息化部、自然资源部、生态环境部、住房城乡建设部、交通运输部、农业农村部、市场监管总局、国家能源局联合印发《2025年数字化绿色化协同转型发展工作要点》（以下简称《工作要点》）。《工作要点》要求，坚持以习近平新时代中国特色社会主义思想特别是习近平生态文明思想、习近平总书记关于网络强国的重要思想为指导，全面贯彻落实党的二十大和二十届二中、三中全会精神，完整准确全面贯彻新发展理念，聚焦经济转型升级、实现高质量发展的关键环节，健全数字化绿色化协同转型发展工作机制，推动新兴领域能效提升，积极运用数字技术、绿色技术改造提升传统产业，发挥绿色化转型对数字产业的带动作用，为加快建设网络强国、美丽中国提供坚实支撑。

《工作要点》部署了4个方面22项重点任务。一是推动数字产业绿色低碳发展。包括推动数据中心绿色化转型、推动基站绿色化运行、推进电子信

息产品绿色制造和使用、引导数字科技领先企业零碳发展。二是加快数字技术赋能绿色化转型。包括推动数字技术赋能电力、采矿、冶金、石化、交通物流、建筑、城市运行、现代农业等8个领域绿色化转型以及推动数字技术赋能生态环境治理、打造数字化绿色化协同转型发展试点示范。三是发挥绿色化转型对数字产业的带动作用。包括升级数字化绿色化基础设施、加快数字化绿色化融合创新、建设数字化绿色化产业体系、培养数字化绿色化复合人才。四是加强统筹协调和整体推进。包括加强组织领导、完善法规政策、深化国际合作、加强宣传引导。

中央网信办等四部门印发《2025年提升全民数字素养与技能工作要点》

原载：“网信中国”微信公众号

近日，中央网信办、教育部、工业和信息化部、人力资源社会保障部联合印发《2025年提升全民数字素养与技能工作要点》（以下简称《工作要点》）。

《工作要点》指出，要坚持以习近平新时代中国特色社会主义思想为指导，全面贯彻落实党的二十大和二十届二中、三中全会精神，进一步健全数字人才培育体系，拓展数字经济增长空间，构建普惠包容数字社会，打造智慧便捷数字生活，营造安全有序数字环境，完善协同联动工作格局，不断夯实新质生产力发展的人力资源基础，助力我国人口高质量发展。

《工作要点》明确了工作目标：到2025年底，我国全民数字素养与技能发展水平再上新台阶，数字素养与技能培育体系基本建成，数字资源供给能力显著增强，数字人才队伍进一步壮大，劳动者数字工作能力明显提高，群体间数字技能鸿沟不断缩小，数字发展环境更加普惠包容，数字生活智慧便捷，网络空间安全有序，数字法治道德伦理水平持续提升。

《工作要点》部署了6个方面16项重点任务。

一是健全数字人才培育体系，包括培养复合型人工智能人才、完善高水平人才培育体系、壮大应用型技能人才队伍、增强劳动者数字工作能力。二是拓展数字经济增长空间，包括释放数字消费潜力、激发企业数字动能。三是构建普惠包容数字社会，包括推进数字助老助残行动、促进教学资源开放共享、实施数字公益志愿项目。四是打造智慧便捷数字生活，包括强化人工智能应用赋能、丰富新型数字应用场景。五是营造安全有序数字环境，包括健全人工智能治理机制、强化法治道德规范意识、筑牢网络安全防护屏障。六是完善协同联动工作格局，包括深化多方协作机制、加强国际交流合作。

中央网信办等四部门印发《2025年数字乡村发展工作要点》

原载：“网信中国”微信公众号

近日，中央网信办、农业农村部、国家发展改革委、工业和信息化部联合印发《2025年数字乡村发展工作要点》（以下简称《工作要点》）。《工作要点》要求，深入贯彻落实习近平总书记关于“三农”工作的重要论述和重要指示精神，全面贯彻落党二十届三中全会精神和中央经济工作会议、中央农村工作会议精神，按照《中共中央 国务院关于进一步深化农村改革 扎实推进乡村全面振兴的意见》的部署要求，深入实施《数字乡村发展战略纲要》，坚持学习运用“千万工程”经验，坚持发挥信息化驱动引领作用，锚定强农惠农富农任务目标，着力推动农业增效益、农村增活力、农民增收入，为加快建设网络强国、推进乡村全面振兴提供坚实支撑。

《工作要点》明确了工作目标：到2025年底，数字乡村发展“十四五”圆满收官。数字技术在确保国家粮食安全、确保不发生规模性返贫致贫中的作用更加彰显。全国行政村5G通达率超过90%，农村地区互联网普及率稳步提升，农业生产信息化率进一步提升，农产品网络零售额持续稳定增长，乡村数字治理效能、信息服务水平不断增强，数字技术加速推动城乡差距缩小、促进城乡融合发展。

《工作要点》部署了9个方面26项重点任务。

一是夯实数字乡村发展基础。包括进一步完善农村网络基础设施、加快农村基础设施数智化改造、有序推进涉农数据资源集成共享。二是有力支撑守牢“两条底线”。包括完善粮食安全数字化支撑保障、强化防止返贫致贫网络帮扶举措。三是加快推进智慧农业发展。包括促进智慧农业技术装备创新应用、提升农业全产业链数字化水平。四是壮大乡村新产业新业态。包括推动农村电商高质量发展、因地制宜推动农文旅融合发展、运用数字技术促进农民就业增收。五是繁荣发展乡村数字文化。包括推进乡村文化文物资源数字化、加大乡村公共文化服务数字化供给。六是提升乡村数字治理效能。包括持续推进农村“三务”信息化建设、提升农村社会治理数字化水平、增强农村智慧应急管理能力。七是深化乡村数字普惠服务。包括持续提升乡村教育数字化水平、持续推进乡村数字健康发展、持续深化农村数字普惠金融服务、强化农村特殊人群信息服务保障。八是推进智慧美丽乡村建设。包括深化农村人居环境整治数字化应用、提升农村生态环境保护监管效能。九是统筹推进数字乡村建设。包括加强数字乡村跨部门跨层级协同联动、实施数字乡村强农惠农富农专项行动、完善数字乡村多元化投入保障机制、多措并举培育壮大数字乡村人才队伍、营造数字乡村发展良好环境。

人工智能气象应用服务办法

原载：“网信中国”微信公众号

中国气象局

国家互联网信息办公室令

第45号

《人工智能气象应用服务办法》已经2025年3月4日中国气象局第1次局务会议审议通过，并经国家互联网信息办公室同意，现予公布，自2025年6月1日起施行。

中国气象局局长 陈振林

国家互联网信息办公室主任 庄荣文

2025年4月23日

人工智能气象应用服务办法

第一章 总 则

第一条 为了鼓励和促进人工智能气象应用服务健康有序发展,规范人工智能气象应用服务,建立人工智能气象应用服务秩序,根据《中华人民共和国气象法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《网络数据安全管理条例》等有关法律法规的规定,结合气象行业实际,制定本办法。

第二条 在中华人民共和国领域和中华人民共和国管辖的其他海域利用人工智能技术开展气象应用服务的,适用本办法。

人工智能气象应用服务提供者(以下简称提供者),是指利用人工智能技术提供气象应用服务的公民、法人和其他组织。

第三条 发展人工智能气象应用,应当坚持总体国家安全观,统筹发展和安全,坚持促进创新和依法治理相结合,对人工智能气象应用服务实行包容审慎和分类分级监管。

提供人工智能气象应用服务,应当遵守法律、行政法规,尊重社会公德和伦理道德,遵循社会主义核心价值观,尊重知识产权,不得生成危害国家安全和利益以及虚假有害信息等法律、行政法规禁止的内容。

第四条 国务院气象主管机构负责指导、监督和管理全国人工智能气象应用服务工作,建立人工智能气象应用服务领域的工作协调机制。国家网信部门在职责范围内依法负责有关行政管理工作。

省、自治区、直辖市气象主管机构在上级气象主管机构和本级人民政府的领导下,负责监督和管理本行政区域内人工智能气象应用服务工作。地方网信部门在职责范围内依法负责本行政区域内有关行政管理工作。

第五条 鼓励提供者加入气象行业组织。气象行业组织应当加强行业自律,推广应用先进技术,组织开展人员培训,提升人工智能气象应用服务行业整体水平。

第六条 国务院气象主管机构应当参与国际气象领域人工智能应用服务的发展和治理,积极开

展平等互利的国际合作与交流,推动参与人工智能气象应用服务相关国际规则、标准的制定。

第二章 支持与促进

第七条 气象主管机构应当加强人工智能与气象监测预警、预报预测、数值预报等领域深度融合应用,推进人工智能气象数据、算法和算力深度发展。

气象主管机构应当推动人工智能在旅游、能源、交通、金融等气象服务领域的推广应用,构建人工智能气象应用服务场景。

第八条 国务院气象主管机构建设气象领域人工智能基础数据库和专题数据集,依法推动数据要素分类分级开放共享和流通。

国务院气象主管机构应当为进入开放共享和流通环节的数据要素匹配气象数据身份标识。气象数据身份标识应当包含气象数据来源、提供者、提供内容、被提供者、使用期限、使用范围等基本信息。

第九条 国务院气象主管机构按需推动人工智能气象应用服务领域的算力基础设施建设,鼓励和支持人工智能气象应用服务领域的算法模型创新,加快面向应用服务的算法模型研发与推广。

第十条 气象主管机构建立健全与科研院所、高等院校、企业之间的对接交流平台,加强人工智能气象应用服务领域的产学研用深度融合,构建人工智能气象应用服务协同创新机制。

第十一条 国务院气象主管机构建立完善人工智能气象应用服务的成果转化机制,健全人工智能气象应用服务领域的知识产权保护机制,依法保护人工智能气象应用服务软件作品、商业秘密等知识产权。

第十二条 气象主管机构联合科研院所、高等院校、企业共同建设人工智能气象应用服务人才实训基地,完善人才的评价与奖励机制,优化人工智能气象应用服务人才发展环境。

第十三条 国务院气象主管机构推动人工智能气象应用服务相关标准建设,鼓励和支持提供者、高等院校、科研机构、企业和其他组织参与标准制

定。

第十四条 国务院气象主管机构建立人工智能气象应用算法和模型的质量评估机制，开展人工智能气象应用示范，推动人工智能在气象业务领域的转化、准入和应用，鼓励人工智能气象服务的应用场景开放。

第三章 应用服务规范

第十五条 从事气象信息服务活动的提供者中的法人和其他组织应当根据《气象信息服务管理办法》的规定，向其营业执照注册地的省、自治区、直辖市气象主管机构备案，并接受其监督管理。

提供具有舆论属性或者社会动员能力的人工智能气象应用服务的，应当按照国家有关规定开展算法备案和安全评估。

第十六条 提供者应当通过合法渠道获取标注相应气象数据身份标识的气象数据，不得窃取或者以其他非法方式获取气象数据。

提供者应当按照国家有关规定添加人工智能生成合成内容标识，确保标识的可读性和安全性，建立信息溯源机制。

提供者应当基于应用服务类型特点，采取有效措施，提升人工智能气象应用服务的透明度，提高应用服务内容的准确性和可靠性。

第十七条 提供者应当依法建立健全算法安全审核、网络安全、数据安全、信息发布审核等管理制度和技术措施，确保人工智能气象应用服务安全、稳定、持续。

提供者应当对人工智能气象应用服务进行全生命周期风险管理和控制，开展安全评估和质量评价，采取必要措施防控风险。

第十八条 提供者应当设置投诉举报入口，用户发现人工智能气象应用服务存在违法行为或者安全风险的，有权通过投诉举报入口反馈，提供者应当及时受理并处理。

第十九条 提供者不得向社会发布和传播非气象主管机构所属气象台站提供的公众气象预报、灾害性天气警报和气象灾害预警信号。

鼓励提供者研究形成的气象预报意见和结论

提供给气象主管机构所属气象台站制作气象预报时参考。

第四章 监督管理

第二十条 气象主管机构可以通过指导约谈等措施促进公民、法人和其他组织依法开展人工智能气象应用服务。

第二十一条 气象主管机构可以进入相关应用服务现场开展监督检查，有权要求提供者提供气象数据身份标识。气象主管机构工作人员对于履行职责中知悉的国家秘密、商业秘密、个人隐私和个人信息应当依法予以保密，不得泄露或者非法向他人提供。

第二十二条 气象主管机构会同网信等有关部门开展人工智能气象应用服务领域的数据安全监管。

发现数据处理活动存在较大安全风险的，有关气象主管机构依法对有关公民、法人和其他组织进行约谈，并要求有关公民、法人和其他组织采取措施进行整改，消除隐患。

第二十三条 人工智能气象应用服务中涉及数据出境的，应当符合法律、行政法规和国家网信部门的有关规定。

人工智能气象应用服务中涉及国家安全、国家秘密的，应当遵守国家安全和保密的法律、法规、规章和有关规定。

第二十四条 任何组织和个人发现违反本办法的行为，可以向气象主管机构投诉、举报。

第二十五条 人工智能气象应用服务提供者初次违法且危害后果轻微并及时改正的，可以不予行政处罚。

第二十六条 违反本办法规定，有下列行为之一的，由有关气象主管机构依据职责责令改正，给予警告，可以处五万元以下的罚款：

（一）非法向社会发布公众气象预报、灾害性天气警报、气象灾害预警信号的；

（二）传播通过非法渠道获取的灾害性天气信息和气象灾害灾情的。

第二十七条 有关主管部门及其工作人员不

依法履行本办法规定的监督检查职责的，由其上级行政机关责令改正，依法给予处分；构成犯罪的，依法追究刑事责任。

第二十八条 气象主管机构、网信等有关主管部门发现人工智能气象应用服务存在其他违法行为的，在职责范围内依照相关法律法规的规定予以处理。

第五章 附 则

第二十九条 本办法自2025年6月1日起施行。

国家互联网信息办公室等七部门联合发布《终端设备直连卫星服务管理规定》

原载：“网信中国”微信公众号

近日，国家互联网信息办公室、国家发展改革委、工业和信息化部、公安部、海关总署、市场监管总局、广电总局联合发布《终端设备直连卫星服务管理规定》（以下简称《规定》），自2025年6月1日起施行。国家互联网信息办公室有关负责人表示，出台《规定》，旨在落实《网络安全法》、《数据安全法》、《电信条例》等法律法规的规定，促进和规范终端设备直连卫星服务健康发展，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益。

近年来，终端设备直连卫星已成为全球移动通信领域发展热点和趋势，产品和服务加快普及，受到社会各界广泛关注。《规定》对终端设备直连卫星服务技术产业发展与促进、设备设施与服务管理、监督管理与法律责任等作出了规定，为终端设备直连卫星服务管理工作提供了具体指引。

《规定》明确，向中华人民共和国境内提供终端设备直连卫星服务，在中华人民共和国境内使用终端设备直连卫星服务，以及生产、组装、提供和销售支持中华人民共和国境内直连卫星服务的终端设备的适用本规定。提出终端设备直连卫星服务管理坚持发展和安全并重、促进创新和依法治理相

结合的原则。

《规定》提出，支持终端设备直连卫星技术研究、卫星通信与地面移动通信融合发展，探索技术融合新应用新业态，构建系统完备的产业体系。鼓励通过终端设备直连卫星服务提高我国网络覆盖水平，促进其在防灾减灾救灾、安全生产、野外作业和搜寻救援等领域应用，支持相关数据依法开发利用，鼓励平等互利开展国际交流与合作。

《规定》要求，向境内提供终端设备直连卫星服务，终端设备接入境内公用电信网和在境内使用无线电频率的，应当依照相关规定取得相应许可和核准。相关基础设施建设活动要符合相关法律法规、主管部门有关规定和国家标准的强制性要求。

《终端设备直连卫星服务管理规定》答记者问

原载：“网信中国”微信公众号

近日，国家互联网信息办公室、国家发展改革委、工业和信息化部、公安部、海关总署、市场监管总局、广电总局联合发布了《终端设备直连卫星服务管理规定》（以下简称《规定》）。国家互联网信息办公室有关负责人就《规定》相关问题回答了记者提问。

问：请简要介绍《规定》出台的背景？

答：当前，终端设备直连卫星已成为全球移动通信领域发展热点和趋势，产品和服务加快普及，在促进经济社会发展、满足人民群众日益增长的通信需求方面具有广阔发展潜力。制定出台《规定》是落实《网络安全法》、《数据安全法》、《电信条例》等法律法规有关终端设备直连卫星服务管理的重要举措，目的是进一步促进和规范终端设备直连卫星服务健康发展，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益。

问：《规定》的适用范围是什么？

答：《规定》明确，向中华人民共和国境内提供终端设备直连卫星服务，在中华人民共和国境内使用终端设备直连卫星服务，以及生产、组装、提供和销售支持中华人民共和国境内直连卫星服务

的终端设备的,适用本规定。符合上述情形的境内外主体,均须遵守《规定》的要求。其中,终端设备是指能够接入卫星通信系统进行语音互通、文字收发或数据交换的民用手持终端、便携式终端、固定终端和航空器、船舶、车辆等载具上搭载的支持直连卫星服务的终端;终端设备直连卫星服务是指利用终端设备通过无线通信方式,不经过中转设备,直接连接通信卫星提供语音互通、文字收发或数据交换服务的活动。

问:《规定》的主要内容是什么?

答:《规定》主要对下列内容进行了规定:一是明确制定《规定》的目的是促进和规范终端设备直连卫星服务健康发展,国家坚持发展和安全并重、促进创新和依法治理相结合的原则,强调不得利用相关服务制作、复制、发布、传播含有法律、行政法规禁止内容的信息。二是明确对终端设备直连卫星技术研发、基础设施建设、融合创新、应用生态、标准研制、人才培养等方面的支持措施。三是强调向境内提供终端设备直连卫星服务等应依照《电信条例》《无线电管理条例》取得相关许可和核准,提供相关服务应履行网络安全、数据安全、违法信息处置等方面的义务。四是明确网信、发展改革、工业和信息化、公安、国家安全、海关、市场监管、新闻出版、广播电视等部门依据职责依法开展监督管理。

问:《规定》对促进终端设备直连卫星技术产业发展提出了哪些措施?

答:《规定》明确了多项促进终端设备直连卫星技术产业发展的措施:一是支持终端设备直连卫星技术研究,支持卫星通信与地面移动通信融合发展,积极推进终端设备直连卫星服务与新一代信息通信技术融合创新。二是鼓励依法依规开展基础设施建设和资源共享,鼓励通过终端设备直连卫星服务提高我国网络覆盖水平。三是建立和完善终端设备直连卫星服务标准体系,鼓励技术人才培养和教育培训。四是鼓励、支持、引导各类组织在产业发展中发挥作用,支持终端设备直连卫星服务典型应用宣传推广,支持相关数据依法开发利用,促进终

端设备直连卫星产业发展。五是鼓励平等互利开展终端设备直连卫星服务有关国际交流与合作,积极参与相关国际规则 and 标准制定。

问:《规定》对提供终端设备直连卫星服务明确了哪些要求?

答:根据《规定》,提供终端设备直连卫星服务要满足以下要求:一是要依照相关法律、行政法规的规定取得相关许可和核准,仅可连接在境内合法运营的卫星通信系统。涉及国际通信的,应当通过国务院电信主管部门批准设立的国际通信出入口进行。二是要依法确定服务资费标准,保障消费者合法权益,不得实施破坏市场秩序行为。三是要使用符合法律法规规定的通信业务资源,完成与境内相关无线电频率使用单位的协调,在应急通信保障时应按照电信主管部门要求优化资源配置、保障应急通信需求。四是要履行网络安全、数据安全和个人信息保护义务,采取必要措施保障服务安全稳定运行,防范终端设备直连卫星服务被用于实施违法犯罪活动。

问:《规定》对设备设施的管理明确了哪些要求?

答:《规定》对终端设备直连卫星服务相关的设备设施管理提出了明确要求:一是开展相关基础设施建设活动要符合相关法律法规、主管部门有关规定和国家标准的强制性要求,属于关键信息基础设施的,还应当遵守关键信息基础设施安全保护相关规定。二是规定任何个人和组织不得实施非法侵入、干扰、破坏终端设备直连卫星服务基础设施的活动。三是规定任何组织和个人不得违反国家有关规定,制作、销售、提供相关设备等,为他人通过终端设备直连卫星服务实施违法犯罪活动提供技术支持等帮助。

问:《规定》在安全保护方面作出哪些规定?

答:《规定》高度重视网络安全、数据安全和个人信息保护:一是要求终端设备直连卫星服务提供者履行网络安全、数据安全和个人信息保护义务,落实网络安全等级保护制度、通信网络安全防护制度、数据分类分级保护和商用密码应用安全性评估

登记制度，采取必要措施保障数据和个人信息安全。二是要求终端设备直连卫星服务提供者发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输，依法采取处置措施。三是要求终端设备直连卫星服务提供者履行电信网络诈骗风险防控义务，建立反电信网络诈骗内部控制机制和安全责任制度，开展涉诈风险安全评估。四是提供和使用终端设备直连卫星服务，涉及数据出境的，应当遵守法律、行政法规和国家有关规定。

问：相关部门如何开展监督管理？

答：《规定》对相关部门开展监督管理工作，以及违反《规定》的法律责任予以明确：一是明确网信、发展改革、工业和信息化、公安、国家安全、海关、市场监管、新闻出版、广播电视等部门依据职责开展监督管理，针对技术和应用特点，建立完善相适应的科学监管方式和工作机制。二是明确国家有关主管部门依据职责、按照相关规定开展监督检查，终端设备生产者、组装者、提供者、销售者和终端设备直连卫星服务提供者应当依法予以配合。三是明确提供和使用终端设备直连卫星服务以及生产、组装、提供、销售终端设备不符合相关法律、行政法规和《规定》的，有关主管部门应采取相应措施予以处置，并依法依规予以处理。

专家解读 | 规范终端设备直连卫星服务 完善空天信息发展治理体系

原载：“网信中国”微信公众号

为促进和规范终端设备直连卫星服务健康发展，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，近日，国家互联网信息办公室会同有关部门发布《终端设备直连卫星服务管理规定》（以下简称《规定》）（下同），对终端设备直连卫星服务作出系统性制度安排。作为我国首部针对终端设备直连卫星服务的专门规定，《规定》是统筹高质量发展与高水平安全的重要举措，对促进卫星互联网技术产业发展、保障技术规范应用、

维护公民合法权益具有重要意义。

一、《规定》坚持发展与安全并重的治理导向

统筹技术发展与安全可控是数字经济时代的核心命题。《规定》在总则中明确提出“坚持发展和安全并重、促进创新和依法治理相结合”的基本原则，体现了“以规范促发展、以安全保创新”的治理思路。一方面，《规定》设立“发展与促进”专章，从技术研发、设施建设、产业融合、应急应用等多个维度释放政策红利。明确支持卫星通信与地面移动通信融合发展，鼓励为地面通信网络信号无覆盖、弱覆盖和易中断区域等提供网络接入服务；推动卫星直连技术在防灾减灾救灾、应急救援等领域的深度应用。这些条款为低轨卫星组网、6G 空天地一体化等前沿技术落地提供了制度指引。另一方面，《规定》合理划定安全红线，有效防范网络安全、数据安全、个人信息泄露风险。如要求服务提供者履行网络安全、数据安全和个人信息保护义务，落实网络安全等级保护制度、通信网络安全防护制度、数据分类分级保护等制度，采取必要措施保障数据和个人信息安全；履行电信网络诈骗风险防控义务，建立反电信网络诈骗内部控制机制和安全责任制度等。

二、《规定》突出全链条合规的管理要求

针对终端设备直连卫星服务“设备—网络—数据”三位一体的技术特征，《规定》构建了覆盖终端设备准入、服务运营监管、数据安全防护的全链条合规管理体系，形成“源头可溯、过程可控、风险可防”的治理闭环。在终端设备管理方面，《规定》明确许可准入机制，要求服务提供者需取得相关许可和核准，仅可支持连接在境内合法运营的卫星通信系统；强化入境设备的海关申报与查验，阻断非法设备流通渠道；明确服务提供者需采取措施防范设备被用于违法犯罪活动。在服务运营监管方面，《规定》落实“实名制+反诈义务”，要求服务提供者核验用户真实身份并建立反诈风控机制；落实国家关于违法信息和不良信息传输的要求；要求服务提供者建立投诉举报机制，及时响应用户反馈。在数据安全保障方面，《规定》衔接《数据安全法》和

《个人信息保护法》，要求服务提供者落实数据分类分级、安全防护等制度，并进一步细化数据本地化存储规则。

三、《规定》构建统筹协调的监管体系

《规定》构建了多主体协同、分工明确的监管框架。一是明确监管职责边界。网信、发展改革、工业和信息化、公安、国家安全、海关、市场监管、新闻出版、广播电视等部门依据各自职责依法开展监督管理，强调国家有关主管部门针对终端设备直连卫星服务技术特点以及在有关行业和领域的服务应用，应建立完善相适应的科学监管方式。二是构建监管协同机制。明确国家网信部门会同有关主管部门建立健全信息共享、会商通报、联合执法、信息公开等工作机制，形成了贯穿事前、事中、事后全流程的监管工作协作体系。三是确立监管实施路径。建立安全评估机制，具有舆论属性或社会动员能力或开通终端设备直连卫星服务时需要进行安全评估；对不符合法律法规的服务和设备，通知有关机构采取技术措施予以处置；监管部门依法开展监督检查，终端设备生产者和服务提供者依法配合。

关于征求《全国一体化算力网 监测调度平台建设指南》标准草案意见的通知

原载：“国家数据局”微信公众号

各有关单位：

为贯彻落实《国家数据标准体系建设指南》《国家数据基础设施建设指引》等文件要求，加快推进全国一体化算力网建设，全国数据标准化技术委员会形成了《全国一体化算力网 监测调度平台建设指南》标准草案。现面向社会征求意见，相关意见请于2025年5月25日前反馈。

联系人：

杨韬手机：13488793861

邮箱：yangtao@nitsrc.cn

许紫媛手机：15901508962

邮箱：xuziyuan@cesi.cn

全国数据标准化技术委员会秘书处

2025年4月25日

国家数据局：分三类建设高质量数据集赋能 AI 发展

原载：“国家数据局”微信公众号

数据是训练 AI 能力的“原料”之一。在第八届数字中国建设峰会 29 日举行的“高质量数据集和数据标注”主题交流活动中，由国家数据局指导的全国数据标准化技术委员会提出，将强化标准引领，分三类建设高质量数据集。

一类为“通识数据集”，包含面向社会公众、无需专业背景即可理解的通用知识，主要用于支撑通用模型落地应用。

一类为“行业通识数据集”，包含面向行业从业人员、需要一定专业背景才能理解的行业领域通用知识，主要用于支撑行业模型落地应用。

一类为“行业专识数据集”，包含面向特定业务场景相关人员、需要较深的专业背景才能理解的行业领域专业知识，主要用于支撑业务场景模型落地应用。

简单举例，互联网百科、问答等为“通识数据集”；行业研究机构报告等为“行业通识数据集”；医院科室特定疾病病例等为“行业专识数据集”。国家数据局相关负责人表示，从发展趋势来看，人工智能模型对数据集的需求正从“通用知识”向“专业知识”延伸拓展，经过专家精细化标注的数据集已成为 AI 价值实现过程中不可或缺的基石，下一步将积极引导做好高质量数据集和数据标注建设工作，为人工智能技术创新和产业应用提供坚实的数据基础。

（总台央视记者 丁雅妮 刘柏煊）

《数字中国建设 2025 年行动方案》近日印发

原载：“国家数据局”微信公众号

近日，国家数据局综合司印发了《数字中国建设2025年行动方案》（以下简称《行动方案》），要求各地区结合实际认真贯彻落实。《行动方案》是国家数据局首次向地方数据管理部门印发的指导开展数字中国建设的文件。

《行动方案》强调，要坚持以习近平新时代中国特色社会主义思想为指导，全面加强党对数字中国建设的领导，深入贯彻党的二十大和二十届二中、三中全会精神，深入实施《数字中国建设整体布局规划》，以数据要素市场化配置改革为主线，加快培育全国一体化数据市场，因地制宜发展以数据为关键要素的数字经济，加快推进城市全域数字化转型，着力提升数字政务智能化水平，一体化推进数字基础设施扩容提质，持续深挖人工智能等数字技术应用新场景，以数字化驱动生产生活和社会治理方式变革，加快推动数字领域国际合作，全面提升数字中国建设水平。

《行动方案》提出，到2025年底，数字中国建设取得重要进展，数字领域新质生产力不断壮大，数字经济发展质量和效益大幅提升，数字经济核心产业增加值占国内生产总值比重超过10%，数据要素市场建设稳步推进，算力规模超过300EFLOPS，政务数字化智能化水平明显提升，数字文化建设跃上新台阶，数字社会精准化、普惠化、便捷化取得显著成效，数字生态文明建设取得积极进展，数字安全保障能力全面提升，数字治理体系更加完善。

