中国人民大学法学院
数字法学教研月报

2025 年第 11 期（总第 23 期） 2025 年 11 月 22 日

本期看点

【数字法治大事件】国家层面密集推进数字法治立法与专项治理，《法治宣传教育法》正式施行筑牢全民法治认知基础，新修订《网络安全法》明确人工智能发展与安全监管要求，多部门联合出台物流数据开放互联方案助力实体经济降本增效；地方层面，天津发布数据标注产业发展行动方案，聚焦高质量数据集建设；专项整治行动持续发力，严打涉退役军人、汽车行业、学术论文买卖等违法违规行为及 AI 仿冒公众人物直播营销乱象，形成全方位治理格局。

【研究动态】本期研究覆盖数字法学核心领域，基础理论聚焦网络与信息法学体系化建构、数字技术规范法律化等；数据法学围绕数据泄露精神损害认定、公共数据产权构造、数据抓取正当性判断等展开；数字司法与行政探讨电子证据取证规范、司法人工智能应用风险等；算法与人工智能治理涉及大模型训练数据合理使用、人工智能特殊侵权责任等；平台治理聚焦平台滥用规则行为的反不正当竞争法规制，为数字法治实践提供多元理论支撑。

【教研活动】第五届数字正义论坛、第五届“数字法治与社会发展”学术论坛等多场高水平会议成功举办，汇聚国内外专家学者，围绕数字经济法治回应、人工智能治理、法治人才培养等前沿议题深入研讨；第 14 届法治国际论坛、首届大湾区金融法治论坛等搭建跨境交流平台，促进数字时代法治变革的中国实践与国际经验互鉴；专题学术沙龙与研讨会聚焦人工智能安全、民法典与数字法学交叉等主题，推动学术交流与人才培育。

【数字法评】

《数据访问地标准：跨境电子取证管辖的中国方案》，《人民检察》2025 年第 11 期，作者：刘品新、赵梓彤。

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

本期目录

学术顾问：王利明

编 委 会：张新宝　丁晓东　王　莹　张吉豫

编 辑 部：阮神裕　毕坤阳　来唯希　吕昊然　邓语鑫　梁因格　王　昊

联系方式：RUCdigitallaw@163.com

本期编辑：梁因格

数字法治大事件

导言：在数字化全面重塑经济社会运行方式的时代背景下，我国不断通过立法、政策部署与专项治理行动，完善数字时代的法治体系与治理能力。从国家法律的实施，到行业规范的推进，再到网络生态的专项整治，一系列密集出台的文件与典型案例，共同构成了中国数字治理体系迭代升级的总体图景。

2025 年 11 月 1 日起正式施行的《法治宣传教育法》为国家推进全民普法、提升全社会法治素养提供了制度化保障，成为数字时代法治认知体系的重要基石。在公民个人信息保护方面，人民日报发布的《检察机关依法惩治侵犯公民个人信息犯罪》及系列案例揭示了信息侵犯犯罪手段不断翻新的趋势，强调司法机关在维护公民权益、净化网络环境方面的关键作用。与此同时，新修订的《中华人民共和国网络安全法》将于 2026 年施行，将进一步夯实国家网络安全法治框架，为数据安全、平台责任以及关键信息基础设施保护提供更加清晰的制度依据。

在网络空间治理方面，中央网信办和相关部门持续开展专项整治行动，集中曝光多起具有代表性的违法违规行为。包括涉退役军人违法违规账号的处置、汽车行业网络乱象的专项整治、打击涉学术论文买卖的违法违规账号，以及针对利用 AI 仿冒公众人物进行直播营销的乱象开展从严查处。这些典型案例不仅反映出网络生态中问题的多样化与技术化趋势，也体现了监管部门始终坚持“依法治网、以网治网”的治理理念，通过精准治理维护网络秩序与公共利益。

在数字产业发展方面，各地各部门也积极谋划布局。天津市印发的《加快数据标注产业发展促进行业高质量数据集建设的行动方案（2025—2027 年）》从地方层面系统构建数据标注产业生态，推动技术创新与产业标准化。国家数据局发布的相关政策和专家解读，如《数字赋能城市生命体 全域转型绘就现代化人民城市新图景》，从“城市生命体”视角阐释数字技术驱动城市治理体系转型的战略路径。

在行业应用与数据要素流通方面，国家发展改革委等部门发布的《关于推动物流数据开放互联有效降低全社会物流成本的实施方案》，强调通过数据开放、互联互通与创新应用促进物流体系降本增效，进一步凸显数据要素在产业链、供应链与实体经济发展中的枢纽作用。

纵观上述法律实施、政策措施、产业规划与专项治理行动，我国正在从法治宣传、网络安全、数据治理、城市数字化转型到网络生态治理等多维度形成系统性合力，构建起数字时代的综合治理体系。这些制度安排不仅体现了国家对数字治理与网络生态建设的高度重视，也为数据时代的公民权益保护、产业创新和现代化城市建设提供了持续而强劲的制度动力。

今日起，《法治宣传教育法》施行

原载：“中国法治实践”微信公众号

法治宣传教育是全面依法治国的长期基础性工作。10 月 30 日下午，国务院新闻办公室举行新闻发布会，介绍法治宣传教育法及全民普法有关情况。

以法治方式推动保障法治宣传教育全面发展

9 月 12 日，十四届全国人大常委会第十七次会议表决通过《中华人民共和国法治宣传教育法》，自 2025 年 11 月 1 日起施行。以法治方式推动和保障法治宣传教育工作守正创新、提质增效、全面发展。

全国人大常委会法工委副主任黄薇表示，法治宣传教育法的通过，标志着我国的法治宣传教育事业全面迈入了制度化、规范化、法治化的新纪元，具有里程碑式的重要意义。

据介绍，法治宣传教育法明确规定，法治宣传教育坚持“贯彻习近平法治思想”；规定“国家实行公民终身法治教育制度”；明确“国家通过多种形式开展宪法宣传教育活动”等。

黄薇表示，“习近平法治思想”首次入法，具有十分重大而深远的意义，它明确了法治宣传教育坚持的正确政治方向和科学理论指引，也将推动习近平法治思想更加深入人心。

推动法治成为社会共识和基本准则

今年是全民普法 40 周年，也是“八五”普法规划收官之年。

“在 14 亿多人口的大国持续开展全民普法，把法律交给亿万人民群众，是中国法治建设史上的一大创举，也为人类法治文明提供了中国智慧、贡献了中国力量。”司法部副部长胡卫列说。

新时代新征程全民普法工作全面创新发展。大力弘扬红色法治文化，传承中华优秀传统法律文化，建成 113 个全国性、5000 余个地方性的法治文化阵地；积极探索“人工智能+普法”“非遗+普法”等普法新模式；全国各类普法新媒体账号 3 万多个，“中国普法”微信公众号订阅用户 4500 余万，累计访问量近 40 亿次。社会主义法治以文化人、以文育人的功能发挥更加充分。

胡卫列表示，作为法治宣传教育的主管部门，司法部将深入贯彻实施法治宣传教育法，推动法治成为社会共识和基本准则，为以中国式现代化全面推进强国建设、民族复兴伟业营造良好法治环境。

深入推进法治教育融入学校教育各个阶段

据了解，我国目前在校学生超过 2.8 亿，学校 47 万所，是法治宣传教育的重要群体和重点阵地。

教育部政策法规司司长张文斌介绍，近年来，教育部持续发力，深入推进青少年法治教育融入学校教育各个阶段。义务教育阶段设置“道德与法治”课程，在孩子们心中播下“法律”的种子；高中教育阶段在“思想政治”等课程当中设置法治教学模块，强调遵纪守法，树立有权利就有义务的观点；高等教育阶段设置“思想道德与法治”等公共基础课程，使大学生进一步深化对法治理念、法治原则的认识与理解。

入耳入脑入心是青少年法治教育的关键，提升法治教育针对性和实效性也是教育部门一直追求的目标。“下一步，我们将认真贯彻落实法治宣传教育法，不断拓展青少年法治教育的深度和广度。”张文斌说。

全面强化网络法治宣传教育

记者从发布会上获悉，截至 2025 年 6 月，我国网民规模达到 11.23 亿，互联网普及率达到 79.7%，互联网已经成为法治宣传教育的主阵地、主渠道之一。

国家网信办网络法治局负责人黄春华介绍，近年来，网信部门会同有关部门充分发挥网络传播优势，推动网络普法成为法治宣传教育的最大增量之一。2024 年国家宪法日前后共推出主题活动 3000 余场次、网络报道 19 万篇次，网上点击量达到 23.5 亿次。

“下一步，我们将以贯彻实施法治宣传教育法为重要契机，切实发挥网络法治的统筹作用，全面强化网络法治宣传教育。”黄春华表示，将严格落实“谁执法谁普法”责任、网络服务提供者公益普法责任，充分利用人工智能、算法等技术推进智慧普法，深化线上线下普法融合互动，综合增强网络法治宣传的效果。

人民日报丨检察机关依法惩治侵犯公民个人信息犯罪

原载：“楚雄州人民检察院”微信公众号

侵犯公民个人信息犯罪花样翻新

检察机关依法惩治共护网络清朗

记者从最高人民检察院获悉：2025 年前三季度，全国检察机关共起诉侵犯公民个人信息犯罪 2100 余件 4400 余人。检察办案发现，侵犯公民个人信息犯罪呈现出的一些新特点新趋势值得关注。

一是根据“市场需求”瞄准特定对象，有针对性地获取公民个人信息。一些不法分子紧密追踪“黑灰产市场”对公民个人信息的需求，有针对性地猎取、梳理、分析公民个人信息，甚至形成专门数据服务商，为下游犯罪提供定制化“原料”支持。

二是犯罪技术迭代更新，犯罪手段更趋智能化隐蔽化。一些不法分子利用网络爬虫、木马病毒、渗透工具等黑客技术入侵存有公民个人信息的各

类系统，批量获取信息后出售，非法牟利。部分个人信息售出后被用于电信诈骗等违法犯罪活动。

三是网络“开盒”助推网暴升级，严重侵害公民合法权益。网络“开盒”行为目的多样。“开盒”行为人通过“社工库”（不法分子通过非法手段收集公民个人信息而搭建的数据库）等非法获取他人隐私信息，并散布引导网民攻击骚扰，对社会、个人及网络生态均造成严重危害。有的网暴不断升级，侵害被害人现实生活。

下一步，检察机关将不断强化侵犯公民个人信息违法犯罪打击力度，维护公民信息权益；严查公民个人信息数据泄露源头，加强行刑双向衔接，全链条打击黑灰产业链；充分发挥公益诉讼检察职能，依法保护公共利益，推动公民个人信息保护多元共治；持续加强以案释法、以案说法，推动形成良好社会氛围和正确行为价值取向，凝聚全社会保护公民个人信息、维护信息安全的共识。

网络安全丨新修订《中华人民共和国网络安全法》自 2026 年 1 月 1 日起施行

原载：“宁夏公路”微信公众号

全国人民代表大会常务委员会关于修改《中华人民共和国网络安全法》的决定

（2025 年 10 月 28 日第十四届全国人民代表大会常务委员会第十八次会议通过）

第十四届全国人民代表大会常务委员会第十八次会议决定对《中华人民共和国网络安全法》作如下修改：一、增加一条，作为第三条：“网络安全工作坚持中国共产党的领导，贯彻总体国家安全观，统筹发展和安全，推进网络强国建设。”二、将第十八条改为第十九条，删去第二款。三、增加一条，作为第二十条：“国家支持人工智能基础理论研究和算法等关键技术研发，推进训练数据资源、算力等基础设施建设，完善人工智能伦理规范，加强风险监测评估和安全监管，促进人工智能应用和健康发展。“国家支持创新网络安全管理方式，运用人工智能等新技术，提升网络安全保护水平。”四、将第四十条改为第四十二条，增加一款，作为第二款：“网络运营者处理个人信息，应当遵守本法和《中华人民共和国民法典》、《中华人民共和国个人信息保护法》等法律、行政法规的规定。”五、将第五十九条改为第六十一条，修改为：“网络运营者不履行本法第二十三条、第二十七条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处一万元以上五万元以下罚款；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。“关键信息基础设施的运营者不履行本法第三十五条、第三十六条、第三十八条、第四十条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处五万元以上十万元以下罚款；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。“有前两款行为，造成大量数据泄露、关键信息基础设施丧失局部功能等严重危害网络安全后果的，由有关主管部门处五十万元以上二百万元以下罚款，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款；造成关键信息基础设施丧失主要功能等特别严重危害网络安全后果的，处二百万元以上一千万元以下罚款，对直接负责的主管人员和其他直接责任人员处二十万元以上一百万元以下罚款。”六、将第六十条改为第六十二条，增加一款，作为第二款：“有前款第一项、第二项行为，造成本法第六十一条第三款规定的后果的，依照该款规定处罚。”七、增加一条，作为第六十三条：“违反本法第二十五条规定，销售或者提供未经安全认证、安全检测或者安全认证不合格、安全检测不符合要求的网络关键设备和网络安全专用产品的，由有关主管部门责令停止销售或者提供，给予警告，没收违法所得；没有违法所得或者违法所得不足十万元的，并处二万元以上十万元以下罚款；违法所得十万元以上的，并处违法所得一倍以上五倍以下罚款；情节严重的，并可以

责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。法律、行政法规另有规定的，依照其规定。”八、将第六十一条改为第六十四条，其中的“并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照”修改为“并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照”。九、将第六十二条改为第六十五条，修改为：“违反本法第二十八条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告，可以处一万元以上十万元以下罚款；拒不改正或者情节严重的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。“有前款行为，造成本法第六十一条第三款规定的后果的，依照该款规定处罚。”十、将第六十五条改为第六十七条，修改为：“关键信息基础设施的运营者违反本法第三十七条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令限期改正、停止使用、消除对国家安全的影响，处采购金额一倍以上十倍以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。”十一、将第六十八条、第六十九条第一项合并，作为第六十九条，修改为：“网络运营者违反本法第四十九条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录、向有关主管部门报告，或者违反本法第五十二条规定，不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告、予以通报，可以处五万元以上五十万元以下罚款；拒不改正或者情节严重的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。“有前款行为，造成特别严重影响、特别严重后果的，由有关主管部门处二百万元以上一千万元以下罚款，责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处二十万元以上一百万元以下罚款。“电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第五十条第二款规定的安全管理义务的，依照前两款规定处罚。”十二、将第六十四条、第六十六条、第七十条合并，作为第七十一条，修改为：“有下列行为之一的，依照有关法律、行政法规的规定处理、处罚：“（一）发布或者传输本法第十三条第二款和其他法律、行政法规禁止发布或者传输的信息的；“（二）违反本法第二十四条第三款、第四十三条至第四十五条规定，侵害个人信息权益的；“（三）违反本法第三十九条规定，关键信息基础设施的运营者在境外存储个人信息和重要数据，或者向境外提供个人信息和重要数据的。“违反本法第四十六条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关依照有关法律、行政法规的规定处罚。”十三、增加一条，作为第七十三条：“违反本法规定，但具有《中华人民共和国行政处罚法》规定的从轻、减轻或者不予处罚情形的，依照其规定从轻、减轻或者不予处罚。”十四、将第七十五条改为第七十七条，修改为：“境外的机构、组织、个人从事危害中华人民共和国网络安全的活动的，依法追究法律责任；造成严重后果的，国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。”本决定自 2026 年 1 月 1 日起施行。《中华人民共和国网络安全法》根据本决定作相应修改并对条文顺序作相应调整，重新公布。

中华人民共和国网络安全法

（2016 年 11 月 7 日第十二届全国人民代表大

会常务委员会第二十四次会议通过 根据2025年10月28日第十四届全国人民代表大会常务委员会第十八次会议《关于修改<中华人民共和国网络安全法>的决定》修正）

目录

第一章 总则

第一条 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

第二条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第三条 网络安全工作坚持中国共产党的领导，贯彻总体国家安全观，统筹发展和安全，推进网络强国建设。

第四条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

第五条 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

第六条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

第七条 国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

第八条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

第九条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

第十条 网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

第十一条 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

第十二条 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

第十三条 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推

翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第十四条 国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

第十五条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

第二章 网络安全支持与促进

第十六条 国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

第十七条 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

第十八条 国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

第十九条 国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

第二十条 国家支持人工智能基础理论研究和算法等关键技术研发，推进训练数据资源、算力等基础设施建设，完善人工智能伦理规范，加强风险监测评估和安全监管，促进人工智能应用和健康发展。国家支持创新网络安全管理方式，运用人工智能等新技术，提升网络安全保护水平。

第二十一条 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

第二十二条 国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

第三章 网络运行安全

第一节 一般规定

第二十三条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；（四）采取数据分类、重要数据备份和加密等措施；（五）法律、行政法规规定的其他义务。

第二十四条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第二十五条 网络关键设备和网络安全专用产

品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

第二十六条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

第二十七条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第二十八条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

第二十九条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

第三十条 网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

第三十一条 国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

第三十二条 网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第二节 关键信息基础设施的运行安全

第三十三条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

第三十四条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

第三十五条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第三十六条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；（二）定期对从业人员进行网络安全教育、技术培训和技能考核；（三）对重要系统和数据库进行容灾备份；（四）制定网络安全事件应急预案，并定期进行演练；（五）法律、行政法规规定的其他义务。

第三十七条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

第三十八条 关键信息基础设施的运营者采购

网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

第三十九条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

第四十条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

第四十一条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。第四章 网络信息安全

第四十二条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。网络运营者处理个人信息，应当遵守本法和《中华人民共和国民法典》、《中华人民共和国个人信息保护法》等法律、行政法规的规定。

第四十三条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第四十四条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第四十五条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

第四十六条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第四十七条 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第四十八条 任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

第四十九条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第五十条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为

的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

第五十一条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

第五十二条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。第五章 监测预警与应急处置

第五十三条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

第五十四条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

第五十五条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第五十六条 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：（一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；（二）组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；（三）向社会发布网络安全风险预警，发布避免、减轻危害的措施。

第五十七条 发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

第五十八条 省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

第五十九条 因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

第六十条 因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

第六章 法律责任

第六十一条 网络运营者不履行本法第二十三条、第二十七条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处一万元以上五万元以下罚款；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。关键信息基础设施的运营者不履行本法第三十五条、第三十六条、第三十八条、第四十条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处五万元以上十万元以下罚款；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。有前两款行为，造成大量数据泄露、关键信息基础设施丧失局部功能等严重危害网络安全后果的，由有关主管部门处五十万元以

上二百万元以下罚款，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款；造成关键信息基础设施丧失主要功能等特别严重危害网络安全后果的，处二百万元以上一千万元以下罚款，对直接负责的主管人员和其他直接责任人员处二十万元以上一百万元以下罚款。

第六十二条 违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：（一）设置恶意程序的；（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；（三）擅自终止为其产品、服务提供安全维护的。有前款第一项、第二项行为，造成本法第六十一条第三款规定的后果的，依照该款规定处罚。

第六十三条 违反本法第二十五条规定，销售或者提供未经安全认证、安全检测或者安全认证不合格、安全检测不符合要求的网络关键设备和网络安全专用产品的，由有关主管部门责令停止销售或者提供，给予警告，没收违法所得；没有违法所得或者违法所得不足十万元的，并处二万元以上十万元以下罚款；违法所得十万元以上的，并处违法所得一倍以上五倍以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。法律、行政法规另有规定的，依照其规定。

第六十四条 网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十五条 违反本法第二十八条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告，可以处一万元以上十万元以下罚款；拒不改正或者情节严重的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。有前款行为，造成本法第六十一条第三款规定的后果的，依照该款规定处罚。

第六十六条 违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

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

第六十八条 违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处

一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

第六十九条 网络运营者违反本法第四十九条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录、向有关主管部门报告，或者违反本法第五十二条规定，不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告、予以通报，可以处五万元以上五十万元以下罚款；拒不改正或者情节严重的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。有前款行为，造成特别严重影响、特别严重后果的，由有关主管部门处二百万元以上一千万元以下罚款，责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处二十万元以上一百万元以下罚款。电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第五十条第二款规定的安全管理义务的，依照前两款规定处罚。

第七十条 网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：（一）拒绝、阻碍有关部门依法实施的监督检查的；（二）拒不向公安机关、国家安全机关提供技术支持和协助的。

第七十一条 有下列行为之一的，依照有关法律、行政法规的规定处理、处罚：（一）发布或者传输本法第十三条第二款和其他法律、行政法规禁止发布或者传输的信息的；（二）违反本法第二十四条第三款、第四十三条至第四十五条规定，侵害个人信息权益的；（三）违反本法第三十九条规定，关键信息基础设施的运营者在境外存储个人信息和重要数据，或者向境外提供个人信息和重要数据的。违反本法第四十六条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关依照有关法律、行政法规的规定处罚。

第七十二条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第七十三条 违反本法规定，但具有《中华人民共和国行政处罚法》规定的从轻、减轻或者不予处罚情形的，依照其规定从轻、减轻或者不予处罚。

第七十四条 国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

第七十五条 网信部门和有关部门违反本法第三十条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，对直接负责的主管人员和其他直接责任人员依法给予处分。网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第七十六条 违反本法规定，给他人造成损害的，依法承担民事责任。违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七十七条 境外的机构、组织、个人从事危害中华人民共和国网络安全的活动的，依法追究法律责任；造成严重后果的，国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

第七章 附则

第七十八条 本法下列用语的含义：（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存

储、传输、交换、处理的系统。（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。（五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

第七十九条 存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。第八十条 军事网络的安全保护，由中央军事委员会另行规定。

第八十一条 本法自 2017 年 6 月 1 日起施行。

地方动态 | 关于印发《天津市关于加快数据标注产业发展促进行业高质量数据集建设的行动方案（2025—2027 年）》的通知

原载：“国家数据局”微信公众号

各相关单位：现将《天津市关于加快数据标注产业发展促进行业高质量数据集建设的行动方案（2025—2027 年）》印发给你们，请结合工作实际，认真贯彻执行。

市数据局

市教委

市科技局

市工业和信息化局

市人社局

市交通运输委

市国资委

市地方金融管理局

2025 年 11 月 11 日

天津市关于加快数据标注产业发展促进行业高质量数据集建设的行动方案（2025—2027 年）

发展数据标注产业、建设行业高质量数据集是推动人工智能发展，进一步释放数据要素价值，支撑促进数字经济和实体经济深度融合的重要举措。为贯彻落实《国务院关于深入实施“人工智能+”行动的意见》（国发〔2025〕11 号），国家发展改革委、国家数据局等部门《关于促进数据标注产业高质量发展的实施意见》（发改数据〔2024〕1822 号）和高质量数据集建设相关工作部署，制定本行动方案。

一、总体要求

以习近平新时代中国特色社会主义思想为指导，全面贯彻落实党的二十大和二十届二中、三中、四中全会精神，深入落实习近平总书记视察天津重要讲话精神和对天津工作一系列重要指示要求，以促进数据开发利用、赋能经济社会发展为主线，积极培育数据标注新业态，大幅提升行业高质量数据集供给水平，加快形成创新驱动、供需互促、区域协同、生态融合的数据标注产业新格局。到 2027 年，打造成为高端数据标注产业和高质量数据集建设先进城市，以高质量数据集有效供给支撑京津冀区域人工智能创新发展，以数据要素价值充分释放赋能重点行业领域数字化转型升级。

——产业规模大幅跃升。数据标注产业规模年均复合增长率超过 20%，推动产业链重点企业拓展数据标注业务，培育引进一批数据标注龙头企业。

——创新服务能力增强。数据标注产业专业化、智能化水平显著提升，建成 10 个以上自主研发、赋能不同行业领域的自动化数据标注平台，打造行业高质量数据集测试评估平台。

——行业数据集量质同升。在科学研究、工业制造、医疗卫生等 20 个以上重点行业领域，推动建设 1000 个数据集，重点打造 100 个以上模态丰富、赋能效果显著的行业高质量数据集。

——专业人才培育壮大。建设数据标注产教融合培训基地，新增培训数据标注相关人才不少于 3000 人，为产业发展提供充足专业人才支撑。

二、重点任务

（一）培育壮大产业

1.孵化培育优质企业。建立数据标注企业梯度培育库，加强政策辅导和产业对接。推动专业化数据标注企业做大做强，带动上下游产业链协同发展。鼓励各行业领域链主企业、电信企业、信息服务业企业、科研院所等企事业单位，根据市场需求建设数据标注团队，并孵化成立新的市场主体，推动数据标注业务向专业化、规模化、标准化、集约化发展。（责任单位：市数据局、市人社局、市工业和信息化局按职责分工负责）

2.引育行业龙头企业。梳理国内数据标注产业重点企业图谱，发挥园区产业、算力资源、应用场景等优势，开展多种形式对接合作，推动行业龙头企业在津设立研发总部或区域总部，开展专业化、智能化的数据标注业务，完善数据标注产业链条，提升数据标注产业整体服务能力。（责任单位：市数据局、市投资促进局、各区数据管理部门按职责分工负责）

3.建立健全产业生态。培育专业数据服务商，提供数据标注、数据脱敏、数据质量评估、数据资产评估、数据交易等服务，构建完整产业生态链。持续推进数据管理国家标准（DCMM）贯标评估，进一步提升企业数据管理能力和数据供给质量。支持企事业单位、行业协会和产业联盟等，围绕数据标注和数据集建设，定期举办技术交流、案例分享、供需对接等活动，搭建产业合作交流平台。（责任单位：市数据局、市工业和信息化局按职责分工负责）

4.加强区域协同联动。发挥京津冀区域数字经济、人才技术、应用场景等优势，注重与北京市在人工智能模型研发训练、行业高质量数据集供需对接等方面进行合作，加强与河北省保定市等城市开展数据标注业务协同，推动形成供需互动、功能互补的区域产业发展格局。依托全市高校外语人才特别是小语种人才丰富优势，鼓励专业化数据标注企业、重点行业领域龙头企业承接国外业务，在数据标注领域与上海合作组织成员国等国家开展国际交流合作。（责任单位：市数据局、市教委、各区数据管理部门按职责分工负责）

（二）强化创新驱动

5.推进技术创新。鼓励企业、高校、科研机构以及数据领域行业组织，基于自主可控技术底座，围绕数据采集、数据清洗、数据标注、数据合成等数据集建设关键环节，开展前沿技术研究，形成一批软件著作权或专利成果。推动多模态标注、标注审查、质量评估、基于思维链的专家标注等智能工具研发，建设适配不同行业领域的自动化标注平台。（责任单位：市数据局、市科技局、市知识产权局按职责分工负责）

6.推动标准制定和应用。支持企事业单位参与数据标注、数据集相关标准的制定和验证，承接国家级行业高质量数据集建设先行先试任务，促进数据标注和数据集领域相关标准、技术专利在重点行业领域的协同创新和成果转化。鼓励企业探索数据标注与区块链、隐私保护计算等技术的融合应用，提升数据安全与标注质量。（责任单位：市数据局、市市场监管委按职责分工负责）

（三）统筹产业布局

7.推动产业协同布局。充分发挥滨海新区在数据标注产业方面的人才、产业、载体等优势，积极建设具有全国影响力的高端数据标注产业聚集地。鼓励津南区、武清区、河北区等其他有条件的区，依据各自资源禀赋、产业基础和人工智能应用场景需求，探索数据标注产业创新发展路径，打造专业化、特色化的数据标注基地或园区。（责任单位：市数据局、有关区数据管理部门按职责分工负责）

8.提升配套服务能力。支持有条件的区根据数据资源基础和产业发展需求，推动完善鼓励数据标注产业聚集发展的配套政策，支持数据标注基地、产业园区建设发展。整合各类资源，为数据标注相关企业提供市场开拓、人才引进、员工培训、技术咨询、创业帮扶、融资信贷、商业调研等综合性服务。依托区内各类数据标注产业聚集载体，打造行业高质量数据集源头供给地，为全市行业高质量数据集建设提供重要支撑。（责任单位：市数据局、有关区数据管理部门按职责分工负责）

（四）建设行业高质量数据集

9.扩大公共数据供给。建立健全全市政务数据资源目录体系，规范全市政务数据共享、公共数据开放，深化政务数据资源开发利用，推动数据开放共享。升级数据资源统一共享交换平台，依法有序推进数据资源流通使用，推动跨部门、跨地区、跨层级公共数据融合应用。鼓励政府部门和企业协同开展政务大模型所需数据的标注业务，并利用标注处理后的高质量数据集进行训练。（责任单位：市数据局、市有关部门、各区数据管理部门按职责分工负责）

10.加强行业领域牵引。推动科学研究、工业制造、交通运输、港口物流、农业农村、智慧能源、金融服务、医疗卫生、教育教学、商务领域、人力资源、文化旅游、应急管理、气象服务、海洋经济、绿色低碳、公共安全、城市治理、智能驾驶、低空经济、生物制造、具身智能等重点行业领域，通过采集汇聚基础数据，打造面向行业典型场景应用的高质量数据集，提高行业领域数字化、智能化水平。（责任单位：市数据局、市科技局、市工业和信息化局、市交通运输委、市农业农村委、市发展改革委、中国人民银行天津市分行、天津金融监管局、市地方金融管理局、天津证监局、市卫生健康委、市医保局、市药监局、市疾控局、市教委、市商务局、市人社局、市文化和旅游局、市应急管理局、市气象局、市规划资源局、市生态环境局、市城市管理委、市住房城乡建设委、市公安局按职责分工负责）

11.激发各类主体需求。发挥各行业领域链主企业、央企驻津单位、市属国有企业、平台企业、数据服务企业等重点企业引领作用，推动高等院校、科研院所、行业协会等各类主体充分挖掘自身优势资源，依法利用采集汇聚的海量数据资源，释放更多数据治理、清洗、标注等数据加工需求。采用自建团队或外包方式，积极谋划建设数据集重点项目，参与行业高质量数据集建设先行先试，打造行业通识数据集、行业专识数据集，支撑行业模型研发训练以及推理应用。（责任单位：市数据局、市国资委、市有关部门、各区数据管理部门按职责分工负责）

（五）健全服务平台

12.打造数据标注公共服务平台。鼓励开发建设集数据加工处理、数据集质量评估、模型基准测试、产教融合实训为一体的数据标注公共服务平台，提升数据标注自动化、智能化水平，支持服务行业龙头企业、中小企业等不同层次数据标注需求。（责任单位：市数据局、有关区数据管理部门按职责分工负责）

13.建设数据集供需对接平台。推动建设天津市行业数据集广场，动态更新数据集资源目录，定期汇总提供政策发布、技术指导和合作交流等服务。鼓励开源社区参与建设高质量数据集，支持各类市场主体建设数据集存储节点，持续更新备份高质量数据集。（责任单位：市数据局、各区数据管理部门按职责分工负责）

14.构建数据流通利用服务平台。加快建设覆盖全市的数联网平台，构建全市统一数据基础设施底座。支持企事业单位按需建设可信数据空间、数据元件等其他数据流通利用设施，打造行业数据基础设施功能节点，并与区域数据基础设施功能节点互联互通。通过隐私计算、区块链等关键技术，推动数据安全可信地传输、共享、融合，促进数据要素价值释放。（责任单位：市数据局、各区数据管理部门按职责分工负责）

（六）建设人才队伍

15.加强专业人才培养。鼓励高校开设数据标注相关专业和课程，培养实用型人才。推动数据标注基地或园区建设产教融合培训基地，鼓励数据标注企业申报就业见习基地，开展订单式人才培养，实现人才培养与企业需求的精准对接，吸引优秀的数据标注专业人才和团队来津发展创业。支持信创产教联合体积极发挥作用，促进产教资源协同，推动校企共同培养数据标注产业适配人才。（责任单位：市人社局、市教委按职责分工负责）

16.推广职业技能等级认定。鼓励符合条件的数据标注领域企业，面向本企业职工自主开展相关

职业技能等级认定；推荐符合条件的企业、院校、社会团体、公共实训基地等备案成为社会评价组织，面向社会开展相关职业技能等级认定，依规颁发技能等级证书，证书信息实现全国联网可查。（责任单位：市数据局、市人社局按职责分工负责）

三、保障措施

市数据局牵头推动数据标注产业发展、行业高质量数据集建设各项工作，统筹协调市有关部门、各区，建立推动数据标注产业发展的协调机制，以及行业高质量数据集的建设、征集、发布和对接机制。充分利用科技创新、产业发展、人力人才等领域惠企政策，支持数据标注产业高质量发展。市有关部门、各区可结合实际需要统筹安排数据产品和服务采购经费，用于支持高质量数据集建设。对于赋能成效显著的数据标注、行业高质量数据集相关项目，将优先推荐至国家部委，积极争取优秀案例、专项资金等国家层面支持，引领促进数据标注产业和行业高质量数据集协同发展。

专家解读 | 数字赋能城市生命体 全域转型绘就现代化人民城市新图景

原载：“国家数据局”微信公众号

2025 年中央城市工作会议明确部署“坚持把城市作为有机生命体系统谋划”，为新时代城市发展贯穿系统性思维与生态化理念。在此背景下，国家发展改革委等部门印发《深化智慧城市发展 推进全域数字化转型行动计划》（以下简称《行动计划》），既是对中央城市工作会议精神的精准落地，更是数字中国战略在城市领域的深化拓展。作为城市生命体的“数字血脉”与“神经中枢”，全域数字化转型正重塑城市生长逻辑、治理范式与发展动能，推动现代化人民城市从“写意勾勒”迈向“工笔细描”。深入把握《行动计划》的理论内核与实践路径，需从数字化与城市生命体的共生关系、系统构建的协同生态、蓝图落地的实践突破三个维度，明晰其时代价值与深层逻辑。

一、共生共荣：数字化与城市生命体的本质联结

城市作为人口、产业、资源的聚合载体，绝非冰冷建筑的简单堆砌，而是具备自我调节、动态演化特征的有机生命体。《行动计划》的核心要义，在于以数字化为“血脉”与“神经”，激活城市生命体的感知、协同、进化能力，实现“人-城-境-业”的共生共荣。这种联结并非技术层面的简单叠加，而是对工业化时代城市发展规律的深度重塑。