《行动方案》部署了体制机制创新、地方品牌铸造、“人工智能+”、基础设施提升、数据产业培育、数字人才培养、数字化发展环境优化、数字赋能提升等8个方面的重大行动。

一是坚持数字中国建设工作“一盘棋”，完善数据工作央地政策协调机制。建立健全全方位多层次的统筹工作体系，加快完善地方数据管理机构的相关职能。

二是着力强基固本，发展彰显优势、体现特色的数字产品和数字产业。加快锻造数据领域“长板”，通过技术创新、功能改造、品牌建设等手段提升竞争力，形成品牌效应与集群效应。

三是深度挖掘人工智能应用场景，积极开展人工智能高质量数据集建设。着力发展智能网联新能源汽车、人工智能手机和电脑、智能机器人等新一代智能终端及智能制造装备。

四是加快推动物联网、工业互联网优化升级，深入实施“东数西算”工程，逐步实现各地区算力需求与国家枢纽节点算力资源高效供需匹配。

五是加强交通、医疗、金融、制造、农业等重点领域数据标注，建设行业高质量数据集。促进公共数据资源开发利用，推动公共数据“一本账”管理、“一平台”运营、“一体化”应用。布局建设数据产业集聚区，探索构建以数据要素驱动、数字技术赋能、数据平台支撑、产业融通发展、集群生态共建为主要特征的产业组织新形态。

六是培养技能型数字人才，深入推进产教融合，支持各地和有关行业举办数字职业技术技能竞赛活动。

七是持续优化营商环境，吸引更多优质数据企业和项目落地。畅通高校和企业数字人才双向流动渠道，将高层次数字人才纳入地方高级专家库。

八是逐年推出一批“高效办成一件事”重点事项，加强地方特色文化遗产的数字化保护与应用，全面推动数字技术和教育、医疗、养老、托幼等公共服务深度融合，加快生态环境、国土空间、水利电力、林业草原等领域的数据资源采集、存储与开发利用。进一步夯实城市全域数字化转型底座建设，完善城市运行和治理中枢功能。

《行动方案》强调，各地要将数字化发展摆在本地区工作重要位置，完善数据管理工作机制。各省级数据管理部门要充分发挥职能作用，会同相关部门建立统筹推进机制，明确责任分工，推动《行动方案》落地见效。各地要深入开展试点试验，及时评估试点试验效果，不断总结经验，加强宣传推广，充分发挥试点示范引领作用。

人民日报 | 《数字中国建设2025年行动方案》印发 不断壮大数字

领域新质生产力

原载：“国家数据局”微信公众号

本报北京5月16日电（记者王云杉）

国家数据局综合司近日印发了《数字中国建设2025年行动方案》。

方案提出，到2025年底，数字中国建设取得重要进展，数字领域新质生产力不断壮大，数字经济发展质量和效益大幅提升，数字经济核心产业增加值占国内生产总值比重超过10%，数据要素市场建设稳步推进，算力规模超过300百亿亿次/秒（EFLOPS），政务数字化智能化水平明显提升，数字文化建设跃上新台阶，数字社会精准化、普惠化、便捷化取得显著成效，数字生态文明建设取得积极进展，数字安全保障能力全面提升，数字治理体系更加完善。

方案部署了体制机制创新、地方品牌铸造、“人工智能+”、基础设施提升、数据产业培育、数字人才培养、数字化发展环境优化、数字赋能提升等8个方面的重大行动。

完善数据工作央地政策协调机制。建立健全全方位多层次的统筹工作体系，加快完善地方数据管理机构的相关职能。

发展彰显优势、体现特色的数字产品和数字产业。加快锻造数据领域“长板”，通过技术创新、功能改造、品牌建设等手段提升竞争力，形成品牌效应与集群效应。

深度挖掘人工智能应用场景，积极开展人工智能高质量数据集建设。着力发展智能网联新能源汽车、人工智能手机和电脑、智能机器人等新一代智能终端及智能制造装备。

加快推动物联网、工业互联网优化升级，深入实施“东数西算”工程，逐步实现各地区算力需求与国家枢纽节点算力资源高效供需匹配。

地方动态 | 山东数字强省建设领导小组办公室关于印发《数字

强省建设2025年工作要点》的通知

原载：“国家数据局”微信公众号

山东数字强省建设领导小组办公室

关于印发《数字强省建设2025年工作要点》的通知

数字强省办发〔2025〕1号

数字强省建设领导小组成员单位、省直有关部门（单位）：

《数字强省建设2025年工作要点》已经数字强省建设领导小组会议审议通过，现印发给你们，请结合实际认真抓好贯彻落实。

山东数字强省建设领导小组办公室

（山东省大数据局代章）

2025年4月7日

数字强省建设2025年工作要点

为全面贯彻落实党中央、国务院关于数字中国建设的决策部署，着力打造数字强省、智慧山东，加快培育新质生产力，赋能全省绿色低碳高质量发展，制定本工作要点。

一、加力释放数据要素价值

1. 强化数据资源管理。扎实开展国家数据要素综合试验区建设，研究制定数据产权、流通交易、收益分配等制度规范。开展数据资产全过程管理试点，推动公共资源交易、企业融资服务、医疗健康、医保结算等领域数据资产开发利用，引导企业开展数据资产入表。（责任单位：省委金融办、省发展改革委、省财政厅、省卫生健康委、省国资委、省医保局、省大数据局）

2. 推动数据高效流通。深入推进数据直达基层。深化政法、文旅、农业、能源、自然资源等领域跨地区、跨部门、跨层级数据共享利用，推动形成数据流通“绿色通道”。推动公共数据资源合规登记，开展公共数据资源授权运营，在交通、医疗健康、金融、海洋、生态环境、乡村振兴等领域探索更多应用场景。打造医疗健康、地理空间、海洋等行业数据流通交易平台，建立数据流通交易第三方专业

服务机构资源池。强化数据知识产权保护,引导重点行业、重要产业深入开展数据知识产权登记。(责任单位:省委政法委、省委金融办、省自然资源厅、省生态环境厅、省交通运输厅、省农业农村厅、省文化和旅游厅、省卫生健康委、省市场监管局、省大数据局、省能源局、省海洋局)

3. 深化数据创新应用。深入开展“数据要素×”行动,打造100个以上数字化典型应用场景。推动城市管理、交通运输、医疗健康、金融、海洋、生态环境、气象等领域数据产品研发。构建全省统一的医保数据资产管理制度和运行机制。推动低空数据开发利用,加快数字低空建设。(责任单位:省委金融办、省生态环境厅、省住房城乡建设厅、省交通运输厅、省卫生健康委、省医保局、省大数据局、省海洋局、省气象局)

二、加力培育数字经济发展新动能

4. 推动实数深度融合发展。深入推进数字技术与一二三产业深度融合,开展实数融合促进行动。推进智能工厂、工业互联网平台建设,规上工业企业数字化转型覆盖率达到94%左右,培育50个“晨星工厂”。加快省级产业大脑能力中心建设,争创国家中小企业数字化转型试点城市,培育5个左右省级中小企业数字化转型引导区。实施数字农业创新突破行动,遴选20个数字农业发展县,打造100个以上数字果园、智慧养殖、智慧渔场等应用场景,累计建成500个智慧农业应用基地。建好用好“齐鲁农云”、“齐鲁农超”等数字化平台。促进服务业数字化升级,加快数字金融、智慧物流、数字教育、数字医疗、数字文旅等业态发展。加快发展平台经济,建设一批“好品山东”电商基地。2025年,力争数字经济总量占全省GDP比重超过50%,数字经济核心产业增加值占比持续提升。(责任单位:省委金融办、省发展改革委、省教育厅、省工业和信息化厅、省交通运输厅、省农业农村厅、省商务厅、省文化和旅游厅、省卫生健康委、省大数据局)

5. 推动数字产业集聚发展。在集成电路、先进计算等领域培育一批数字产业集群。聚焦高端软件、集成电路、空天信息等数字产业“十大工程”领域,

推出一批数字产业重点项目。实施新一轮元宇宙、集成电路产业财政奖补政策,遴选一批示范效应强的元宇宙创新产品和应用场景。继续实施数据产业“三优两重”培育行动,优化大数据产业生态。(责任单位:省发展改革委、省工业和信息化厅、省大数据局)

6. 完善数字经济支撑体系。出台加快推进数字经济高质量发展、支持数据企业高质量发展、促进平台经济创新发展等政策措施。建立省级数字经济监测分析指标体系,常态化开展数字经济运行监测分析。谋划储备数字经济高质量发展项目,积极争取数字经济中央预算内投资专项资金和“两重”“两新”建设项目资金支持。开展省级数字经济创新发展试验区建设,建设一批数字经济集聚区。培育“领军型”数字经济企业100家。(责任单位:省发展改革委、省财政厅、省统计局、省大数据局)

三、加力推进数字政府效能创新

7. 提升政务服务效能。实施数字政府建设一体化综合改革,加快构建“1751”数字政府运行工作体系。深化“高效办成一件事”改革,打造一批企业和群众可感可及的“一件事”集成应用场景。全领域深化“无证明之省”建设,持续推进跨省电子证照共享,实现“免证办”“跨域办”。探索建设沿黄省(区)数据共享带,实现商事登记、政务服务、公积金业务等协同办理。升级“爱山东”政务服务平台,完善提升“鲁惠通”政策兑现平台,扩大政策“直达快享”覆盖面。(责任单位:省政府办公厅、省发展改革委、省大数据局)

8. 提升社会治理效能。深化数字法治体系建设,打造一批政法综治多跨场景应用。推广应用“齐鲁一表通”,减轻基层重复填表负担。建设地方金融治理平台,强化金融重点工作“一屏统揽”。加强监管数据与公共信用、企业信用公示数据共享,提高监管及时性、精准性。加快建设“鲁执法”平台,打造全省行政执法“一张网”,实现涉企检查、执法办案和执法监督全流程数字化运行。(责任单位:省委政法委、省委金融办、省政府办公厅、省发展改革委、省司法厅、省市场监管局、省大数据局)

9. 提升辅助决策效能。健全经济社会数据指标体系,完善经济社会数据库,为经济社会发展趋势研判、政策精准调控、民生精准保障等提供智能化支撑。强化重点行业经济运行监测分析,提升自然资源、工程建设、卫生健康、食品药品、特种设备、市场秩序、交通运输、应急管理、气象、消防管理等领域智能预警水平。深化“齐鲁智脑”建设,加强与部门平台、各市“城市大脑”互联互通,支撑经济运行、社会治理等领域应用场景建设。(责任单位:省发展改革委、省自然资源厅、省住房城乡建设厅、省交通运输厅、省卫生健康委、省应急厅、省市场监管局、省统计局、省大数据局、省气象局、省消防救援总队)

10. 提升机关运行效能。做强做优“山东通”,高效支撑机关内部办公、办会、办事。持续推动机关党建、组织人事、财务管理、机关事务、档案管理等内部共性业务跨部门跨层级统一规范办理。深入推进数字纪检监察体系建设,推动数字技术赋能正风反腐。(责任单位:省纪委监委机关、省委办公厅、省委组织部、省档案馆、省政府办公厅、省财政厅、省机关事务局、省大数据局)

11. 提升数智支撑能力。推进一体化数智平台建设,持续加强统一身份认证等共性能力支撑,建设跨层级、跨部门、跨地域的“多跨业务中台”,构建一体化基础大模型服务体系,推动各类数字资源共建、共享、共用。建设省级政务云网一体化监管平台,推进政务云网统筹监管,确保省级政务云可靠率达到99.99%。(责任单位:省大数据局)

四、加力推动数字社会转型升级

12. 提升公共服务数字化水平。开展社保、医保、医疗健康、教育、交通、公安等领域“一件事”场景建设。推行数智就业新模式,试点建设“数智就业”服务区。推进养老机构智慧化建设,打造30家智慧养老院。全面推广医疗卫生机构检查检验结果互通互认,加快商业健康保险就医费用一站式结算体系建设。深化国家智慧教育平台试点,构建齐鲁智慧教育公共服务平台。推动电商平台业态模式创新,持续丰富居家生活、体育休闲、交通出行等

数字生活场景。(责任单位:省教育厅、省公安厅、省民政厅、省人力资源社会保障厅、省交通运输厅、省商务厅、省卫生健康委、省体育局、省医保局、省大数据局)

13. 推进文化数字化发展。探索文化和科技深度融合协同创新机制,优化提升文化科技创新平台,加速文化科技创新成果转化。开展文化数据资源开发利用,建设山东文化数据库和齐鲁文化大模型,打造文化数字化展示应用场景。实施“齐鲁文化基因解码利用工程”,开展曲阜“三孔”、大运河、泰山等重要文化遗产数字化采集,完善“好客山东 云游齐鲁”智慧文旅平台,加快全省智慧图书馆建设。(责任单位:省委宣传部、省科技厅、省工业和信息化厅、省文化和旅游厅、省广电局、省大数据局)

14. 加快城市全域数字化转型。开展城市全域数字化转型“双百”行动。推进城市数据底座统建共用,开展城市基础设施生命线安全工程建设,完善提升城市运行管理服务平台功能,实现城市管理“一网统管”。推进城市“数字更新”,推动数字化与绿色化协同转型,打造宜居、韧性、智慧城市。推动济南、青岛都市圈联动发展、协同开放。深入推进智慧社区建设,建成不少于5000个智慧社区。高水平举办2025新型智慧城市发展创新大会。(责任单位:省发展改革委、省住房城乡建设厅、省大数据局)

15. 推进数字乡村建设。加速乡村信息基础设施优化升级,实现行政村地区“村村通千兆”,优化城乡数据流通和共享,加强乡村地区数字化人才培养,弥合城乡数字鸿沟,增强乡村数字化发展支撑。推动利用数字技术因地制宜发展现代农业和特色产业,打通农业生产、加工、流通、消费全环节,持续发展农产品电商,推动乡村产业链提档升级。推动以数字化赋能乡村教育、医疗、社保、法律、文化、气象等公共服务领域。(责任单位:省委网信办、省教育厅、省司法厅、省人力资源社会保障厅、省农业农村厅、省商务厅、省文化和旅游厅、省大数据局、省气象局、省通信管理局)

五、加力提高数字科技创新能力

16. 加强数字核心技术攻关。聚焦多模态智能、生成式智能、具身智能等前沿基础理论，布局 150 项以上基础研究项目。聚力突破大模型开发、先进芯片制造等“卡脖子”技术，提升人工智能国产化水平。加强农业传感器与专用芯片、农业核心算法、农业机器人、盐碱地遥感监测、极端灾害性天气监测预警等关键核心技术攻关。（责任单位：省发展改革委、省科技厅、省农业农村厅、省气象局）

17. 强化数字技术协同创新。加快构筑数字领域高能级创新平台体系，新培育一批国家企业技术中心和省企业技术中心、工程研究中心。推动高校、科研院所专利产业化，促进科技创新与产业发展的融通创新。优化科技型企业梯次培育政策体系，组织实施科技型中小企业创新能力提升工程，支持数字经济领域科技型企业深化产学研协同创新。（责任单位：省发展改革委、省科技厅、省工业和信息化厅、省市场监管局）

六、加力推进人工智能应用创新

18. 强化人工智能发展支撑。出台加快人工智能赋能重点领域高质量发展的推进方案。在人工智能领域加快布局新兴产业创新中心、制造业创新中心、技术创新中心、重点实验室等载体。高标准建设济南—青岛人工智能创新应用先导区、新一代人工智能创新发展试验区、海洋人工智能大模型产业集聚区。落实“算力券”奖补政策，引导存量数据中心部署支持人工智能的高质量算力。加快算法创新与应用，推动行业共性算法研发和供给，形成一批具有推广效应的算法产品和工具。推动工业、农业、交通运输、医疗健康、地理空间、应急管理、海洋、气象等行业领域打造高质量数据集，构建多模态中文语料数据库。（责任单位：省发展改革委、省科技厅、省工业和信息化厅、省自然资源厅、省交通运输厅、省农业农村厅、省卫生健康委、省应急厅、省大数据局、省海洋局、省气象局）

19. 加强人工智能创新应用。强化人工智能场景源头供给，推动政府治理、社会民生、产业升级等场景应开放尽开放，建立场景“机会与需求清单”

滚动发布机制，定期推介优秀场景与产品。深入推进“人工智能+”场景应用，围绕工业制造、现代海洋、医疗健康等领域开展标杆场景建设，鼓励省属重点企业、单位率先打造标杆场景。打造政策文件解读和精准推送、12345 市民热线智能办理、应急管理 etc 等人工智能政务应用场景，加快推进人工智能技术与化工、铝业、生物医药等重点产业和出行、家居、医疗、文旅、气象等民生领域深度融合。（责任单位：省发展改革委、省科技厅、省工业和信息化厅、省交通运输厅、省商务厅、省文化和旅游厅、省卫生健康委、省应急厅、省国资委、省大数据局、省海洋局、省气象局）

七、加力夯实数字底座支撑

20. 加快网络基础设施建设。部署 200G/400G 超大容量光传输系统，扩大全省互联网出口带宽。深化“双千兆”网络建设，推动重点场所、行政村、近海重点航路实现 5G 移动网络深度覆盖。支持 5G 工厂建设。加快建设青岛国际通信业务出入口局。（责任单位：省工业和信息化厅、省通信管理局）

21. 加快算力基础设施建设。优化算力基础设施布局，鼓励新建数据中心向枢纽节点集聚，引导各地按需布局各类边缘数据中心。建设全省一体化算力服务平台，推动重点算力中心全面纳管，打造全省算力一张网。力争 2025 年底全省总算力达到 12.5E，智算占比达到 35%。（责任单位：省发展改革委、省大数据局、省通信管理局）

22. 加快数据基础设施建设。开展国家数据流通利用基础设施试点，开展数场、数联网、隐私计算、区块链等数据流通利用基础设施建设，分类施策推进企业、行业、城市等可信数据空间建设和应用。打造 10 个左右省级数据基础设施“标杆型”“引领型”工程，推出一批数据基础设施建设应用试点示范案例。（责任单位：省大数据局）

23. 加快融合基础设施建设。建成交通运输智慧大脑，围绕智慧扩容、安全增效、产业融合、体制机制创新，推动公路水路交通运输基础设施数字化转型升级，打造北斗导航、车路协同等创新应用，提升路网运行监测预警和基础设施安全监测水平。

持续推进电网数字化智能化升级，加快公共充电基础设施建设，全省各类充电基础设施达到120万台以上。持续完善水利感知与监测网络，全省小型水库实现水位、雨量、图像信息自动采集。推进城市供水、排水、照明、燃气、热力等设施动态感知和智能化管理。完善立体气象智能感知与监测网络，面向多领域开展气象人工智能应用，助力行业用户实现气象驱动的智能化升级。（责任单位：省住房城乡建设厅、省交通运输厅、省水利厅、省能源局、省气象局）

八、加力优化数字化发展环境

24. 完善法规标准。加快推进《山东省数字经济促进条例》《山东省数据条例》立法工作。高质量编制“十五五”数字强省建设规划，编制数字经济、数字政府、数据资源、数字社会、数据基础设施等5项专项规划和各行业领域内数字化发展规划。深化数字山东标准体系建设，制修订一批发展亟需的标准规范。（责任单位：省人大常委会法工委、省工业和信息化厅、省司法厅、省市场监管局、省大数据局等省直有关部门）

25. 强化数字安全。统筹推进数字安全体系建设，加强数据收集、存储、使用、加工、传输、提供等全过程安全监管。深化数字安全防护，开展重

点领域数据安全态势监测分析，提高联防联控能力。健全数据安全事件通报和应急处理机制，定期开展多部门联合演练。建立完善网络安全能力评估体系和实施指南，持续开展网络数据安全检查评估工作。

（责任单位：省委网信办、省大数据局等省直有关部门）

26. 壮大数字人才队伍。建设全省数字人才库，实施泰山人才工程，支持数字领域重点企业、重点平台引进急需紧缺人才。完善数字技术人才职称评价体系，支持业绩卓越、贡献突出的数字技术人才破格申报高级职称。举办数字工程师大赛、数字赋能高质量发展职工创新大赛。大力培育“数字工匠”，提升数字经济企业职工数字素养。（责任单位：省委组织部、省总工会、省发展改革委、省人力资源社会保障厅、省大数据局）

27. 营造良好氛围。举办数字强省宣传月等系列活动，积极推进数字化知识进企业、进机关、进社区、进乡村，提高全社会知晓度和参与度，营造全民主动参与、共建共享的良好氛围。及时总结数字强省建设典型经验做法，加大宣传力度，提高山东数字强省建设工作在全国的影响力。（责任单位：省委宣传部、省大数据局、省直有关部门）

（技术编辑：何芮）

研究动态



基础理论

1.论公司董事的数据安全保障义务（陈洪磊）

来源：《当代法学》2025年第2期

在数字经济时代，公司数据安全已经成为影响公司利益和公司可持续发展的重要因素之一。由位于公司治理中心位置的董事们负担数据安全保障义务，可以最大限度地降低数据安全风险治理成本。然而，我国数据治理体系呈现组织法逻辑的缺失、负担数据安全保障义务的主体不明以及对应责任的模糊，这导致我国并未续造出追究董事数据安全保障责任的司法与执法经验，难以实现数据安全风险的终局性消解。观察域外经验发现，董事对公司数据安全负有保障义务已成为数据治理的共识，这对我国具有重要的启示意义。首先，董事数据安全保障义务衍生于董事的信义义务，包括建置数据安全体系的义务、保障体系有效运行的义务、补救的义务、信息披露的义务以及推动公司建立匹配数据安全要求的董事会结构的义务，而且董事的数据安全保障义务与公司的数据安全保障义务并不等同；其次，对董事数据安全保障义务的审查应当配置较为严格的且体现差异的审查标准；最后，采纳

网络安全保险以及董事责任保险机制，在鼓励董事积极探索数据利用新模式与防范数据安全风险之间寻求平衡。

2.公共数据开发的边缘计算风险及其规制（姜漪）

来源：《东方法学》2025年第2期

边缘计算可以赋能公共数据开放供给端与政务应用端，还在开放中履行代理者、情景经理人和切割者等重要角色，引入该技术符合数据开发长远发展的底层逻辑。但是，边缘计算引入也存在一定的技术风险、治理问题与安全隐患。基于此，应当从技术标准与法律规范两个层面优化边缘计算技术在公共数据运营平台建构中的应用。在技术标准上致力于探索全面、精准、权威的标准体系，引入专门人工智能技术弥补技术不足，并明确边缘技术自身的话语界限。在法律规范上强调基础设施的组织与监管，构建数据保护的协调机制，充分发挥其在公共数据开发机制建设中的治理效能。

3.论大模型训练中使用数据的著作权规制路径（张伟君）

来源：《东方法学》2025年第2期

在人工智能大模型技术快速发展的背景下，训

练过程中使用受著作权保护的作品引发了著作权侵权争议。大模型训练中使用数据引发的著作权侵权纠纷,是我国和外国(特别是美国)法院需要共同应对的新问题。因为大模型生成的内容可能是对享有著作权的作品的抄袭或复制,所以能否依据合理使用规则豁免大模型训练中的著作权侵权责任存在不确定性,而“豁免训练端、管住生成端”是更为合理与可行的方案。只要针对性开展执法,并允许著作权人对生成端可能出现的个案涉嫌侵权内容进行有效维权,就可以完全豁免模型训练中使用作品的著作权侵权责任。这样既能满足大模型训练对海量数据的客观需求,又能实现其与保护著作权人利益之间的平衡,同时也不会对著作权人造成实质性损害。

4.元宇宙空间刑事风险与类型化规制(杨猛)

来源:《东方法学》2025年第2期

元宇宙空间刑事风险主要体现为空间权益的侵害风险。元宇宙空间权是以数据权利为基底而形成的类型化的权利束类集合,元宇宙空间权类型及其风险规制应以数据的权利属性作为划分依据。在具体的元宇宙空间场景中,可将数据三权分置的权利内容与数据相关法益相衔接,进而衍生出以不同权利内容为核心的元宇宙空间权:一是元宇宙虚拟房地产空间体现的持有权;二是元宇宙数字藏品知识产权空间体现的使用权;三是元宇宙金融交易空间体现的经营收益权。对以上权利内容的侵害也正是元宇宙空间刑事风险生成的逻辑基础。结合规范保护目的理论,可在类型化的规范范式下解释适用传统罪名,进而探究元宇宙空间刑事风险的规制路径。

5.元宇宙空间虚拟财物的孪生耦合与刑法解构(王魏)

来源:《东方法学》2025年第2期

技术嵌入使元宇宙虚拟物到虚拟财物的转化加速,价值、支配与流动性在助力虚拟“财物”摆脱中心化弊端的同时,也赋予虚拟物财产性表象。虚拟泛化加强了虚拟物与虚拟财物的孪生耦合,单

一路径已然无法消解虚拟“财物”的强复合性涉罪困局。在元宇宙统一度量衡阙如及共识瓦解下,内部秩序不能仅停留于镜像模仿和企图径直移植来促成标准的数字化蜕变。为了实现价值体系的跨场域联动,需在外部鉴定中结合技术嬗变、规范保护能力及必要性综合限缩虚拟财物入罪口径。凭借多元标准的回溯限定,能够在剥离元数据与虚拟物后更新财物认定模型,通过法益内容的分层解构完成财产型数据与虚拟型财产等内容的刑法考察,在超拟像样态中落实规范的分块协同。

6.新质生产力驱动下的法治范式转型——以DeepSeek为例(王涛)

来源:《东方法学》2025年第2期

新质生产力正以数字化、智能化、网络化为显著特征,深刻重塑着生产关系,传统法律体系开始受到系统性挑战。立足唯物史观,新质生产力对法治变革的影响深入至法律主体地位界定、权利客体范畴拓展、法律关系重构等多个维度,使传统法理范式面临全面革新。应对智能革命的挑战,法治现代化须实现三重转型:一是突破人类中心主义桎梏,构建人机协同的法律本体论;二是建立开放动态的规则体系,以前瞻立法、柔性规制回应技术迭代;三是推进法律形式与技术逻辑深度融合,促进制度创新、技术赋能与文化重塑协同发展。以美国对中国的DeepSeek大模型实施技术遏制措施为研究样本,立足“技术—制度”互构的分析框架,通过“理念—规则—实践”三个维度的系统考察,剖析新质生产力语境下法治变革的理念重塑,并提出制度重构的路径。

7.数据要素赋能新质生产力的法治展开(房慧颖)

来源:《东方法学》2025年第2期

数据要素赋能新质生产力的基础是数据要素参与市场资源配置,科学的数据监管机制是数据要素高效参与市场化配置的法治保障。但是,目前的数据要素监管机制,存在包容性监管立场缺位、单向度监管模式主导、监管措施滞后性等缺陷,严重阻碍了数据要素在推动新质生产力生成中作用的

发挥。为克服前述缺陷,应当在法治框架下,以包容审慎的监管立场确立新型监管制度供给的基本框架;由单向度主导的监管模式转向协同监管体系,提升监管质效;创新适应监管需求的监管措施,凝聚多元监管工具的监管合力。通过以上措施,构建规范性与灵活性兼备且具有可操作性的数据要素监管机制,从而促进以数据要素为核心的生产力的转型与创新。

8.数字化背景下公共数据的刑法保护(苏永生)

来源:《法商研究》2025年第2期

数字化从广度和深度上大幅提升了公共数据的价值,形成了值得刑法保护的公共数据法益。我国现行刑法虽然为公共数据提供了一定程度的保护,但是保护的专门性、完整性和体系性明显不足。应对关涉国家安全的数据予以绝对保护,对关涉其他国家利益和社会公共利益的数据予以相对保护,并采用多元保护、专门保护、附带性保护相结合的保护模式,在危害国家利益和社会公共利益的犯罪中增设危害公共数据犯罪。应将危害公共数据犯罪的行为类型构造为毁坏公共数据、非法利用公共数据和不形成公共数据3类;将基本犯构造为对公共数据的实害犯,只能由故意构成,且属于微罪,配置1年有期徒刑以下刑罚,同时配置选处罚金;将加重犯构造为对国家利益或者社会公共利益的实害犯,罪过形式包括过失,根据不同的情况配置1年以上3年以下有期徒刑和3年以上7年以下有期徒刑两个刑罚幅度,同时配置并处罚金。

9.我国网络安全风险的保险治理困境与法治化纾解(徐浩宇)

来源:《法商研究》2025年第2期

数字经济时代,网络安全风险治理法治化是推进国家治理体系与治理能力现代化的必然要求。保险在分散网络安全风险的同时,也日益成为网络安全风险治理的重要工具。传统政府规制模式向社会自我规制模式的转换和保险社会治理功能的拓展,是网络安全风险保险治理的理论逻辑;法定义务契约化、规则制定私人化以及风险控制市场化三者间