（一）生命体视角：重构城市数字化本质认知

传统智慧城市建设多聚焦技术应用的单点突破，《行动计划》则将城市视为“有机生命体”，突出数字化转型的“全域性”与“系统性”。这一视角革新，意味着城市数字化不再是“给机器装芯片”，而是为城市生命体构建全域“循环系统”——通过数据要素流动，打通城市“资源代谢、要素配置、安全防控”等核心功能，实现从“物理集聚”到“数字协同”的质变。

正如人体需血液输送养分、神经传递信号，城市生命体的健康运行，同样需要数据作为“养分载体”、数字基础设施作为“传导网络”。《行动计划》提出的“设施联通、数据融通、平台互通、业务贯通”，本质是为城市生命体搭建“四通”循环体系，让数据像血液般渗透到城市治理、产业发展、民生服务的每一个“细胞”，让数字技术像神经般串联起城市运行的每一个“器官”。其中，城市信息模型（CIM）、国土空间信息模型（TIM）、建筑信息模型（BIM）的协同应用，以及实景三维中国数据的开发利用，更是为“四通”循环体系提供了空间维度的技术支撑，推动城市从“平面管理”向“立体治理”升级。

（二）互塑机制：构建人城境业数字协同新范式

城市生命体的核心是“人”，数字化转型的终极目标是让城市更宜居、更韧性、更有温度。《行动计划》通过“数智赋能治理”“数字美好生活”等行动，构建“城育人、人塑城”的互塑机制：一方面，城市通过数字化升级为市民提供更精准的服

务（如高效处置“一件事”、高效办成“一件事”）、更安全的环境（如城市生命线监测预警），其中医疗电子处方流转、费用一站结算、诊疗数据共享、社会保障卡居民服务“一卡通”跨省通用等高频民生场景的落地，让服务精准度与便捷性显著提升；另一方面，市民通过数据反馈、场景参与（如民意速办、接诉即办、未诉先办）反向塑造城市生命体的数字化自修复能力，形成“需求-响应-迭代”的良性循环，而基层报表“一数一源”“统采共用”机制的建立，则进一步降低了市民与基层组织的数据填报负担，让参与渠道更畅通。

这种互塑不仅体现在人与城之间，更延伸至“境”与“业”：通过城市数字更新行动，推动基础设施数字化改造，让生态环境（境）治理更精细（如智慧环保监测）；通过数字经济赋能行动，以数据要素价值化实现“以城带产、以产促城”，让产业（业）成为城市生命体的“肌肉组织”，支撑城市持续生长。

（三）进化逻辑：实现城市治理能力质的跃升

城市生命体的核心特征是适应环境变化的进化能力。《行动计划》通过“城市智能中枢建设”“适数化改革”等部署，为城市生命体注入“学习能力”——通过数据沉淀形成的“城市知识图谱”、算法迭代构建的“决策模型”，让城市能够从历史数据中提炼规律、从实时数据中感知异常、从多元数据中预判趋势，实现从“事后处置”到“事前预防”的跨越。

正如超大特大城市率先建设的“智慧高效治理新体系”，本质是为城市生命体安装“智慧大脑”，通过“一网统管”实现对交通拥堵、环境污染、公共安全等“健康指标”的实时监测与动态调节；而“城市运行体征指标体系”的构建，则如同为城市建立“健康体检报告”，让治理者精准把握城市运行状态，推动治理从“经验决策”转向“数据决策”。

二、八网联动：六项行动构筑城市数字生态体系

《行动计划》部署的六项行动（智慧高效治理提升、数字美好生活、数字经济赋能、城市数字更新、数字化转型筑基、适数化改革创新），并非孤立割裂的任务清单，而是以数据流为纽带，构建起“设施网、数据网、业务网、知识网、创意网、产业网、民心网、安全防护网”八网联动的数字生态体系，为城市生命体提供全维度支撑。这一体系的核心，是打破“条块分割”的传统壁垒，实现“网网相连、网网赋能”。

（一）基础支撑网：筑牢城市生命体“骨骼”与“血脉”

城市生命体的正常运行，依赖强健的“骨骼”（基础设施）与畅通的“血脉”（数据流动）。《行动计划》通过“城市数字更新行动”“数字化转型筑基行动”，构建“设施网”与“数据网”协同支撑格局：

设施网以“物联、数联、智联”为目标，整合感知终端、算力网络、通信设施，如同为城市生命体打造“神经网络末梢”，实现对交通流量、管网状态、环境质量等细微变化的实时感知。例如，“城市数字基础设施”的集约建设，避免了“重复开挖”“系统孤岛”，让设施资源像骨骼般形成整体支撑；而低空数据基础设施的适度超前布局、智能化路侧基础设施与云控基础平台的建设，则进一步为低空经济、自动驾驶等新兴场景提供了设施保障，提升车路协同水平。

数据网通过“公共数据一本账”“数据产权制度探索”，推动数据跨部门、跨区域、跨层级流通，如同为城市生命体打通“血液循环系统”。《行动计划》提出的“数据要素价值化实现”，正是让数据从“沉睡资源”变为“流动养分”，通过“数据券、模型券”等创新工具，激活数据在民生服务、产业创新中的价值潜能。

（二）功能协同网：激活城市生命体“肌肉”与“大脑”

如果说基础支撑网是“硬件”，那么“业务网”与“知识网”则是城市生命体的“肌肉”（治理能力）与“大脑”（决策智慧）。《行动计划》通过“智慧高效治理提升行动”与“适数化改革创新行动”，推动治理能力与知识沉淀协同升级：

业务网以“一网统管”“高效处置一件事”为核心，打破部门壁垒，构建“监测预警-事件流转-指挥调度-闭环落实”全链条机制，如同为城市生命体训练“协同肌肉”，让交通管理、应急处置、民生服务等功能形成“联动反应”。例如，“数字化城市综合运行和治理中心”的建设，实现了城市运行、应急管理等系统的“多脑协同”，避免了“各自为战”的治理困境。

知识网依托“城市智能中枢”“模型即服务”生态，沉淀治理经验、产业规律、服务模式为可复用的算法模型，如同为城市生命体构建“记忆与学习系统”。《行动计划》提出的“超大特大城市率先落地一批先进可用、自主可控城市大模型”，正是让城市能够从海量数据中提炼知识，实现治理与服务的“智能迭代”。

（三）发展活力网：培育城市生命体“细胞”与“灵魂”

城市生命体的活力，源于“细胞更新”（产业创新）与“精神共鸣”（民心凝聚）。《行动计划》通过“数字经济赋能行动”“数字美好生活行动”，构建“产业网”“创意网”“民心网”协同发展格局：

产业网以“以城带产、以产促城”为路径，通过“数据创新型产业社区”“城市首试首用体验场”，推动数字技术与实体经济融合，如同为城市生命体培育“活力细胞”。例如“数字产业集群”的发展，既提升了产业竞争力，又为城市创造了就业机会，实现“产城共生”；而数据保险、数据信托等金融服务产品的探索，则进一步丰富了产业网的支撑工具，降低企业数据创新风险。

创意网鼓励“智创品质生活”“数字友好人居环境”，支持市民、企业、社会组织参与数字化场景创新，如同为城市生命体注入“创新基因”。《行动计划》提出的“城市首试首用体验场”，让市民从“被动接受服务”变为“主动参与创造”，催生了智慧养老、社区微治理等个性化场景。

民心网聚焦“高效办成一件事”“民意速办服务”，让市民感受到数字化带来的便利与温度，如同为城市生命体凝聚“精神共识”。智慧社区建设中提出的数字惠民服务生活圈、幸福邻里综合体，让民心在“数据血脉”的流动中更加凝聚；同时，针对老年人、儿童、残障人士等群体的公共空间与数字服务适老化、适幼化、无障碍改造，以及“一老一小”公共服务资源一站式集成，进一步让民心网覆盖更广泛群体，弥合数字鸿沟。

（四）安全防护网：守护城市生命体“免疫系统”

城市生命体的健康成长，离不开“免疫系统”的守护。《行动计划》通过“数字化转型筑基行动”中“筑牢数字化转型安全防线”的部署，构建“安全防护网”，为城市数字生态保驾护航：一方面，强化网络安全、数据安全防护能力，健全政务云网安全保障体系，实现城市数据基础设施的可信接入、安全互联、跨域管控、全栈防护；另一方面，推进数据安全治理，建立数据安全风险防控体系，强化数据分类分级保护与全生命周期安全管理，完善个人信息保护制度，压实政府、企业、社会组织等各类主体的安全责任，确保数据在流动与应用中“安全无虞”，为城市生命体的数字化进化提供稳定环境。

三、落地突破：从蓝图到实景的实践进阶

如果说 2024 年《关于深化智慧城市发展推进城市全域数字化转型的指导意见》是全域转型的“发令枪”，那么《行动计划》则是具体的“路线图”与“施工图”。推动蓝图落地，需把握目标锚定的阶段性特征、路径创新的关键突破、因地制宜的差异化推进，让城市生命体的数字化成长既见实效、亦具特色。

（一）目标锚定：2027 年标杆引领与 2035 年远景展望的衔接

《行动计划》明确提出“到 2027 年建成 50 个以上全域数字化转型城市”，这一目标并非简单的数量指标，而是对城市生命体数字化成熟度的阶段性定义。转型城市的核心标志，在于形成“智慧高效治理、美好生活普惠、数字经济活跃、数字更新有序”的良性生态，具备可复制、可推广的转型经

验；同时，超大特大城市需率先建成智慧高效治理新体系，落地一批先进可用、自主可控城市大模型，形成头部引领效应。

从长远看，《行动计划》还明确了“到 2035 年，涌现一批具有国际竞争力、全球影响力的现代化城市”的远景目标，与 2027 年阶段性目标形成“短期突破-长期跃升”的完整时间轴。从具体指标看，“高效处置一件事”覆盖城市运行重点事件，意味着城市治理的“响应速度”与“解决效能”大幅提升；“高效办成一件事”覆盖高频民生事项，标志着市民“获得感”的实质性增强；“自主可控城市大模型”落地，体现了城市“智慧大脑”的自主进化能力。这些指标共同构成城市生命体数字化成熟的“体检标准”，指引各地精准发力。

（二）路径创新：制度供给与主体协同的双轮驱动

从蓝图到实景，关键在于突破“制度壁垒”与“协同难题”。《行动计划》通过“适数化改革创新行动”，构建制度与技术双轮驱动的落地路径：

制度创新聚焦“流程再造”与“规则重构”，例如“加快城市运行管理服务平台体系建设，完善城市运行管理工作机制”“跨部门数据合作机制”“线下网格与线上网络联动协同机制”等城市综合治理机制，打破传统治理的“条块分割”，让城市生命体的“协同反应”更顺畅；同时，加快推进数据确权规则、数字权证应用、行政管理与政府采购等制度改革，为数据要素流通扫清制度障碍。“长效运营运维模式”则通过“用户满意度导向的运营预算与评价考核机制”，建立运营运维评价动态反馈和发布机制，强化评价结果运用，确保数字化建设“建得好、用得久、管得优”，避免“重建设轻运营”的短期行为。

主体协同强调“政府引导、市场主导、社会参与”，让多元主体像“细胞协作”一样形成合力。例如，“数据要素价值化”通过“数据即服务”“模型即服务”生态，吸引企业、科研机构参与数据开发，激活全社会创新活力；而“立体化运营体系”（涵盖数据运营、场景运营、设施运营）的建立，则进一步明确政府、企业、社会组织在运营中的权责分工，形成协同闭环。

（三）因地制宜：差异化发展塑造城市数字竞争力

城市生命体的魅力在于其独特性，数字化转型同样不能“千城一面”。《行动计划》鼓励各地立足资源禀赋、发展阶段，分类分级有序推进：超大特大城市可聚焦“智慧高效治理新体系”，利用人才与数据优势，在城市大模型、跨区域协同治理上率先突破；中小城市可侧重“数字基础设施补短板”与“特色场景创新”，例如结合农业优势发展智慧农业、依托文旅资源打造数字文旅场景；资源型城市可强化“数字赋能绿色发展”，通过智慧环保、碳足迹监测等场景，实现生态保护与经济发展的平衡。这种差异化发展，如同自然界中不同物种的“生态位分化”，让每座城市在数字中国的大生态中找准定位，形成“百舸争流、各具特色”的生动局面。

（四）组织保障：多方联动与能力建设的支撑

《行动计划》落地需强化“顶层统筹-基层落实-能力支撑”的全链条保障：在国家层面，由国家发展改革委数据局会同财政部、住房城乡建设部、自然资源部等部门加强工作指导，分类分级有序推进，强化部门协同与上下联动；在地方层面，支持各地建立高层级统筹推进机制，针对重大需求、重大场景、重大改革集中发力；同时，加大对数字化转型技术攻关、重大项目、试点试验的资金支持，强化数字化转型、数据合规、数据服务等专业人才队伍建设，并通过优秀实践与典型案例的提炼推广、深化国际交流合作，为各地提供经验借鉴与能力支撑，确保转型路径不偏、力度不减。

结语：迈向数字文明时代的现代化人民城市新图景

从“数字福州”的探索到“数字重庆”的实践，从“一网通办”的便民到“一网统管”的高效，我国城市数字化转型已走过十余年历程。《行动计划》的出台，标志着这一进程进入“系统重构、质效提升”的新阶段——不再是技术的简单叠加，而是城市生命体的“系统性重塑”；不再是单点的创新突

破，而是全域生态的“整体性进化”。站在新的历史起点，推进全域数字化转型，需以系统思维呵护城市生命体的健康成长，以创新精神破解转型中的难点堵点，让数字化真正成为滋养城市、服务人民的“源头活水”，为中国式现代化注入澎湃的城市高质量发展动能。

作者：中央财经大学政府管理学院城市管理系主任 王伟

国家发展改革委等部门关于印发《关于推动物流数据开放互联有效降低全社会物流成本的实施方案》的通知

原载：“国家数据局”微信公众号

国家发展改革委等部门关于印发《关于推动物流数据开放互联 有效降低全社会物流成本的实施方案》的通知

发改数据〔2025〕1387 号

各省、自治区、直辖市、新疆生产建设兵团发展改革委、数据管理部门、党委网信办、交通运输厅（局、委）、市场监管局（厅、委），海关总署各直属海关，各地区铁路监督管理局，民航各地区管理局，各省、自治区、直辖市邮政管理局，各铁路局集团公司：

为全面贯彻党的二十大和二十届历次全会精神，落实中央财经委员会第四次会议部署和《有效降低全社会物流成本行动方案》有关要求，推动建立物流数据资源开放互联机制，促进有效降低全社会物流成本，国家发展改革委、国家数据局、中央网信办、交通运输部、海关总署、市场监管总局、国家铁路局、中国民航局、国家邮政局、中国国家铁路集团有限公司制定了《关于推动物流数据开放互联 有效降低全社会物流成本的实施方案》。现印发给你们，请结合实际抓好落实。

国家发展改革委

国家数据局

中央网信办

交通运输部

海关总署

市场监管总局

国家铁路局

中国民航局

国家邮政局

中国国家铁路集团有限公司

2025 年 11 月 3 日

关于推动物流数据开放互联有效降低全社会物流成本的实施方案

物流是实体经济的“筋络”，联接生产和消费、内贸和外贸。推动物流数据开放互联，是提升资源配置效率，畅通实体经济循环的重要举措。为深入贯彻落实党中央、国务院决策部署，建立物流数据资源开放互联机制，促进有效降低全社会物流成本，制定本实施方案。

一、总体要求

以习近平新时代中国特色社会主义思想为指导，全面贯彻党的二十大和二十届历次全会精神，落实中央财经委员会第四次会议要求，着力夯实物流数据开放互联基础，依法合规推进物流公共数据共享开放，促进企业物流数据市场化流通利用，深化物流与信息流、资金流整合，打通多式联运数据堵点，优化物流资源配置，释放产业赋能潜力，为降低全社会物流成本、建设全国统一大市场、构建新发展格局提供有力支撑。

二、夯实物流数据开放互联基础

（一）推动数据高效采集汇聚

深化物流行业数字化转型和智能化改造，推动物流基础业务线上化、可视化、数据化。拓展物联网、云计算、大数据、人工智能、区块链等技术在物流领域的规模化应用，实现物流数据实时采集、广泛连接和高效汇聚。支持物流骨干企业、平台企业强化物流数据治理，遵循“共享协同、多源校核、动态更新”原则，推动跨主体、跨行业、跨领域数据互联互通。

（二）健全物流数据标准规范

构建物流数据标准体系，研究制定物流数据分类分级保护、采集汇聚、共享开放、质量评价等标

准规范，强化数据标准衔接，统一数据共享交换规则，加强国内国际标准接轨。推进物流数据标准宣贯实施，开展标准实施效果评价，提升标准的有效性和适用性。围绕产品数字化和业务协同，推广标准化数据接口和解决方案，持续提升物流数据标准化水平。