的有机联结,共同勾勒出网络安全风险保险治理的实践逻辑。在网络安全风险保险治理场域中,保险治理制度框架缺失、规范供给不足以及风险信息互联互通不畅的现实困境,催生政府与市场相结合的二元协同治理结构,并成为网络安全风险保险治理的应然范式选择。未来在完善网络安全风险保险治理的制度框架、补足网络安全风险保险治理的规范体系以及强化网络安全风险保险治理的信息互联之外,还应健全网络安全风险保险治理的定期汇报、同行评议与容错机制,以期协同推进网络安全风险保险治理的法治化。

10.数据训练的著作权法分析(商建刚)

来源:《法学论坛》2025年第2期

利用他人作品进行数据训练,具有侵犯著作权的可能。采用合理使用制度进行规制,表面上阻断了数据训练的非法性,但实质上并未回应该行为是否落入著作权保护范围这一前提要件。作品的利用方式可分为表达性使用和非表达性使用,前者是对作品独创性表达的利用,后者是对作品技术上的利用。在事实层面上,数据训练设计的目的并非产生侵权的作品,数据训练过程仅对作品进行数据挖掘;在理论层面上,数据训练过程中对作品的利用并非是一种表达性使用,而是对原作品思想的利用。故此,数据训练实际上并未落入著作权的保护范围,本质上不是一种侵权行为。

11.数字经济时代民间金融犯罪违法性的三重检验标准之提倡(徐彰)

来源:《法学论坛》2025年第2期

我国现有的民间金融刑事治理模式在应对数字经济时代的民间金融犯罪时存在违法性判断上的缺陷,导致了数字民间金融行为必然构成犯罪的泛罪化现象。应对刑事风险的泛化必须对目前的违法性检验标准作出修正,以限缩民间金融犯罪圈。数字经济时代民间金融犯罪的违法性需要经过三重检验,首先检验行政违法性层面是否具备“违反国家法律法规”和“未经有关部门许可”,两者是耦合关系。其次检验刑事违法性层面是否侵害了投融

资双方资金安全法益，与前者呈阶层关系。通过违法性三重检验标准的提倡，严格限缩数字经济时代的民间金融犯罪圈，以排除仅具备形式构成要件而缺乏实质违法性的一般违法行为被评价为犯罪，提高金融领域全面深化改革的刑事保护效能。

12.集体主义数据治理的权利困境与法治出路——兼与邵六益教授商榷（朱孔武）

来源：《法制与社会发展》2025年第2期

“数据人民性”理论作为全球范围内集体主义数据治理学术探索的重要组成部分，源于对资本主义、新自由主义及基于个人权利的数据治理模式的深刻批判。该理论通过解构传统的财产权和基本权利框架，尝试通过集体主义路径重新配置数据的权属关系，旨在实现数据资源的公平分配与社会福祉。然而，这一理论模式在数据确权问题上存在显著局限，其将数据权等同于财产权的延伸，未能充分认识到个人信息保护作为独立公法权利的特性，并且忽视了个体在数据价值链中的独特地位与作用，倾向于将个体数据不加区分地纳入集体数据管理范畴。这种治理模式不仅未能有效应对集体行动困境，反而可能削弱数据治理的整体效能，抑制数字技术的创新活力，并对现有法治框架的稳定性与适应性构成潜在威胁。因此，数据治理的法理框架应秉持谦抑性、开放性与回应性原则，在技术与法律的协同发展中寻求平衡，既促进技术创新与经济发展，又确保个体数据权利的充分实现。

13.基于主观程序正义的技术性正当程序——我国算法治理的一种路径（冯健鹏）

来源：《法制与社会发展》2025年第2期

程序导向的治理路径是算法治理体系的重要组成部分。算法技术对传统的正当程序原则提出了挑战，技术性正当程序应运而生，但相关的制度建设仍有不足。主观程序正义关注人们对特定程序的感受及规律，有助于技术性正当程序的制度探索。从“算法厌恶”研究成果来看，“基于主观程序正义的技术性正当程序”这个提法是可行的，这种可行性具体包括理论结构、规范基础和研究基础三个方

面。以程序赋能为目标，“基于主观程序正义的技术性正当程序”的研究路径包括：研究“算法社会中的人”，研究当事人视角的算法应用场景，坚持研究的本土化和开放化。从“基于主观程序正义的技术性正当程序”出发，建立算法程序治理的各种制度，有助于推动我国算法治理体系的完善。

14.GDPR 会破坏互联网吗？公共数据异常的情况（Gareth Davies）

来源：International Data Privacy Law, Vol.14, Issue 4 (2024)

根据法院的理解，通用数据保护条例（GDPR）认为互联网搜索和在线阅读涉及数据处理。它还赋予那些数据被处理的人被告知这一点以及由谁完成的权利。从表面上看，阅读或在线搜索的简单行为——在纯粹的家庭环境之外——迫使读者与他们阅读的人取得联系，并告诉他们他们在做什么。本文表明，这种义务对数据主体的地位没有任何帮助，但对读者的权利提出了真正的风险。它考虑了如何解释 GDPR 以避免这种不良结果，并建议最好、最有效和最优雅的做法是法院为告知义务构建公共数据例外。

15.塑造真实性：数字产品护照如何塑造商标法的未来（Christophe Gösken）

来源：Journal of Intellectual Property Law & Practice, Vol.20, Issue 2 (2025)

在不断发展的时尚行业格局中，新兴监管框架（如数字产品护照（DPP）法规）、商标和关于真实性的叙述之间的相互作用对于塑造消费者的购买决策至关重要。本文探讨了营销、法律和技术如何影响未来的消费者行为，并重点介绍了可能出现的法律问题。通过文献综述、对当前 DPP 框架的分析、对近期市场举措的考察和案例研究，本文表明 DPP 可以降低商标在市场上的重要性。事实上，通过为消费者提供与真实性叙述相关的可验证的数字参考点，DPP 将降低商标对降低消费者搜索成本的重要性，从而挑战其经济基础。研究结果强调了技术对消费者选择的影响越来越大，商标专家需要

重新评估他们在制作品牌叙事中的作用，以及重新定义商标法基础的日益增长的需求。最终，本文旨在为重新调整商标保护以提供可作的见解，以促进更具创新性的时尚行业。

16.时尚 4.0 和新兴设计师：利用数据和 AI 推动全球供应链监管的创造力、创新和合规性（Eleanor Rockett, Mark Fenwick & Paulius Jurcys）

来源：Journal of Intellectual Property Law & Practice, Vol.20, Issue 2 (2025)

本文提出了关于时尚行业和监管的三个相互关联的论点。首先，本文提出 Bertola 和 Teunissen 的时尚 4.0 概念为理解当今全球时尚的组织提供了一个强大的框架。该模型强调了主导全球时尚行业的“智能工厂”、“智能网络”和“智能产品”的动态、分散和技术驱动特征。英国的当代例子说明了这一框架的价值。其次，本文认为，日益增长的监管要求对公司在运营和供应链的多个方面施加了不确定且代价高昂的合规义务。本文的讨论强调了与知识产权、价值链监控和 AI 监管相关的挑战的交汇。本文认为，中小型企业，尤其是新兴设计师，不成比例地受到这种监管负担的影响——本文称这种现象为当代合规的“悲剧性特征”。最后，本文探讨了在日益复杂的商业和监管环境中驾驭挑战如何需要部署越来越复杂的数字技术，尤其是 AI。本文概述了此类技术在整个时尚行业的几种潜在应用。总之，本文认为，在时尚 4.0 的背景下，了解不同监管计划之间的相互作用及其对行业利益相关者的影响正变得越来越重要，但越来越复杂和不透明。这就提出了一个难题，即法律和其他监管计划在时尚领域培养创新、可持续和对社会负责的商业实践方面的局限性。

个人信息保护

1.共同个人信息的理论基础与保护路径（赖成宇）

来源：《东方法学》2025年第2期

共同个人信息的存在具有客观必然性，其在经济价值和主体控制能力上与单个个人信息存在显

著差异。当前，共同个人信息侵权问题日益突出，而个人本位保护理论已无法提供全面有效的保护。因此，强化对共同个人信息的差异化保护显得尤为紧迫。保护共同个人信息，应遵循诚实信用、利益共享、禁止权利滥用以及合法、正当、必要等基本原则。构建共同个人信息保护规则，需从多方面入手：首先，明确信息主体的保管义务，限制其擅自处理行为；其次，增设个人信息处理者的去个人标识义务，实现保护共同个人信息的同时兼顾有效利用；最后，在不宜采用去个人标识化技术的场景下，建立可溯源的算法保护机制，实现共同个人信息处理过程可追溯、可监管。

2.论为订立或履行合同所必需的个人信息处理活动（程啸）

来源：《法律科学（西北政法大學學報）》2025年第2期

为订立或履行合同所必需是我国《个人信息保护法》规定的一类无需取得个人同意即可处理个人信息的情形。这一规定旨在协调个人信息权益的保护与正常的经济活动秩序之间的关系。个人作为一方当事人在订立合同过程中所作出的意思表示不同于个人对个人信息处理作出的同意，二者在告知义务、形式要件、能力要件、法律后果、效力判断及撤销或撤回等方面都有明显的差异。为提供产品或服务所必需被为订立或履行合同所必需包含，但为订立或履行合同所必需却不一定是为提供产品或服务所必需。在解释论上，我国法律应当将个人主动向处理者提出请求作为为订立合同所必需的一项限制要件。个人作为一方当事人的合同仅限于民事合同，不包括行政协议，但该合同必须是合法有效的。在认定处理者的个人信息处理活动是否为履行合同所必需时，应当综合考虑当事人的共同目的、合同的主要权利义务、合同的性质和类型等因素。同时，个人信息处理者应当采取对个人权益影响最小的个人信息处理方式。

3.个人信息处理规范依据的公私二分（李群涛）

来源：《法律科学（西北政法大學學報）》2025年第

2 期

一般认为,《个人信息保护法》第13条第1款中7项个人信息处理规范的适用主体包含公共部门与私营部门,即公私不分。然而,该款所借鉴的GDPR第6条第1款第1分款,虽表面上也似公私不分,但实质上是公私二分。公私二分的原理是:在大数据时代,公法活动、私法活动的进行均深度仰赖个人信息处理,故公法活动、私法活动的自由范围(“法无授权即禁止”和“法无禁止即自由”)决定着个人信息处理的自由范围,而有关个人信息处理的自由范围正是个人信息处理规范建立的依据。在公私二分思路下,应将第13条第1款解释为:公共部门仅能适用部分规范,总体上以禁止处理个人信息为原则,仅因履行法定职责、维护公共利益方可处理个人信息;私营部门则可适用全部规范,总体上以允许处理个人信息为原则,仅因违反三类禁止性规定方禁止其处理个人信息。如是,第13条第1款就能与数据要素流通利用的政策导向和时代需求相适应。

4.数字服务合同中个人数据对价化的规范构造(黄清新)

来源:《法学》2025年第3期

在数字服务合同中,消费者以个人数据换取数字服务的意思表示以及个人数据提供的给付对待性,构成个人数据对价化的理论基础。然而,个人数据对价化与个人数据处理同意的任意撤回之间存在价值抵牾,二者冲突缓和之路径在于确立数字服务合同与个人数据处理关系的双层构造,并厘定任意撤回同意的个人数据之类型。在个人数据对价化下,消费者撤回个人数据处理同意的债法效果应予修正。具言之,在义务履行层面,若消费者撤回个人数据处理之同意,则经营者仍可主张同时履行抗辩权,但存在适用边界;在损害赔偿层面,应类推适用《民法典》第1022条第2款,使消费者对撤回同意致经营者合理信赖落空所生损害承担赔偿责任,而且,基于个人信息保护与消费者倾斜保护的法政策考量,消费者撤回同意的损害赔偿范围宜

限定为信赖利益损失。

5.“两面扩张,三层转介”:数字法律行为的法理分析(许娟)

来源:《法学评论》2025年第2期

法学研究具有回应法现象并适时提炼法概念的积极功能。《个人信息保护法》中的个人信息处理行为的一部分有价值的数据集进入数据市场交易,通过算法算力改变着数据交易行为的内容和本质。数字法律行为是数据交易产权化行使过程中的个人信息行为法益保护,是对传统法律行为的“两面扩张”:一是由行为规范扩张至裁判规范,二是从利益衡量扩张到行为法益衡量。数字法律行为通过产权化行使的“三层转介”实现个人信息保护目标:一是保护转介,即从自由选择转介为获得保护;二是内容转介,即从商品交换转介为产权转移;三是属性转介,即私法转介为公法行为保护。

6.个人和消费者数据生态系统中的残疾推断问题(Christian J. Rozolis)

来源:Berkeley Technology Law Journal, Vol.40, Issue 1 (2025)

本文提出了一种新的消费者数据保护方法,其中包括对个人残障信息的专业保护。消费者数据生态系统由多个参与者组成,这些参与者在多个传输层中使用数据,从收集到聚合,再到应用数据驱动的见解。在这个数据系统中,残疾标志物隐含和明确地存在于数据中,这增加了数据驱动歧视的风险。本文首先探讨了消费者数据生态系统的三个层次,然后将残疾状况置于其中,将其视为与其他形式的个人身份信息不同的独特特征。由于残疾状况是一种可变特征,并且由于《美国残疾人法案》通过其“被视为”标准承认关联残疾歧视,因此应采用独特的数据监管方法来更好地防止数据驱动歧视的风险。本文接下来研究了现有的环环相扣的数据保护法,以及它们如何在商业数据生态系统的不同阶段进行干预,例如场馆门票销售、住房、信贷决策和刑事判决。最后,本文最后论述了新的监管方法来保护个人的残疾数据。基本调整,例如在信

贷决策中将残疾视为受保护的特征,或限制分发任何必须收集的残疾身份证明,是现有监管框架用于加强对残障人士的数据保护的简单方法。

7. 在自动决策系统中进行合理推断的权利,作为巴西及其他地区保护个人数据的基本权利的展开 (Eduardo Magrani, Paulo Rodrigo de Miranda)

来源: International Review of Law, Computers & Technology, Vol.39, Issue 1 (2025)

本文建议通过承认从数据保护的基本权利和人格自由发展原则中得出的合理推论权来扩大个人数据保护。使用基于档案的预测算法和相关性的自动化系统可能会产生负面后果,尤其是对泛化的区分或相关性不足。这些系统通常不考虑个人的独特性。文章强调,自动化系统中不完美的相关性通过破坏人格和信息自决的自由发展来威胁个人权利。承认合理推论的权利可以加强数据保护的客观维度,这对于防止歧视性推论至关重要。它还要求数据控制者证明实施此类系统的合理性。为了实现这一目标,该研究建议解释巴西第 13.079/2018 号数据保护法,称为“LGPD”,将合理推断权定位为数据控制者的行为指南。这种解释强调透明度、可理解性和问责制。承认这项权利旨在促进对责任原则的遵守,并确保处理和管理负面后果所需的透明度。

数据确权与流通

1.从“权能分离”到“权利分置”:数据产权结构性分置的法构造(王年)

来源:《比较法研究》2025年第2期

将政策中的数据产权理解为由数据持有、数据使用和数据经营等多个权能所构成的单一产权体系的学说,不仅不符合“淡化所有权,强调使用权”理念下所形成的避免数据专有和垄断的要求,更难以应对“数据共生与数据独占冲突”“人身利益与财产利益并存”“产权排他与数据共享悖论”等数据产权建构难题。数据产权是一个集合性概念,其上应该并且可以进行权利分解,从而形成“权利分置”

结构。这一结构是以数据处理者的数据持有权为核心,以数据来源者权和数据使用权为两翼,在数据生产和流通两大阶段渐次展开的数据产权“双阶二元结构”。这一结构的内在机理是数据来源者、数据处理者和数据使用者之间基于数据从生产到流通阶段“分散—聚合—分散”的形态变迁形成的“财产利益集散机制”。在此机制下,数据来源者权、数据持有权、数据使用权得以渐次形成和展开。数据处理者享有控制和利用数据,并排除他人干涉的数据持有权。数据来源者对由其贡献所生数据享有复制、访问和转移等公平使用权。数据使用者对经由流通取得的数据享有加工使用、对外经营以及获取收益等数据使用权。

2.我国数据跨境流动规制措施与 RCEP 服务贸易规则相符性及应对(宋俊荣)

来源:《当代法学》2025年第2期

对于影响服务贸易的数据跨境流动规制措施,RCEP 项下服务贸易规则的适用优先于数据跨境流动规则。判断我国数据跨境流动规制措施是否受制于 RCEP 服务贸易规则,需要具体考察我国在该措施所影响的服务部门和服务提供模式下是否已承担义务。在我国已承诺承担义务的情况下,我国数据跨境流动规制措施有可能违反 RCEP 服务贸易章的市场准入、国民待遇、最惠国待遇和当地存在条款,其是否符合 RCEP 服务贸易章一般例外条款的关键在于执法实践是否符合该条款前言要求。此外,我国针对关键信息基础设施运营者开展的数据出境安全评估活动符合 RCEP 安全例外条款。在国内层面,我国应从三个方面完善数据跨境流动规制措施以确保其与 RCEP 服务贸易规则的相符性。在国际层面,我国在未来 RCEP 负面清单的谈判中应力争给予数据跨境流动规制措施足够的关照。

3.论数据产权保护的范式转换:从“利益保障”到“行为许可”(刘政廷)

来源:《法律科学(西北政法大学学报)》2025年第2期

数据产权的“利益保障”范式是法学界关注的

重要命题。但该范式的理论分歧较大，主要原因在于数据产权保障方式无法聚焦某种具体利益，数据产权概念具有较强的抽象性和不确定性。相较于“利益保障”范式，“行为许可”范式能够修正数据产权的制度价值，明晰数据产权的法律属性，锚定数据产权的经济法定位。在“行为许可”范式的全新视角下，数据产权可被理解作为一种基于数据产业活动而生成的“行为许可权”，在“保护结构”“市场结构”和“强制结构”下衍生出不同的权利内容。借助“行为许可”范式与“数据二十条”的制度框架，我国数据产权的法治保障可以通过构建“三级行为许可机制”“行为许可监督机制”以及“行为许可保障机制”加以实现，进而推动我国数据产权理论和法律制度的发展。

4.数据确权的宪法之维（程迈）

来源：《法学家》2025年第2期

传统理论与制度在处理数据确权时出现了一定的应对乏力现象，这与数据作为法律权利客体表现出全新特性，在找寻数据确权方案时不同部门法间存在着一定的价值碰撞，以及传统理论和制度难以充分解决数据利益分配问题有关。这些难题的出现，为宪法理论与制度的进一步发展提供了良机。数据是一种社会化程度极高的新型生产要素，在设计可以促进这种数据生产要素获得充分利用的法制框架的过程中，宪法促进法制整体协调发展的功能也面临着新的挑战。在有中国特色的社会主义市场经济体制中，数据确权过程中还会涉及各级各类政府机关的自身利益，这也对宪法制度与理论提出了更高发展要求。数据确权问题同时涉及宪法中的一阶与二阶共识。数据确权中的不同立场都可以在宪法的一阶共识体系中找到支持，问题最终解决需要充分运用二阶共识，以平衡各利益相关方的诉求，最终构建出共同持有、促进数据采集利用的数据权利制度。

5.企业数据担保融资的法律适用（程乐）

来源：《法学家》2025年第2期

企业数据担保融资存在数据权利质押贷和数

据资产抵押贷款两条入法通道。数据权利质押贷是企业基于数据财产权的交换价值，换取银行融资贷款的一种方式。数据资产抵押贷款侧重数据的经济价值和流通性，以不转移占有的方式，兼顾抵押权人的受偿需求和抵押人的数据利用需求。数据担保应以登记为生效要件，目前可依托各数据交易平台的互认，实现权利公示和权属查询。数据担保融资贷款金额受数据现时价格 p ，担保总量 q ，担保率 α 的综合影响。鉴于 p 的波动性，数据估值应是该数据多个优先应用场景下的价值区间，并由估值机构提示数据价值波动风险。为了避免担保数据因时效而贬值，未来融资实践或可尝试数据动态质押的方式，允许出质人在质押期间利用数据并更新数据，以实现数据流通共享和财产担保的双赢。

6.论企业数据产品的质押：底层逻辑与制度构建（徐海燕）

来源：《法学论坛》2025年第2期

为充分挖掘数据产品的商业价值、推动全国统一数据要素大市场的繁荣与可持续发展，企业数据产品设定质押具有合法性与合理性。企业数据产品的财产价值具有客观性、可计量性、可控性与可转让性。建议《民法典》将数据产品权益上升为财产权利，并明确允许数据产品设定质权。企业数据产品的适格担保形式是权利质押，而非权利抵押。登记生效要件模式是企业数据产品质押登记的理想方案。建议抓紧制定《数据交易与质押登记法》，建立统一的数据产品确权、转让与质押登记制度。只要当事人未约定禁用条款且出质人继续使用数据产品不贬损质权的交换价值，就应允许出质人继续使用出质的数据产品。除非双方当事人有相反约定，出质人可转让或许可第三人使用出质的数据产品。为维护质权公信力，应确认质权人的事先知情权与嗣后追及权。若出质的数据产品价值因出质人在质押期间亲自使用或许可第三人使用而增值，增值部分应成为质押财产的组成部分。若出质人许可第三人使用出质的数据产品时导致数据产品市场竞争力降低并影响债权实现，质权人有权要求出质

人补充提供担保或将许可使用费提前偿债或提存。

7.数据权益之权能体系的再思考（阮神裕）

来源：《法学评论》2025年第2期

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

人工智能

1.人工智能应用的界限及其规制：以保护人的尊严为底线（黄文婷）

来源：《比较法研究》2025年第2期

人工智能应用带来了人类能在多大程度上容忍其改写自身主体性地位和价值的现实问题。人工智能应用应当以人的尊严为底线，然而，该底线面临着三重风险，即人类在物种层面的支配性、公民在社会层面的主体性以及个人在个体层面的自主性受到挑战。为保护人的尊严，应当绝对禁止将个人当成纯粹的手段伤害且不会对个人、社会和人类产生任何福祉的人工智能应用，相对禁止对人的尊

严产生风险但也会带来福祉的人工智能应用。在相对禁止的路径下，应当以人工智能应用侵犯人的尊严的风险程度划分不同的人工智能类型，同时采用比例原则进行比较权衡，以划定人工智能应用的界限。具体而言，法律应当严格规制带来重大风险的特定人工智能应用，合理规制带来有限风险的其他人工智能，同时法律有必要将保护人的尊严底线转化为应用者的主体性义务，并强调静态的合比例论证与动态的风险控制。

2.人工智能价值链的法律型塑（李润生）

来源：《东方法学》2025年第2期

人工智能价值链是对人工智能组织过程的科学描述，是人工智能立法的重要线索。相较于有形产品和传统软件，人工智能价值链是一个整体协作、双轮驱动、动态发展和不透明的组织过程，这决定了人工智能的法律规制应当遵循协作规制、全生命周期规制和集中明确规制的核心理念。人工智能价值链的制度建构包含三个主要步骤，即提炼法律身份、选定中心节点和分配法律义务，以通用模型提供者、应用系统提供者、应用系统部署者和受影响者四种法律身份搭建人工智能价值链的组织骨架。其中，通用模型提供者和应用系统提供者位处中心节点，应当担负关键职责，推动构建公平、稳定和可信的人工智能价值链，应用系统部署者和受影响者也应当担负与其功能定位相匹配的义务和职责。

3.人工智能时代科技伦理的专利法回应（刘鑫）

来源：《法商研究》2025年第2期

科学技术的迭代与革新带来诸多科技伦理难题，也使专利法面临相应的伦理挑战。在前人工智能时代，专利法为应对科技伦理挑战，形成了公序良俗原则与伦理审查规则相结合的基础性规范设计。在人工智能时代的新兴科技伦理挑战面前，专利伦理规范不可避免地会出现道德非议超越阐释限度及产业运营制约适用程度的制度失灵问题。从人工智能算法模型到人工智能生成发明，人工智能科技成果的不断涌现使专利法面临着前所未有的

科技伦理挑战，既包含专利客体范畴扩张的伦理难题，也涉及专利主体定位突破的伦理困境。专利法不仅要立足人工智能场景对公序良俗原则与伦理审查规则等基础性专利伦理规范展开法律释义，还要进一步聚焦人工智能科技伦理难题，以法律续造的形式，搭建规避人工智能算法模型专利保护中伦理风险、破解人工智能生成发明专利保护中伦理困境的规范体系。

4. 人机共驾接管失败时安全员的过失责任——从信赖原则的适用切入（杨宁）

来源：《法学家》2025年第2期

目前，人机共驾接管失败致死的案件备受瞩目，对于安全员虽未履行接管义务，但可否主张信赖原则而不承担过失责任，存在肯定论与否定论的争议。从肯定论看来，人机信任建立在人工智能可信任性的基础上——机器有自主性、能动性和以人类为中心的意向性，并偏重人类对机器的信任。对高度分工、高风险的人机信任适用信赖原则，是组织模式的一种延展，不会导致责任稀薄，更符合刑事责任性质，具备合理性。信赖原则例外否定过失责任时，以不同自动驾驶水平下安全员、自动驾驶系统和人机交互作为客观因素，可具体判断信赖的相当性。安全员没有履行接管义务的行为具有客观违法性，但当其合理信任自动驾驶系统能够执行预期功能时，不能具体预见结果的发生，由此信赖原则在责任阶段否定过失，发挥后端风险结果分配的作用。

5. 论生成式人工智能推进应用中的能源数据安全“分类分级治理体系”建构——基于国家大安全的审视（斜晓东）

来源：《法学论坛》2025年第2期

在能源领域GAI的推进应用中，鉴于能源数据的特殊性与GAI应用的叠加风险，能源数据安全已成关乎国家大安全的重要命题。面对所凸显的“能源数据安全与数据主权主张、数据隐私与共享发展背离、GAI迭代与安全防护性能显弱、数据跨境流动与国际协同冲突、算法黑箱与监管公开透明相

悖、责任主体模糊与义务交叉叠加”系列难题，须立足“安全与利益增进平衡”机理，依托“数据分类分级—适应性安全监管—责任衡平分配—数据跨境动态推进—协同共治网络搭建”五个维度，建构基于“分类分级”的能源数据安全治理体系，超越零和博弈，守护国家大安全，助力数字文明演进与现代科技对话中的治理新秩序重塑与人类命运共同体构建。

6. 人工智能、偏见和国家安全定性（Laurie N. Hobart）

来源：Berkeley Technology Law Journal, Vol.40, Issue 1 (2025)

人工智能（AI）是一种越来越多地用于搜索、排序和分析数据的工具，它有可能加剧政府在国家安全调查中根据民族和“种族”、国籍和宗教进行剖析的现有趋势。AI正在或可能用于国家安全刑事调查，情报、反间谍或反恐活动，观察名单做法，边境安全和移民调查和监控计划。本文概述了AI在国家安全调查中大规模复制人类偏见的方式。它认为，目前的判例法不足以保护公民权利和公民自由免受人工智能的歧视性使用。它讨论了根据第四修正案、平等保护、第一修正案和正当程序先例应对宪法挑战的潜在障碍；对Bivens索赔的限制；以及由保密、国家机密原则和国家安全背景下的一般司法尊重引起的问题。在解释当前判例法如何面对AI分析时危及民权和公民自由的同时，本文还为民权倡导者提供了在现状下进行诉讼的策略。首先，它认为1996年最高法院的Whren v. United States案通常将分析挑战限制在平等保护而不是第四修正案的主张上，不应适用于AI分析的情况。其次，它认为，根据平等保护法，人工智能偏见应被视为可起诉的差别处理，而不是不可起诉的差别影响。行政政策也不足以解决歧视性AI带来的潜在危害。本文讨论了三项行政政策的有用和有问题的方面：2023年司法部关于使用嫌疑人类别的执法指南；2020年人工智能道德框架，以及2023年人工智能行政命令及其实施备忘录。文章最后向国会、法院和政府检察官提出了建议，以防止人类和机器对国

家安全进行定性分析。

7.人类，太人类：考虑生成式大型语言模型中的自动化偏差（Irina Carnat）

来源：International Data Privacy Law, Vol.14, Issue 4 (2024)

本文研究了由于自动化偏见而导致潜在用户在决策过程中过度依赖生成式大型语言模型（LLM）输出所造成的问责差距，这种偏见受到拟人化和事实不正确文本生成现象（称为“幻觉”）的青睐。本文批评了提出人机协同解决方案的技术解决方案主义，认为从纯粹的技术角度解决“幻觉”问题可能会自相矛盾地加剧用户对算法输出的过度依赖，因为拟人化和自动化偏见。本文还批评了监管机构对人工监督的乐观态度，通过比较欧盟《人工智能法》第14条和欧盟《通用数据保护条例》中“有意义的”人工干预概念，质疑其是否足以有效解决自动化偏差问题。最后，本文提出了一个全面的社会技术框架，该框架整合了人为因素，促进人工智能扫盲，确保不同使用环境下的适当自动化水平，并通过设计实现认知强制功能设计。本文提醒人们不要过分强调人为监督是万能药，而是主张在整个人工智能系统的价值链上实施问责措施，以适当调整用户对生成式LLM的信任度。

8.大规模处理可公开访问的在线数据以训练大型语言模型的合法性（Taner Kuru）

来源：International Data Privacy Law, Vol.14, Issue 4 (2024)

随着大型语言模型的不可阻挡的崛起，使用可公开访问的在线数据训练它们的合法性开始受到质疑。本文以ChatGPT为例，在欧盟数据保护的背景下探讨了这个问题，以了解是否可以这些处理活动找到有效的法律依据。到目前为止，该讨论的重点是GDPR第6条第（1）款第（f）项，并询问OpenAI是否以及在多大程度上具有处理可公开访问的在线数据以训练ChatGPT的合法利益。但是，考虑到欧盟法院的相关判决，本文建议GDPR第9条应适用于这些处理活动。因此，本文研究了GDPR

第9条第（2）款中列出的例外情况，OpenAI可以依赖这些处理活动。因此，本文认为，虽然OpenAI实际上不可能获得并证明其可公开访问的个人数据用于训练ChatGPT的数据主体的明确同意，但数据主体明显公开的个人数据池，因此可用于训练大型语言模型似乎是有限的。考虑到OpenAI或其他开发人员目前没有提到只有如此有限数量的个人数据被用于训练他们的模型，本文呼吁所有利益相关者进行澄清。最后，本文推测了可能的前进方向，并概述了所有相关利益相关者的责任，以确保负责任地开发这些模型。

9.值得信赖的人工智能的监管沙盒——全球和拉丁美洲体验（Thiago Moraes）

来源：International Review of Law, Computers & Technology, Vol.39, Issue 1 (2025)

本文探讨了如何使用监管沙盒来促进值得信赖的人工智能（AI）系统的发展。该分析侧重于数据保护机构（DPA）的经验，他们一直在试验沙箱，以促进在AI系统中实施隐私设计原则。在整个书目研究中，本研究——（1）强调了国际AI监管框架中与隐私相关的元素；（2）探讨隐私设计（PbD）的概念及其一些策略、模式和技术，例如隐私增强技术（PET）；（3）反思监管沙盒的影响；（4）分析如何在AI监管框架的背景下讨论监管沙盒。虽然本研究带来了监管沙盒的全球视角，但它也通过介绍该地区举措的不同发展阶段，在拉丁美洲背景下进行了相关分析。本文的主要发现之一是，目前文献缺乏对如何在AI系统设计和治理的背景下使用设计隐私的分析。它还表明，监管沙盒可能能够整合PbD原则来促进可信AI的发展，尽管需要对此进行进一步研究。

10.版权和AI训练数据 - 透明度来拯救？（Adam Buick）

来源：Journal of Intellectual Property Law & Practice, Vol.20, Issue 3 (2025)

生成式人工智能（AI）模型必须在大量数据上进行训练，其中大部分数据由受版权保护的材料组

成。但是, AI 开发人员经常在未经权利人许可的情况下使用此类内容, 导致呼吁要求披露有关 AI 训练数据内容的信息。通过将此类要求纳入欧盟的 AI 法案, 这些要求已经取得了初步成功。本文认为, 仅靠这种透明度要求并不能将我们从如何最好地应对生成式 AI 对版权法构成的根本挑战的难题中解救出来。这是因为透明度要求的影响取决于现有的版权法; 如果这些不能充分解决生成式 AI 带来的挑战, 透明度将无法提供解决方案。《人工智能法案》的透明度要求就是一个例子, 这些要求明确旨在促进根据《数字单一市场指令中的版权》执行选择退出文本和数据挖掘的权利。由于透明度要求并未充分解决此选择退出的潜在缺陷, 因此它们不太可能为个人权利持有人的处境提供任何有意义的改进。因此, 透明度要求是在创新和保护权利持有人之间实现公平公正平衡的必要但不是充分的措施。因此, 政策制定者必须超越这些要求, 并考虑采取进一步行动来应对生成式 AI 给版权法带来的复杂挑战。

平台治理

1. 谁有权获得 POI 数据上的权益 (张韬略)

来源:《东方法学》2025 年第 2 期

“信息点”或“兴趣点”(POI)数据来源构成复杂, 法律属性也呈现多样性, 数字平台与平台内经营者之间围绕 POI 数据的控制和利用的需求冲突, 以及数字平台利用其市场支配地位或相对优势地位扭曲契约机制、实施不公平交易行为的能力, 是厘定平台内经营者 POI 数据权益边界时需要重点考虑的因素。应从数据来源角度将 POI 数据细化为门店推广数据、用户评价数据和等级评级数据, 逐一分析其原始的利益结构和法律边界, 然后才能正确评价平台协议对数据权益的再分配方案是否符合我国相关法律规定, 并纠正可能侵犯平台内经营者数据权益的不公平交易行为。

2. 公共性视角下平台协议的法律规制研究 (马辉)

来源:《法学家》2025 年第 2 期

作为格式条款在数字经济时代的最新演变, 平台协议的单方意志性、行为规训性与实施闭环性使其丧失了交易媒介功能, 而应被视作建构和维持私人秩序的权力工具。因此, 平台协议规制的关键是避免私权力滥用。经数字技术赋能, 不断膨胀的平台私权力会对市场效率和公民基本权利产生巨大威胁, 引发公共性贬损的后果。为了导正私权力的公共性面向, 法律体系演化出从公平价格管制到公共承运人拟制、再至公用事业管制的一系列公共性规制安排, 这为规制平台协议私权力提供了参照。平台协议的公共性规制应交叉检视需求侧和供给侧维度, 综合考量需求侧的非竞争性、用途多元性、需求派生性, 以及供给侧的应然与实然竞争约束。规制方案建构应依循结构主义的程序控权思路, 提升平台协议制定程序的公开性和参与性, 并对平台协议的实施植入排除偏私与听取意见的程序要求; 监管部门应对平台落实程序控权的自我规制活动开展外部元规制。

3. 契约抑或组织: 电商平台管治本原探寻 (周游)

来源:《法学评论》2025 年第 2 期

电商平台同时具有契约和组织的特征, 其理论基础是经济学上有关“企业的边界”的讨论。电商平台作为一种市场经济背景下的商业运作模式, 相关管治策略需要合乎商业逻辑。电商平台管治需要兼顾契约和组织两个面向的问题。在契约面向, 法律需关注平台商业模式多元化趋势, 不同的契约关系会受到特殊组织架构的影响而呈现不同的法律结构。《电子商务法》有关“相应的责任”的规定即是这一面向的反映。在组织面向, 法律需关注平台治理机制多元化趋势, 因应不同公司治理需求设置以专门委员会构建为核心的规则选择。专门委员会的设置不只是关注组织内部治理的需求, 更需要回应组织外部通过契约及其他方式形成的利益相关者的权益保护问题。由此, 平台管治侧重强调事前的风险防范和事中的法律关系识别, 有助于平台企业的规范经营和平台经济的健康发展。

4.机构间协调与数字平台监管：巴西 Whatsapp 案例的经验教训（Beatriz Kira）

来源：International Review of Law, Computers & Technology, Vol.39, Issue 1 (2025)

本文探讨了巴西首次大规模数字平台监管跨机构协调背后的驱动因素和障碍。它利用精英半结构化访谈和文件分析，调查了巴西国家数据保护局（ANPD）和其他联邦机构如何合作审查 WhatsApp 隐私政策和 2021 年 1 月宣布的服务条款变更的法律影响，包括对透明度、合法利益和同意的担忧。研究表明，虽然存在合作协议等正式的制度安排，但个人关系等非正式因素在促进协调方面发挥了重要作用。然而，相关机构内部的能力和自主性问题阻碍了更实质性的协调，并可能解释了对数据保护立法的解释存在分歧。研究结果强调了加强数字平台监管机构间协调机制的重要性，特别是考虑到监管生态系统内部和之间的能力和自主性问题，为其他司法管辖区提供了见解，特别是对于面临与巴西类似的公共治理限制的发展中国家。

数字行政与司法

1.行政机关利用个人信息进行自动化决策的合宪性检视（王明敏）

来源：《法学》2025 年第 2 期

自动化决策的深度应用是数字政府建设的内在驱动力。行政机关利用个人信息进行自动化决策实质上构成行政权对基本权利的限制，需在合宪性法秩序中加以检视，分别从权力正当性与基本权利干预的合宪性视角来考察。行政自动化决策本质上是算法赋能行政权，其权力运作同时遵循传统行政权和算法行政权的双重逻辑。宪法和行政法尚未明确行政自动化决策的行为性质，当前法规范对其规制存在诸多不足。从规范依据来看，行政机关利用个人信息进行自动化决策的宪法基础是个人信息自决权及其基本权利功能；作为对基本权利的限制，行政自动化决策应受比例原则、法律保留原则等法治原则的拘束。合宪性法秩序是人的主体性和人类智能的最后屏障，为检视和控制公权力乃至

演化中的算法权力提供了价值基础和规范依据，对数字法治政府建设中多重价值目标的平衡与兼顾具有关键意义。

2.行政法治的数智化法理（齐延平）

来源：《法学家》2025 年第 2 期

行政法治的数智化再造，将实现对传统行政权力和行政相对人权利的一体技术宰制，但其依然应当坚守人本法理，没有亦不允许突破基于人本的行政法律关系主体理论，以及基于自由意志的行政法律责任认定与归结原则。由面对面行政到界面行政所体现的执法去人格化逻辑，契合主观性执法不断客观化的法治演进规律。通过执法规范代码指令化、中介要素技术化、执法场景去人化，行政法治实现数智化孪生，其正当性的维系，有赖于自动化系统的安全可信、行政裁量梯度量表的科学化以及对行政规范算法化运行之社会共识的达成，而程序合法和实体正义是达致上述目标的法理基石。

3.数字时代刑事诉讼中人的主体地位（郑曦）

来源：《法制与社会发展》2025 年第 2 期

在刑事诉讼中确立人的主体地位具有重要意义。判断何者为刑事诉讼主体，需遵循特定标准。在数字时代，新型工具的运用对在刑事诉讼中的主体地位构成了威胁，尤其是刑事诉讼中运用的智能化工具已经初步形成“类主体”的地位，冲击了办案人员和当事人的刑事诉讼主体地位，导致人的尊严受到贬损。在此种情形下，基于明确工具服务于人的目的、兼顾“目的合理性”和“价值合理性”、警惕技术逻辑之必要，应重新强调数字时代刑事诉讼中人的主体地位，并从规则层面保障人的主体地位。首先，应明确工具在刑事诉讼中的辅助性地位；其次，应充分保障当事人在刑事诉讼中的参与权；最后，应落实司法责任制的要求，保证办案人员在办理刑事案件时权责统一，从而保障人的主体地位。

4.强化正义的时效性：刑事远程审判的程序规范立法（崔永存）数字行政与司法

来源：《法制与社会发展》2025年第2期

在《刑事诉讼法》迎来法典化倡议和第四次修改契机的时代背景下，探讨与论证刑事远程审判的程序立法问题，实现从技术理性向制度理性的升级跨越，正当其时。远程信息技术对程序价值的增益作用不限于降本增效，其更深刻的法治意义在于强化正义的时效性与可得性。实践发展的实然倾向、理论解释的趋于收敛和程序价值的时代意义均表明，在法律上有必要对刑事远程审判程序予以确认。同时，考虑其程序特殊性、功能有限性与实践失范性，须建立专门的、体系性的法律规制方案，以确保程序运行的正当化与规范化。就立法进路而言：在适用范围上，宜采取“包容性授权+限制性启动”的辩证化方案；在法庭秩序规范上，须兼顾场域环境、法庭纪律和审判流程三方面的秩序性问题；在技术正当程序规范上，须纳入知情同意权规则和技术公正性规则。

5.使用机器学习仔细审查假释听证会（Kristen Bel et al.）

来源：Berkeley Technology Law Journal, Vol.40, Issue 1 (2025)

本文在刑法中应用了一种新的机器学习方法：我们不是构建技术工具来预测通过系统的人的行为，而是构建工具来审查系统中掌权者的决策和说话模式。我们在假释听证会的背景下部署我们的方法，使用自然语言处理来分析 35,000 份听证会记录，总字数约为 7 亿字。我们发现，当主持假释听证会的官员的批准率历史上较低时，获得假释的几率也较低。我们进一步发现，私人聘请的律师比指定律师使用更复杂的法律语言，并且这种更复杂的语言与假释的几率增加有关。除了推进有关假释决定的知识外，本文还展示了如何利用机器学习作为工具来揭示刑事法律系统中潜在的不平等模式。

虚拟财产

法学理论尚未给出有力回应。对此，既需要科技、经济、政治领域复合性、系统性的外部规制，也需要证据法规则体系、运行机制的内部完善。

32 / 69

1.企业数据出资的法理逻辑与制度设计（刘颖）

来源：《当代法学》2025年第2期

企业数据作为新型生产要素出资入股，是公司法回应数字时代的重要举措之一。企业数据出资符合非货币财产出资的基本要素，有利于提升公司的信用和增进公司整体价值，符合企业大数据数尽其用原则，顺应数字时代公司法的发展趋势。企业数据出资的基本逻辑在于，企业数据应依据不同类型和范围的差异化出资，注重企业数据出资中自治与强制的利益平衡以及承担数据安全保护的法定义务。基于企业数据具有与传统生产要素不同的价值易变性、可复制、非排他性等特点，企业数据出资规则应当在出资比例、出资人竞业限制和为公司经营所必须等方面作出特殊限制。企业数据出资的风险防范需将公司法路径作为一般防范机制，以及将合同法路径作为特殊防范机制，多维度保障其他股东、公司和债权人利益。

2.虚拟货币犯罪的证据法困境及其破解（王静）

来源：《东方法学》2025年第2期

以区块链为底层技术的虚拟货币因其分布式、匿名化、跨境转移便捷等诸多特性给金融犯罪打击工作造成诸多困扰。虚拟货币犯罪所依凭的新型技术给传统证据法理论与实践形成巨大冲击。在证据方面，存在虚拟货币犯罪取证难，传统鉴定与鉴真模式难以有效适用等问题；在证明方面，存在虚拟货币犯罪数额证明难、完整证明链条难以构建、高度依赖口供印证等问题。究其成因主要包括与虚拟货币犯罪相关的概念和称谓混用导致虚拟货币犯罪证据和证明出现混乱；区块链技术的先进性与电子数据的虚拟性、流动性导致证据收集和固定陷入困境；证据规模巨大、货币价格变动与技术实力不足给犯罪数额的证明带来一系列不确定性。虚拟货币犯罪所涌现出的证据、证明问题，立法、司法、

3.国有企业数据资产保护的法律制度架构（姚佳）

来源：《法律科学（西北政法大学学报）》2025年第

2 期

在数智化背景下,数据逐渐成为驱动社会发展的核心元素。理论上,数据并非当然属于资产,其能否成为资产以及如何成为资产,应在数据资源、管理学和会计学意义上的资产等多重理论视域下进行论证。国有企业在国家经济发展中具有重要地位,数据资产是新类型新业态的国有资产。从性质上看,数据资产属于经营性国有资产,故应严格遵循我国《企业国有资产法》等法律,防范国有资产流失,确保国有资产保值增值,防范数据安全风险。从微观上看,数据资产的保护工作包括对数据资产的识别、归集、确权、登记等基础性内容;数据资产的利用涉及数据资产的交易流转和数据要素的流通利用等制度体系。在深化国资国企改革、数据要素市场化配置改革等多重维度中,系统探讨国有企业数据资产的制度架构,能够更好地发挥国有企业在促进国家经济和社会发展中的重要功能和作用。

4.网络虚拟财产的离婚分割(李姗萍)

来源:《法商研究》2025年第2期

网络虚拟财产是一种具有人身专属性的新型财产,其人身专属性主要体现为创设专属性、运营专属性、个人信息专属性以及社会关系专属性等方面。网络虚拟财产的人身专属性会影响其在离婚分割时的归属。强人身专属性的网络虚拟财产必须且只能分配给有人身关联的一方;中等强度人身专属性的网络虚拟财产原则上应当分配给有人身关联的一方,同时由取得方对另一方给予经济补偿;弱

人身专属性的网络虚拟财产之分割与一般的夫妻共同财产分割相似。当特定网络虚拟财产的实名注册方与实际运营方不一致时,应将其分配给实际运营方。网络虚拟财产的价值可协商确定,协商不成时可参考用户买入价、官方平台回收价或交易价、第三方平台交易价、评估机构估价等方式来确定。补偿标准适用离婚财产分割的一般性原则,即推定双方各享一半份额,同时可参考双方的实际贡献等因素予以调整。

5.数字支付中财产性利益的物法逻辑与财产犯罪认定(赵桐)

来源:《法学论坛》2025年第2期

随着数字支付手段的发展,民法中的物债当然二分的结构遭到现实挑战,虽然数字支付中的财产性利益表征的是基于合同而产生的债权债务关系,但其同时呈现出物权化特征,应当按照物法逻辑予以判断。按照物性控制权的来源方式,取得财产性利益的财产犯罪行为可以被区分为转移型与虚设型。转移物性控制权的行为应按照“破坏排他性支配”“排除直接支配可能性”的步骤,判断构成盗窃罪抑或侵占罪,其中的犯罪数额应以财产性利益的市场价格或实际可抵扣的价值来确定。虚设物性控制权的行为则应结合支配关系是否变更判断,行为人自行支配财产性利益并兑换的行为属于虚构债权债务的欺骗行为,平台预设的核销机制可被认定为错误处分,即使兑换行为只抵消了部分货款,也应基于法益相关的目的落空而认定平台存在财产损失。

(技术编辑:李佳丽、麻卓妍)

教研活动

会议 | 人工智能时代的民事权益保护学术研讨会顺利召开

为贯彻习近平总书记关于人工智能的重要讲话精神，保障民事主体的合法权益，促进人工智能产业健康发展，2025年5月12日，由清华大学法学院、清华大学法学院个人信息保护与数据权利研究中心主办，北京清律律师事务所协办的“人工智能时代的民事权益保护”学术研讨会在清华大学法学院顺利召开。来自全国人大常委会法制工作委员会、最高人民法院、法律出版社等单位的专家，以及来自北京大学、清华大学、中国人民大学、中国社会科学院法学研究所、吉林大学、中国政法大学、武汉大学、复旦大学、华东政法大学、中央财经大学、东南大学、西北工业大学、国家检察官学院、大连海事大学、西南财经大学、安徽大学、海南大学、湖南师范大学、广州大学、上海师范大学等高校、研究机构的学者六十多人参加了本次研讨会。



人工智能时代的民事权益保护学术研讨会合照

开幕式

清华大学法学院副院长程啸教授主持开幕式并致辞。他首先向各位专家、学者的到来表示热烈的欢迎和衷心感谢！他表示，此次会议聚焦“人工智能的民事责任”和“智能时代个人数据的保护和利用”两大主题，旨在通过学术界与实务界的理论研讨和观点碰撞，进一步深化人工智能领域民事法律问题的研究，助力人工智能法律治理体系的完

善，确保人工智能安全、可靠、可控。



清华大学法学院副院长程啸

主题一：“人工智能的民事责任”

主题一“人工智能的民事责任”阶段的主题发言单元，由全国人大常委会法制工作委员会民法室副主任马正平、最高人民法院研究室民事处处长陈龙业共同主持。



全国人大常委会法制工作委员会民法室副主任

马正平



最高人民法院研究室民事处处长陈龙业

中国人民大学王利明教授、杨立新教授、张新宝教授和华东政法大学马长山教授就生成式人工智能的侵权责任认定、自动驾驶汽车交通事故责任以及人机混同行为等问题作了主题发言。



中国人民大学王利明教授



中国人民大学杨立新教授



中国人民大学张新宝教授

主题一“人工智能的民事责任”阶段的第一个议题研讨单元，由中央财经大学法学院院长尹飞教授、中国人民大学法学院副院长朱虎教授共同主持。



中国人民大学法学院副院长朱虎教授

北京大学法学院常鹏翱教授、中央财经大学法学院朱晓峰教授、清华大学法学院长聘副教授蒋舸、北京清律律师事务所首席合伙人熊定中、中国人民大学法学院助理教授阮神裕等围绕人工智能侵权责任的归责原则、人工智能产品责任与人工智能服务责任的区分、人工智能侵权责任中因果关系与过错的证明等问题展开讨论。

主题一“人工智能的民事责任”阶段的第二个议题研讨单元由中国社会科学院法学研究所商法室副主任赵磊研究员，《当代法学》主编、吉林大学法学院曹险峰教授共同主持。

西北工业大学王延川教授、中国人民大学法学院熊丙万教授、北京大学法学院长聘副教授贺剑、安徽大学法学院副院长夏庆锋副教授、武汉大学法学院特聘副研究员宁园等围绕人工智能侵权责任的损害赔偿的范围、生成式人工智能侵权责任问题、自动驾驶机动车交通事故责任等问题展开讨论。

主题二：“智能时代个人数据的保护与利用”

主题二“智能时代个人数据的保护与利用”阶段的主题发言单元，由《中国法律评论》常务副主编、编辑部主任袁方，国家检察官学院赵玉教授共同主持。



《中国法律评论》常务副主编、编辑部主任袁方



国家检察官学院赵玉教授

中国社会科学院法学研究所研究员姚佳，全国人大常委会法制工作委员会经济法室副处长林一英，清华大学法学院教授、《清华法学》副主编王洪亮，中国人民大学法学院丁晓东教授，清华大学法学院程啸教授就生成式人工智能中的个人信息保护问题、数据交易合同、数字时代侵权法的变革以及个人数据交易中的合法性审查义务等问题作了主题发言。



中国人民大学法学院丁晓东教授

主题二“智能时代个人数据的保护与利用”阶段的第一个议题研讨单元，由《比较法研究》副主编丁洁琳、《中国法学》副编审任彦共同主持。

中央财经大学法学院武腾教授、西南财经大学法学院张芸教授、北京市第二中级人民法院民二庭庭长邹治、复旦大学法学院葛江虬副教授、上海师范大学法政学院吴玄副教授、清华大学法学院助理研究员王年等围绕人工智能训练及应用中的个人数据保护与利用、个人信息可识别性和匿名化的认定、人工智能应用中未成年人个人信息保护以及个人数据财产利益的归属与实现等问题进行了研讨。

主题二“智能时代个人数据的保护与利用”阶段的第二个议题研讨单元，由《中国应用法学》副主编、编辑部主任杨奕、法律出版社法律教育分社社长吴昉共同主持。

海南大学法学院杨芳教授、东南大学法学院王苑副教授、抖音集团法律研究与合作负责人丁道勤、北京市第三中级人民法院立案庭庭长黄海涛、北京市第四中级人民法院立案庭庭长张勤缘、大连海事大学法学院助理教授吴晓晨、广州大学法学院特聘副研究员杨嘉祺、湖南师范大学法学院助理教授李西岭等围绕自动化决策与个人信息保护问题、具身智能中的隐私及个人信息保护、个人信息可识别性与匿名化的司法认定、征信数据中的个人信息保护、神经数据共享中的个人信息保护等问题展开讨论。



抖音集团法律研究与合作负责人丁道勤

闭幕式

闭幕式由北京清律律师事务所首席合伙人熊定中律师主持，清华大学法学院副院长程啸教授作总结发言。他首先对与会嘉宾百忙之中，拨冗参加本次会议再次表达了衷心感谢，并指出本次会议促进了理论界与实务界在人工智能法律研究领域尤其是人工智能侵权责任、个人数据利用与保护等问题的深度交流，形成了观点交锋与思想碰撞，在凝聚共识的基础上提出了未来需要理论界与实务界共同努力研究的新问题。

经过一天的深入研讨，与会专家一致认为，法律必须适应人工智能技术的发展，努力协调民事权益保护与鼓励技术创新的关系，研讨会促进了我国人工智能法律问题的理论研究，对于推动未来我国人工智能相关立法、司法审判具有重要意义。

本次研讨会得到了清华大学文科建设“双高”计划创新方向建设专项《智能时代个人数据法律体系研究》的资助！

湖南师范大学赴中国政法大学数据法治实验室考察交流

4月25日上午，湖南师范大学一行来到中国政法大学数据法治实验室考察并开展座谈交流。湖南师范大学外国语学院院长曾艳钰，人工智能与精准国际传播研究院院长高协平，人工智能与精准国际传播研究院常务副院长、外国语学院副院长蒋莉华，人工智能与精准国际传播研究院副院长、语言与文

化研究院副院长杨安，人工智能与精准国际传播研究院现代化新湖南国际传播应用中心主任马纳克，人工智能与精准国际传播研究院面向国际传播的智能计算研究中心主任曾道建，人工智能与精准国际传播研究院助理研究员王纯、专职秘书王耀光以及中国政法大学副校长、数据法治实验室主任时建中，数据法治实验室副主任王立梅，数据法治研究院副教授张涛，讲师王煜婷、章颖、王申、杜牧真参加会议。活动伊始，湖南师范大学一行参观了中国政法大学数据法治实验室，深入了解实验室在智慧司法、数字检察领域的研究成果与实践应用。



座谈交流会现场

随后，双方在会议室举行座谈交流会。会议由数据法治实验室副主任王立梅主持。会上，时建中对湖南师范大学一行的到来表示欢迎，并介绍了数据法治实验室在专业学科、人才培养以及科研平台等方面的建设情况，他希望，双方可以在哲学社会科学实验室建设和人工智能交叉领域等方面持续开展交流。曾艳钰表达了对中国政法大学数据法治研究院的感谢，并介绍了湖南师范大学外国语学院的办学历史以及语言传播和国际交流方面的研究情况。高协平对人工智能与精准国际传播实验室的建设背景和发展历程作了简要介绍。他表示，人工智能在国际传播中发挥着重要作用，希望与中国政法大学数据法治实验室在人工智能与文化传播交叉领域展开深入交流与合作。

党的二十大报告明确提出，“坚守中华文化立场，加强国际传播能力建设，全面提升国际传播效能，推动中华文化更好走向世界”。人工智能凭借强大的数据处理和智能分析能力，能够有效突破语言壁垒和文化鸿沟，拓展中华优秀传统文化和国际多元

文化的正向互动。双方将加深在人工智能与国际传播领域的了解与合作，积极探寻能够充分发挥人工智能优势、有效赋能中华文化国际传播的可行举措，为科技向善贡献更多智慧。



交流圆满结束

第二届网络与信息法学学科建设论坛

2025年5月10日，“第二届网络与信息法学学科建设论坛”在湘潭大学法学学部隆重召开，本次论坛以“推进网络与信息法学学科高质量发展”为主题，由中国法学会网络与信息法学研究会主办，湘潭大学法学学部，湖南省法学会网络法治研究会共同承办。



第二届网络与信息法学学科建设论坛现场

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，湘潭大学党委副书记、校长廖永安，湖南省高级人民法院党组成员、副院长郭正怀，湖南省人民检察院党组成员、副检察长向新林，湖南省法学会党组成员、副会长高可议等出席会议并致辞，开幕式由中国法学会网络与信息法学研究会常务副会长兼秘书长、中国社会科学院法学研究所研究员周

汉华主持。

来自中国社会科学院、北京大学、中国人民大学、武汉大学、中国政法大学、西南政法大学、华东政法大学、中南财经政法大学、西北政法大学、四川大学、西安交通大学、南京航空航天大学、中南大学、西北工业大学、中央财经大学、北京科技大学、福州大学、内蒙古大学、南昌大学、华南师范大学、合肥工业大学、暨南大学、江南大学、深圳大学、福建师范大学、江西财经大学、甘肃政法大学、上海政法学院、湘潭大学，《法学研究》编辑部、《法学评论》编辑部、《环球法律评论》编辑部、《清华法学》编辑部、《法学》编辑部、《法律适用》编辑部、《数字法治》和中国法治出版社等单位的专家学者，和来自中央网信办、公安部、中国网络空间研究院、湖南省高级人民法院、湖南省人民检察院、湖南省委网信办、湖南省法学会、北京互联网法院、广州互联网法院等单位的实务专家近百人，共同为推动网络与信息法学学科高质量发展提供智慧。

开幕式

廖永安对本次论坛的顺利举办表示热烈祝贺。他表示，国内网络与信息法学学科建设仍处于探索与完善阶段，要深入贯彻习近平总书记关于网络强国建设的重要论述精神，聚焦网络与信息法学学科前沿理论和创新实践问题，系统优化网络与信息法学学科的理论体系、学科体系、教材建设与人才培养模式，培养造就更多德法兼修的网信卓越法治人才。