三、推动物流公共数据开放互联

（三）加强物流公共数据共享开放

建立国家物流公共数据共享开放清单，根据行业管理和政务服务需要，明确物流公共数据共享范围，加强企业资质、从业人员、车船注册、通关物流等数据归集共享。对已在国家有关部门实现集中管理的物流公共数据，加大“总对总”共享力度，健全信息更新维护机制，提升物流公共数据共享质效。加大基础设施、运力、价格等物流公共数据开放力度。

（四）完善物流公共数据授权运营机制

实行物流公共数据资源分类分级管理，规范开展物流公共数据授权运营，扩大路网、轨迹、企业、人员等数据供给。推动用于公共治理、公益事业的物流公共数据有条件无偿使用，对用于产业发展、行业发展的物流公共数据产品和服务，按照相关规定实行政府指导价管理，根据经营成本、市场需求等合理定价，降低社会用数成本。加强物流公共数据授权运营跟踪监管和信息披露，规避数据违规交易。

（五）提升物流公共数据应用服务水平

面向“港口与海关”“运输与外汇”“企业与资质”“保险与海事”等业务联动场景，深化物流公共数据跨行业、跨地域、跨层级应用。加强物流相关政务服务数据整合，提升实名认证、电子证照、资质核验等公共服务便利化水平。

四、促进企业物流数据市场化流通利用

（六）推动企业物流数据开放互联

依托国家物流枢纽、综合货运枢纽等建设，强化物流数据标准落实，推动区域性物流数据整合共享。支持物流骨干企业、平台企业等共建物流行业可信数据空间，建立健全企业数据采集、提取、应用、保护等机制，促进物流数据可信流通和协同利用。

（七）扩大物流数据产品和服务供给

鼓励企业面向物流追踪、关务协同、智慧云仓、共同配送等应用场景，以及冷链、医药、烟草、危化、军民融合等专业物流发展需要，开发多样化物流数据产品和服务，促进运输、仓储、配送、通关等环节高效衔接，提升物流资源配置效率。丰富物流市场分析、趋势洞察、风险识别等行业级数据产品和服务，为中小企业生产经营提供决策支持。支持有条件的企业打通跨境数据链路，破解国际物流信息不对称问题，为跨境商贸活动提供有力支撑。

（八）打通多式联运数据堵点

推进多式联运相关单证认证、鉴真等技术应用，实现单证可信流转、货物全程追溯，促进多式联运“一单制”“一箱制”加速落地。支持铁路、公路、水路以及第三方物流等骨干企业，向多式联运信息集成服务商转型。发挥交通强国建设试点等引领作用，围绕物流骨干企业、国家物流枢纽，创新多式联运数据交互模式和解决方案，畅通公铁联运、海铁联运、公水联运衔接。依托中欧班列、国际陆海贸易新通道等载体，推动跨境数据融合应用，推进国际多式联运综合服务模式创新和推广应用。

（九）加快释放产业赋能潜力

推动物流数据与产业数据等多源数据融合应用，促进产业结构和空间布局优化，为能源、交通、物流等相关基础设施规划建设提供参考依据，促进结构性降本增效。鼓励物流企业顺应现代产业体系发展需要，面向智能制造、现代农业、商贸流通等行业领域，深化跨行业数据整合利用，提升数字化供应链集成服务能力。深化物流数据在金融行业的应用，优化融资、保险等产品服务，助力解决企业特别是中小企业融资难、融资贵问题，降低企业经营风险。

五、保障措施

（十）加强统筹协调

国家发展改革委、国家数据局会同有关部门和

单位，统筹推进物流数据开放互联，抓好督促落实，协调解决重点、难点问题。建立物流公共数据共享开放清单更新机制，定期通报数据共享情况。

（十一）强化激励引导

深入推进物流数据开放互联试点，打造一批典型场景和创新模式，推广先进经验。加强政府投资对物流数据流通利用相关的基础设施建设支持力度。开展监测评估，引导相关部门、地方和企业持续深化物流数据开放互联和开发利用。

（十二）筑牢安全保障

建立健全物流数据开放互联安全防护体系。压实相关部门和单位安全管理责任，制定完善网络安全、数据安全事件应急预案，及时处置相关安全威胁和事件，并按照规定向有关主管部门报告。落实物流数据分类分级保护要求，鼓励加强区块链、隐私计算等技术应用，促进数据可信交互，切实保障数据安全。

涉退役军人违法违规账号处置典型案例

原载：“网信中国”微信公众号

根据“网上涉退役军人不当行为和有害信息内容专项整治”工作安排，近期，我办指导各网站平台从严整治以退役军人名义售卖假冒伪劣商品、进行低俗表演、消费军旅情怀、损害退役军人形象等问题，处置一批违法违规账号。

现将部分典型案例通报如下：

一、发布低俗内容。网络账号“颜班长（退役女兵）”“小颜班长（退役女兵）”“漠九”等，自称退役军人，发布穿着暴露，含有性暗示、性挑逗的低俗擦边内容。网络账号“王兴奇”等，穿着我国武装力量现行或曾经装备的制式服装及其仿制品，在直播过程中开展低俗舞蹈表演吸引用户打赏。

二、传播有害言论。网络账号“宋班长（正能量）”“睿智人生”等，以讲授从军经验、咨询部队情况等名义，发布“在某地服役有什么危害”“在部队患上这样那样的疾病”等导向不良言论。

三、散布虚假信息。网络账号“防 炎炎夏日”“中国梦# ”等，利用人工智能、深度合成等技术，制作发布“边疆站岗 20 年，如今带着有病的孩子走在路上”等谣言信息，以及虚假退役军人图片、视频等，误导公众认知。

四、不当营销牟利。网络账号“A-后勤仓库 正品协调”“迷彩仓”“贩卖人间快乐”等，借退役军人身份，违规售卖军服及其仿制品，或发布提供各类定制服务的营销信息。网络账号“红旗白鸽”等，以提供“转业安置咨询”等为噱头，歪曲解读涉军政策，违规提供收费咨询服务。

汽车行业网络乱象专项整治行动公开曝光一批典型案例

原载：“网信中国”微信公众号

近期，国家网信办会同工业和信息化部等部门深入开展汽车行业网络乱象专项整治行动，从严整治散布虚假不实信息，恶意抹黑诋毁汽车企业、汽车产品等违法违规行为。现将部分典型案例通报如下：

1.“大眼哥说车”等账号发布贬损性信息，侵害企业商誉和产品信誉。抖音账号“大眼哥说车”、今日头条账号“电电加电”、快手账号“森哥电车”等，随意发布贬损性言论，恶意诋毁某汽车企业品牌、辱骂企业家并持续炒作。涉及的账号已被依法依约采取关闭等处置措施。

2.“高见观潮”等账号散布虚假不实信息，恶意诋毁攻击企业。今日头条账号“高见观潮”、微信公众账号“象视汽车”、微博账号“大 D 有态度”等，编发涉某汽车企业虚假信息，诋毁攻击企业产品质量，恶意唱衰企业经营状况。涉及的账号已被依法依约采取处置措施。

3.“我是大彬同学”等账号恶意集纳企业负面信息，诋毁攻击企业产品。微博账号“我是大彬同学”、抖音账号“石头搞机”、哔哩哔哩账号“赛车星冰乐”等，为博眼球、吸流量，集纳企业负面信息、蹭炒涉企热点事件、煽动群体对立。涉及的账号已被依法依约采取处置措施。

4.“易车榜”等账号巧立名目发布汽车销量榜单，干扰企业正常生产经营。微博账号“易车榜”“中汽数研”“大侠侃车”等，频繁发布未经核实，甚至捏造、杜撰的汽车销量数据，误导消费者，干扰汽车企业正常生产经营。涉及的账号已被依法依约采取处置措施。

5.“王武松”等“转世”账号继续发布不实信息，抹黑诋毁汽车企业。抖音账号“王悟空说车”“987 疯狂奶爸”因多次歪曲事实诋毁新能源汽车性能，恶意抹黑某汽车企业形象声誉被依法依约关闭。上述账号使用主体，在抖音、小红书、百度等平台注册“王武松”“疯狂斯坦森”等账号，继续发布主观测评信息，抹黑攻击某新能源汽车企业产品质量。涉及的账号已被依法依约采取关闭措施。

中央网信办严打一批涉学术论文买卖违法违规账号

原载：“网信中国”微信公众号

近期，部分网络账号违规提供学术论文买卖、代发、代投服务，严重扰乱网络秩序，污染网络生态。我办依法严惩一批违法违规账号，现将部分典型案例通报如下：

一、明码标价实施学术论文买卖行为。网络账号“琪瑞派论文咨询”“苏苏老师论文辅导咨询”“本硕博毕业服务旗舰店”等，利用“毕业论文全天加急”“文章代笔”“辅导至毕业”等宣传营销话术，明码标价提供学术论文买卖、代发、代投服务。上述账号已依法予以关闭。

二、引流圈群实施学术论文买卖行为。网络账号“木木学姐论文咨询”“GYuan-论文指导”“A1 孙少军 09”、微信公众账号“数典汽车排行榜”孙编辑”等，以“论文辅导”“期刊咨询”“论文降重”等隐晦话术，诱导用户添加微信、QQ 等私域圈群联系方式，违规提供学术论文买卖、代发、代投服务。上述账号已依法予以关闭。

三、利用话题暗示提供违规服务。网络账号“司徒说创业”“官子随笔”等，发布“AI 代写业务招商”“招募兼职写手”等话题，在其简介、评论互动等环节暗示提供学术论文买卖、代发、代投服务。上述账号已依法予以关闭。

网信部门从严整治利用 AI 仿冒公众人物开展直播营销问题乱象

原载：“网信中国”微信公众号

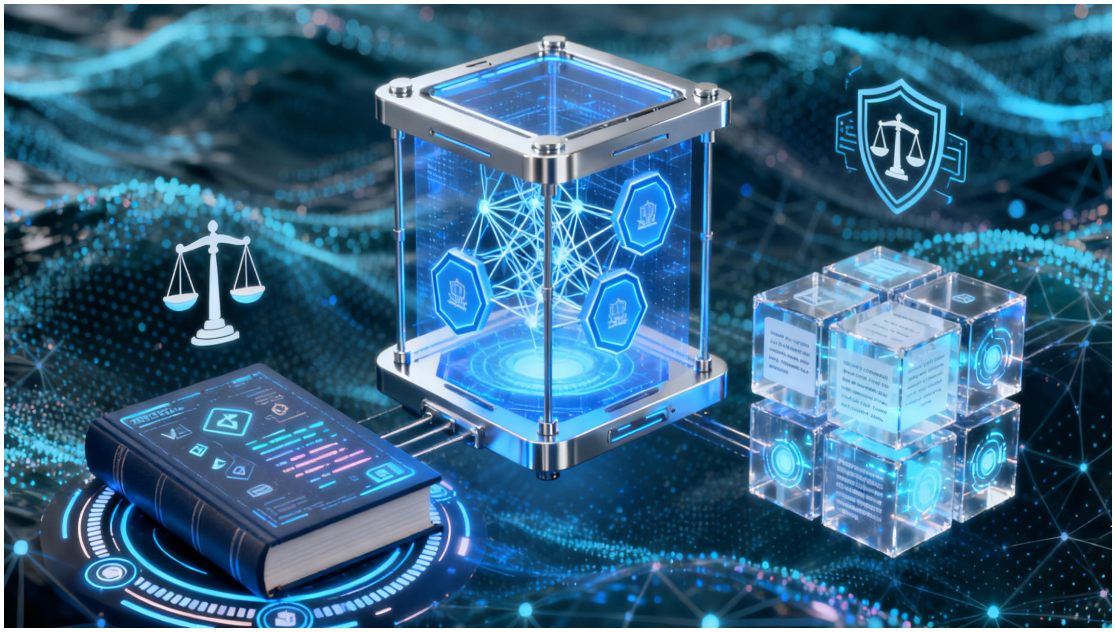
近期，有网络账号利用 AI 技术仿冒公众人物形象，在直播、短视频等环节发布营销信息，误导网民，涉嫌虚假宣传和网络侵权，严重破坏网络生态，造成不良影响。

网信部门严厉处置“百货超市小店”“娜娜好物联盟”“环球护肤美妆甄选”等一批违法违规网络账号。同时，督促网站平台发布治理公告，举一反三，开展集中清理整治，目前已累计清理相关违规信息 8700 余条，处置仿冒公众人物账号 1.1 万余个。

下一步，网信部门将继续压实网站平台主体责任，对利用 AI 仿冒公众人物开展直播营销问题保持高压严管态势，对恶意营销账号，发现一批、处置一批、曝光一批，维护良好网络生态。

（技术编辑：来唯希）

研究动态



基础理论

1、中国网络与信息法学的体系化建构（周辉）

来源：《法律科学(西北政法大学学报)》2025 年第 5 期

中国网络与信息法学的体系化建构是推动中国自主知识体系建设、统一学科名称、推动中国网络法治发展和专业人才培养的关键。中国网络与信息法律制度是网络与信息法学的实践基础和研究重点，目前已经形成网络法、数字法、智能法、信息法的支撑框架。网络与信息法学基础理论以新型主体、新式客体、新类内容为特点推进法律关系理论演变，赋予传统法律命题新内涵，并发展出本学科的核心范畴。在研究范式上，应统筹研究法律规范与平台规范，贯通法治思维与互联网思维、数字思维、人工智能思维，实现价值定性分析与数据模型定量分析并重，采用敏捷回应与有效塑造网络与信息法治实践方法，在汲取全球经验中推动中国网络与信息法学的守正创新。网络与信息法学已经从领域法发展为以塑造核心范畴、保障新质生产力发展为时代任务的独立的新型二级法学学科，属于兼具全球视野与中国特色的新兴学科和交叉学科。未来，应在进一步完善基础理论、完善制度建设、革新研究范式和加强国际交流的基础上，更好地构建本学科的自主知识体系。

2、数字技术规范法律化与数字平台善治（孙晋）

来源：《中外法学》2025 年第 5 期

在数字经济时代，技术规范是指利用互联网、大数据、人工智能等现代数字技术手段，在数据处理、算法运行与信息交互等环节中形成且具有事实支配力的技术性规则体系。数字平台的搭建与运营以数字技术规范为基础，数字平台的新型违法行为与数字技术规范之间存在深度关联。在数字平台治理中，传统监管面临监管理念滞后、规则表面化、效果低效等问题。推动数字技术规范法律化，借助数字技术实现多元主体协同治理，或是克服难题的可行路径。为实现数字技术规范法律化，在宏观层面，应通过软法的制度过渡和多方主体的广泛参与，奠定共识与方向；在微观层面，应通过具体的法律技术机制予以落实，实现制度设计与操作方式的有效衔接。借由数字技术规范的法律化，可促进平台法律规则的“良法化”，以及平台自我规制的“善治化”。

3、网络时代刑法罪名体系应用的基本立场（喻海

松）

来源：《法学论坛》2025 年第 5 期

网络技术的发展给刑法带来巨大挑战。增设网络犯罪专门罪名当然是刑法应对的重要方面，但如何将其与既有罪名融合，实现在网络空间的妥当适用，则更为值得关注。在计算机网络犯罪专门罪名的适用方面，计算机犯罪专门罪名日益网络化，与网络犯罪专门罪名逐渐融合，一体实现在网络空间的应用；当然，计算机网络犯罪专门罪名也存在由线上向线下的反向适用。在传统犯罪罪名的适用方面，其逐渐迁徙至网络空间，呈现出明显的网络化态势，日益成为网络犯罪应对的主力军。展望未来，就基本立场而言，要审慎设置计算机网络犯罪专门罪名，实质审查判定网络危害行为的性质，充分考虑线上线下双向适用的差异，借助不断健全的前置规范明晰争议，最大限度地促进网络时代刑法罪名体系的应用。

数据法学

1、论数据泄露受害人精神损害的认定（解正山）

来源：《法商研究》2025 年第 5 期

数据泄露不仅意味着受害人失去对其个人信息的控制，而且将导致其遭受不同程度或形式的未来侵害风险。尤其是，与这些风险关联的焦虑、恐惧等负面精神反应还将打破数据泄露受害人原本享有的精神平稳或安宁之状态。鉴于未来侵害风险的真实与否关系到精神损害的存在性与严重性，因此精神损害真实与否的司法审查首先应采高度盖然性标准对数据泄露受害人面临的未来侵害风险进行评估；其次，精神损害“严重”与否的解释论可转向客观合理性标准而非严格的可证实标准，着重对受害人精神损害的真实合理性进行审查。同时，为避免对信息控制者构成过度威慑，数据泄露受害人精神损害的赔偿应具有必要的限度。