湘潭大学党委副书记、校长 廖永安

高可议指出,当前新一代信息技术迅猛发展,对网络与信息安全提出了新的挑战,要在坚持自主知识体系的前提下,注重融入涉外法治元素;在推动学科深度融合的基础上,持续促进学术研究繁荣;在发挥学科地方优势的实践中,着力打造特色育人高地,书写网络与信息法学学科建设的崭新篇章。



湖南省法学会党组成员、副会长 高可议

向新林表示,网络与信息法学正式列为法学二级学科,标志这一新兴交叉学科迈入规范化、体系化发展新阶段。面对人工智能、区块链等新技术带来的法律挑战,湖南省检察机关始终将服务网络强国战略作为重要使命,依法加大危害网络安全犯罪的惩治力度,依法保护、规范和促进数字技术、数字产业和数字市场发展,加强检校合作,协同加强法学教育和法治人才培养,为维护网络空间安全和服务数字经济健康发展贡献力量。



湖南省人民检察院党组成员、副检察长 向新林

郭正怀指出,以大数据、人工智能为代表的新一轮网络与信息技术革命,对司法实务带来的影响愈发深远。近年来,湖南法院深入贯彻习近平法治思想,履行审判职能,惩治网络暴力违法犯罪;积极推动智慧法院建设,畅通便民渠道,提升办案能力;提炼司法审判经验,以网信司法实践推动网络法治保障规则体系的完善;及时响应科技创新和人工智能发展的司法需求,重视网信司法工作在发展

新质生产力方面的重要作用。未来,湖南法院将深化与湘潭大学等相关高校的合作,为网信法治人才培养搭建平台,为湖南“三高四新”和数字中国建设贡献湖南法院力量。



湖南省高级人民法院党组成员、副院长 郭正怀

姜伟强调,当前网络与信息法学学科建设处于探索期的初创阶段,网络与信息法学学科建设要注重创新性,从理论创新方面提炼具有中国特色的学科核心命题,在方法创新方面形成学科独具的研究范式,在教学创新方面增强学生适应法律科技的操作能力;要注重体系化,持续推进网络与信息法学学术体系、课程体系、教材体系和话语体系建设,建构具有中国特色和国际视野的自主知识体系;要注重融合度,突出“法学+技术”的复合特色,打破传统法学学科边界,强化交叉学科属性,构建理论与实践并重的法治人才培养体系。



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

主旨演讲

主旨演讲阶段由中国社会科学院学部委员、一级教授、法学研究所研究员,《法学研究》主编陈甦主持。

武汉大学法学院教授、《法学评论》主编秦前红,

华东政法大学法律学院教授、数据法律研究中心主任高富平，西南政法大学人工智能法学院院长陈亮教授，上海政法学院人工智能法学院院长杨华教授，中国人民大学法学院副院长张龔教授，北京大学法学院副院长戴昕长聘副教授，湘潭大学法学学部副部长，知识产权学院、信用风险管理学院院长肖冬梅教授分别发表了主题演讲。

与谈环节中，中国社会科学院法学研究所编审、《环球法律评论》编辑部主任姚佳，《清华法学》编辑部主任、编审徐雨衡分别发表了与谈意见。

分论坛一：中国法学自主知识体系建设和网络与信息法学学科发展



分论坛一现场

分论坛一的议题为“中国法学自主知识体系建设和网络与信息法学学科发展”，由中国法学会网络与信息法学研究会副会长、中国政法大学王立梅教授主持。

中南财经政法大学法治发展与司法改革研究中心主任徐汉明教授，广州互联网法院党组成员、副院长邵山，北京互联网法院党组成员、政治部主任栾淼淼，中央财经大学法学院副院长、《财经法学》副主编刘权教授，陕西省法学会信息安全法学研究会秘书长、西安交通大学法学院王玥教授，江南大学法学院副院长叶敏教授，南昌大学法学院副院长张恩典副教授，分别作了主题演讲。

分论坛二：网络与信息法学的学科方向与培养方案



分论坛二现场

分论坛二的议题为“网络与信息法学的学科方向与培养方案”，由中国法学会网络与信息法学研究会副会长、北京科技大学法学院徐家力教授主持。

内蒙古大学法学院党委书记龙长海教授，南京航空航天大学人文与社会科学学院院长高志宏教授，西南政法大学研究生院副院长、民商法学院孙莹教授，中国法学会网络与信息法学研究会常务副秘书长、中国社会科学院法学研究所网络与信息法研究室副主任（主持工作）、副研究员周辉，深圳大学法学院副院长宋旭光副教授，福建师范大学法学院院长助理林艺芳副教授，湖南省法学会网络法治研究会秘书长、湘潭大学法学学部文禹衡副教授，分别作了主题演讲。

分论坛三：复合型网络与信息法治人才培养与学术共同体建设



分论坛三现场

分论坛三的议题为“复合型网络与信息法治人才培养与学术共同体建设”，由湖南省法学会网

络法治研究会副会长、湘潭大学法学学部副部长连光阳副教授主持。

江西省法学会数据法学研究会会长、江西财经大学数据法律研究院院长饶传平教授，中国网络空间研究院网络法治研究所副所长李晓娇，陕西省法学会人工智能与大数据法学研究会会长、西北工业大学公共政策与管理学院法学系张敏教授，福州大学法学院副院长贾丽萍教授，安徽省法学会数字法学研究会秘书长、合肥工业大学文法学院副院长霍敬裕教授，湖南省法学会网络法治研究会副会长、中南大学法学院张新平副教授，华南师范大学法学院数字政府与数字经济法治研究中心主任马颜昕副教授，分别作了主题演讲。

分论坛四：网络与信息法学的教材体系、课程体系和课堂体系建设



分论坛四现场

分论坛四的议题为“网络与信息法学的教材体系、课程体系和课堂体系建设”，由中国法治出版社总编助理舒丹主持。

四川智慧社会智能治理重点实验室主任、四川大学法学院王竹教授，甘肃政法大学民商经济法学院（知识产权学院）院长马莉，华东政法大学数字法治研究院副院长、法律学院韩旭至副教授，广东省法学会网络与电子商务法学研究会秘书长、暨南大学法学院/知识产权学院韩书立副教授，中国社会科学院大学刘灿华副教授，西北政法大学民商法学院讲师尉钊，江西财经大学数据法律研究院研究员李钊，分别作了主题演讲。

闭幕式

闭幕式由中国法学会网络与信息法学研究会常务副秘书长、中国社会科学院法学研究所网络与信息法研究室副主任（主持工作）、副研究员周辉主持，中国法学会网络与信息法学研究会常务副会长兼秘书长、中国社会科学院法学研究所研究员周汉华，湘潭大学法学学部部长、湖南省法学会网络法治研究会会长李仕春教授作闭幕致辞。



第二届网络与信息法学学科建设论坛圆满结束

首届数字法治理论与实务对话暨《数字法治》创刊两周年座谈会在沪举行

为深入贯彻习近平法治思想，4月18日，由人民法院出版社、上海市高级人民法院联合主办的首届数字法治理论与实务对话暨《数字法治》创刊两周年座谈会在国家法官学院上海分院举行。



座谈会现场

最高人民法院党组成员、副院长杨临萍，上海市高级人民法院党组书记、院长贾宇，最高人民法院咨询委员会副主任委员、中国法学会网络与信息法学研究会会长、《数字法治》专家委员会主任委员姜伟，吉林大学哲学社会科学资深教授、中国法学会法学

教育研究会会长、教育部社会科学委员会法学学部召集人**张文显**，全国人大代表**朱丽平**出席座谈会。

杨临萍表示，作为全国首个聚焦数字法治发展的专业期刊，《数字法治》是理论与实务的双向奔赴，专家学者的真知灼见为司法进步注入智慧源泉，实务界产业界的实践探索为理论创新提供沃土滋养。杨临萍指出，要聚焦新技术发展带来的法治问题，探讨数字时代的司法举措，为国际社会数字法治发展贡献中国智慧和方案。要聚焦数字法院建设，助力推进审判工作高质量发展。同时，积极参与全球数字治理，提升国际规则影响力，持续夯实《数字法治》期刊学术阵地，做深做优理论与实践交流互促，把深入贯彻习近平法治思想和习近平总书记关于网络强国的重要思想，推进数字法治建设的成果和经验更好地传播开来，共同讲好新时代中国数字法治故事。

贾宇代表上海高院对《数字法治》创刊两周年表示热烈祝贺，并表示，此次座谈会的召开，为我国数字法治现代化建设注入新动能，推动数字法治理论与实践探索进入协同发力新阶段，为构建数字法治创新发展的理论框架与治理体系，推动数字法治高质量发展贡献智慧。贾宇指出，要深刻认识数字法治建设的重大战略意义，深入推进数字法院建设与研究，积极推动数字法治刊物蓬勃发展，积极参与全球数字法治规则、数字法治评估和认证体系的构建，输出中国数字法治的技术标准和产品服务成果，增强我国在全球数字治理领域的国际话语权，为全球治理贡献“中国智慧”。

姜伟表示，此次座谈会既是对《数字法治》期刊创刊两年经验的系统总结，也是对未来发展的规划展望。数字法治建设是国际数字治理竞争的战略高地，是国家治理体系和治理能力现代化的重要支撑。数字法治研究是建构中国法学自主知识体系的组成部分，是增强国际话语权、推动全球治理模式创新的重要路径。《数字法治》期刊是数字法治知识生产、传播的平台载体，希望《数字法治》期刊推动我国数字法治研究从“技术驱动”走向“规则引领”，从“理论创新”走向“知识体系”，成为

数字时代法治文明的记录者与塑造者。

座谈会上，主办方向与会人员发放人民法院出版社出版的“数字法院三部曲”——贾宇著述的《数字法院概论》，贾宇主编的《数字法院前沿探索与理论构建》，以及贾宇主编、最高人民法院审判管理办公室审定的《数字法院场景建设指引》。这三本著作总结凝练了上海数字法院建设中的理论研究成果和相关经验做法，体现了在数字司法领域中的上海智慧。



人民法院出版社出版的“数字法院三部曲”

立足数字法治核心议题，本次座谈会与会人员围绕“数字时代的司法应对及法学期刊的使命”“人工智能法治”两大主题，通过主旨演讲、圆桌对话等形式，深度多维探析数字法治建设的中国方案与全球治理图景。

来自最高人民法院，学术界、期刊界代表，上海法院代表，其他司法机关代表，数字经济技术领域代表，媒体记者等参加此次座谈会。

会议期间，杨临萍与应邀参会的全国人大代表、中国铁路上海局集团有限公司财务部会计科科长朱丽平座谈交流，听取意见建议。

联合国教科文组织东亚办事处启动“中日韩人工智能伦理治理项目”

2025年4月30日，联合国教科文组织(UNESCO)东亚区域办事处在线召开“中日韩人工智能伦理治理项目”启动会。联合国教科文组织东亚办事处代表夏泽翰教授、教育处主管 Mee Young Choi 博士等出席会议并致辞。项目总负责人中国政法大学张凌寒教授主持会议，并联合日本上智大学森下哲

朗教授、韩国科学技术院金炳弼教授等专家共同组建三国研究团队，正式启动这一聚焦人工智能伦理治理的区域性研究合作。

锚定区域协同，构建伦理治理新范式

在中国司法大数据研究院的调研活动中，研究院随着人工智能技术在中日韩三国的快速发展和深度应用正深刻影响社会结构与价值体系，伦理治理已逐渐成为实现区域可持续发展的关键保障。为系统评估三国在人工智能伦理治理方面的政策基础与实践能力，教科文组织发起面向东亚的区域级

三国专家共议研究路径，深化方法论共识

在项目启动会上，首席专家张凌寒教授系统介绍了本次区域合作研究的总体设计与实施路径，强调通过应用《人工智能伦理建议书》及其评估工具，推动东亚三国在人工智能伦理治理领域开展结构化、可比较的评估工作。会议同时由中日韩三国专家分别代表本国团队分享了初步调研成果，涵盖人工智能政策体系、监管体制机制及利益相关方图谱等关键内容。作为项目研究等关键方法之一，基于评估工具初步设计的结构化问卷聚焦不同调研对象的治理角色，提升伦理政策评估的精准性与适应性。教科文组织东亚办事处代表夏泽翰教授表示，项目的顺利启动和阶段性成果充分体现了区域协作研究的可行性与有效性，也印证了中日韩专家团

人工智能伦理治理创新项目，依托教科文组织《人工智能伦理建议书》及其配套工具《准备状况评估方法》和《伦理影响评估方法》，开展全面分析与比较研究。项目由中日韩专家团队协同推进，其中中方团队依托中国政法大学数据法治研究院的学术优势，牵头设计研究框架。该项目将开启国别政策对话与机制互鉴，推动三国在人工智能伦理治理核心议题上的经验交流与互学互鉴，探索契合区域特征的治理基础与治理模式，进一步丰富全球人工智能治理体系中的东亚路径与智慧。

队在专业性与协同力方面的突出表现，为项目目标的实现和研究成果的政策转化奠定了坚实基础。

明确后续行动

据悉，项目组将于 2025 年 5 月中旬提交首阶段研究成果，并于 10 月完成全面评估报告。本次合作不仅标志着中日韩专家在科技伦理治理领域迈出协同合作的重要一步，更成为落实全球发展倡议、推动构建人类命运共同体的生动实践。正如教科文组织始终倡导的“和平与合作”理念所体现的精神，三国专家携手探索的治理路径，有望为全球人工智能治理提供跨区域协作的有益范式，推动技术治理与人类共同价值的深度融合，为国际人工智能伦理体系建设作出积极贡献。

技术编辑：林诗敏

数字法评

敏感个人信息保护制度的解释性重构

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

作者:丁晓东

摘要:我国与域外法律大多以类型列举或存在严重侵害风险界定敏感个人信息,在保护方式上采取二元保护、强化保护。但敏感个人信息保护的理解与适用存在挑战,其界定存在不确定性,保护方式也不尽合理。这一挑战的根源在于敏感个人信息具有场景化特征,个人信息并非因其本身而敏感。在立法层面对敏感个人信息保护进行重构不具有必要性与可行性,应在解释与适用过程中对其进行重构。敏感个人信息的界定应以目的解释为主、参照文义解释,价值判断应以我国国情为依据,风险认知判断应以专家判断为主、兼顾公众感知风险,判断因素应考虑信息主体、处理主体、处理方式、识别概率等。敏感与非敏感个人信息的分类保护应迈向场景化、动态化:在行政监管中,应采取自下而上的场景化保护;在司法与行政执法案例中,应采取以案释法的场景化保护。就强化保护措施而言,应迈向监管下的自我监管。衔接敏感个人信息与私密信息,应在个人信息保护与隐私权保护两种制度下进行分析。

一、引言

敏感个人信息保护是个人信息分类分级保护的重要制度。我国《个人信息保护法》在第二章第二节中专门规定了敏感个人信息的处理规则。其中,第28条规定了敏感个人信息的定义和一般规则,将敏感个人信息界定为“一旦泄露或者非法使用,容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息,包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息,以及不满十四周岁未成年人的个人信息”;

在处理规则方面,该条规定处理敏感个人信息必须“具有特定的目的和充分的必要性,并采取严格保护措施”。第29条至第32条、第55条进一步规定了处理敏感个人信息的特殊保护方式,例如,取得个人的单独同意,向个人告知处理敏感个人信息的必要性以及对个人权益的影响,处理未成年人信息应当取得未成年人的父母或者其他监护人的同意,事前进行个人信息保护影响评估等。域外部分国家和地区也采取了类似立法,例如欧盟《一般数据保护条例》第9条将某些类型的数据列为“特殊类型个人数据”,对其设置严格的强化保护制度。

敏感个人信息的法律解释与制度适用面临挑战,尤其面临互联网与大数据等技术变革所带来的法律挑战。一方面,敏感个人信息的概念解释与界定方法存在争议。敏感个人信息应当以法律中的列举为准,还是以处理个人信息可能导致自然人“受到危害”为准?^[1]目前,大量常见类型的个人信息是否属于敏感个人信息尚不明确,例如,个人照片、个人视频、个人声音、身份证号码、手机号码、工作单位、家庭住址信息未被我国《个人信息保护法》所列举,但这类信息也可能在某些场景下具有敏感性。另一方面,敏感个人信息保护方式也存在争议。在敏感个人信息界定不确定性的背景下,我国《个人信息保护法》中所规定的敏感与非敏感个人信息的二元保护框架是否合理?是否应当像有的学者所言,个人信息保护应放弃敏感个人信息这一概念以及相应的制度工具?^[2]

针对敏感个人信息法律保护,学界已经进行了很多分析与研究,但仍然存在众多空白与不足。首先,已有研究并未充分引入比较法与历史研究视角。其次,已有研究并未对敏感个人信息“因何敏感”问题进行深入分析。最后,已有研究并未对敏感个人信息的制度困境提供具体解决方案。本文努力在这些方面进行创新性论述:在视角方面,全面分析敏感个人信息保护的来龙去脉以及欧美等国家和地区在敏感个人信息问题上的立场;在原理层面,对敏感个人信息为何具有不确定性、其制度为何存在过严或过宽问题进行法理思考,阐述敏感个人信

息因何敏感；在制度层面，对个人信息保护界定与保护方式提出了新方案。笔者认为，在立法层面，敏感与非敏感个人信息的二元划分具有表达功能，可以向社会传递敏感个人信息强化保护的信息。考虑到我国《个人信息保护法》制定不久，域外各国也普遍在立法中引入敏感个人信息概念，并对其进行特殊保护，笔者认为，在立法层面对敏感个人信息制度进行重构既无必要、也不可行，但在法律解释与法律适用层面可以对这一制度进行重构。基于此，本文首先分析敏感个人信息界定与保护方式的挑战，此后从历史与原理的角度对其进行反思，最后对敏感个人信息的界定与保护方式进行解释性重构。

二、敏感个人信息界定与保护的难题

敏感个人信息保护面临两方面的挑战或难题：其一，敏感个人信息的范围不确定，这对敏感个人信息的界定提出了挑战。其二，对敏感个人信息的保护方式也存在难题，无论是敏感与非敏感个人信息的二元保护、敏感个人信息的强化保护措施、敏感个人信息与私密个人信息的交叉，都存在若干难题或困境。^[3]

（一）敏感个人信息界定的难题

敏感个人信息首先面临界定的难题。我国《个人信息保护法》采取了“法律目的+开放列举”的定义方式，一方面将“一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息”界定为敏感个人信息，另一方面又采取了列举式的规定，将“生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息”7类信息列举为敏感个人信息。^[4]从法律解释来看，对上述规定可以采取文义解释与目的解释两种方法。如果采取文义解释的方法，那么《个人信息保护法》第28条所列举的7类个人信息就必然属于敏感个人信息。与之相对，如果采用目的解释的方法，则法律对敏感个人信息的界定应当以侵害风险为标准。如果某一信息并不会带来较为严重的侵害风险，即使此类信息属于被列举的范围，其也不应

被纳入敏感个人信息范畴。同样，即使某类信息从未被纳入《个人信息保护法》或相关法律法规和标准中的敏感个人信息范畴，但只要其存在更大的侵害风险，则此类信息仍然应当被视为敏感个人信息进行保护。^[5]

基于法律目的的解释方法还可以进一步细分。《个人信息保护法》第28条并未直接说明判断个人信息敏感性的主体。第一种理解是这种主体是信息处理者，即敏感个人信息是相对信息处理者而言的，如果信息处理者能够利用此类信息造成重大侵害，则此类信息就属于敏感个人信息。第二种理解则将此主体界定为个人信息主体，只要个体感觉某类信息处理具有敏感性，则此类信息就应当被划入敏感信息。第三种理解则将此主体界定为技术人员或不特定公众，从他们的角度判断个人信息泄露或非法使用的风险。在很多情形下，不同主体对于敏感性的判断可能非常不同。

即使对敏感个人信息采取统一的界定与解释方法，敏感个人信息的范围也仍然具有不确定性，因为很多看上去非敏感的个人信息的推断出敏感个人信息。以《个人信息保护法》第28条所列举的医疗健康信息为例，个人的就诊记录、用药记录、病史、身体症状可以直接揭示个人的医疗健康信息，但个人的食品消费记录、运动习惯、网页浏览记录也可以间接揭示个人的医疗健康情况。法律如何归类此类可以间接推断出敏感个人信息的一般个人信息将是一个两难问题：如果法律将此类可以推断出敏感个人信息的信息排除在外，那么其结果将是很多具有敏感个人信息特征的信息无法得到严格保护；相反，如果将可以推断出敏感个人信息的信息包括在内，那么大量的普通个人信息都会成为敏感个人信息。因为通过个人信息的比对、分析与汇聚融合，信息处理者或第三方都有可能推断出敏感个人信息。甚至一些看似非个人信息的信息，也可能在某些场景下成为敏感个人信息。^[6]例如，微博、抖音等社交软件上显示的用户IP所属国家与省份，这类信息一般不会成为个人信息，因为一个国家与省份至少有上百万或上千万的人口，但如

果某位网络用户前一天的IP地址在国内某个省份,第二天显示在域外某个国家,这就显示了这位网络用户的行踪轨迹,其IP地址就可能成为个人信息甚至是敏感个人信息。

在互联网与大数据时代背景下,敏感个人信息的界定存在更多不确定性。在网络搜索等技术的帮助下,人们可以获取大量的公开个人信息和相关背景信息,相关主体通过将这些信息与某一信息结合,就可能将某一信息转化为敏感个人信息。例如,美国某在线网站曾经公布了2千万条经过匿名化处理的个人搜索记录,单从这些搜索记录来看,这些信息并不是敏感个人信息,甚至可能都不算个人信息,但是相关主体通过将这些信息与网络可以获取的公开信息进行结合比对分析,就很容易破解其中的很多信息。《纽约时报》甚至随机选取了一位用户,通过公开信息比对分析找到了这位用户的家庭住址并登门拜访。^[7]再比如,在“剑桥分析丑闻案”中,剑桥分析公司最初收集的主要是个人的非敏感个人信息,但通过大数据的汇聚与融合分析,最终推断出了大量个人的政治倾向等敏感个人信息。^[8]随着信息技术的发展与数据分析行业的兴起,可以预见,从非敏感个人信息中推断出敏感个人信息的情形将更为常见。

(二) 敏感个人信息保护方式的难题

敏感个人信息的保护方式也存在难题与挑战。首先,在敏感个人信息界定不确定的背景下,对这一类型的信息进行特殊保护的制度设计是否仍然有必要?已经有不少学者表达了对敏感个人信息保护的担忧甚至反对。例如,保罗·奎因和吉安克劳迪奥·马尔基里对欧盟《一般数据保护条例》中的敏感个人信息保护进行了研究,指出欧盟在界定敏感个人数据上具有很大的不确定性。这种不确定性包括两方面:一方面是敏感个人信息面临不断膨胀的难题,很多传统上被认为不属于敏感个人信息的信息,都可能在大数据时代被纳入敏感个人信息的范围,这一情形可能使敏感个人信息保护失去意义;另一方面,敏感个人信息的范围也可能被人为限制或缩小,导致很多具有敏感性的个人信息未能得到

应有的更高级别保护。^[9]美国学者丹尼尔·索洛夫的立场则更为激进,其不仅指出了敏感个人信息的高度不确定性与制度困境,而且直接主张废除敏感个人信息这一概念与相应制度。索洛夫认为,个人信息保护应当关注数据的“使用、伤害和风险”,而不是个人信息是否敏感。^[10]

其次,敏感个人信息的强化保护措施也需要进一步讨论。我国《个人信息保护法》主要从以下方面对敏感个人信息进行强化保护:其一,在合法性基础方面,处理敏感个人信息应当具有特定的目的和充分的必要性,即在一般个人信息的目的限定与最小必要等原则基础上进行升级;^[11]其二,在告知同意方面,处理告知同意除了应当向个人告知一般个人信息所需要告知的事项,还应当“向个人告知处理敏感个人信息的必要性以及对个人权益的影响”,而且应当取得个人的“单独同意”;^[12]其三,在预防与技术保护措施方面,处理个人信息除了遵循一般个人信息所需要的要求,还应当进行个人信息影响评估与采取其他强化保护措施。^[13]但上述制度设计存在不少落地难题,其解释与适用存在争议。例如,就合法性基础而言,如果个人信息的敏感性可能在收集后发生变化,那么对于某一信息的收集是否需要在收集之初就区分一般目的限定和特定目的限定、最小必要性和充分必要性?就告知同意而言,告知同意的问题已经被广泛讨论,其核心问题在于这一制度日益流于形式,无法真正保护个人信息权益。^[14]在此背景下,敏感个人信息保护所要求的强化告知同意是否可以有效保护敏感个人信息?就预防与技术保护措施而言,《个人信息保护法》所设置的相关制度是否可以对敏感个人信息进行有效保护?

最后,敏感个人信息与私密信息的制度衔接也需要回应。我国《民法典》没有采用敏感个人信息的概念,但引入了私密信息的概念。相反,《个人信息保护法》则采用敏感个人信息的概念,并未规定私密信息。在敏感个人信息与私密信息存在交叉的背景下,^[15]法律适用将面临一系列问题,例如,私密信息与敏感个人信息如何区分?当某类个人信

息既属于私密信息又属于敏感个人信息时,法律应当如何适用?在此类信息处理中,个人信息主体与监管机构除了依据《个人信息保护法》提起权利主张和进行监管之外,个人是否也可以依据隐私权框架对相关行为提起隐私侵权之诉?

三、敏感个人信息的场景化特征

分析上述难题,需要追溯个人信息保护以及敏感个人信息的发展历史,从原理或法理层面对敏感个人信息保护进行分析。个人信息保护的制度目标并非保护个人信息本身,而是保护个人信息处理中的相关权益。因此,敏感个人信息呈现场景化特征,其敏感性往往因为其处理所涉及的不同因素与其保护的不同权益而不同。

(一)敏感个人信息场景化的历史性

在很长一段时间内,个人信息保护制度都未明确规定敏感个人信息。例如,美国1973年发布的奠定个人信息保护制度雏形的《公平信息实践准则》未规定敏感个人信息。甚至直到今天,美国联邦层面制定的一系列法律也并未直接区分敏感与非敏感个人信息。在欧洲,敏感个人信息的概念虽然在20世纪70、80年代就已经在瑞典、德国黑森州的立法中出现,但法律并未对其作出特殊规定。1980年,经济合作与发展组织(OECD)在制定《保护隐私及个人信息跨境流动指引》时提到了敏感个人信息,但认为各国对于何种个人信息具有敏感性有不同的认知,因此统一敏感个人信息的界定是不可能的。^[16]

美国虽然没有引入敏感个人信息的概念,但其联邦层面的立法却与敏感个人信息立法具有类似性,主要通过以下法律针对某类具有敏感性、风险性的个人信息进行规制:1970年制定的个人信息保护法的雏形《公平信用报告法》针对征信类个人信息,1974年制定的《家庭教育权利与隐私法》针对学生的教育类个人信息,1974年制定的《隐私法》针对美国规制机构所收集的个人信息,1988年制定的《视频隐私保护法》针对涉及视频租借、购买等的个人信息,1994年制定的《司机隐私保护法案》针对司机的个人信息,1996年制定的《健康保险便

携性和责任法案》针对医疗健康类个人信息,1998年制定的《儿童在线隐私保护法》针对在线收集的儿童类个人信息,1999年制定的《格拉姆-里奇-布莱利法案》针对金融类个人信息进行保护,2008年制定的《基因信息非歧视法案》针对基因类个人信息,等等。综合而言,美国在联邦层面没有统一的个人信息保护法,其所制定的法律仅仅针对特殊类型或具有敏感性的个人信息。

敏感个人信息保护正式成型的关键节点是1981年由欧盟国家所主导的《在个人数据自动处理方面保护个人的公约》(以下简称《108号公约》)。^[17]这部公约将“种族出身、政治观点、宗教或其他信仰、健康或性生活”、与犯罪记录相关的个人数据等列为“特殊类型”的数据,并规定除非成员国法律提供充分保护,不得对此类数据进行自动化处理。^[18]不过《108号公约》并没有设定统一的敏感个人信息保护规则,各缔约国可以自行采用不同的保护措施。其后,1995年欧盟制定的《数据保护指令》采取了开放列举的界定方法,将“揭露种族或民族出身、政治观点、宗教或哲学信仰、工会会员资格、有关健康或性生活”的数据列入“特殊类型”范畴,但规定成员国可以在此基础上增添敏感个人数据的类型。在处理规则方面,《数据保护指令》规定除非具有个人“明确同意”等合法性基础,成员国原则不得处理此类数据。^[19]2016年制定的《一般数据保护条例》继承了《数据保护指令》关于敏感个人数据的大部分规定,同样规定了除非获得数据主体的明确同意以及为了少数特定目的,数据处理者原则上不得处理敏感个人数据。不过《一般数据保护条例》也有若干不同:一是扩大了敏感个人数据的范围,在列举范围中增加了基因数据、生物特征数据、性生活和性取向几类数据;二是采取了穷尽式列举的方法,明确规定敏感个人数据只限于其列举的类型,成员国不得再增加敏感个人数据的类型。

在欧盟《一般数据保护条例》的影响下,美国州层面制定的综合性个人信息保护法也引入了敏感个人信息保护。美国加利福尼亚州于2020年制定的《加利福尼亚州隐私权利法案》首次引入了敏

感个人信息概念。根据其界定,这类信息主要包括:披露消费者社会保险、驾照、州身份识别、护照号码的个人信息,消费者的登录账户、金融账户、借记卡或信用卡号码,以及允许访问账户的任何必需的安全或访问代码、密码或凭据,消费者的精确地理位置,消费者的种族或民族出身、宗教或哲学信仰或工会会员资格,消费者购物中心、电子邮件和短信的内容,消费者的基因数据、生物特征信息,与消费者健康、性生活或性取向有关的个人信息。之后,美国科罗拉多州、弗吉尼亚州、犹他州、康涅狄格州的个人信息保护法也引入了敏感个人信息保护。^[20]

我国的敏感个人信息保护同样受到域外特别是欧盟的影响。在《个人信息保护法》制定之前,我国法律并未明文规定敏感个人信息。《网络安全法》《电子商务法》《消费者保护法》都未区分敏感个人信息与一般个人信息。《民法典》也没有采用敏感个人信息的概念,而是采取“私密信息”的概念,规定对“私密信息”适用隐私权的相关规定。不过在行政法规、国家标准层面,一些制度引入或采用了敏感个人信息概念。国务院于2013年发布的《征信业管理条例》规定,征信机构不得采集“个人的宗教信仰、基因、指纹、血型、疾病和病史信息”。2013年实施的国家标准《信息安全技术公共及商用服务信息系统个人信息保护指南》明确提出了个人敏感信息,将其界定为“一旦遭到泄露或修改,会对标识的个人信息主体造成不良影响的个人信息”。该标准还提出,“各行业个人敏感信息的具体内容根据接受服务的个人信息主体意愿和各自业务特点确定。例如个人敏感信息可以包括身份证号码、手机号码、种族、政治观点、宗教信仰、基因、指纹等”^[21]。2021年,《个人信息保护法》借鉴了欧盟的相关规定并结合我国国情,正式在法律层面确立了我国的敏感个人信息保护制度。

(二) 敏感个人信息场景化的具体表现

综合敏感个人信息保护的发展历史可以发现,敏感个人信息的界定与保护取决于不同因素,这促成了敏感个人信息的场景化特征。以美国为例,美

国联邦层面之所以对某些特定领域进行立法,是因为这些领域的个人信息处理产生了较大风险,特别是此类风险引起了公众关注。例如,针对征信个人信息立法是因为20世纪70年代美国征信企业获取了大量的消费记录等信息;针对教育个人信息立法是因为很多教育机构泄露学生的个人信息;针对规制机构的个人信息立法是因为美国的水门事件等一系列事件引发了公众对于美国政府的不信任。在此类立法过程中,一些突发性的公共事件也促成了美国国会立法,从而将一般个人信息转换为敏感个人信息。例如,美国著名的保守派法官罗伯特·伯克在被里根总统提名为美国最高法院法官人选后,其个人录像租借记录被一些记者获取和报道,导致其提名失败,这一事件促成了1988年的《视频隐私保护法》。再比如,一位疯狂的粉丝通过购买司机的驾驶信息,找到并枪杀了好莱坞女星丽贝卡·谢弗尔,这一事件促成了1994年制定的《司机隐私保护法案》。^[22]

相较而言,欧盟对敏感个人信息的界定与保护偏重身份性因素,与反歧视的制度目标密切关系。^[23]分析欧盟在多个文件中所列举的敏感个人信息,会发现其主要类型都是容易导致身份歧视的个人信息。《108号公约》《数据保护指令》和《一般数据保护条例》都包含了种族出身、政治观点、宗教或其他信仰等个人信息。《一般数据保护条例》所增加的基因数据、为了特定识别自然人的生物性识别数据以及和自然人健康、个人性生活或性取向相关的数据,也都与反歧视的制度目标密切相关。相反,一些可能导致人身财产损害却不太可能引发歧视风险的数据反而未被欧盟视为敏感个人信息。例如,即使是个人的金融账号与密码、家庭住址、个人通信信息等类型的个人信息,《一般数据保护条例》也没有将其列入敏感个人信息。有关调查表明,欧洲的很多民众也认为金融账号等信息具有高度敏感性,^[24]但欧盟《一般数据保护条例》等个人信息保护法并未将其列入敏感个人信息范围,反而将其他民众感知不那么敏感、但容易导致身份歧视的个人信息纳入其中,这凸显了欧盟的个人信息保护法将

反歧视视为其核心制度目标。^[25]

我国的敏感个人信息保护受到欧盟与美国的影响,但具有鲜明的中国国情因素。一方面,我国《个人信息保护法》中的敏感个人信息保护类似欧盟,其列举的“生物识别、宗教信仰、特定身份、医疗健康”等敏感个人信息也与欧盟的规定基本重合。这种列举表明,我国也将反歧视视为个人信息保护的目标之一。但另一方面,我国《个人信息保护法》将敏感个人信息界定为“一旦泄露或者非法使用,容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害”,并且将“金融账户、行踪轨迹”也列举为敏感个人信息,这充分说明我国的敏感个人信息保护并不局限于反歧视,而是具有保护公民人身、财产以及其他人格尊严等多重目标。而且,即使是反歧视这一制度目标,我国的个人信息保护法也与西方存在较大区别。由于美欧历史传统中较为特殊的种族、民族等歧视,西方的反歧视具有较为强大的反区分传统(anti-classification)或“遮蔽身份”(identity-blind)的观念,^[26]这使得西方特别是欧盟将某些特定类型的身份性信息视为天然具有敏感性^[27]。我国与欧盟的反歧视观念与面临的问题并不完全相同,我国更注重个人身份所引发的个体侵害与社会不公,而非消除所有的身份识别。例如,对于“民族”类信息,我国并不认为识别个人民族信息就一定会导致歧视,而是将民族信息视为辨识公民身份的公开或半公开信息。《个人信息保护法》的一审稿曾经将个人的“民族”信息也列举为敏感个人信息,但在终稿中被删除,就反映了我国与西方在看待敏感个人信息方面的差异。

综合而言,某类个人信息之所以敏感或不敏感,并非这类个人信息天然敏感或不敏感。相反,某类个人信息之所以敏感,是因为此类个人信息涉及某些重要的个人权益,对其进行处理或保护不当会带来重大风险;在不同场景下,处理某类个人信息所带来的风险非常不同,这就导致了敏感个人信息的界定容易受到多重因素的影响。

四、敏感个人信息界定的解释性重构

在我国与域外对敏感个人信息进行事前统一

界定的背景下,可以通过法律解释将敏感个人信息的界定合理化。本部分分别从解释方法、价值判断、考虑因素出发,对我国敏感个人信息的界定进行解释性重构。

(一)敏感个人信息的解释方法

由于数字时代的立法面临一系列滞后性与不适应性的难题,在解释方法上应对《个人信息保护法》第28条采取目的解释的方法,将“敏感个人信息是一旦泄露或者非法使用,容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害”作为判断敏感个人信息的最终依据。而对于法律所列举的“生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息,以及不满十四周岁未成年人的个人信息”,则可以将其作为参考标准而非终极标准。

采取目的解释的方法可以使得敏感个人信息界定更为合理。一方面,即使立法者明确列举了敏感个人信息的类型,这些个人信息也可能敏感程度不高,对其进行更严保护并不合理。例如,《个人信息保护法》所列举的特定身份未必比其他个人信息更为敏感,很多人都愿意公开或半公开自己的职业、社团归属等特定身份,并不觉得这类信息有多敏感。个人行踪轨迹也未必比个人家庭住址更为敏感,很多人可能愿意公开自己的行踪轨迹,但不愿意公开自己的家庭住址,因为公开自己的行踪轨迹主要涉及少量个人隐私,而公开家庭住址则可能给自己和家人带来侵扰甚至是安全威胁。另一方面,法律未列举的个人信息也可能在很多场景下具有高度敏感性,将它们视为非敏感个人信息可能造成保护不足。例如,个人照片、个人声音、个人视频、家庭住址、工作单位地址、阅读记录、网页浏览记录、消费购买记录,甚至是个人的IP地址、个人的Mac号、车架号等设备类信息,都可能成为敏感个人信息,这些信息不但可以推断出个人的生物识别信息、行踪轨迹等个人信息,而且一旦被犯罪分子掌握,也可能给个人带来较大风险。

文义解释的方法则可以作为界定敏感个人信息的参考方法。对于我国法律所列举的7种敏感个

人信息,可以将其作为判断某类个人信息是否为敏感个人信息的重要参照,例如,可以推定这些属于敏感个人信息,但允许相关主体根据目的解释的方法对这些归类进行辨析。一方面,法律法规既然将某些个人信息列举为敏感个人信息,这些列举就反映了立法者的考量,而且这些列举也较为清晰。如果完全不顾法律法规的列举类型,则立法的权威性将受到威胁。另一方面,立法者对于敏感个人信息的界定也明确了以保护目的作为最终依据。在敏感个人信息具有不确定性,敏感个人信息与非敏感个人信息容易相互转换的背景下,如果以文义解释为最终依据,则法律对于个人信息相关的权益就可能保护过严或保护不足,违背了敏感个人信息保护的初衷。

(二) 敏感个人信息界定中的价值判断

就价值判断而言,敏感个人信息的界定首先应首先结合我国国情,由我国民众对其进行判断。对于何谓敏感,不同国家和地区往往有不同价值取向。惠特曼曾经提出,欧洲人常常以“尊严”的视角看待隐私,而美国人则常常以“自由”的视角看待隐私。^[28]在立法层面,欧洲各国在2018年《一般数据保护条例》实施之前对敏感个人信息进行了不同界定。例如,德国和奥地利等国家长期拒绝对敏感个人信息进行法律统一界定;芬兰将工会成员信息纳入敏感个人信息;葡萄牙和爱沙尼亚将基因数据列入敏感个人信息,但将个人财物数据排除在外。^[29]《一般数据保护条例》统一界定了敏感个人信息,对其进行封闭式的列举。但这种做法的主要目的是统一欧盟法与欧盟的“数字统一市场战略”(digital single market strategy),避免欧盟个人信息保护的分裂割据,而不是指这类列举就是普适性、无可争议的。

对我国而言,敏感个人信息更应当结合我国的具体国情进行判断。与欧盟和美国不同,我国的隐私与个人信息保护文化与我国独特的政治、经济、社会现状密切相连。在法律解释与适用层面,我国对于敏感个人信息的界定也应当以我国民众对于个人信息敏感性的价值判断为最终标准。当然,在

数据跨境流通问题上,敏感个人信息涉及不同国家和地区,当我国和其他国家与地区对于敏感个人信息的判断标准不同而导致数据跨境难题时,对敏感个人信息的判断就不能仅仅采取单边主义的立场,而应根据相关协议、标准与双边磋商来解决。^[30]

在具体风险认知问题上,应注重中立性专业人员对敏感个人信息的判断,^[31]同时结合普通个人对敏感个人信息的风险感知。在个人信息的敏感性判断中,专业人员往往依据个人信息泄露或违规使用带来的实际风险进行客观判断,而个人则常常依据其感知进行主观判断,二者并不总是一致。笔者认为,应首先注重中立性专业人员的判断,因为此类判断不仅可以合理判断与预防相关风险,还可以提供相对客观统一的标准。^[32]同时,法律也应当兼顾公众或普通个人的一般风险感知,因为公众的风险感知关乎民众对于个人信息处理的信任。^[33]如果公众对个人信息保护丧失信心,那么即使个人信息处理没有造成实际风险,也会影响个人信息的合理保护与合理利用。^[34]当然,参与判断个人信息敏感性的应当是一般民众,而非具体的个体。具体个体对于个人信息敏感性的判断千差万别,如果以每个个体的感知作为判断标准,敏感个人信息将完全无法判断。

(三) 敏感个人信息界定的考虑因素

其一,个人信息的敏感性应考虑个人信息主体的身份。一些风险防御能力较弱的当事人的个人信息应归入敏感个人信息,其中,最为典型的是未成年人个人信息。未成年人由于心智尚未成熟,缺乏自主意志,其个人信息处理可能带来较大风险。^[35]某些场景下的老年人也可能处于弱势地位,具有较高的被侵害可能性。例如,老年人的联系信息一旦被诈骗分子获取,再加上其他部分可信信息,就可能会成为电信诈骗的重点对象。残障人士、性少数群体等主体由于在社会上较为容易遭受歧视,反映这类群体身份的个人信息应当被认定为敏感个人信息。不过正如上文所述,我国的个人信息保护虽然将反歧视作为重要目标,但并不是将其作为唯一目标。《个人信息保护法》第28条明确提到敏感个

人信息的界定范围要考虑“人格尊严”“人身、财产安全”等因素,说明个人信息与敏感个人信息所要保护的法益更为多重,与反歧视法的制度框架并不完全重合。就此而言,一些不具有歧视风险的个人信息主体可能会因为其身份而被纳入敏感个人信息,例如未成年人;一些具有一定歧视风险的个人信息主体则可能不会因为其身份而被纳入敏感个人信息,例如女性群体。此外,特殊身份的处理也可能有助于反歧视。^[36]

其二,个人信息的敏感性应考虑处理主体。目前,各国法律实务与法学研究没有对个人信息的处理主体作出明确界定,或者进行了不同界定。例如,我国《个人信息保护法》没有明确说明识别个人信息的主体,第28条对敏感个人信息的界定中也未明确说明造成侵害风险的主体;欧盟《一般数据保护条例》“重述”第26条规定,个人信息识别的主体包括“控制者或其他人”;英国的信息委员会(ICO)规定,个人信息的识别主体为“有动机的侵入者”;^[37]美国早在20世纪70年代就通过《隐私法》将政府机构视为重点规制对象。对于不同的处理主体或识别主体,个人信息的敏感性将非常不同。例如,对于进行自动化处理的大型企业而言,个人家庭住址、工作单位地址可能并不敏感,因为大型企业一般都对这类信息进行加密化、去标识化处理,大型企业处理此类信息一般不会直接带来风险。但对于潜在的个人处理者而言,此类信息则具有高度敏感性,因为个人处理者更有可能泄露此类信息,对他人生活安宁与家庭安全造成威胁。国家机关与非国家机关处理个人信息所带来的风险与所涉敏感个人信息的界定也存在区别,因为二者对个人信息的利用方式、保护方式、侵害风险都非常不同。^[38]此外,在分析判断敏感个人信息时,还需要分析个人信息是否被其他处理者共享或者违规泄露,如果信息被共享或违规泄露可能被哪些主体获取。

其三,敏感个人信息界定应考虑信息处理方式。个人信息的处理方式千差万别,罗纳德·李恩斯曾经归纳了不同识别类型:L类查找型识别(look-up)是为了查找某一个体,例如,通过姓名、电话或护

照号码等标识符对特定个人进行查找;R类确认型识别(recognition)是为了验证某人的身份,例如,利用人脸识别信息验证银行顾客的身份;C类归类型识别(classification)是为了对某人进行归类,例如,将某人归入某一种族或某一消费群体;S类会话型识别(session)是为了不同设备之间的交互与对话,例如,网站利用cookie技术识别顾客先前添加在购物车里的购买商品,以便进行下一步操作。^[39]在不同的识别类型中,个人信息的敏感性会发生变化。例如,在L型查找型识别的情况下,身份证号码、护照号码等具有唯一标识性的识别可能导致特定个体被唯一识别,此类个人信息理应归入敏感个人信息的范畴。但在C类归类型识别或S类会话型识别中,身份证号码、护照号码不仅不具有敏感性,甚至都无法直接识别个人。而对于种族出身、政治观点、宗教或其他信仰、性取向等身份类信息而言,这类信息可能在C类归类型识别中识别个人的特定身份,带来歧视风险,但在其他识别类型的识别中,这类信息则很难直接识别具体个人,其敏感性程度要低很多。

其四,敏感个人信息界定应考虑信息被识别的概率或可能性。敏感个人信息在被收集后,信息处理者往往对其进行一定的加密、去标识化处理,但此类个人信息一般仍然被认为属于个人信息,因为其仍然可以被间接识别或通过关联的方式而识别个人。不过从侵害风险来看,个人信息的识别程度显然会影响个人信息的敏感性。^[40]如果个人信息被识别的概率较高,其可以轻易被直接识别,则此类信息应具有更高的敏感性;相反,如果个人信息被重新识别的概率较低,则此类信息的敏感性应较低。个人信息的扩散性则是个人信息被识别概率的另一个维度,个人信息已经在多大程度上公开,是否容易进一步扩散,会直接影响个人信息被不特定主体识别的概率。^[41]在司法实践中,曾有案例对司法诉讼文书中所公开的姓名、性别、家庭住址、电话号码等个人信息是否属于敏感个人信息有过争论。^[42]判断这类有限公开的个人信息是否属于敏感个人信息,应结合其进一步扩散所增加的识别概率

以及可能带来的风险进行分析。

需要强调的是,敏感个人信息由于其场景化特征,其判断因素并不局限于上述列举因素。在域外,已有众多学者对其进行讨论,例如,法理学与个人信息保护领域研究的专家雷蒙·瓦克斯指出,敏感个人信息界定应当结合信息披露的规模、信息的历史久远程度、信息的可能接受者等因素进行综合考虑。^[43]信息隐私领域研究的学者海伦·尼森鲍姆也提出,隐私保护应当考虑具体场景,分析个人信息所涉及的行为者、信息种类、传输原则等要素。^[44]我国学者也进行了类似的讨论与分析。例如,有学者指出,敏感个人信息应当结合“泄露该信息是否会导致重大伤害”“给信息主体带来伤害的几率”“社会大多数人对某类信息的敏感度”这三个因素进行判断。^[45]有学者认为个人敏感数据应以“损害后果、一般隐私期待”为判断标准的静态列举模式结合以“损害后果、一般隐私期待、使用目的”为标准的动态场景模式予以认定。^[46]有学者主张结合“损害的严重性、发生可能性、公众认可度、技术可预见性等因素”判断个人信息的敏感性。^[47]有学者从个人信息内容与个人信息所处的环境进行分析,主张分析个人信息是否“具有强工具性和唯一识别性”,分析“信息处理者的认知能力、信息应用能力及信息存在状态”。^[48]还有学者指出,应当“综合考量个人信息主体、信息处理者、第三方主体、信息性质和处理目的等五个要素,动态界定敏感个人信息”。^[49]这些观点各自提供了独特视角,也揭示了敏感个人信息的场景化特征。^[50]本文的研究与这些研究具有一定的共通性,但本文和其他学者所列举的因素仅仅有助于分析某类个人信息在具体场景下是否具有敏感性,而非可以衡量某一类型个人信息是否必然属于敏感个人信息,因为,个人信息并非由于其本身而敏感或不敏感,其敏感性会随着具体场景而变化。

五、敏感个人信息保护方式的解释性重构

敏感个人信息的保护方式也应当通过法律解释进行重构。首先,基于法律解释的敏感个人信息保护应当抛弃“先界定、后保护”的保护方式,转

为在不同场景中对敏感程度不同的个人信息进行区分保护。其次,敏感个人信息的强化保护框架应当给予信息处理者一定的自我监管空间,在此基础上进行强制监管,促使其保护措施与具体场景中的风险相适应。最后,应认识到隐私权与个人信息保护两种制度的差异,在此基础上实现私密信息与敏感个人信息制度衔接的协调。

(一) 从二元区分到行业区分与个案区分

上文提到,由于敏感个人信息的高度场景化,包括索洛夫在内的一些学者主张彻底抛弃敏感个人信息,转而关注个人信息的使用、伤害和风险。笔者认为,索洛夫的这种分析对于揭示敏感个人信息的高度不确定性具有重要意义,但其提出的这一对策过于激进,忽略了当今人们普遍接受敏感个人信息的现实,而且也不符合个人信息分级分类保护的要求。更为合理的方案是,在承认与接受敏感个人信息的不确定性的基础上,采取更具有操作性、动态性和贴近个人信息场景化特征的保护模式。这种保护方式并不直接依赖于法律法规对个人信息的界定,而是根据不同场景对不同个人信息进行动态保护。事实上,对于一般个人信息,索洛夫自己也采取这种进路,批评欧姆放弃个人信息界定的主张。欧姆曾主张,在大数据时代,个人信息与非个人信息的区分已经没有意义,任何非个人信息都可以演变为个人信息,因此应当放弃个人信息这一概念,改由风险规制的路径对相关信息实践进行规制。^[51]但索洛夫批评了这种主张,指出个人信息概念仍可以作为一种有效的制度工具,并提出已识别个人信息、可识别个人信息、不可识别个人信息的三元保护框架。^[52]在敏感个人信息问题上,索洛夫前期较为实用主义与稳健性的主张应该得到延续,其废除与取消敏感个人信息的主张则过于激进,反而是欧姆教授在敏感个人信息问题上的稳健性立场值得肯定。^[53]不过,为了适应敏感个人信息界定的场景化特征,法律也应当避免对其进行事前统一界定,在行政监管与司法或行政执法案例中采取更为场景化的保护方式。

在行政监管层面,相关法律解释与行政法规、

规章可以对敏感个人信息采取自下而上的场景化保护方式。该保护方式指的是,法律避免在较高级别对敏感个人信息进行统一强化保护,但在较低位阶的规章、行业标准、具体领域操作规范层面对敏感个人信息进行分领域与分场景界定。尤其是在各个行业性与细分领域,由于具体行业与细分领域的业态相似,其处理个人信息的收集方式、种类、利用方式、存储与保护方式、泄露与下游风险都会具有类似性,因此由具体行业与细分领域对敏感程度不同的个人信息进行区别保护更具合理性。此外,具体行业与细分领域制定的行业标准与领域规范也更容易调整,可以根据个人信息所带来的风险动态调整不同类型个人信息的区别保护,^[54]避免高级别的法律法规制定后所形成的滞后或步调不一致问题。

在司法或行政执法案例中,法律应通过个案对敏感个人信息进行场景化保护。相比监管规则,敏感个人信息的司法或行政执法案例既有弱势也有优势。弱势在于,司法或行政执法案例往往缺乏专业机构所需要的专业性人才,而且对于相关案例的裁决都是事后的,难以对敏感个人信息进行事前规制与事前风险预防。不过司法或行政执法案例对敏感个人信息保护也有优势。首先,在司法或行政执法案例中,裁决者具备接触正反双方意见的机会,可以通过双方举证、辩论等形式而深入个人信息实践的具体场景,这可以使裁决者获取更为完整全面的信息,更为场景化地感知某一具体场景下个人信息的敏感性。其次,敏感个人信息的事前界定常常不科学,存在过宽和过窄保护,而敏感个人信息的事后保护则可以避免此类问题。通过案例来形成敏感个人信息的相关规则,也是许多国家在个人信息保护领域的长期实践,更为符合敏感个人信息与一般个人信息保护的相关特征。例如,美国联邦贸易委员会积累了丰富的个人信息保护实践判例,形成了个人信息保护的“普通法”规则;^[55]欧盟法院、欧洲人权法院以及欧盟各国监管机构的判例已经成为个人信息保护的重要法律渊源;欧洲数据保护委员会(EDPB)在其发布的各类个人信息保护指南

中也列举了大量案例,通过案例来阐述和把握其个人信息保护的一般规则。我国近年来也积极在法院与监管部门推动个人信息保护的典型司法案例与执法案例,以此应对个人信息保护的场景化与不确定性问题。通过司法或行政执法案例保护敏感个人信息,更符合一般原理。正如大量研究表明,通过自下而上的案例串联来形成规则,在很多场景中比自上而下的规则确定更为合理。即使在成文法时代,司法或行政执法案例也具有其独特优势,应当发挥其制度功能。^[56]

(二)敏感个人信息统一强化保护的重构

对敏感个人信息进行一般性的强化保护,可能同时导致保护不足与保护过度。解决上述困境,应首先认可信息处理者具有较强能力和一定动力对敏感个人信息进行强化保护。在实践中,信息处理者也会对个人信息进行分级分类保护,但这种分级分类并不一定对应敏感与非敏感个人信息的二元划分和二元保护措施。在有的情形中,信息处理者可能对某些看似非敏感的个人信息进行严格保护。例如,社交软件企业一般对通讯信息、小范围公开的朋友圈信息进行最高级别保护,严防此类信息的泄露与违规使用。在其他情形中,信息处理者可能将信息的敏感性分为两级以上的多个级别,或者对所有信息进行一体化的严格保护,而非仅仅将其列为敏感个人信息与非敏感个人信息。对于信息处理者自发采取的敏感个人信息保护或分类分级保护,法律应给予信息处理者自我规制一定的空间,允许信息处理者对敏感个人信息进行一定程度的自我界定、自我分级与自我监管(self-regulation)。

不过信息处理者的分类分级保护也应当受到法律的强制性监管,而非完全的自我监管。完全自由放任的自我监管可能带来一系列问题。信息处理者的分类分级保护可能并不科学合理,甚至可能通过虚假的分类分级保护规避监管。例如,信息处理者可能采取“代理”(proxy)策略,即通过处理非敏感个人信息实现对敏感个人信息的处理。信息处理者也可能刻意混淆与掩盖其处理敏感个人信息所带来的风险,或者并未采取与处理敏感个人信息

风险相应的保护措施。在这些情形中,完全自我监管都可能导致大量敏感个人信息无法得到合理保护。^[57]尤其是一些没有市场竞争压力、从第三方获取信息的信息处理者,以及没有严格上级监管压力的公权力机构,由于缺乏外在压力,他们在进行信息处理时往往缺乏对个人信息进行合理保护的动机,同时也没有足够的个人信息保护能力。在这类情形中,应当避免赋予此类信息处理者的自我监管权力。^[58]赋予信息处理者对敏感个人信息进行一定程度的自我监管,应当仅限于已经采取严格个人信息保护措施的信息处理者。法律对于敏感个人信息的保护在发挥信息处理者积极性的同时,应当积极履行其整体性的监管职责,实现“监管下自我监管”(regulated self-regulation)。^[59]

首先,就敏感个人信息处理的合法性基础而言,机械性地监管将导致个人信息保护与利用平衡的难题。一方面,如果对合法性基础进行严格解释,要求处理所有可能推断或演化为敏感个人信息的信息都必须满足“特定的目的和充分的必要性”,将导致大量一般个人信息无法得到合理利用。另一方面,如果对合法性基础进行宽松解释,允许信息处理者处理所有并非具有显著敏感性的个人信息,则信息处理者可以轻松规避法律对于敏感个人信息的强化保护。为避免此类困境,法律应当赋予信息处理者一定程度的自我规制,允许其对处理敏感个人信息的必要性进行解释与说明,但同时应当对这类解释与说明进行严格监管,预防信息处理者过度收集与处理不必要的敏感个人信息。在这一过程中,法律应当重点监管收集与处理对产品或服务不具有改善作用的敏感个人信息。

其次,在告知同意流于形式的背景下,机械性解释告知同意将无助于法律真正保护敏感个人信息,^[60]反而给用户体验带来更多的干扰^[61]。为了真正发挥告知同意的作用,一方面,信息处理者应当在符合业务场景与遵循行业惯例的情形下对告知同意进行一定程度的优化设计,避免过多弹窗、同意选项对个体造成的侵扰;另一方面,法律应当对信息处理者的告知进行重点监管,对处理敏感个人

信息所带来的风险,法律应要求信息处理者在其隐私政策中进行重点说明与详细披露,以便为信息处理者内部组织、执法机关、社会组织与个人提供信息索引。^[62]告知同意虽然无法在交互场景下让个体充分知情,但对于信息处理者内部组织、执法机关、社会组织与非交互场景下个人,却可以成为他们的个人信息说明书,有利于敏感个人信息保护从高度依赖个体本位保护走向社会保护与合作治理。^[63]因此,敏感个人信息告知同意制度的设计虽然可以适度放松,但应当充分履行处理敏感个人信息的特殊告知与说明义务。