2、论数据权益容他（付大学）

来源：《中外法学》2025 年第 5 期

数据作为数字经济时代的关键生产要素之一，其价值的实现依赖于流通与使用，其制度基础在于数据权益的容他性而非排他性。数据权益容他是驱动数字经济发展的底层逻辑，旨在通过法律与技术手段促进数据的开放共享与流通交易。尽管学界对数据确权存在争议，但数据权益容他是各方理论观点的公因式，共同目标为促进数据的生产、利用与流通。数据权益容他的理论根源在于：宏观层面以法律价值多元主义为哲学基础；中观层面以财产的人类繁荣理论为社会目标；微观层面以数据的非竞争性为技术支撑。其实践价值体现为：降低“用数”成本、提升数据利用效率、促进创新并抑制数据垄断。基于原始数据与衍生数据的二元划分，数据权益容他应采取差异化路径：原始数据通过强制开放、不予赋权(法定容他)与可信数据空间实现有序容他；衍生数据通过产权分置(法定容他)、契约分享(意定容他)与多元化共享技术实现有限容他。

3、论公共数据产权的法律构造（邓文昊）

来源：《行政法学研究》2025 年第 5 期

公共数据产权法律构造的核心命题，在于界定多元主体对公共数据的权利归属与行使边界。然而，现有学说难以回应公共数据产权共享开放与独占控制等内在冲突。因此，需以公共数据产权的运行实践为基础，明确公共数据产权法律构造的理论范式。在法理构造层面，公共数据是国家所有的公共财产，具有“宪法上国家所有/民法上国家所有权”的双重意蕴，二者分别构成产权分配和授权运营的宪法依据；公物法理论、权利束理论和分配正义原理共同构成了公共数据产权的法理基础。在权利构造层面，依“三权分置”框架，围绕持有权、使用权和经营权，构建开放共享与要素流通并重的权利体系。在制度建构层面，先通过适用类型化区分的登记确权制度明确权属，再对政务公共数据和加工公共数据分别适用非营利的限制制度和有限盈利的运营制度，以遏制行政垄断、释放数据价值，保障公共数据产权规范运行。

4、数据出境安全评估的制度构造（王玎）

来源：《法律科学(西北政法大学学报)》2025 年第 5 期

《个人信息保护法》将关键信息基础设施运营者和处理个人信息达到规定数量的个人信息处理者向境外提供数据的活动作为安全评估制度适用的条件。但在实践中，由于《网络安全法》《数据安全法》《个人信息保护法》所规定的数据出境安全评估的要求不同，个人信息、重要数据的类型存在差异，数据出境场景多样，导致安全评估制度目的不清、制度规定错位、适用规则混乱以及实践部门对行政救济机制的误解等问题。对此，应澄清数据出境安全评估属于数据安全审查，明确安全评估的目的是维护国家安全和社会公共利益，将评估作为重要数据出境的必要条件和个人信息出境的附加条件，重新审视数据出境安全评估的适用规则。《数据安全法》第 24 条规定的数据安全审查制度为数据出境安全评估免予司法审查提供了合法性依据。同时，法院不具备审查数据出境安全评估实体结论的专业能力，如对数据出境安全评估程序进行合法性审查会使行政诉讼程序空转，故而复评作为数据出境安全评估救济机制具有正当性。

5、论数据抓取行为的正当性判断（王文君）

来源：《比较法研究》2025 年第 5 期

数据抓取行为的正当性判断标准模糊，三重利益评估模式考察的因素过于情景化，数据价值动态变化导致难以甚至无法评估竞争损害，不符合实质性替代规则以结果为导向的逻辑，实质性替代规制本身也存在悖论。数据确权说与否定说均认为数据产权仅具有有限排他性，并不等同于传统财产所有权。从数据利用的非排他性和数据效用的不确定性分析，数据抓取正当性评价应考虑保护意愿、技术措施是否被突破、数据集合的价值（竞争性权益）、抓取数据集合的合理限度四个方面的因素。从利益衡量理论入手，数据抓取的合理限度得以明确。对不涉及个人信息的数据抓取，利益衡量实际上是在保障数据自由流通的前提下，根据数据控制者是否采取以及采取何种技术性措施，识别值得通过禁止数据抓取的方式予以规制的数据竞争优势。对涉及个人信息的数据抓取，还应结合个人信息的识别度落实抓取方的个人信息保护义务。

6、论数据交易信赖保护的公开市场规则（申卫星、李卓凡）

来源：《法制与社会发展》2025 年第 5 期

数据交易市场因信息不对称与信赖基础缺失而陷入失灵困境,亟需构建适配数据要素特性的信赖保护规则。传统善意取得制度以占有、登记等具体权利外观作为信赖基础,然而数据的动态性、非竞争性特征,加之我国结构性分置与平行持有的数据产权设计,导致具体权利外观与真实处分权限之间的对应关系瓦解,占有与登记无法有效表征权限归属。因此,信赖基础应从具体外观向抽象外观转换,依托公开市场创设“场景信赖”,并借助国家信用背书与程序规范性重塑市场信任机制。公开市场规则包含三重要件:第一,交易市场具备公共性、公开性与合法设立性;第二,交易过程具有规范性、典型性、惯常性;第三,交易主体主观上须为诚实善意。符合公开市场规则的受让人能够受到分层信赖保护,在满足排他性交易与可归责要件的前提下,可被赋予高阶的积极信赖保护。对于核心数据、重要数据及未去识别化的个人数据等流通受限的数据类型,以保护静态交易安全为先,不适用公开市场规则。

7、个人信息保护刑事附带民事公益诉讼的理论证成与构造优化（丁金钰）

来源：《法学论坛》2025 年第 5 期

刑事附带民事公益诉讼是检察机关履行公益诉讼职能的重要途径之一。但由于法律供给不足，涉信息网络犯罪刑事附带民事公益诉讼在当事人适格、诉前公告履行、刑民责任承担等问题上存在诸多争议，相关的司法实践呈现出复杂多样的审理样态。首先，在个人信息保护领域，由其他法定组织提起民事公益诉讼的情形极少，且检察机关与其他组织

为平权关系，诉前公告程序并无必要且会影响诉讼效率，应予废除。其次，由于刑事诉讼与民事诉讼中责任认定标准等事项的差异，适度扩大被告主体范围有助于最大限度地保护公共利益。最后，检察机关在附带民事公益诉讼中虽能主张惩罚性赔偿，但应保持谦抑与克制，只有当刑事罚金远远达不到惩罚、预防和公益保护的效果时，才有追究惩罚性赔偿责任的实益。

8、公共数据授权运营的国家担保责任重构（赵舒捷）

来源：《东方法学》2025 年第 5 期

公共数据授权运营在营利性与公益性之间存在分歧，本质上是其中的国家责任定位不明确，仅凭国家任务分析难以形成有效结论。作为形式民营化的特殊形式，公共数据授权运营排除“出售国有资产”和“国家退出”两种责任模式，国家的担保责任得以重新证立。传统国家担保责任模型存在原则和制度的预设，但在公共数据授权运营中面临国家控制力与民营化目的间的张力，须结合经济背景与数字场景进行重构。担保责任的经济范畴应基于社会主义市场经济体制实现扩展，经济基本权利、公平竞争秩序与共同富裕构成担保责任的经济内涵。据此，国家应保障竞争性数据市场中的平等权利，完善市场决定价格机制，建立固定授权费标准与绩效考核机制，最终通过税收和公有制参与调节收益分配。数字主权理念下国家的有效控制力成为担保责任的前提，应区分内部与外部担保责任，确立国家对自我规制的主导地位，并将兜底责任前置以实现有效接管。当前公共数据授权运营的监管结构应作相应优化。

9、所有权在数据场景中终结了吗？——数据平行所有权论（郭轩扬）

来源：《东方法学》2025 年第 5 期

数据的非竞争性特征与多方平行持有现象，使得一物一权、独占支配、绝对排他、完全物权、权能分离等经典所有权教义出现失灵。然而，所有权的识别不以其形式特征是否变更为标准，应从归属推导出权能，而非从权能反证归属是否存在。多重所有权与相对所有权在所有权的制度演进史中均有迹可循，数据场景下的所有权亦可通过一数多权、平行支配、有限排他、完整权利束、权能增殖等原理的重述实现制度再生。在此基础上，应构建区别于按份共有、区分所有的平行所有制度，引入产权链理论为数据之上的多元主体多元权益格局提供观测模型，并通过链间隔离的基本规则为数据的价值共创提供制度供给。

10、数据资产化：数据资产入表的法理基础（高富平）

来源：《东方法学》2025 年第 5 期

数据作为生产要素意味着其可以成为资产投入生产活动，而具有价值只是数据成为资产的必要条件，同时还须从数据价值的形成和实现机制出发，探寻数据资产化的制度和方法。作为技术经济治理模式的资产化理论可作为构建数据资产化的理论方法。数据价值的形成和实现是基于数据基础设施开展系列管理活动的结果，最终形成可支撑企业业务的数据智能系统，使企业成为数据资产持有者（管理者）。合法数据资产持有者可以自用和他用而实现数据的价值利用，支撑业务决策，为企业创造价值资产化门槛，而产品化流通交易只是数据资产价值实现的一种方式。数据资产化的法理基础是管理性劳动，这一过程不需要确权，只需要合法规范管理数据，覆盖从数据获取到价值实现的全过程。数据能否成为资产的关键在于从法律与会计两个角度，既要确认组织对数据资产所产生收入流的合法控制，又要计量该过程的成本和价值。合法数据持有者地位的确认与科学计量规则，可共同支撑数据资产化及其数据社会化重用的秩序。基于数据持有者权的治理范式可作为数据资产化落地的制度基础。

11、超越个体赋权：群体数据利益保护及其推进进路（斜晓东）

来源：《东方法学》2025 年第 5 期

群体数据分析技术的兴起使数据处理者可通过群体特征推断群体成员的个人数据，该推断行为游离于《个人信息保护法》的规制范围，引发新型数据风险。群体隐私理论与数据关系理论将该群体应免受不当数据分析的利益（群体数据利益）作为不可拆分的集体利益对待，但该解决方案不可行。群体数据利益是个人数据利益之和，可以通过保护个人数据利益间接实现群体数据利益保护。信息不对称、有限理性等因素使个人数据利益需要公私法融合保护。对涉及敏感个人信息的预测行为，鉴于其高风险性，应通过数据安全保障义务构建公法规制制度。对其他个人信息预测行为，可赋予个人自动化决策拒绝权，退出分析预测，但不宜扩张至其他个人数据权利主张。

12、论数据要素收益再分配：以用户公平参与分配为中心（于楚涵）

来源：《当代法学》2025 年第 5 期

在当前通行的“免费数据换免费服务”的互联网商业模式下，数据要素创造的收益几乎被厂商独占，而未向用户这一数据提供者分配，造成了严重的分配不公。这一问题根源于市场失灵，因此需要依靠政府干预加以解决。政府可以通过介入不同的分配环节来解决问题，具体包括参与初次分配、主导再分配以及引导三次分配。综合评估这三重路径的实施效果与实施难度，再分配的路径在现阶段最具比较优势，是应对数据要素收益分配不公问题的最佳选择。数据要素收益再分配的具体方案为：一方面，向厂商征收数据所得税以调节其过高收入；另一方面，将这些税收收入以参照全民基本收入发放现金、投资数字基础设施的方式返还给用户，以补贴其过低收入。这些举措通过将厂商的部分收入转移给用户来实现收益的再分配，能够在客观上达到使厂商将本应属于用户的收益返还给用户的效果，从而推动数据要素收益的公平分配。

13、个人信息收集中法律保留原则的梯度适用（张硕）

来源：《行政法学研究》2025 年第 5 期

《个人信息保护法》第 34 条将作为行政法基本原则的“法律保留”进行了具体化，要求行政机关收集个人信息应当具有法律或行政法规之授权。但对于纷繁多元的个人信息收集行为，该法条并未明确授权规范的纵向位阶与横向类型的适用问题。这也导致法律保留难以有针对性地关照多元场景下的差异化信息收集行为，协调个人信息保护与利用间的平衡。事实上，法律保留作为一项法律原则，其适用本就具有密度性特征，即针对不同事项可在纵向上适用由狭义法律授权的绝对保留或由行政立法授权的相对保留；在横向上适用由根据规范授权的行为保留或由组织规范授权的组织保留。据此，有必要依据收集行为的强制性、收集信息的敏感性、收集手段的自动化程度对行政机关的个人信息收集行为进行分类，并根据不同类型行为所干预公民权利的重要性、构成损害的风险性，将其与法律保留的密度结构进行动态耦合，建构一种强干预、高风险收集对应高密度法律保留，弱干预、低风险收集对应低密度法律保留的梯度适用方案。

14、数字资产财产犯罪的支配关系逻辑与规范判断（赵桐）

来源：《法学评论》2025 年第 5 期

数字资产是超越了物债二分结构的财产犯罪新型研究对象，物债二分财产权结构导出所有权与整体财产两种财产犯罪解释进路，前者在数字资产犯罪中引发罪名区分困境，后者无益于发挥财产犯罪法益限定功能。财产犯罪行为通过对支配关系的改变，打破与建立新的法律关系，进而导致经济利益减损，因而财产犯罪保护的法益本质上应当是支配关系的合法则运转。支配能力是支配关系存在的根基，保证了权利人排他性处分、使用或放弃数字资产，窃取与毁坏行为通过剥夺支配能力，直接导致支配关系法益受损，从而构成财产犯罪。支配意思保证了数字资产变动的正当性，诈骗、敲诈勒索与侵占行为通过压制被害人支配意思，或使得被害

人支配意思落空，实质损害支配关系法益，进而构成财产犯罪。

数字司法与行政

1、第三方网络平台配合电子证据取证的规范构造论（自正法）

来源：《东方法学》2025 年第 5 期

在网络犯罪案件复杂化、传统犯罪案件网络化的背景下，每个案件都可能涉及电子证据取证，而具有数据占有优势与数据技术优势的第三方网络平台，逐渐在电子证据取证中成为重要的参与力量。可以基于以下三个维度进行方案：一是学理维度，立足于犯罪控制与人权保障的目的，第三方网络平台的配合源于对公民基本权利保障的法律义务以及维护社会公共利益的社会责任，并顺应电子证据特性侦查的实际形势需要。二是规范释义维度，第三方网络平台配合电子证据取证的目的，在于追求客观真实，制定技术性指引，并明确取证程序的启动与执行。三是实践维度，第三方网络平台配合电子证据取证中出现界限模糊、程序宽泛、角色颠倒以及监督缺失等现象，不利于刻画电子证据取证中第三方网络平台配合的规范愿景，也可能造成同一主体以及不同主体间的义务冲突与利益减损。针对此类溢出风险，须厘清电子证据取证中第三方网络平台的配合前提，通过具体场景指引适用，并以数据分类为导向构建不同层级的审批程序，明确程序执行中第三方网络平台的辅助角色，以期解决第三方网络平台配合电子证据取证时的“后顾之忧”，实现电子证据取证兼具质量和效率的执行。

2、生成式人工智能助推司法审判的规制策略论（赵谦）

来源：《行政法学研究》2025 年第 5 期

生成式人工智能助推司法审判是推进智慧法院建设、深化我国司法改革的应有之义。对其实施规制旨在依托更具技术理性的强人工智能手段，围绕技术与司法之间的融通要求，通过梳理生成式人工智能的相应技术特征，明晰乃至规范人工智能司法应用的运行图景。探究生成式人工智能助推司法审判的规制策略，应立足于作为规制理据之生成式人工智能的功能定位和生成式人工智能助推司法审判的作用面向，从端口化定位下的技术支持、自动化定位下的文书处理和标准化定位下的类案裁判这三个方面，具体阐明相应的规制样态及其规制要义。首先，高技术特征导向下助推司法审判技术支持的起点型规制，旨在厘清数据处理的端口化集成和文本生成的端口化匹配，从而为优化司法审判活动提供必要的物质支撑。其次，高效能特征导向下助推司法审判文书处理的手段型规制，旨在从裁判文书要素的自动化解码和裁判文书内容的自动化拟制这两个方面，尝试推动将裁判数据运算后输出的计算语言更具效率地转化为所需要的法律文本语言。最后，高质量特征导向下助推司法审判类案裁判的目标型规制，旨在从类案事实的标准化认定和类案依据的标准化适用这两个方面，尝试促进在类案裁判数据知识谱系乃至类案裁判标准面向的客观化决策。

3、司法人工智能的应用逻辑与风险治理（李涛）

来源：《行政法学研究》2025 年第 5 期

数字时代，科技日益成为推动社会发展的重要力量，司法作为国家治理现代化的重要组成部分，也必然要顺应科技发展的潮流。引入司法人工智能是司法系统实现现代化转型的重要举措，也是科技发展的必然选择，有助于提升司法的智能化水平，增强司法在社会治理中的效能，更好满足公众对公正、高效司法的需求。在当代司法发展的进程中，科技与法律于司法系统内部实现融合是技术理性与法律实践内在需求之间双向驱动的必然结果，具有深刻的理论和实践逻辑。人工智能在智慧司法构建过程中展现出巨大潜力的同时，也暴露出其固有的局限性，以及随之而来的一系列法律、技术、伦理以及司法功能异化风险，这些风险有可能从潜在状态转化为现实困境。司法人工智能的应用是对司法工作的补充和提升，为有效应对风险，应秉持辅助司法、提高司法效率及更好实现司法公平正义等