最后,就安全保护措施而言,以形式合规要求信息处理者采取相关措施,信息处理者可能也会采取形式主义的对策,即在形式上采取相关措施,但实质上却未必真正合理保护敏感个人信息。为了避免安全保护措施走向形式主义,法律应当允许信息处理者采取符合具体场景与现实风险的保护措施,同时对此类自我监管措施进行监管。目前,《个人信息保护法》在安全保护措施方面设置了事前个人信息影响评估,事中加密、去标识化、专人保护,事后实施应急预案等措施。敏感个人信息保护除了按照法律规定应当进行事前个人信息影响评估,加密、去标识化等保护方式也应当被重点监管,以降低敏感个人信息的泄露风险与侵害风险。

(三) 私密信息与敏感个人信息保护衔接的重构

对于私密信息与敏感个人信息保护的衔接,应首先认识到私密信息与敏感个人信息是隐私权保护与个人信息保护两种制度下的概念,应在两种制度框架中分析二者的区别与关系。就隐私权保护与个人信息保护而言,二者的核心区别是隐私权保护属于传统人格权保护的范畴,^[64]其保护以侵权法为依托,将侵权方与被侵权方拟制为一对一的平等主体。而个人信息保护则是一种公私法混合的制度,其针对的是信息处理关系。^[65]波斯特将这两种制度区分为尊严隐私与数据隐私。^[66]个人信息保护制度之所以产生,是传统的隐私权保护无法应对具有“大规模微型侵权”特征的信息处理关系。在处理

关系中,个人很难对较为隐蔽和专业化的个人信息处理进行预防与救济。为了解决隐私权保护的不足,在个人信息保护框架中,法律除了仍然对个体进行赋权之外,同时引入了国家保护义务与监管责任,^[67]以此弥补个体救济能力与动力的不足。

从隐私权保护与个人信息保护的关系出发,就能理解私密信息应基于侵权法在司法个案中判断,其范围无需也难以进行事前界定。《民法典》第1032条第2款规定,“隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息”;第1034条第3款规定,“个人信息中的私密信息,适用有关隐私权的规定;没有规定的,适用有关个人信息保护的规定”。《民法典》在引入私密信息概念的同时,并未对这一概念进行界定。不过从私密个人信息所依赖的侵权法特征来看,这种立法留白反而更为合理。因为相比敏感个人信息,私密个人信息的判断更具有主观性,更可能因为人际关系等场景的变化而变化,也更可能因为具体人际关系和信息获取规范的变化而变化。^[68]例如,家庭住址信息是否为私密信息,如果涉及私密信息侵权的原告和被告为朋友关系,则人们可能认为此时的家庭住址信息不是私密信息;但如果原告和被告是陌生人关系,则人们可能认为此时的家庭住址信息属于私密信息。相对而言,敏感个人信息虽然也具有不确定性,但此类不确定性相对较弱。特别是在具体行业与细分领域,对敏感个人信息的范围以及如何处理此类信息有一定的共识。对私密信息则很难进行此类行业性与领域性界定,因为私密信息的概念是隐私侵权的下位概念,一旦个案中的隐私侵权成立,则该案中涉及的个人信息在这一个案中就成为私密信息。反之,当个案中的隐私侵权不成立,则该案中涉及的个人信息就不应当被认定为私密信息。

私密信息保护与敏感个人信息保护两种制度也可以更好衔接。对于不存在信息处理关系的情形,应在具体司法个案中确定私密信息的范围,因为这类情形主要依赖于侵权法保护,并不涉及一般行政释对敏感个人信息保护进行重构,使得这一制度更加合理。具体而言,对敏感个人信息相关法律法规

监管。较为复杂的是存在信息处理关系,^[69]而又同时提起隐私权之诉与个人信息之诉,此时就可能同时涉及私密信息保护与敏感个人信息保护两种制度的衔接。例如,在“朱某诉百度公司隐私权纠纷案”中,朱某在某互联网企业搜索“减肥”“丰胸”等关键词后,会在浏览相应的网页时出现诸如“减肥”“丰胸”“人工流产”等广告。^[70]在此类案件中,如何界定私密信息与敏感个人信息?在笔者看来,此类情形的基本原理仍然未变,仍然应按照隐私权保护与个人信息保护的不同制度框架来判断。就私密信息而言,其分析关键是此类信息处理在特定场景与关系中是否违背个体的合理隐私期待;就敏感个人信息而言,其分析关键则是此类个人信息处理是否违背了互联网广告行业对于敏感个人信息的界定,以及结合个人信息主体的身份、识别主体、处理方式等因素,分析此类情形的处理是否给个人带来较高风险。^[71]总而言之,只要从隐私权保护与个人信息保护两种制度框架出发,私密信息与敏感个人信息保护的关系就可以迎刃而解。

六、结语

作为个人信息分类分级保护的制度工具,敏感个人信息的统一界定与特殊保护在立法层面已经成为我国和大多域外国家和地区的共识。但在界定上,敏感与非敏感个人信息的边界日趋模糊。在保护方式问题上,敏感与非敏感个人信息的二元保护框架、敏感个人信息保护的强化保护、敏感个人信息与隐私权和私密信息的交叉性也面临众多挑战。对这些问题与挑战进行分析,可以发现其根源在于个人信息保护的目标与特征。个人信息保护的目的在于通过个人信息保护具体场景中的相关权益与预防相关风险,而非保护个人信息本身。因此,个人信息的敏感性必然具有场景化特征,不可能一成不变或通过其本身去判断。

在各国立法或实证法对敏感个人信息统一界定与特殊保护具有高度共识的背景下,修改现行立法并不现实。较为现实与可行的方法是通过法律解释的解释应采取目的解释的方法,同时参照文义解释;对敏感个人信息的价值判断应以我国民众的价值

判断为最终依据，对敏感个人信息的风险认知应当以中立性专家为主、兼顾民众感知风险，对敏感个人信息的判断因素应当考虑个人信息主体、信息处理主体、处理方式、识别概率等因素。在法律解释与法律适用过程中，应当放弃绝对化的敏感与非敏感个人信息二元保护，转而采取动态化、场景化的分类保护。在涉及行政监管的法律解释中，应当采取自下而上的分类保护；在涉及司法与行政裁判的

法律解释中，应当采取案例式的分类保护。就涉及强化保护措施的法律解释而言，对敏感个人信息进行执法应当采取自我规制下的强制性规制。就私密信息与敏感个人信息的关系而言，应分别在隐私权保护与个人信息保护的制度框架下进行判断。综合而言，敏感个人信息保护制度虽然面临挑战，但通过对其进行解释性重构，这一制度仍然可以保持生机与活力。

智能时代的知识产权制度和理论发展

此处删除了原文脚注，全文请参见《法制与社会发展》2025年第3期，转载或引用请注明出处。

作者：张吉豫

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

如同哲学社会科学各学科一样，中国自主的知识产权法学必须立足当前时代、回答时代之问、适应时代所需、推动时代进步。那么，我们正处在一个什么时代？或者说，应当如何标识和表征我们所处的这个时代？在学术界，学者们从不同维度、用不同的概念（词语）标识和表征我们所处的时代，例如“信息爆炸时代”^[1]“知识经济时代”^[2]“技术经济时代”^[3]“信息时代”^[4]等等。这些概念和判断都从某个侧面揭示了现时代的特征。从知识产权法学和数字法学的视域和维度，本文倾向于把我们所处的这个时代称为“智能时代”。智能时代以智能科技革命为主要标志，以算法和代码为底层逻辑。智能科技革命呼唤知识产权保驾护航，推动知识产权制度创新，以系统完备的知识产权法治体系创造美好的“数字未来”。在此背景下，本文首先概括智能时代的鲜明特征，接下来分析智能时代的特征特别是智能科技发展在知识产权制度方面引发的现实问题和变革性驱动。在此基础上，提出知识产权界应

当以抢抓机遇的历史主动精神，坚持问题导向和实践导向，加快丰富、发展和创新知识产权理论，以积极回应时代性问题和变革性挑战。

一、智能时代的鲜明特征

智能时代的鲜明特征可以用“四化”概括，即数字化、智能化、全球化、法治化。这“四化”均包含知识产权元素，也全面推动着知识产权法律和法学的演进发展。

（一）数字化——智能时代是数字化时代

数字化，即信息的存在以及对信息的处理方式越来越趋向于数字形式。将许多复杂多样的信息转变为可以存储和计算的数字格式的数据，在计算机中建立起适当的数字化模型对数据进行分析处理，并通过数字技术重构传统工作模式或工作流程，这就是数字化的基本过程与现象。数字化时代是指，以数字技术为核心、以算力资源为运行基础、以网络通信技术为连接支撑、以数据资源为关键要素、以算法和模型为重要运作规则的信息时代。

数字化时代具有与既往时代不同的一系列鲜明特征：第一，数字技术被广泛应用。互联网、大数据、云计算、区块链、人工智能等技术的快速发展，改变了人们的生产、生活、工作以至生存方式和思维方式，使得信息传递更加迅速，数据处理能力大幅提升。第二，数据成为重要资源。在数字化时代，数据被视为新的生产资料。随着数据采集、加工和处理能力的迭代升级，数据资源在经济发展、民主政治、社会建设、社会治理、文化教育科技创新、生态文明演进等方面发挥了前所未有的作用。第三，产业结构转型升级。传统产业通过数字化转型，实现了生产方式变革、生产效率提高和业务模式创新，新兴产业如互联网经济、共享经济、零工经济等迅速崛起。第四，消费模式深刻变化。电子商务、移动支付、远程医疗、网络游戏等新模式的出现，极大地便利了人们的生活，也逐渐改变着人们的消费习惯和模式，极大提高了人类的物质生活和精神生活质量。第五，工作方式转型变革。远程办公、视频会议、灵活就业、智能辅助等新型工作方式逐渐普及，人们的工作时间和空间更加灵活，市场对劳

劳动者技能的要求也在悄然发生变革。第六,社会治理和环境治理智能化创新。将数字化技术应用于城乡社会治理、城市运行管理、公共安全维护、环境监督保护、城乡社会治理等领域,提高了社会和环境治理的精准性和效能。第七,教育模式转变。在线教育、混合式学习、人智互动等新型教育模式的发展,使得教育资源更加丰富、人们的学习方式更加个性化,推进了个体全面而自由的发展。第八,文化创新和传播多样化。数字技术促进了作品创造和文化传播的多样化,网络共创、网络文学、社交媒体、短视频、直播等新型文化形态层出不穷,打破了少数人对文化生产和传播的垄断,推动了人类文化多样化和文明交流互鉴。当然,数字化也对国家安全、社会稳定、公民权利等带来了不可忽视的挑战。随着数字化程度的加深、数字技术的广泛运用,网络安全、数据安全、公民个人信息安全等问题日益凸显,成为社会关注的焦点和依法治理的关键问题。

数字化在知识产权领域引发的影响最早也最为突出。不断创新的数字化内容、产品和服务已经融入人们工作和生活的方方面面,这不仅使知识创造的数量和传播范围较之数字化之前大幅度增长和拓宽,也带来了更多平衡知识产权保护与公共利益的需求。妮娃·埃尔金科伦(Niva Elkin-Koren)等指出:“直到20世纪的最后10年,知识产权法还只是法学研究与实践中的一个小分支……对知识产权整体关注的增长,特别是对经济利益的增长,是信息时代的副产品。”“知识产权对当今人类生活各个方面的重要影响是信息时代技术革命的结果。”^[5]数字化、信息化的发展浪潮构成了知识产权理论创新、制度创新、执法司法创新的重要推动力。

(二) 智能化——智能时代是人工智能泛在的时代

我们所说的智能时代,其本质规定和最显著的标志是人工智能技术的蓬勃发展和广泛应用。“人工智能是引领这一轮科技革命和产业变革的战略技术,具有溢出带动性很强的‘头雁’效应。”“人工智能加速发展,呈现出深度学习、跨界融合、人

机协同、群智开放、自主操控等新特征,正在对经济发展、社会进步、国际政治经济格局等方面产生重大而深远的影响。”^[6]

在智能化浪潮面前,党和国家高度重视新一代人工智能的发展。习近平总书记强调:“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。”^[7]新时代以来,我国政府一直把发展人工智能作为重要议题。2015年国务院出台的《关于积极推进“互联网+”行动的指导意见》就将“人工智能”纳入了重点任务。2017年,国务院印发《新一代人工智能发展规划》,强调“牢牢把握人工智能发展新阶段国际竞争的战略主动,打造竞争新优势、开拓发展新空间,有效保障国家安全”。^[8]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》更加明确地提出:“培育壮大人工智能、大数据、区块链、云计算、网络安全等新兴数字产业。”^[9]这些文件中关于推进人工智能发展的方针政策明确了人工智能持续健康发展的方向和路径,为推进我国进入智能时代发挥了积极作用。2024年11月发布的《生成式人工智能应用发展报告(2024)》显示,我国人工智能核心产业规模已接近6000亿元,知识管理、内容生成、自动驾驶、语音交互等各种人工智能应用系统正向纵深演进。^[10]根据国家互联网信息办公室(以下简称“国家网信办”)发布的生成式人工智能服务已备案信息公告,截至2024年12月31日,共302款生成式人工智能服务在国家网信办完成备案。^[11]人工智能作为基础性、驱动性的技术力量,与制造、医疗、教育、文艺、交通、农业等各个领域深度融合,创造出新产品、服务和商业模式,有效推动传统行业转型升级和社会经济结构变革。能够承载家居设备控制功能、家务助手功能、健康管理能力和安全监控能力等的人工智能产品已经开始进入寻常百姓家。在世界范围内,我国将率先迈进人工智能新时代。

如何建构智能时代的社会秩序是我们要回答的时代之问。人工智能技术的发展将朝向“以人为

本”“智元共生”的和谐生态和秩序迈进。“以人为本”是人工智能治理的终极关怀与首要理念，体现为，从人类福祉、人类安全、人的尊严和权利、人的全面发展出发，充分尊重和保障人权，确保人工智能解决方案以人为主体、人工智能的使用以人为中心，发展人工智能归根结底是为全体人民提供优质的公共服务，确保人工智能技术成果普惠共享。

“智元共生”指人类与人工智能通过双向赋能实现人机能力互补、和谐共生。其中，“智元”指具备深度学习能力和一定程度的自主决策能力的智能单元，如数字空间的人工智能体、物理空间的智能机器人等。随着人工智能体、智能机器人的进一步发展和应用，特别是人工智能作为新一代基础设施的构建，人机共生将成为常态。“共生”指人类与人工智能体、智能机器人通过数据共享、能力互补实现人机互动、人机和谐。在“智元共生”中，必须始终保障人的主体地位，坚持人类意志优先，确保人类对于人工智能的控制能力。

人工智能不仅为人类能力边界的拓展带来了新的可能性，也给知识产权制度带来了许多全新的发展与挑战。一方面，人工智能技术的研发和运用促进了知识产权事业的体量增长。截至2023年底，我国人工智能发明专利有效量达到37.8万件，同比增速超过40%，是全球平均增速的1.4倍。^[12]深度思索、豆包、kimi、通义千问、文心一言、讯飞星火等人工智能大模型产品和服务层出不穷、应用普及推广。人工智能也正在赋能加速更多更广泛领域的作品和发明创造的产生。另一方面，人工智能带来了新的知识创造模式、新的知识传播模式以及层出不穷的涉及知识的新的应用和商业模式，引起了许多涉及知识产权的法理探究和诉讼纠纷，为知识产权的进一步发展提出了时代之问。

（三）全球化——智能时代是“新全球化”时代、“再全球化”时代

20世纪中叶以后，人类社会快速进入全球化时代。全球化深刻地改变了人类的生产方式、生活方式、文化形态、思维方式，影响着人类社会的经济、政治、法律、文化、教育、科技发展。进入21世纪

之后，在互联网和数字科技的有力支撑和推动之下，全球化的程度急速加深。现在，人类的活动大多发生在全球层面。在这个全球社会交往互动的潮流中，或主动或被动，我们都是其中的一分子。用一个词语来形容这种现实，即“全球化”。“全球化”是社会科学领域最具普适性、共识性、标识性的概念，其表征着人类活动范围和组织形式从地方到国家再到世界范围的扩大。全球化不只是经济的全球化，还是人类社会经济、政治、文化、科技、环境、治理结构等方面的综合性发展趋势。

近年来，世界出现了一些“逆全球化”“反全球化”的思潮，产生了一些单边主义、保护主义、霸权主义现象。但是，我国始终坚持构建“人类命运共同体”的倡议和立场。尽管在一段时期和一些领域，全球化可能会面临一些困难和阻碍，但全球化的历史潮流不可阻挡，全球化的发展趋向不会改变。特别是以互联网、大数据、云计算、区块链、人工智能等为代表的数字科技的蓬勃发展、广泛运用，已经引领人类社会发生着数字化变革和智能化变迁，数字科技的连接和融合作用推动着全球化全方位深层次转型，形成了数字全球化新态势。数字全球化以无比强大的力量重新定义和证成了全球化的必然性和合理性。

以数字全球化为标志的新全球化、再全球化必然离不开知识产权及知识产权法律、法治和法学。例如，全球经济一体化和金融全球化强调资本、技术、商品、服务等经济要素的跨国流动和优化配置，以促进全球经济的迅速发展，但知识产权保护问题越来越成为国家之间尤其是发达国家和发展中国家之间的贸易谈判、签订协议的关卡问题。此外，伴随数字科技的发展，新的知识产权议题不断呈现。在数据跨境流动和全球流动、互联网治理、人工智能治理、大模型治理等方面，知识产权都是其中的焦点问题之一。涉及数字技术的跨国企业间的知识产权诉讼层出不穷。同时，信息高速公路、国际互联网的兴建，一方面使得信息无疆界流动成为可能，促进了全球信息的共享和交流，降低了交易费用，提高了效率，但是另一方面也引发了信息、数据使

用的不对称、不平等。在全球文化传播方面,各国的文学艺术作品可以通过数字化的载体在全球范围内被更便利地传播,这不仅使人们能够接触并欣赏到不同国家的文化、丰富人们的精神生活,还促进了全球文化的多样性和包容性,但这种传播和交流存在大量著作权等知识产权保护问题。知识产权激励和保护创作,但也可能成为文化信息流动的限制因素。不同国家和地区人工智能发展的差距则可能进一步加深数字鸿沟,影响文化多样性保护。一方面,国际社会倡导人工智能训练数据的多样性和包容性;但另一方面,其也需要保障训练后的人工智能能够更好地服务发展中国家和最不发达国家和地区。这也带来了新型的知识产权保护与社会福祉间的平衡和规则塑造问题。2024年7月1日,第78届联合国大会协商一致通过中国主提的加强人工智能能力建设国际合作决议,^[13]140多个国家参加了决议联署,^[13]这体现了新全球化时代数字互助、合作共建的需求。2025年2月,在法国举办的人工智能行动峰会上,60个国家和组织签署了《关于发展包容、可持续的人工智能造福人类与地球的声明》。《声明》既强调了能力建设,也明确将知识产权列为需要进行全球反思的重点问题。可以看到,在智能时代的全球化秩序塑造中,知识产权仍然是核心议题之一,也是最具难度的问题之一。对此,知识产权法学研究必须提供能够取得最佳平衡的智慧和方案。

(四) 法治化——智能时代是法治化时代

无论是互联网还是人工智能,都不是“法外之地”。在智能时代,我们既不能让算法随意暗箱操作,也不允许人工智能脱缰狂奔。数字科技自身的发展迫切需要法治引领、规范和保障。应将智能时代建构成为一个法治时代。

根据我国法学家张文显、李林、黄文艺等人的研究和概括,^[14]理论界普遍认为,法治化时代最鲜明的特征在于:法治成为国家和社会的核心价值,成为国家和社会治理的基本方式,成为支撑国家现代化的强大力量;法律规范科学完备统一,每一项立法都符合宪法精神、反映人民意愿、得到人民拥护,

切实保证国家统一、法制统一、政令统一、市场统一,有力保障经济发展、政治清明、文化昌盛、社会公正、生态良好;全体人民尊重法治、信仰法治、坚守法治,尊法学法守法用法护法在全社会蔚然成风;宪法具有极大权威,法律具有普遍实效,任何组织和个人都自觉在宪法法律范围内活动;人权和公民权利得到切实尊重和保障,公权力受到有效制约和监督;国家在国际关系和全球治理中拥有公认的话语权和规则制定权。

在全面依法治国实践中,法治化意味着国家各方面工作法治化。第一,国家改革、开放、发展、安全等具有全局性的各项工作,经济建设、政治建设、文化建设、社会建设、生态文明建设、国防军队建设等具有主干性的各项事业均应被纳入法治轨道,在法治化轨道上得到有序推进。第二,政党治理、政府治理、军队治理、社会治理、经济治理、互联网治理、人工智能等新兴科技治理、公共卫生治理、生态治理等,“一国两制”、港澳治理、外交事务等国家治理工作均应被纳入法治轨道,在法治化轨道上得到有效推进。第三,国家和地方的立法、执法、司法、普法等专门法治工作均应被纳入法治轨道,应依法立法、严格执法、公正司法、精准普法,在法治轨道上全面推进良法善治的法治中国建设。第四,应统领“两个大局”,综合考虑和运用国内国际两类规则,统筹推进国内法治和涉外法治,协调推进国内治理和国际治理,践行共商共建共享的全球治理观,积极参与全球人工智能治理、应对气候变化全球治理、联合国维和行动等。^[15]

近年来,世界各国已经纷纷关注到人工智能的发展与安全问题,特别是认识到,人工智能技术的发展和普及不仅会深刻改变人类的生活和工作方式,也可能带来权益保障、经济秩序、社会稳定、国家安全等方面的许多问题,包括对于知识产权制度的影响和挑战。为此,国家网信办等有关部门联合出台了《互联网信息服务算法推荐管理规定》《互联网信息服务深度合成管理规定》《生成式人工智能服务管理暂行办法》等部门规章,我国相关部门也发布了《新一代人工智能治理原则——发展

负责任的人工智能》《新一代人工智能伦理规范》《全球人工智能治理倡议》《人工智能安全治理框架》等一系列文件,以期逐步调整和建构智能时代所必需的社会秩序。此外,欧盟通过了《数字单一市场版权指令》《人工智能法》等一系列立法。美国白宫颁布了一系列关于人工智能的行政命令。特别是2024年9月22日,联合国大会未来峰会通过了《全球数字契约》(Global Digital Compact, GDC)(第79/1号决议)。《全球数字契约》提出,“为所有人创造一个包容、开放、可持续、公平、安全和可靠的数字未来”,并确立了以人权为基石、以发展为导向、以安全为底线、以治理为动力的基本原则。这些措施必将对全球数字技术发展和数字文明进步产生深远的历史影响。

在智能时代的数字治理中,知识产权法的发展刻不容缓。最近这些年,人们普遍关注智能时代数字科技研发和运用中的伦理问题、风险问题,但对于智能时代新型“创作”对社会思潮和社会文化的影响的研究不足,对于新兴知识产权的关注不够,法治建设跟不上对新兴知识产权的确认和保护迫切需要。对于智能时代日益复杂的、新形态的侵犯知识产权的问题应对不充分,也影响了知识产权法激励创新的制度功能的实效。法治建设是一个整体。上述人工智能相关的伦理和法治发展,也为知识产权法的进一步发展提供了重要基础。

同时,数字化、智能化时代的法治化建设是与数字科技、智能科技紧密结合的。以劳伦斯·莱斯格(Lawrence Lessig)为代表的研究者们对数字科技与法律的关系进行了深度探讨,推进了数字科技与法律的良性互动。^[16]推进“符合伦理的设计”(ethically aligned design)、“通过设计保障伦理”(ethics by design)等被认为是治理数字科技的重点路径。罗杰·布朗斯沃德(Roger Brownsword)在对“法律3.0”概念的阐释中,强调应利用技术性方案来实现政策目标,即应当通过技术措施,将规范性要求转化为实际的设计。^[17]数字科技与法治深度融合的新时代法治化,也是当前知识产权制度发展的重要背景。

综上所述,数字化、智能化、国际化和法治化是智能时代的鲜明特征,构成了知识产权制度演进的重要时代背景和发展动因。我们需要紧密结合智能时代的新特征、新发展,去探求知识产权法中争议问题的解决路径,进一步发展知识产权制度和理论。

二、智能时代科技创新引发的知识产权问题

上述关于智能时代特征的概括在总体上勾勒了这个时代的外部轮廓。科技的迅速发展进一步推动着社会的数字化、智能化程度,与全球化的发展与挑战、法律制度的回应与理论发展交织在一起,形成相互作用、相互影响的发展格局。在知识产权法的视域下,关注焦点突出地集中于时代发展的内在核心驱动力——创新,包括科学思想创新、技术创新、创作创造模式创新、经济组织形态创新、知识产权规则和制度创新、法律实施形态创新等环环相扣的全新实践。

当前,智能时代的科技创新已经引发了许多知识产权问题和争议,突出体现为:

一是主体的模糊与扩张争论。在智能时代,人工智能的发展一度使得知识产权主体范围面临模糊与扩张的困境。人工智能在创作、发明等活动中展现出超越以往工具的能力,人类对生成内容的创造性贡献程度较之从前有不同程度的减弱。人工智能生成的内容是否应被视为具有知识产权,进行了怎样贡献的自然人可以成为权利主体,乃至人工智能本身能否成为作者、发明人或者知识产权主体,已成为学界和实务界争论的焦点。例如,在一些著作权登记、专利申请实践中,人工智能系统DABUS(Device for the Autonomous Bootstrapping of Unified Sentience)被申请人斯蒂芬·塞勒(Stephen Thaler)博士主张为作者或发明人。尽管这些登记和申请几乎都被行政机构或法院否定了,但也出现过一些例外。例如,在澳大利亚的相关司法诉讼中,澳大利亚初审法院认为人工智能系统可以是发明人,^[18]但该判决被二审推翻。^[19]南非专利局则通过了以DABUS为发明人的申请。^[20]这些实践反映出,关于人工智能是否可以作为发明人的问题仍然存

有不同观点。但整体上而言,在当前阶段,主流观点认为,人工智能不具备主体资格。其核心理据在于,人工智能不具有自由意志。许多学者指出,现代法学上的主体概念是以意志自由为核心而建构的。^[21]德国学者卡尔·拉伦茨指出,民法上的“人”是从伦理学上的人的概念出发的。“这一概念的内涵是:人依其本质属性,有能力在给定的各种可能性的范围内,自主地和负责地决定其存在和关系、为自己设定目标并对自己的行为加以限制。”^[22]我国哲学家高海清指出:“究竟什么是‘主体’?在哲学术语中说得很复杂,其实道理是很简单的,核心一点,就是能否做到是你自己生命活动的主人。你做到了这点,就能通过生命活动去支配外界对象,你就是主体;你如果连本能都不能超越,只是生命本能的奴隶,那么,你就不会有主体性。这就是‘主体’的原始含义,它同人之为人的本性是联在一起的。”^[23]从人工智能治理中“以人为本”的原则及其理据出发,也可以更进一步形成对人工智能工具地位的共识。即使不考虑人工智能本身的主体地位问题,在实践中,关于人工智能生成作品的作者和发明人的认定也面临诸多挑战。以人工智能生成内容为例,对算法进行设计和优化的人工智能研发者、对训练数据进行筛选和标注的训练数据准备者,或者对内容生成进行具体提示词指导和调整的人工智能使用者,都或多或少地影响了输出的内容。这些主体是否可以被认定为作者?这些主体中的何者可以被认定为作者?或者,一个主体对内容生成作出了怎样的贡献或影响,才应当在法律上认定生成的内容是该主体的具有独创性的表达?这些问题看似主要是主体问题,实际上意味着,在智能时代,对于知识产权法中的“创作”“独创性”等基本概念,需要进行进一步的反思和理论塑造。

二是保护对象的创新与界定难题。智能时代带来了知识产权法潜在保护对象的创新与丰富,同时也引发了保护对象界定上的难题。

首先,人工智能生成内容,如人工智能生成的文章、图像、视频等,是否可以成为著作权法保护的对象?人工智能生成的技术方案、外观设计是否

可以被授予专利权?这些问题都是争议的焦点。其次,人工智能技术创新本身,如算法、大模型等,其可专利性也面临挑战。涉及人工智能算法的发明创造在何种条件下可以受到专利法的保护?对其创造性应当如何审查?充分公开要求如何具体化?这些问题涉及的规则关乎产业创新发展,也是国家知识产权局近年来的一项重点工作内容。面向新一轮科技和产业革命的需求,国家知识产权局在2019年末发布了《关于修改〈专利审查指南〉的公告》(第343号),专门增加了一节“包含算法特征或商业规则和方法特征的发明专利申请审查相关规定”。^[24]国家知识产权局还在2024年末发布了《人工智能相关发明专利申请指引(试行)》,^[25]以回应人工智能领域创新主体普遍关切的热点法律问题。这些工作推进了相关规则的发展,但关于具有一定通用性的人工智能相关发明的专利适格性、目前的充分公开标准是否恰当、人工智能生成发明是否必须填写发明人等问题,仍存在一些不确定性或争议,有待进一步深化研究。