指导理念，强化顶层设计，通过制定规范体系、构建应用规则、建设监管制度、加强伦理审查等手段，确保技术始终服务于司法正义。

4、合成数据赋能数字法治政府建设的风险及其规制（霍敬裕）

来源：《行政法学研究》2025 年第 5 期

一致性、兼容性和可信性的数据不仅是“开放性”和“责任性”互协演进治理框架的智能化底座，亦是“技术系统”与“职责体系”双向调适治理路径的数字化纽带。合成数据作为新兴的数据范式，兼具模拟性、预测性和经济性多重优势，其构成的仿真数据工具平台在智能决策、辅助执法、组织运行、绩效评测等典型数字法治政府应用场景中可有效补齐数据安全短板，防范“数据赤字—治理失灵”恶性循环，其产生的“技术—权力”耦合效应加速行政决策从经验驱动向数据驱动转型，产生技术赋权与权力结构化互构效应。合成数据的场景化嵌入虽能突破原始数据采集的物理边界与合规困境，但其衍生出的“虚拟—现实”双重治理维度，却加剧了法律事实认定标准的解构风险。为破解合成数据的赋能风险，亟需构建“技术可解释性审查”为程序性要件和“风险梯度响应”为实体性标准的双轨制衡机制，动态校准数字治理效能与法治核心价值间的制度均衡。

5、数字政府协同原则的规范内涵及制度展开——基于行政组织关系的视角（展鹏贺）

来源：《行政法学研究》2025 年第 5 期

在数字政府模式中，“协同”既是政府履职方式的具体表现形态，又是制度规则体系构建的基本原则。在政府治理信息化与法治化相融合的要求下，明确“协同”在塑造行政组织关系时的规范内涵，是将协同原则从抽象法政策转化为具体组织法和行为法制度的重要前提。借助协同学理论的观察，国家行政任务目标本身即蕴含着行政组织间“同频共振”的协同要求。受职权法定与行政一体原则影响，科层制结构下的组织关系在既有规范体系中同时面临着来自管辖权界限的协同阻力，以及任务目标导向的协同动力。组织协同并非以整齐划一的制度形式呈现，而是在组织法概括承认协同原则的基础上，由行为法结合特定任务目标创设具体制度规则。面对数字政府在技术原理上天然显现出的协同本质，以及当前围绕管辖权联合和连接形成的协同实践，协同原则的制度构建应当以破除制度壁垒和填补规范真空为导向，从推动统一的基础设施建设模式、形成普遍兼容的数据归集标准，以及划定匹配数字业务协同的责任机制等方面具体展开。

6、论数字司法中价值的数据化及其挑战应对（彭中礼）

来源：《行政法学研究》2025 年第 5 期

在数字时代，建设数字司法已经成为迎接新一轮科技革命的时代选择。在人工智能深度参与司法决策中，算法发挥了核心作用。算法的核心能力是高速处理数据和执行逻辑运算。算法的设定受到算法工程师以及人类决策者们道德观念的影响，算法运行的结果也包含价值内容，因而不可避免地蕴含价值判断。算法嵌入司法程序，其进行价值判断的一般理路是植入特定价值观念、开启算法价值对齐以及防范算法价值风险等。在数字司法过程中进行价值判断，最重要的前提就是要实现司法价值的数据化。人工智能具有可计算性是价值数据化的前提，海量数据是人工智能算力水平不断提升的必然需要，且价值数据化可以通过经验方式形成海量的价值数字。推进价值数据化，需要对法律价值进行自然语言处理、提取法律价值的向量特征以及进行机器学习。价值数据化在数字司法中具有广阔的应用前景，但同时也面临一些挑战和风险。从根本上说，数字司法需要算法进行价值判断；而推进价值数据化是实现数字司法价值判断的关键。

7、论法律的数字化与司法裁判的标准化难题（孙海波）

来源：《行政法学研究》2025 年第 5 期

法律数字化的迅猛发展，使人工智能前所未有地改

变了法律实践，特别是在司法中得到广泛应用。从智慧法院建设到数字司法的变革，司法变得越来越智能化和信息化。从整体上看，目前人工智能在司法裁判中的运用主要是辅助性的，并未从根本上改变司法权的运行逻辑。从概念的性质上看，法律自身的规范性品质决定其难以被完全数字化，“法律即代码”的主张无法在普遍的意义上成立。同时，裁判是整个司法的核心环节，法律推理又是司法裁判的基本运作方式。人工智能基于规则和基于案例的两种推理系统，均未从根本上突破传统的法律推理方式，因而无力改变司法裁判的基本结构。基于计算主义的裁判预测论，法体系中不可避免的裁量及价值判断，均为司法裁判数字化制造了理论和实践上的困难，从而使得计算法学想要建构的那种标准程式的裁判难以实现。我们既要正视人工智能带来的法律数字化现象，又同时警惕它可能带来的各种消极影响，尤其是认识到法律数字化力图构建的标准化裁判模式并不符合客观现实。

8、大数据证据的鉴定意见化问题研究——以金析为证为例的分析（褚福民）

来源：《法学杂志》2025 年第 5 期

按照公安机关开展的金析为证改革，大数据证据在诉讼过程中以鉴定意见的方式呈现，按照鉴定意见的规则进行审查、质证，相关的分析技术、程序适用鉴定活动的相关规则，由此提炼出大数据证据的鉴定意见化问题。大数据证据的鉴定意见化具有特定的生成机制，包括资金数据分析成果无法转化为诉讼证据的困境，公安机关对资金数据的分析方式、实践操作更契合鉴定活动，资金数据分析成果符合鉴定意见的属性特征，相关法律规定提供了制度空间，以及检察官、法官对资金数据分析类型鉴定意见的认可态度。尽管如此，大数据证据的鉴定意见化仍面临一系列困境和挑战，包括转化的正当性问题，转化对象的界定不清，资金数据类型鉴定意见的可靠性质疑，对其有效质证、认证的现实困境，以及从资金数据分析成果到其他大数据证据的延伸问题。未来，大数据证据的鉴定意见化的完善，应当针对以上问题进行对应性解决。

9、大语言模型在刑事司法证明中的应用问题研究（孟晓帆）

来源：《法学》2025 年第 11 期

大语言模型以概率分布进行序列建模，在方法论上与以盖然性为特征并通过概率性推理形成内心确信的司法证明高度契合。大语言模型依托注意力机制及强大的非线性建模能力对海量法律规范及裁判文书进行深度学习，通过归纳并模拟证据推理与评价的规律来矫正经验法则的主观偏差。经过法律语料训练的大语言模型可以将从证据语料到事实认定的生成过程量化为概率计算，从而辅助法官减轻因系统性认知偏差所形成的预判与偏见，在很大程度上有利于解决传统自由心证推理路径不可见、评价标准不明等问题。然而，大语言模型的应用仍存在责任归属模糊化、算法决策“黑箱”化以及数据安全和隐私保护等问题。对此，可构建系统责任链条，确立强制性透明度要求，以此提升大语言模型在司法证明中的可解释性，并强化数据安全与隐私保护。

10、自动化行政中正当程序原则的重构（唐安然）

来源：《比较法研究》2025 年第 5 期

正当程序原则传统的个体防御功能在自动化行政中产生“法律—技术”张力。实践中表现为具有普遍适用性的自动化系统与个体防御程序难以共存，导致专家系统消解个体防御程序、机器学习系统欲保障个体防御程序需放弃自动化系统。深层原因是既有法规范将采用自动化系统视为行政裁量，使得以个体防御为目的的行政程序法只能问责行政，而无法问责自动化系统。对此，正当程序原则有必要从“行政权力—公民权利”双方调整结构转向“行政权力—算法权力—公民权利”三方调整结构，发挥个体防御与集体受益的利益权衡功能，通过“为行政程序增添技术翻译”与“为技术效果赋予行政意涵”来适应技术应用。为重构正当程序原则，在程序正义上，应用技术正当折抵、强化与再造程序

正当，实现替代正义、优势正义与未来正义；在行政程序上，应增设算法规则适用的转译程序、自动化决策与人工决策的比较程序，以及自动化系统纠错的更新程序，作为数字时代的程序正当新要件。

11、数字化行政中行政主体与行政相对人关系的体系构造（耿思远）

来源：《法制与社会发展》2025 年第 5 期

在数字化行政中，行政权力、行政相对人权利及二者关系的变革是体系性的，局部视角难以根本回应“权力—权利”平衡问题。数字化行政中存在着既有权力的行使、新型权力的行使和违法滥权的权力行使。这三类权力行使对行政相对人权利产生的影响具有本质不同。行政相对人的实体性权利得到有限扩充，程序性权利被严重弱化，诉讼权利行使遭遇困顿。以程序性权利和诉讼权利为重心的传统平衡方案未能适配数字化行政的技术特点。数据、技术和智力等权力资源向行政主体集中，使其在数字化行政中获得了压倒性优势。“行政自制”应在促进数字化行政的“权力—权利”平衡中发挥更重要的作用。根据不同权力行使现象的特点，可以分别从行政行为合理性和合法律性维度，构建对行政主体的权力控制体系。行政相对人权利的体系建构应着重加强实体性权利保障，实现诉讼权利的有效行使。

12、论大数据证据的多元关联性（王燃）

来源：《法制与社会发展》2025 年第 5 期

司法证明领域的通常观点认为，大数据证据的相关关系与传统证据的关联性存在冲突。实际上，传统证据的关联性兼具物理载体的接触性和证据事实的因果性；而大数据证据则具有因果关系与相关关系的双重属性。在“证据事实→待证事实”阶段，大数据证据与传统证据同样遵循因果逻辑；但在“证据载体→证据事实”阶段，大数据证据则呈现出独特的相关关系。这种相关关系的理解难点源自逻辑驱动型算法的制度黑箱和机器学习型算法的技术黑箱。大数据证据关联性审查的关键在于构建符合人类因果思维的解释机制。在数据层面，应审查数据源是否具有载体关联性，训练数据是否与分析对象具有一致性。在算法层面，应围绕模型逻辑一致性、推理过程透明性和特征变量因果性，构建面向司法证明场景的分层解释机制，对关键特征变量进行因果验证。此外，可借助概率值对大数据证据进行辅助解释，审查算法输出的准确度是否达到人类经验的准确度及司法证明标准。

13、论数字检察视域下虚假仲裁有效法律监督路径构建（牛正浩）

来源：《法学论坛》2025 年第 5 期

虚假仲裁是当前困扰我国仲裁制度公正性与持续发展的最大隐患，检察机关具备国家法律监督机关与公共利益维护者的双重职能，对虚假仲裁进行法律监督具有制度与理论的正当性，数字检察战略的实施为虚假仲裁的有效法律监督提供了全新应用场景和更高治理要求。当前检察机关针对虚假仲裁的法律监督存在实践和理论层面的双重困境，对此应遵循“个案办理—类案监督—系统治理”模式，充分运用大数据思维与人工智能技术，从建立并完善虚假仲裁数据共享机制、构建虚假仲裁数字监督模型、研发虚假仲裁识别预警系统、加强重点人群虚假仲裁数字监管四个维度，并辅以相应程序法革新，着力构建针对虚假仲裁的有效法律监督路径。

算法与人工智能治理

1、法律解释的算法驱动及其应用规范（温荣）

来源：《法商研究》2025 年第 5 期

法律解释经常面对解释概念界定、解释方法选择、解释论据收集和解释结论权衡等多重不确定性，且始终处于竞争性甚至冲突性的语境，需要通过充分论证来减少争议。法律解释的论证过程既需要传统的逻辑推理和“概念计算”，也需要适时引入定量计算以优化论证饱和度与分量权衡。这些计算过程的科学性和规范性可以通过算法思维和技术予以强化。论证图式挖掘算法可以丰富法律解释的论证

图式类型，回应法律解释的论证程序匹配问题；语料库语言学、实验法、社会网络分析等可以为语义辨别、体系解读乃至价值判断提供扎实的论据来源和科学的分析方法，从而提升解释性论证的分量饱和度；重力公式等算法可以更好地辅助多个解释性论证的评估权衡，并进行择优选择。算法驱动法律解释也会遭遇论证上的可靠性、可接受性以及经济性等问题，需要遵循简约化、透明性、融贯性和辅助性要求，进行相应的规范约束。这意味着算法在法律解释中只能是备选工具而非主导选项。

2、论大模型训练数据的合理使用（李铭轩）

来源：《法学家》2025 年第 5 期

大模型训练数据的主要来源是网络上的公开数据，开发者一般通过爬取公开网页和收集开源数据来大规模获取训练数据。随着数据财产权益保护的强化，获取海量训练数据的主要方式面临着合法性挑战。数据财产权益人众多、数据使用行为难追溯导致交易成本升高，大模型开发者无法通过市场机制获得数据财产权益人的许可来确保训练数据的合法性。在市场失灵的情形下，允许开发者合理使用数据进行大模型训练，可以增进社会福利，且一般不会损害数据财产权益人的市场利益。采取集体管理或法定许可等替代方案给数据财产权益人带来的收益非常有限，却会产生更高的制度成本，并给我国大模型的发展造成不利影响。因此，我国应当建立大模型训练数据的合理使用制度，为技术发展提供合法性预期。在规则设计上，大模型训练数据合理使用的对象应限于公开数据；目的应限于预训练；方式应包括训练涉及的数据处理行为；应允许数据财产权益人以技术措施选择退出合理使用。

3、人工智能时代公民隐私权的刑法保护（刘宪权）

来源：《法学家》2025 年第 5 期

普通人工智能时代相关技术不能创设或改变公民隐私权的权利人，但可能催生出“用户行为数据画像”等新型隐私权法益。在弱人工智能时代，生成式人工智能对公民个人信息采集、处理和再利用的行为，正在不断压缩公民行使隐私权的空间。公民的隐私控制权可能从“知情—决定”向“默认—接受”转变。生成式人工智能处理数据的能力使大量“低敏感度”信息在经过大模型处理之后，具备了对个体的可识别性进而成为衍生性隐私数据。强人工智能机器人的超强信息处理能力可能引发公民隐私权存续问题的思考。现行刑法没有专门规制严重侵犯公民隐私权的独立罪名，而是将公民隐私权笼统地依附于其他人身权利或社会管理秩序之中予以间接保护。刑法理论与司法实践中仍普遍存在将公民隐私与公民个人信息以及公民个人数据相混同的情形。我国刑法应增设侵犯公民隐私权罪，以构建刑法对公民隐私权直接保护与间接保护并行的制度。法律需要进一步明确平台和技术提供者管理过失责任的认定标准。

4、从工具客体到关系主体：基于算法法律地位的本体论重构（王治国）

来源：《比较法研究》2025 年第 5 期

基于实体本体论与主客二分的算法规制范式已无法有效回应算法系统的非线性演化等复杂现象。研究引入关系本体论，主张将算法系统视为关系网络中的动态节点，其法律地位应由网络位置、关系特性与结构影响力动态确立。通过比较大陆法系、英美法系与中国法律传统的算法本体认知差异，构建了“关系密度—关系质量—关系自主性”三维分析框架，建立从技术人格到伦理人格的演化模型，进而形成包含动态认定、分布式责任与融合创新的关系本体论治理路径。该理论路径系统阐释了算法系统由工具客体向关系主体的本体跃迁机制，为动态主体识别、网络责任归属与人机协同治理提供范式支撑。

5、人工智能统一立法的论争与选择（袁康）

来源：《比较法研究》2025 年第 5 期

面对人工智能立法的时代需求，推进我国人工智能立法已成共识，但立法模式的选择仍面临着“统分之争”与“急缓之辩”的激烈论争。担忧统一立法

可能导致规制僵化、法律滞后、创新抑制、规则场景错配的疑虑，是对统一立法任务定位与制度品格的误解。而统一立法所具备的体系协调、价值平衡、规则奠基与实践引导等多重制度功能亦被忽视。制定一部统一且通用的人工智能法，发挥其在人工智能法律体系中的基础性、框架性和统领性地位，避免碎片化的分散立法造成规则冲突，对实现人工智能的良法善治具有重要意义。我国应继续稳步推动人工智能统一立法进程，坚持基础性立法定位，平衡发展导向与底线思维，确保制度规则的敏捷与弹性，发挥立法过程的治理效果，探索人工智能法治的中国方案。

6、论基于风险的人工智能监管——以欧盟《人工智能法》为视角展开（江海洋）

来源：《法学论坛》2025 年第 5 期

当前，世界大多数国家与地区对人工智能的监管，都选择了“基于风险”的方法。基于风险的监管由两个步骤组成：风险评估和风险应对。“基于风险的监管”将风险作为一种工具，以与实际损害相称的方式确定执法行动的优先顺序和目标。然而，以欧盟《人工智能法》为例，“基于风险”的人工智能监管存在“权利”风险的计量、风险效益分析缺失、封闭式风险分类导致涵盖过广或涵盖过窄等诸多困境。对此，为真正实现基于风险的人工智能监管，一方面，必须树立诸如包容审慎、技术中立、基于证据的风险评估与分类、合比例监管等与“基于风险的监管”相符合的理念；另一方面，必须采取契合“基于风险的监管”的相应措施。针对人工智能侵害基本权利的风险评估问题，应在“基于权利的方法”框架中纳入“基于风险的方法”要素，并引入各种参数，从客观和主观两个角度来评估基本权利受干扰的严重程度。同时，风险分类应原则化，并采用多种风险监管工具对不同阶段的风险进行全流程的系统化防控。

7、人工智能特殊侵权责任的理论证成及规范储备（李丹）

来源：《东方法学》2025 年第 5 期

人工智能侵权责任认定是人工智能立法的核心挑战，一般侵权和特殊侵权路径难以有效应对人工智能侵权中的过错判定模糊、因果关系证明困难及损害结果不确定等问题。同时，还会引发责任间的竞合冲突，导致设计者/生产者、服务提供者与用户等多重侵权主体间的责任划分难题。立法需突破现有侵权类型框架，将人工智能侵权设置为一种独立的新型特殊侵权责任，构建复合归责体系：对设计者/生产者适用无过错责任，通过强制保险分散技术风险；对服务平台适用过错推定责任，减轻受害人的求偿难度，对专业服务提供者维持过错责任原则以契合行业规范；对普通用户适用过错责任以公平分配责任。责任形态涵盖连带责任、按份责任和补充责任，辅以技术发展免责与过失相抵规则，以此回应技术迭代下的责任偏差。

8、智能投顾规制的信义法路径（钟维）

来源：《法学评论》2025 年第 5 期

我国现行规则将投资建议型和全权委托型智能投顾分别纳入投资顾问和资产管理的规制框架，且试图以普通资产管理产品的相关规则来规制全权委托型智能投顾，产生了削足适履的效果，而一些真正需要关注的问题则未涉及。在信义法的路径下，智能投顾规制的关键问题主要体现在三个方面：第一，由于智能投顾向客户提供的是全权委托账户管理服务，在内部结构上不同于资产管理产品的信托结构，在对外关系上也不同于资产管理产品的销售者与客户之间的关系，因此在其注意义务的塑造上应当以个性化要求为核心。第二，与一般资产管理产品信息披露的要求不同，智能投顾最重要的是对其利益冲突的披露，这是其履行忠实义务的核心问题。第三，由于智能投顾的行为是由算法决定的，因此除后端违信责任的承担之外，在其服务的前端和中端，很大程度上需要通过算法规制来落实其信义义务。

9、论算法个性化定价的私法调整（王俐智）

来源：《当代法学》2025 年第 5 期

营者采用的一种定价方式。是否规制以及如何规制算法个性化定价是一个颇具争议的问题。算法个性化定价私法调整的必要性在于，算法个性化定价中的“价格合意”存在缺陷，算法个性化定价中的“算法控制”侵害个人信息权益。算法个性化定价的私法调整亦应从合同自由与信息自决两个维度展开。定价自由只是经营者享有的单方自由，不能取代双方共享的合同自由。算法个性化定价也不得妨碍消费者的选择自由。信息自决旨在维护人格尊严与自由发展，以个人信息处理为基础的算法个性化定价不得损害信息自决。因此，算法个性化定价应当获取主体的知情同意。算法个性化定价私法调整的具体路径应当兼顾合同自由和信息自决的双重价值立场，从事前同意和事后退出两个维度展开：事前同意既包括对个性化定价合同的同意，也包括对实施个性化定价所需的个人信息处理的同意；事后退出则包括算法个性化定价合同的撤销和算法个性化定价模式的退出机制。

10、人脸识别技术应用的累进式法律规制（文禹衡）

来源：《法律科学(西北政法大学学报)》2025 年第 5 期

人脸识别技术的使用在增进人类福祉的同时，引发了过度监控、歧视、隐私侵害和数据泄露等法律风险。人脸识别法律治理问题可以类型化地表述为人脸识别技术应用的法律规制问题和人脸信息的法律保护问题，前者可分为人脸识别技术准入、人脸识别设备部署和拟识别人脸技术信息运用的规制三个层次，后者属于个人信息法律保护范畴的问题。人脸识别技术应用的法律规制应选择“基于向善”“基于风险”和“基于权利”三种治理路径，随着数字时代的到来，算法个性化定价成为部分经将目的合法、因素替代分别作为人脸识别技术准入的可信赖前提和必要性判断，将影响最小作为人脸识别设备部署的行为约束，将知情同意作为拟识别人脸技术运用的正当性基础，进而构建以准入规则和边界规则为支点的累进式规则体系，解决人脸识别技术“该不该用”和“如何用好”的问题。

网络平台治理

平台滥用规则行为的反不正当竞争法规制（殷继国）

来源：《比较法研究》2025 年第 5 期

当前，平台“内卷式”竞争问题引起全社会的广泛关注。平台经济领域出现“内卷式”竞争的重要原因是平台经营者滥用规则制定权和执行权，而规则制定权和执行权源于平台特殊商业模式下法律法规的授权、用户权利让渡和平台技术赋权。因用户对平台经营者具有较强的依赖性以及政府公权力的制约机制不健全，平台经营者为追逐自我利益最大化实施滥用规则的行为。由于以意思自治、契约自由为内核的民法典在规制平台滥用规则行为上力有不逮，价格法、电子商务法覆盖面较窄和针对性不强以及反垄断法规制的高门槛，催生了对反不正当竞争法规制的需求，过度竞争理论、依赖性理论和国家担保责任理论为反不正当竞争法规制提供理论支撑。为有效规制平台滥用规则的行为，应当在“公权力—私权力—私权利”三元框架下构建公权力规制、平台自我规制和用户私权利制约相结合的规制体系，明确将合理原则作为平台滥用规则行为的分析原则，确立行为本身是否滥用和行为后果是否扰乱市场竞争秩序两个认定标准，健全反不正当竞争法与相关法律的协调机制。

（技术编辑：毕坤阳）

教研活动

第五届数字正义论坛顺利举办

2025 年 11 月 1 日，由北京航空航天大学法学院、北京航空航天大学数字发展法治研究院、北京航空航天大学“网络空间国际治理研究基地”、工信部“工业和信息化法治战略与管理重点实验室”主办，北京航空航天大学数字正义研究中心承办的第五届数字正义论坛“数字经济时代的法治回应与正义图景”于北京航空航天大学会议中心第八会议室成功举办，来自中国法学会、北京大学、四川大学、中国人民大学、北京师范大学、上海交通大学、中国政法大学、西南政法大学、中国社会科学院、对外经济贸易大学、中国人民公安大学、中央财经大学、北京理工大学、北京工商大学、北京航空航天大学、工信部、北京市人民检察院、北京互联网法院、人民法院出版社、中国信息通信研究院等多名专家、学者参加了本次论坛，共同为构建数字经济法治体系贡献智慧。

开幕式暨颁奖典礼

最高人民法院咨询委员会副主任，中国法学会网络与信息法学研究会会长**姜伟**发表致辞。姜伟会长指出，本届论坛聚焦“数字经济推动法治模式发展”，非常必要、意义重大。姜会长分享了关于数字法治变革、挑战与坚守的观察与思考，强调数字法治建设不仅是技术的革新，也是制度的变革，更是治理理念的更新，数字法治的关键是让技术成为法治的仆人而非主人，应当构建负责任、透明、可审计、以人为本的数字法治体系。

姜伟 最高人民法院咨询委员会副主任
中国法学会网络与信息法学研究会会长

北京航空航天大学法学院院长**泮伟江**教授发表致辞。泮院长指出，数字经济已经成为影响正义的关键变量，催生出一系列关于数字经济治理的全球法治议题，为本次学术探讨提供了现实基础和时代契机。泮院长回顾了数字正义论坛的历届主题和设立初衷，强调北航法学院将继续致力于持续为数字时代的法治建设贡献北航智慧与法学力量。

泮伟江 北京航空航天大学法学院院长、教授

为鼓励青年学者积极开展数字法治研究，本次论坛继续面向 35 周岁以下青年学者和实务工作者开展论文评奖活动。论坛共收到 258 篇参评论文，经资格审查、两轮外审专家匿名评审，最终确定 16 篇获奖论文。在颁奖典礼上，姜伟会长、泮伟江院长为获奖作者颁奖。

主旨发言

中国人民大学法学院吴玉章高级讲席教授，中国法学会网络与信息法学研究会副会长兼学术委员会主任**张新宝**作了题为《作为知识产权客体的数据与作为数字经济要素的数据之“并联包容”关系探讨》的报告。

张新宝 中国人民大学法学院吴玉章高级讲席教授
中国法学会网络与信息法学研究会副会长兼学术委员会主任

张教授从《民法典》第 123 条和第 127 条的制

定历程切入，指出作为知识产权客体的数据受到知识产权法保护的关键在于其具有独创性、创新性，而作为数字经济要素的数据是大数据，二者是并联包容关系。政府监管部门的设置与权限只是政府机构的分工安排问题，有关部门应当依法履行职责，促进数字经济发展。

北京航空航天大学人文与社会科学高等研究院院长、教授，中国法学会网络与信息法学研究会副会长**龙卫球**作了题为《面向数智化镜像世界的法律治理》的报告，指出人类已经进入以 AI 为主导的平台经济新阶段，经济将在镜像世界中运行，经济关系模式将发生根本变化，提出数字新阶段应当坚持以经济建设为中心，兼顾社会主义公平，关注目标与问题双重导向的制度创新及面向镜像世界的特殊规范需求。

龙卫球 北京航空航天大学人文与社会科学高等研究院院长、教授
中国法学会网络与信息法学研究会副会长

四川大学杰出教授，中国法学会刑事诉讼法学研究会副会长**左卫民**作了题为《基于 DeepSeek 的法律 AI 新风貌》的报告，指出基于 DeepSeek 等大模型的法律 AI 在法学研究和实践中的应用趋势已经毋庸置疑，应当进一步关注其实际运用效果。通过基于案例的实证研究，发现大模型在处理案例时表现的差距小于预期，但深层问题依旧存在。法律 AI 作为决策主体存在固有局限，当下的关注重点不在于机器能否取代人，而是如何构建更为高效、可靠且合乎伦理的人机协同机制。

左卫民 四川大学杰出教授
中国法学会刑事诉讼法学研究会副会长

中国政法大学副校长、钱端升讲座教授**刘艳红**作了题为《数字时代“网络开盒”的系统性治理》的报告，指出有效治理网络开盒现象可以从以下三方面入手：一是算法行政下政府部门应当切断网络开盒信息的获取来源途径，二是网络平台应优化算法技术、履行“看门人”职责，三是应当完善相关法律保护体系、防止未成年人参与网络开盒。从政府、平台、个人等多个层面入手，构建轻重有序、权责分明的系统性治理体系，以维护公民权益、营造良好网络生态环境。

刘艳红 中国政法大学副校长、钱端升讲座教授

对外经济贸易大学副校长、教授**梅夏英**作了题为《人工智能时代的人机关系》的报告。在人机关系的性质层面，关注 AI 与人类是否属于同一种智能以及 AI 是否具备自我意识，应当将 AI 定位为高度智能化的技术，以此为基础构建人机关系框架，遵循非人化原则、人类优先原则和安全原则。就人机关系的内容而言，关注人机对齐、人机信任以及人机伦理问题，而对上述问题的判断仍有待 AI 技术的进一步发展。

梅夏英 对外经济贸易大学副校长、教授

北京大学法学院教授，《中外法学》主编，中国法学会网络与信息法学研究会副会长**王锡锌**作了题为《数字行政与裁量正义的新问题》的报告，关注数字化技术如何嵌入行政裁量以及由此产生的影响。行政裁量领域正义的核心在于平衡形式正义和“量体裁衣”正义之间的张力。当下，运用数字化技术提升裁量正义质量已成为数字政府建设的重要内容，如何充分发挥数字化技术的互补性功能，减缓对抗性功能，是数字化裁量正义面临的重要课题。

王锡锌 北京大学法学院教授，《中外法学》主编
中国法学会网络与信息法学研究会副会长

北京航空航天大学法学院副院长**周学峰**教授作了题为《法律视角下的数字经济要素》的报告，关注了数字经济在不同视角下的内涵与外延，指出在法律视角下，应当从数据、数字基础设施、数字技术三个要素对数字经济进行界定，此外还需针对人工智能和网络平台等非要素对象进行立法规制。

周学峰 北京航空航天大学法学院副院长、教授

专题一

北京师范大学法学院教授、数字法学研究中心主任**汪庆华**作了题为《数字正义视野下的法律大模型》的报告，指出当前大模型在法律领域的应用处于“有能无智、有智无心”阶段，核心使命是服务数字正义，不会替代法律人的专业判断。法律大模型目前存在稳定性不足、“幻觉”问题突出、责任划分模糊、公私领域界限消融等核心风险，对此，法律基座大模型具有重要价值。应当坚持“人机协同”与“多元共治”，既要“人在环路”，也要“正义在环路”，将数字正义的理念植入法律大模型的应用中，筑牢数字法治根基。

汪庆华 北京师范大学法学院教授、数字法学研究中心主任

中国人民大学法学院教授、未来法治研究院执行院长、中国法学会网络与信息法学研究会常务副秘书长**张吉豫**作了题为《人工智能开源模型提供者的注意义务》的报告，指出开源模型治理的核心是平衡其社会赋能价值与潜在风险。针对侵权责任界定，应当从效益主义视角出发，关注预防损害的合理成本在多主体间的分配，按照开源程度、规模性质、是否获利等多因素综合判断注意义务水平。未来还需引入社会协同机制，推动开源基础大模型实现多元共治。

张吉豫 中国人民大学法学院教授、未来法治研究院执行院长
中国法学会网络与信息法学研究会常务副秘书长

中国信息通信研究院政策与经济研究所主任工程师**程莹**作了题为《情感陪伴 AI 的风险解构与法律规制》的报告，指出情感陪伴 AI 在快速发展的同时，产生内容安全风险、科技伦理风险、人格权益侵害等问题。监管情感陪伴 AI 的重点难点主要体现为四方面，一是对情感陪伴的概念特性、边界范围达成共识；二是实现全流程监管，包括从安全评估到伦理审查、从算法模型备案到角色审查、从内容标识到交互透明度；三是未成年人保护，政府、企业等多主体采取举措解决未成年人识别难题；四是关注自杀自残极端事件风险防控。

程莹 中国信息通信研究院政策与经济研究所主任工程师

北京理工大学法学院**洪延青**教授作了题为《美国的人工智能“全栈封阻”和我国的法律应对》的报告，从中美博弈视角切入，剖析美国 AI 管控策略及我国破局路径。美国提出全新的国家安全治理框架，多维度实施“全栈封阻”，将对中国企业产生规模效应削弱的负面影响。对此，政府层面应当建立专题工作组，国际层面应当积极参与多边治理机制，企业层面应当提升合规工程能力，推动形成灵活应对不同法域监管差异的运营策略和治理框架。

洪延青 北京理工大学法学院教授

专题二

中央财经大学法学院副院长**刘权**教授作了题为《数字经济包容审慎监管的法治逻辑与制度构建》的报告，指出“包容审慎监管”从政策话语转为法律概念的核心逻辑是追求发展与安全的动态平衡。包容审慎监管实施存在权衡困境、监管执法不确定性等问题，根源在于数字经济不确定性、监管机制不健全、行政裁量权过大及部分公职人员缺乏担当。为此，有必要实现有效市场和有为政府更好结合，开放决策程序以提升行政理性，借助试验机制促成监管的包容审慎，以容错机制激励市场与政府探索创新，完善监管机制以确保行政便宜性与最佳性的有机统一。

刘权 中央财经大学法学院副院长、教授

中国人民公安大学法学院教授、数据法学研究院院长**苏宇**作了题为《公共数据质量的制度保障》的报告，聚焦于公共数据质量的法律保障问题，指出当前公共数据在客观性、完整性、时效性等方面存在普遍缺陷，应采纳“通过设计的精细保障”的进路，建构公共数据法益确认制度以明确“保护什么”，质量缺陷参与治理制度以明确“谁来保护”，数据质量深度监测制度以解决“如何保护”，应对监控不同场景下海量分散公共数据质量的任务。

苏宇 中国人民公安大学法学院教授、数据法学研究院院长

北京市人民检察院第四检察部副主任、三级高级检察官**刘丽娜**作了题为《数字时代知识产权保护履职实践与展望》的报告，结合北京检察实践，系统分析了数字时代知识产权案件的新型挑战与检察应对。刘丽娜检察官介绍了全国首例侵犯北京冬奥吉祥物玩偶形象著作权案、宁某等人侵犯著作权案等典型案例，强调检察机关在助力形成新业态领域知识产权保护“规则之治”的作为，展现了检察机关在适应数字技术发展、强化知识产权综合保护方面的职能作用。

刘丽娜 北京市人民检察院第四检察部副主任、三级高级检察官

数字正义论坛征文二等奖获得者、中国人民大学博士研究生**赵舒捷**作了题为《公共数据授权运营的国家担保责任重构》的报告，指出公共数据授权运营属于形式民营化而非“出售国有资产”和“国家退出”，国家应当承担担保责任。传统担保责任模型在公共数据授权运营中面临挑战，应当以数字主权理念为指导重构担保责任理论。