此外,在智能时代,数据成为驱动经济和社会发展的新型生产要素,关于数据利用的纠纷频繁发生,特别体现在大量反不正当竞争案件之中。我国也开展了数据知识产权登记工作。是否应当建立数据产权制度?数据产权是否应被归类于知识产权?这些问题也亟待研究与回答。

三是权利保护面临挑战和机遇。一方面,在智能时代,知识产权保护面临全新的挑战。首先,随着智能技术的发展,知识的传播和利用方式发生了巨大变化。例如,智能推荐算法可以向每个用户定向进行个性化内容推荐,生成式人工智能可能动态性地产生侵权内容,这使得权利人保护知识产权的难度加大,但同时这些新技术的研发者、部署者在当下又难以彻底消除用户在使用中侵犯他人著作权的风险。再如,使用数据进行大模型训练及各种文本数据挖掘,是否可以构成合理使用,也是存在争议的话题。侵权责任的合理界定与分配,将深刻影响知识产权的保护和人工智能技术的创新发展,其中,技术发展的动态性也增加了判断合理注意意义

务的难度。如何在知识产权保护与技术创新发展之间取得良好平衡,成为知识产权制度面临的重要问题。其次,智能时代的许多技术创新都发生在“软件层面”,且往往部署在服务器端来供用户接入使用。这种特性增加了发现侵权、证明侵权的难度,需要在举证责任分配上进行考虑。另一方面,智能技术的发展也为权利保护和权利人的收益提供了新的机遇。区块链、智能合约、智能识别和过滤等技术的发展,为探索智能时代的权利保护机制提供了技术支撑。

智能时代知识产权法的发展是一个持续而动态的过程。上述问题是当前凸显的一些主要问题。随着科技的不断进步和社会的发展,知识产权法将面临更多新的挑战 and 机遇。持续研究和完善智能时代的知识产权法具有至关重要的意义。知识产权法的完善不仅关系到创新者的权益保护,更关系到整个社会的创新活力和经济发展。通过不断研究和完善知识产权法,能够更好地激发创新主体的积极性和创造性,促进智能技术的创新和应用,大力发展新质生产力,推动经济社会的高质量发展。同时,这也有助于维护公平竞争的市场秩序,保护消费者的合法权益,促进知识的传播和利用,增进社会的公共利益。

三、智能时代知识产权法律制度和法学理论发展的关键维度

对智能时代科技发展引发的知识产权问题的回应不应当是分散而孤立的,而应当紧密结合时代特征和发展趋势,在分析和解释法律问题对熟悉的概念和原则背后的理论基础进行更深层次的追问,以突破问题的表象,形成更具说服力和包容性的理论,从而作出妥善的解释或制度安排。从发展趋势来看,知识产权法应更加注重与数字科技、智能科技的深度融合,不断适应智能技术创新带来的创新保护需求和经济模式变迁,从而进一步完善知识产权法治体系。在立法方面,立法机关应更加积极地回应智能时代的新问题,为智能技术创新成果提供更有力的法律保障、更合理的制度预期。在司法实践中,司法机关应针对动态发展时期的知识产

权纠纷积极发挥司法能动性,通过一个个鲜活的个案裁判来确立有利于智能时代经济社会发展的司法审判规则。

本文认为,知识产权界应以回应智能时代提出的知识产权问题为新的动力和契机,对知识产权法中的核心理论问题开展新一轮的研究探索,为具体问题的解决提供理论基础和广泛共识,同时进一步推进知识产权法的理论化、体系化、现代化。

(一) 知识产权法保护对象理论的体系化建构

人类社会的发展,不断拓展着知识产权的可能边界,但知识产权法保护对象理论的体系化程度还不够充分。罗伯特·莫杰斯(Robert Merges)认为,知识产权法犹如发展中国家中无序蔓延的大城市,建筑施工随处可见,新的成长杂乱无章,而新增的建筑并不考虑旧城原有的构造及氛围。^[26]肖东梅也认为,现代知识产权法是一个综合性的法律规范体系,该领域正呈现一种无序的膨胀状态。客体扩张是知识产权制度变革最鲜明的外在表现。^[27]因此,我们需要进一步加强关于知识产权法保护对象理论的体系化研究,科学建构关于知识产权法保护对象范围的规则。

明确知识产权法保护对象的实质属性是对其进行体系化建构的基础,这样既可以厘清知识产权法各分支之间的内在关联性,又可以为新的对象之上的行为规范的建构提供基本理论和基本模式参考。以数据为例,2019年10月党的十九届四中全会通过的《中共中央关于坚持和完善中国特色社会主义制度推进国家治理体系和治理能力现代化若干重大问题的决定》指出,“健全劳动、资本、土地、知识、技术、管理、数据等生产要素由市场评价贡献、按贡献决定报酬的机制”,^[28]明确将数据列为生产要素之一。2020年3月中共中央、国务院发布的《关于构建更加完善的要素市场化配置体制机制的意见》提出,“研究根据数据性质完善产权性质”。^[29]2020年5月中共中央、国务院发布的《关于新时代加快完善社会主义市场经济体制的意见》提出,“完善数据权属界定”。^[30]2022年11月国家知识产权局办公室发布的《国家知识产权局办公室关于确

定数据知识产权工作试点地方的通知》提出了“数据知识产权”的概念，并推动了数据知识产权登记实践。^[31]2022年12月中共中央、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》提出，“建立数据资源持有权、数据加工使用权、数据产品经营权等分置的产权运行机制”。^[32]实践的需求、党和国家的政策推动，使得数据权属问题引发了广泛研究和讨论。

从私权角度看，知识产权法已为满足特定条件的数据提供了一些保护。然而，这种保护是否能够作到全面覆盖以及保护模式是否恰当，还有待进一步研究。特别是数据相关的财产性权益是否应被纳入知识产权体系进行讨论，是当下受到热议的一个问题。

著作权、专利权、商标权等权利，何以被合称为知识产权？针对这一理论问题，我国法学界曾经就知识产权法保护对象的本质展开了一场理论思辨。知识产权是一种无体财产权，但仅“无体”还不足以反映其本质。法学界提出或阐释了“信息说”“信号说”“知识说”“符号说”等不同的观点。其中，“信息说”主张，客观世界是由物质、能量和信息三者构成的，知识产权法保护的对象即指向信息，这也是知识产权的价值所在。^[33]“信号说”^[34]“知识说”^[35]“符号说”则均指向信息的非物质载体这一层次，而非信息本身。其中，“符号说”的发展程度较高。该学说认为，知识产权法保护的对象是符号组合。作品、发明和商标作为知识产权法保护的客体对象不仅在外观形态上都表现为符号组合，而且本质上与符号的非物质性、整体性和任意性特征吻合。^[36]卡西尔的符号学理论指出，人在自然世界之外，还要创造一个自己所能理解的人为世界。这个世界的建设不是通过自然界的物质和能量，而是通过人自己创设的符号来进行的。^[37]李琛认为，知识产权法学界所说的非物质的智力成果就是利用符号进行的创造，是符号组合或符号形式。符号本身属于公有领域，只有利用符号形成新的组合，且组合的程度达到法律的要求时，才能成为客体的对象。^[38]类似地，我国学者王坤论述了知识产权法保

护的对象是符号组合，知识产权是对符号世界中知识资源的有限支配。^[39]熊文聪进一步提出，“符号说”不仅可以说明作品、技术方案、商标的统一基础，还有助于阐释三者受不同的知识产权制度保护的原因，并为知识产权重叠保护问题的解决提供启示。^[40]

以“符号说”为基础构建知识产权法保护对象的体系化理论，有助于厘清数据在私法体系中的定位。“符号说”研究明确区分了物理层、符号层、信息层。许多数据法律研究者也提出了对于数据权属制度进行分层思考的基本框架。德国学者赫伯特·蔡希（Herbert Zech）将物理层面的信息载体区分为第一阶的信息载体和第二阶的信息载体。第一阶的信息载体通过物体本身体现信息内容而不包含符号，第二阶的信息载体则因该载体承载符号而能够包含信息。^[41]数据即属于这里所说的“符号”。纪海龙认为，对于数据可以进行物理层、符号层和内容层三个层次的区分。^[42]申卫星指出，拉德布鲁赫（Radbruch）基于秩序概念提出了类型思维层级性，即同一类型的范围可以由数个不同的层级构成，不同层级间可以相互流动过渡，并呈现出一种次序排列的状态。他进一步指出，数据产权的制度设计应采取秩序概念基础上的层级性思维，并将数据分为符号层和内容层，内容层的数据即进入个人信息等范畴。^[43]

互联网和数字系统本身也往往采取分层设计。这种设计主要是为了实现模块化和灵活性，使得系统的不同部分可以得到独立开发和维护，同时确保整体的协调运作。举例来说，互联网协议就是典型的分层设计。例如，开放式系统互连（Open System Interconnect, OSI）的参考模型包括物理层、数据链路层、网络层、传输层、会话层、表示层和应用层等7层架构。每一层都专注于特定的通信任务，如最底层的物理层负责传输原始的比特流，而最上层的应用层则为用户提供网络应用服务以及与用户直接交互的接口。这导致了不同层次的研发建设可能由不同的主体负责，有着不同的信息知识，也带来了从法律上进行层次区分的意义。美国网络法研

究者劳伦斯·莱斯格以及尤查·本科勒在早年研究网络法时,也分别讨论了信息在物理层、代码层、内容层这三个层面的支配和控制问题^[44]这些研究从更广的范畴探讨了数字空间治理的层次化制度设计,也为数据法律问题的层级化分析提供了启示。

因此,在智能时代,面对互联网和数字系统的客观实际以及知识产权法保护对象理论体系化建构的双重驱动,应以“符号说”为基础,进一步探讨知识产权法保护对象理论的体系化,为数据财产权益的法律秩序建构等问题的解决提供更加坚实的理论基础和建构路径。

(二) 创新方式变革引发的对保护条件的反思重塑

“符号说”可以为知识产权法保护对象确定基本范畴,但若想得知在此基本范畴之内的对象需要满足怎样的条件才能获得保护、应当提供何种保护模式,则需要进一步开展关于保护条件的理论建构。人工智能已经开始替代一部分“脑力劳动”和“智力创造”,这引发了学界对于知识产权法中“智力成果”“独创性”“创造性”“创作”“创造”等核心概念的解释争议。我国绝大多数知识产权研究者并不认同人工智能的主体地位,而是将其作为工具对待。探究人们使用这类新型工具产生的文字篇章、图案图像、音频视频、技术方案、产品设计等内容在知识产权法视域内应当如何被定性,如何解释和塑造前述保护条件相关的核心概念等问题,对于文化科技创新和社会发展具有重要影响。

不同研究者对于如何判断人工智能生成内容的可版权性提出了不同的观点。例如,仅针对“独创性”概念,就呈现了侧重从主体视角强调“人类创作”或“人类智力贡献”、^[45]从过程视角强调创造与机械性活动的区别^[46]以及对人工智能生成内容中表达性要素的直接决定性、^[47]从结果视角强调人工智能生成内容与既有作品或公有领域内容之间存在客观可识别的显著差异^[48]等不同观点。我国的“威科先行案”^[49]“Dreamwriter案”^[50]“Stable Diffusion案”^[51]和“蝴蝶椅子案”^[52]等案件也都呈现了既有共性又有差异的观点。

尽管理论界与实务界仍然存在一定争议,但我国法院在说理分析中强调,基于我国著作权法,只有当涉案内容生成的过程能体现自然人的个性化选择、取舍时,该内容才可以被解释为自然人的创作,构成著作权法意义上的作品。即结合司法实践来看,要求作品中体现人类的智力贡献、反映人类对于表达的编排取舍,是具有高度共识的观点。然而,在需要何种程度的对于表达的智力贡献方面,我国法学界仍然存在分歧。

在对保护条件的解释和建构上,特别应当注重两个方面:

一是对于保护条件对时代发展和公共利益影响的观察。北京互联网法院对“Stable Diffusion案”的判决反映了其对时代发展的重视和思考,其中有两方面要点值得重视。^[53]

首先,法院考虑到了艺术创作形式的发展。法院认为,使用模型画图虽然不同于过去用画笔、传统绘图软件画图,并不能精确控制表达,但作者通过设置并不断调整提示词和参数,最终获得涉案图片,这一过程体现了作者的个性化选择。一些研究者在论证反对人工智能生成内容构成作品的观点时,将现在使用人工智能进行艺术创作的方法与过去进行艺术创作的经典方法进行对比,基于二者存在的差异来证明前者不构成艺术创作,实际上是采取静止不变的视角看待这个日新月异的时代。我国著作权法从未明确要求作者对表达进行精确的控制。从过往的典型实践中推导出艺术创作的特征,并将其泛化为一般要件是不可取的。

其次,法院关注到了创作门槛的降低和创作的普及化能够带来公共利益。新工具的发明,使人们可以更低成本、更自由地实现创意,法律不应当对人们使用新工具设置不必要的阻碍。法律对使用人工智能创作的内容的认可,将在精神上和未来可能得到的财产利益上对人们形成激励。同时,当前影视和动漫产业已经在使用人工智能辅助生成内容,未来可能有进一步的产业应用。我们认同传统艺术创作的高度价值,并认为人类对于表达细节的控制能力和深厚艺术素养的形成,目前还远不能由人机

协作代替。但是,生成式人工智能帮助人们打开了新的创作空间,可能进一步释放人们的创造力。尽管可能存在大量的使用人工智能生成的低质量作品,这类作品的确不值得保护,但过往著作权法的长期实践和相关理论表明,人们也不会去积极主张这类作品的权益,正如在理论上一个孩童的很多画作都可以构成作品,但绝大部分这类画作并不会引发著作权许可申请或相关诉讼。但是,如果我们错误地设置保护条件,则可能无法为那些希望利用人工智能创作作品的自然人提供激励。

二是对于概念背后的理论基础和发展历程的分析。例如,在关于使用人工智能生成的技术方案能否获得专利法保护问题的讨论中,特别突显了专利制度的功利主义理论基础。通过回顾专利制度的发展历史可以看到,人的“创造性智力贡献”并非现代专利制度的理论基石,专利制度的“发明人”也并非总是指作出创造性贡献的人。尽管以人类发明者为中心是目前专利制度外在形式体系的表现,发明人的自然权利学说也的确在特定历史时期深刻影响了专利制度,但它们并不在真正意义上构成专利制度的基石。^[54]在国际往来并不便利的时期,许多国家专利法中的“新颖性”标准都是“相对新颖性”标准,即如果某专利技术在他国公开使用过但在本国没有公开使用过,那么引进该专利技术的人也可能成为发明人,获得授权。例如,1474年《威尼斯专利法》规定,只要“在本城邦制造本城邦内先前未曾有人制造”的机械装置,就可以去登记并获得保护。再如,尽管英国1623年《垄断法》规定专利必须被授予“真正的最初发明人”,但在该法颁布后的很长一段时间内,英国专利制度中的“发明人”仍然包括将新产品、新工艺引入英国的人。我国《专利法》也是在2008年修正时,才将“新颖性”标准修改为“绝对新颖性”标准。

因此,面对当前人工智能带来的创作、创造方式的变化,我们需要重新反思和解释“创作”“发明”“独创性”“创造性”等基础概念,有必要追溯其发展源流,区分实质与修辞,厘清核心理论基石与附带制度功能,结合不同知识产权制度背后的经济结

构差异与不同保护条件的关系,积极地回应新的时代中技术基础和生产生活模式的变迁。

(三) 面向智能时代创新特点的知识产权制度调适

智能时代的创新具有汇聚性和动态性的特点。因此,我们应从理论上解决好两个关键问题:一是,面对智能时代创新的“汇聚性”,即知识成果的集成化创新特征以及合作创新模式,应通过制度调适来降低知识集成成本,从而构建更加适配的合作创新激励机制;二是,面对智能时代技术创新高速迭代的“动态性”,尤其是在智能科技引领新一轮产业革命的背景下,应通过合理的责任分配及免责条件设置等制度调适,平衡知识产权保护和技术创新发展之间的关系。

就第一个问题而言,智能时代的一个重大特点是,很多创新中聚集了大量创新,或者说,很多创新依赖于大量知识产权的集中。以大语言模型 GPT-3 为例,其在训练中使用了约 45TB 的文本数据,参数量达到 1750 亿。基于当前的研究,在模型规模达到一定程度之后,才可能出现“智能涌现”现象。^[55]但是,海量的训练数据中包含着大量受著作权法保护的作品,逐一去获得许可既不现实也缺乏效率,且许可费的堆积可能使很多小微企业望而却步,以至遏制创新和竞争。我国学者丁晓东指出,从原理层面分析,数据汇聚面临的难题在于市场机制失灵,微型权益的聚合难以通过市场机制实现。^[56]此即“大规模微小利益汇聚”问题。

科技密集型的数字产品、智能产品本身也存在类似问题。许多产品中都汇聚了大量来自不同主体的知识产权。在专利制度设计之初,一个新的设备或机器常常只涵盖一项专利。然而在过去的几十年间,特别是在化工、生物技术、计算机硬件和软件领域,越来越多的产品不是只涵盖一项新发明,而是由许多不同的部分组成一个整体,每个组成部分都可能涵盖一项或几项专利。特别是在信息技术领域,微处理器、手机或存储设备等现代产品很容易就会涵盖几十项甚至上百项不同的专利。^[57]有研究报告显示,在 WCDMA 与 CDMA2000 技术标准制

定中,有 7796 项专利被宣称为标准必要专利,分为 887 个专利族,分别为 41 家公司所有。^[58]H.266(多功能视频编码标准)涉及 2387 项标准必要专利。^[59]大量的创新汇聚,也带来了交易成本高昂、损害公平竞争等问题,持续激烈的标准必要专利纠纷就是突出的体现。因此,面对不同的创新汇聚问题,需要综合研究适当的知识产权限制方式、合理的侵权责任界定方式和救济方式,并研究集体管理组织、标准化组织、专利联盟、数据服务商、大数据中心等组织或平台的制度设计,以更有效地降低交易成本、保障公平竞争、促进创新发展。

与此同时,凭借互联网强大的跨越地域的连接能力,开源共创、开放创新、“众包”式共创等模式纷纷发展,开源软件、开源大模型等也成为实现“技术平权”、缩小数字鸿沟的重要助力,这些模式促进了技术民主化和普惠化,并且有力推动着后续创新。面对这种通过网络连接分布在世界各地的创新者以及计算设备的能力,如何进一步使之更好地发挥实质功效,也应当是智能时代知识产权法的重要课题。

就第二个问题而言,针对新技术新产业的创新发展,进行适当的责任分配,设置合理的免责条件,调整好在先创新者与在后创新者的关系,平衡好知识产权人与社会公众的利益,一直是知识产权法发展中的重要课题。智能科技及其社会应用都处在高速发展之中,人工智能科技正引领新一轮产业革命,日益成为决定国家竞争力和国家安全的重大战略性新兴产业。然而,人工智能科技在发展中也面临很多知识产权方面的挑战。除前述模型训练中大量作品使用的合法性问题之外,其他挑战包括:在输出的结果中如果包含侵权内容,应当如何界定相关主体的责任?如何合理界定生成式人工智能服务提供者的注意义务?是否应当建立明确的免责条件?如何通过法律规则引导人工智能向善发展?诸如此类的问题,都是影响人工智能创新发展的知识产权制度和理论问题。

在互联网发展过程中,以“通知—删除”规则为核心的避风港规则曾经被认为实现了最佳利益

平衡,并且可以提供一种良好的合作机制,^[60]使著作权人和网络服务提供者协同起来发现和制止侵权。随着侵权检测技术的进一步发展,司法上也通过结合技术发展等多项要素来综合判定网络服务提供者对于存在侵权的内容是否构成“应知”,促使网络服务提供者合理采用进一步的技术措施防止侵权,体现了“科技向善”的基本理念。当前,生成式人工智能等技术还处在发展初期,这种在发展初期关注技术发展状况、考虑多元主体的合理责任分配的思路,仍然值得延续和借鉴。同时,对于始终回应技术创新的知识产权法,我们应当进一步发展面向新技术动态发展阶段的法律规则,以更加系统的理论实现良好的利益平衡。

(四) 智能科技与知识产权法治建设的有机融合

科技与法治的有机融合是智能时代法律发展的必然方向,也是知识产权法治建设的重点。数字科技为知识产权的运用、知识产权对象的传播、知识产权的保护都提供了技术基础,并可以根据法律的引导进行调整和不断发展。我们需要以科技和法律相结合的视野,研究智能时代的知识产权法治建设。

自互联网和数字技术诞生以来,技术措施和权利管理信息等技术手段就被积极用于解决各种著作权问题,为数字空间中的著作权保护提供技术加持。对于用户上传侵权内容问题,著作权制度也积极考虑内容比对和过滤技术的发展情况,综合多种因素对网络服务提供者是否履行了注意义务进行分析判断。

法律和技术的结合也有利于推动作品传播利用、降低交易成本、促进社会发展。在此方面,已经出现了一些富有想象力和创造力的实践。例如,在 20 多年前,在开源软件的启发下,莱斯格等人推动了“知识共享”(Creative Commons)的发展,其针对权利人有时愿意让作品在某些条件下得到传播或利用但无法简单地向社会公众表达许可意愿这一客观现实,开发了三个层次的许可协议表达:面向公众的符号标识层、面向许可合同清晰表达需求

的法律文本层,以及计算机可读的代码层。著作权人在网络上发布作品时,可以选择适当的许可协议。例如,著作权人如果选择了“署名—禁止商业性使用—禁止演绎”的许可协议,则公众能够获得在保留作者署名的前提下传播作品的许可,即可以出于非商业目的在其它平台传播作品,只要保留作者的署名、不改动作品内容即可。对于遵守法律的公众而言,看到这样的许可协议标记,就可以方便地传播作品。作品的传播可能为著作权人带来更多关注和更好的声誉,实现各方共赢。^[61]

区块链技术的发展也使得更灵活的作品著作权登记、授权许可、侵权检测和证据留存成为可能。^[62]以腾讯等推出的区块链版权保护解决方案为例,用户在平台上创作或上传作品后,可以直接在区块链中进行存证,并进行著作权登记。应权利人要求,平台可以实时监测互联网上是否有侵犯其著作权的行为。平台监测到侵权行为,可以自动留存侵权证据并进行区块链存证,并且可以自动向平台发送侵权通知,请平台删除侵权内容。权利人如向法院起诉,法院在审理中可以调取区块链中关于作品和侵权内容的证据。^[63]这样的系统发展,为创作者提供了保护权利的便利。

人工智能技术也被用于支持知识产权行政和司法工作,从而更好地便利知识产权保护。例如,世界知识产权组织已经开发并提供了一系列人工智能驱动的服务和工具,包括自动专利分类、国际商标数据库中的图像相似性检索、维也纳分类(《商标图形要素国际分类》)助手等。这些服务和工具利用人工智能技术来提高专利、商标等知识产权分支领域的制度运行效率和准确性,降低了公众获取知识产权信息及申请知识产权的成本。^[64]再如,我国法院系统也开发了“版权AI智审”等智能工具,^[65]辅助知识产权纠纷的解决。

人工智能的发展,为优化知识产权法治实践提供了新的可能性。无论是知识产权法学研究者还是法律实务工作者,都应该更加积极地拥抱科技发展,以法律和科技相结合的视野,为知识产权发展和保护提供更多的创新方案。

(五)围绕国际知识产权规则开展对话和协调

在数字化、智能化、全球化、法治化时代,研究知识产权法学问题必须放眼全球问题、树立全球观念。与数字科技发展和治理的全球性相一致,智能化、全球化时代的知识产权法学问题都是全球性问题,知识产权的确认和保护是全球议题、人类责任。习近平总书记指出:“中国愿同世界各国一道,把握数字时代新趋势,深化数字领域国际交流合作,推动智能产业创新发展,加快构建网络空间命运共同体,携手创造更加幸福美好的未来。”^[66]我国“十四五”规划也明确提出:“推进网络空间国际交流与合作,推动以联合国为主渠道、以联合国宪章为基本原则制定数字和网络空间国际规则。”^[67]进入21世纪以来,数字领域的全球合作越来越广泛、越来越紧密。基于发展和安全的有机统一性,中国政府发布了若干关于互联网建设和治理、人工智能发展和治理、数据跨境流通的倡议,并积极推动在全球范围内形成广泛共识、发表宣言、制定契约。以2024年9月22日联合国大会未来峰会通过的《全球数字契约》(Global Digital Compact, GDC)为例,中国政府和民间机构积极参与对《全球数字契约》的讨论、磋商、议定,为该契约的顺利通过作出了突出贡献。《全球数字契约》深刻分析了数字技术的发展现状、巨大潜力、已经显现的挑战和不确定的风险,广泛凝聚了全球各方共识,充分体现了全人类共同价值观,是全球人民的共同契约和共同宣言。《全球数字契约》为全球数字发展和治理注入了新的动力和活力,既是我们在数字领域的行动纲领,也是推进数字法治进步、创新数字法学研究的丰厚资源。《全球数字契约》旨在为所有人创造开放、自由、安全的数字未来,提出发展优先,普惠包容,创新驱动,保护数字空间文化多样性,营造开放、公平、包容和非歧视的数字发展环境等理念。其宗旨和理念与中国法制与社会发展政府提出的全球发展倡议、全球安全倡议、全球文明倡议、全球人工智能治理倡议的理念相连相通,顺应了促进数字发展、加强数字治理、推动数字文明的时代潮流。《全球数字契约》就互联网治理、大数据治理、人

工智能治理等达成普遍共识,其中也包括有关知识产权保护等的共识。

世界知识产权组织也高度重视人工智能的知识产权问题。2019年9月27日,世界知识产权组织召开了第一次知识产权和人工智能对话,并于2019年12月公布了人工智能可能引发的知识产权问题清单草案。2020年5月29日,世界知识产权组织发布了关于知识产权政策和人工智能的修订议题文件,概述了16项将受人工智能影响的知识产权问题,并于2020年7月及11月开展了第二次和第三次对话,促成了全球范围内的集中讨论。此后,世界知识产权组织又陆续开展了主题对话。^[68]我国学界和实务界也积极参与其中。世界知识产权组织在2024年发布了经济研究工作论文《人工智能和知识产权:一个经济视角》,^[69]指出人工智能正不可避免地改变着当前知识产权提供的激励平衡,研究者要冷静地进行观察,就像每次重要技术变革一样,利益相关者需要时间来适应,新的商业模式需要时间来出现,法院需要时间来解释法律,行业惯例需要时间来得到巩固。2024年,世界知识产权组织还发布了《帮助创新生态系统做好准备迎接人工智能:知识产权政策工具包》,^[70]旨在为政策制定者提供一个框架和指南,帮助各国更好地应对人工智能给知识产权生态系统带来的挑战,并最终找到符合国家政治、经济和社会需求的最佳前进道路,建立一个全球生态系统,让人工智能创新惠及所有人。

解决智能时代数字领域的知识产权问题,各国需要协调规则、合作共赢。知识产权法学研究必须坚持系统观念和全球视野,注重比较研究,特别是需要关注美国、英国、日本、欧盟等国家和地区的知识产

权法学研究现状和趋势、立法情况及司法实践的比较分析,在比较分析中明晰中国的立场、观点、制度和实践,借鉴域外好的制度和作法,吸收外国学者的研究成果,发展中国的知识产权理论,推动知识产权学科建设。在当前和今后一个时期,以数字科技领域的知识产权问题为重点研究对象的知识产权法学研究,应当以习近平总书记关于数字法治和知识产权的重要论述为指导,把我国数字治理的法律法规和公共政策与《全球数字契约》等文本及世界知识产权组织的相关工作结合起来,以数字契约精神为基本范式,开创中国特色知识产权法学新理论新制度,为世界知识产权发展作出贡献。

结语

智能时代的科技创新带来了知识产权法发展的新需求和新机遇。智能时代的鲜明特征包括数字化、智能化、全球化、法治化。这“四化”均包含知识产权元素,也全面推动着知识产权法律和法学的演进发展。我国在智能科技发展运用方面处于世界前列,这样的社会前沿实践为知识产权制度的发展提出了现实需求,也为我国研究者提供了率先深度研究和发展知识产权理论的机遇。智能时代的知识产权法应着力于知识产权法保护对象理论的体系化建构、创新方式变革引发的对保护条件的反思重塑、面向智能时代创新特点的知识产权制度调适、智能科技与知识产权法治建设的有机融合、围绕国际知识产权规则开展对话和协调等重点方面,应对人工智能给知识产权生态系统带来的挑战,推动知识产权的进一步发展,服务于智能时代的全球创新和文化繁荣。知识产权法学通过理论与实践相结合、当下与未来相贯通,必将形成与智能时代相适应的对知识产权发展规律的科学认知,建构中国自主的知识产权法学知识体系和学科体系。

(技术编辑:艾薇)