赵舒捷 数字正义论坛征文二等奖获得者
中国人民大学博士研究生

专题三

对外经济贸易大学法学院教授、数字经济与法律创新研究中心主任**许可**作了题为《司法如何回应数字经济政策？》的报告，指出数字经济领域中政策对社会与市场的影响远大于法律，核心源于传统法律的稳定性难以应对数字经济的飞速发展。有必要将数据三权与特定的法律规范相勾连，通过找法、释法实现司法对数字经济政策的有效回应，推动法治从行为规则性司法向权利界定性司法转变。

许可 对外经济贸易大学法学院教授
数字经济与法律创新研究中心主任

上海交通大学凯原法学院**李学尧**教授作了题为《人机协同视野下的数字法院建设》的报告，基于实证研究系统反思了当前数字法院建设的三种主流思路，包括效率提升论、辅助论及技术适应制度论，认为数字法院建设应增强司法认知能力以超越“效率提升论”，再造数字司法制度以超越“技术适应制度论”，构建“程序性信任机制”以超越“工具性信任”，呼吁以更开放的态度面对技术带来的制度变革可能性。

李学尧 上海交通大学凯原法学院教授

北京互联网法院党组成员、副院长**孙铭溪**作了题为《以高质量司法审判服务保障数字经济高质量发展》的报告，介绍了北京互联网法院在数字经济治理中的司法职能与创新实践，指出北京互联网法院坚持“以裁判树规则、以规则促治理、以治理助发展”的审判理念，在数据权益确认、网络空间治理、人工智能规制等新兴领域审理了一批具有规则意义的前沿案件，以积极回应技术发展带来的法律挑战。

孙铭溪 北京互联网法院党组成员、副院长

北京市人民检察院第四检察部三级高级检察官**李慧**作了题为《涉虚拟财产领域司法实践问题研究》的报告，一是分析了虚拟货币的法律属性界定以及虚拟货币的扣押、追踪等实践争议；二是介绍了公安机关在实践中处置涉案虚拟货币的基本模式；三是探讨了涉案虚拟货币的价值认定问题，提出了比特币购买价格、案发时交易价格以及销赃价格等多种方案。

李慧 北京市人民检察院第四检察部三级高级检察官

数字正义论坛征文一等奖获得者、北京警察学院侦查系讲师**苏泽琳**作了题为《确定性的幻想：区块链证据认证形式化的实证反思》的报告，基于实证研究指出当前司法实践中区块链证据尽管采信率极高，但存在认证形式化问题，认为要改善区块链证据认证形式化的现象，应反思“印证理论”过度依赖证据关联关系的理论缺陷，明确法院在证据审查中的主体责任。

苏泽琳 数字正义论坛征文一等奖获得者

北京警察学院侦查系讲师

专题四

对外经济贸易大学法学院教授、数字经济与法律创新研究中心主任**张欣**作了题为《人工智能 2.0 时代风险治理的困局与进阶》的报告，指出人工智能 2.0 时代根本性地挑战了目前的治理逻辑，反思现有风险治理路径的可行性，并提出了相应的风险治理进阶方案：基于大模型的同质性，人工智能风险治理仍然具有可行性，可以将风险区分为“已知的已知”“已知的未知”“未知的未知”三方面，并在此基础上展开具体的制度设计。

张欣 对外经济贸易大学法学院教授

数字经济与法律创新研究中心主任

上海交通大学凯原法学院**林洹民**副教授作了题为《数据财产权的营业权属性及其体系效应》的报告，指出数据产权的基本功能在于促进数据的有效流动与合理保护，应当从功能出发对数据产权进行界定，并提出了基于营业权的解释方案，强调营业权的宽泛性特征有助于保持讨论的开放性，契合数字经济的发展阶段和变革需求。

林洹民 上海交通大学凯原法学院副教授

北京航空航天大学法学院**王琦**副教授作了题为《数字复活》的报告，指出法律对于“数字复活”应当秉持“在允许中规范，在发展中规制”的态度。数字复活的发起必须遵循“三层次依据”：一是本人的有效生前安排，二是近亲属的追思纪念，

三是人格权的合理使用。法律应当明确数字复活的发起依据和运行界限，并为数字人相关利益主体提供针对性保护，以包容且精准的方式引导人工智能向善发展，让技术真正服务于人的尊严与福祉。

王琦 北京航空航天大学法学院副教授

北京理工大学法学院**陈姿含**副教授作了题为《数字正义与自动化拒绝权的实现》的报告，指出拒绝权的运行空间被挤压，拒绝权的正义应该是一种信息优先规则。信息规则对算法规则的优先性并非简单的 “法律压制技术”，而是通过制度设计、技术嵌入和司法裁判的协同作用，构建起技术与法律的共生生态。其核心在于将算法从“自主运行的技术工具”重塑为“受法律调控的社会治理手段”，最终实现数字经济发展与个人权益保护的动态平衡。

陈姿含 北京理工大学法学院副教授

数字正义论坛征文二等奖获得者、西南政法大学人工智能法学院**罗有成**讲师作了题为《数字社会对正义理论的挑战与重塑》的报告，指出在数字时代，传统正义理论面临深刻挑战与重构可能。数字正义并非对传统正义的替代，而是在数字环境下对其逻辑、认知与原则的深化与扩展，是面向技术时代的重要理论补充与发展。

罗有成 数字正义论坛征文二等奖获得者
西南政法大学人工智能法学院讲师

第五届“数字法治与社会发展”学术论坛成功召开

2025 年 11 月 2 日，由中国法学会法理学研究会、最高人民检察院检察理论研究所、《国家检察官学院学报》、中国司法大数据研究院、华东政法大学共同发起，《华东政法大学学报》主办，《国家检察官学院学报》《中国刑事法杂志》《东方法学》《政治与法律》《浙江社会科学》《求是学刊》《学习与探索》《山东大学学报（哲学社会科学版）》《法学论坛》《社会科学研究》及华东政法大学数字法治研究院、山东科技大学数字法治研究院、中国报道《中国实践》频道共同协办的第五届“数字法治与社会发展”学术论坛成功召开。

本次论坛由来自全国多所高校的专家学者、司法实务界专业人士以及互联网公司相关部门的负责人与会。

开幕式

华东政法大学副校长**洪冬英**教授指出数字技术正深刻重塑社会治理格局，法治必须积极回应数字时代的需求。本论坛立足这一时代命题，形成了独特风格，主要体现为四大特色：一是构建跨界交流的高端平台，论坛突破学科与行业壁垒，推动司法界、产业界、学术界和期刊界的深度融合，构建开放包容的学术生态；二是打造创新引领的前沿阵地，论坛聚焦全球数字化变革，紧跟国际前沿，围绕数字司法、生成式人工智能、数据治理等主题，形成国内研究的重要风向标；三是培育青年人才的成长摇篮，论坛始终关注青年学者的培养和扶持，为新生代学术力量提供展示平台；四是形成智库孵

化的重要支撑，论坛注重理论与实践结合，依托华东政法大学数字法治研究院与多家司法机关和高校共建的数字司法实践基地，推动研究成果转化，形成智库报告，为国家数字法治建设提供决策参考。数字法治是一项系统工程，离不开司法、实务与学术界的协同努力。华东政法大学将以本次论坛为契机，深化研究与合作，为推动我国数字法治的发展作出新的贡献。

洪冬英 华东政法大学副校长

中国司法大数据研究院**梁新**院长指出党的二十届四中全会提出，要强化原创创新和关键核心技术攻关，推动科技与产业深度融合，建设数字中国，加强数字法治正是实现这一目标的重要保障。自 2016 年成立以来，中国司法大数据研究院始终坚持以习近平新时代中国特色社会主义法治思想为指导，在最高人民法院的领导和支持下，锐意进取，在国家治理决策支持、数字法院建设以及社会服务等方面都取得了显著成果。在数字法院建设方面，研究院积极推动现代科技与司法审判的深度融合，研发了类案推送、量刑辅助等系统，强化智能审判与管理能力，助力全国法院实现信息化、智能化发展。同时，研究院运用数据模型帮助金融机构防范风险、协助企业完善合规体系，并为数字政法一体化平台建设提供技术支撑，致力于打造世界一流的司法大数据智库，设立了社会治理、金融司法、互联网司法等研究中心，长期关注数字治理体系建设。中国司法大数据研究院的相关研究工作也离不开业务人士的携手共建，期待各位嘉宾的指导与交流。

梁新 中国司法大数据研究院院长

最高人民检察院检察技术信息研究中心主任、中国科技法学会副会长**刘喆**提出，随着信息化与智能化的快速推进，社会生活方式正在发生深刻变革，数字技术已成为全球科技革命和产业变革的关键力量。中央多次强调，要充分利用数字技术，推动其融入社会治理全过程。数字化不仅改变了社会的运行模式，也深刻重塑了我们的司法理念与办案方式，催生了数字侦查、数字检察、数字法院等创新成果，同时也带来了数字鸿沟、算法偏见和数据隐私等新型法律治理问题。首先，数字化改变了司法认知与证明方式，使原本依赖主观判断的部分，通过可度量的数据转化为客观、可验证的表述，从而提升了证据的客观性与证明力。其次，数字化推动检察技术信息中心由传统信息化建设向数字化治理转型，利用大数据与人工智能改进证据分析和案件研判方式，实现从以经验为主向以知识驱动、数据驱动的转变。最后，数字化催生了数字检察战略的实施，使检察机关在长期信息化基础上实现了数据的深度挖掘和智能辅助，推动案件办理从个案指导向整体知识体系转变，为司法决策提供更加科学的支撑。数字技术既是机遇，也是挑战。作为法律工作者，我们应当主动拥抱科技变革，将数字技术深度融入法律监督与司法办案全过程，持续提升法治能力与治理效能，努力让人民群众在每一个司法案件中切实感受到公平与正义。

刘喆 最高人民检察院检察技术信息研究中心主任、中国科技法学会副会长

最高人民法院咨询委员会副主任、中国法学会网络与信息法学研究会会长**姜伟**作了三点总结和提炼。首先，数字司法是时代必然。人工智能与大数据技术的发展，为解决传统司法效率低、法律适用不统一等问题提供了前所未有的机遇。人工智能在案件数据处理、模式识别及裁判辅助方面具有高效性和稳定性，我国建设数字法院以来，数字司法持续推进，并借鉴欧盟、德国、英国等国际经验，从全球范围看，司法智能化发展的趋势已然不可逆转。其次，数字司法仍面临现实困境。智能技术虽提升效率，但可能带来公平正义风险，如数字鸿沟、数据偏见、算法黑箱及与正当程序的冲突。在刑事诉讼等敏感领域，必须谨慎处理技术工具属性与法治核心价值之间的张力，确保算法服务司法而非取代司法，权利保障、公平与正义仍是首要原则。最后，人机协同将成为司法新常态。人工智能可承担基础性、重复性工作，为法官提供辅助参考，但裁判责任和价值判断仍由法官承担。规范化、系统化的人工智能应用，应坚持司法主导逻辑，防止技术依赖导致算法凌驾于法律之上，实现效率提升与司法公正的平衡。人机协同不仅提升司法效率，更体现司法智慧与人文关怀，努力让人民在每一案件中感受到公平正义。总体而言，数字司法既是技术发展的必然趋势，也面临价值与制度上的挑战。未来应以人机协同模式推进，兼顾效率与公平，推动技术与法治理念有机融合，实现更高水平的司法治理。

最高人民法院咨询委员会副主任、中国法学会网络与信息法学研究会会长姜伟

第一单元 主旨演讲

最高人民法院第一巡回法庭分党组副书记、副庭长**刘峥**以《数据权益保护的司法应对之策》为题分享了相关观点。他认为互联网、数字化已经渗透进入各行各业，与此相伴的法律纠纷数量也日益增长，许多新问题也成为“理论上的热点”和“实践中的难点”。面对新情况，我们应当大力推进专业化体制机制建设，构建互联网审判体系，形成互联网纠纷在线审理规则体系，优化互联网法院管辖制度，公正高效审理一大批具有示范意义的典型案件；充分发挥司法裁判在新兴行业领域发展的规则引领和政策保障作用，始终坚持互联网司法本质上仍是司法，仍然坚守司法的基本原则、价值理念和裁判方法，发挥互联网法院的先行示范作用，坚持“谁投入、谁贡献、谁受益”，兼顾安全与流动，探索多主体、多层次的数据权益保护；积极促推理论、科技和司法的深度融合，加强科技创新、理论研究和个人才培养，力求形成“1+1>2”的研发合力，共同以高质量数字法治建设护航数字经济高质量发展。

刘峥 最高人民法院第一巡回法庭分党组副书记、副庭长

上海市高级人民法院党组副书记、副院长**陆卫民**以《数字法院建设的实践探索与思考》为题分享了上海市数字法院建设的相关情况。陆院长指出上海数字法院建设以数字化手段推动司法高效、公正，并向社会治理方面延伸。首先，通过全流程监管，实现立案、审判、执行等环节智能化管理，有效甄别虚假诉讼、治理程序空转，显著提升案件审理效率和质量。其次，数字技术赋能专业化审判，通过类案比对、量刑预警、争议焦点归纳及文书生成，促进同类案件提质增效，缩短审理周期。最后，数字法院成果延伸至社会治理，利用司法大数据分析潜在风险，为金融机构、中小企业及社会管理提供决策支持，实现协同治理。整体来看，上海数字法院建设体现了由点及线、由局部到系统的推进模式，为数字时代司法创新与法治实践提供了经验示范。

陆卫民 上海市高级人民法院党组副书记、副院长

浙江省人民检察院副检察长**柴志华**以《数字检察的实践探索》为题分享了数字检察的“浙江样本”。柴检察长提到浙江检察机关正在积极推进数字检察建设，通过数字赋能监督、办案、管理和服务，提升法律监督效能和司法公正。首先，利用大数据和人工智能建立法律监督模型，实现线索发现、案件甄别及分级动态监管，推动法律监督从个案向社会治理延伸。其次，在办案环节，通过智能辅助系统实现证据比对、立案推送、量刑建议和文书生成，提高办案效率和质量。再次，数字化管理手段使检察业务从经验驱动转向数据驱动，实现全流程、全方位监控和质效分析，强化内部管理。最后，数字化公共服务拓展至线上，提供案件查询、法律风险提示及未成年人犯罪预测等服务。他总结道，数字检察既提升监督与办案效率，也推动制度创新与协同治理，同时强调“让数字说话，但不让数字做决策”，确保司法责任和公正。

柴志华 浙江省人民检察院副检察长

上海市人民检察院检察委员会专职委员**吴云**以《数字检察的“上海范式”》为题作了分享。他首先回顾了华东政法大学对于数字司法研究的悠久历史和渊源，并希望华东政法大学能够继续发挥数字司法研究的重要阵地功能，为实务界提供智力支持。他分享道，上海检察机关积极推进数字检察建设，通过全流程在线办案、个案全景地图、智能辅助办案模型、AI 助手和数据驾驶舱等标杆应用，实现办案、管理和监督的数字化赋能。全流程在线办案覆盖受理至归档的办案行为，结合电子送达、电子笔录等线上场景，实现规模化、高质量的数据治理和规范办案。智能辅助办案模型通过类案推送、量刑预测、证据审查和文书生成，提高办案效率与质量，减少畸轻畸重现象，并对刑法新旧司法解释进行智能比对。并且赋能科技，以数据驾驶舱和管理模块形式实现全流程、全生命周期监督，为业务管理、案件管理和安全管理提供精准决策支持。

吴云 上海市人民检察院检察委员会专职委员

清华大学法学院副院长、教授**程啸**以《生成式人工智能服务提供者的侵权责任》为题从民法学者视角分享了数字技术的发展问题与应对。程啸教授指出，当前司法实践中已出现 AI 换脸、声音盗用、AI 陪伴软件侵害人格权，以及“奥特曼”案等侵害著作权的新型案件，凸显了问题的紧迫性与复杂性。核心争议聚焦于三大问题：第一，归责原则。程啸教授倾向于适用过错责任原则。第二，生成式 AI 能否适用现行网络侵权规则。他指出，不宜直接或类推适用《民法典》第 1194 条以下的“通知—删除”规则。理由在于，生成式 AI 服务并非单纯的网络技术服务提供者，其通过算法、模型和数据深度参与了内容的生成，责任性质已超出了“不作为”的范畴，应被视为一种新型的服务提供者。第三，构成要件与证明责任。由于 AI 具有自主性与不透明性，其在因果关系、过错等方面的认定上面临全球性挑战，应当予以精细研究。总体来看，人工智能侵权责任需结合生成特性、法律解释和司法实践，形成针对性规范。

程啸 清华大学法学院副院长、教授

第二单元 基调演讲

杭州互联网法院院长**陈增宝**以《数字法治视野下的司法新形态——以杭州互联网法院为样本的考察》为题分享了杭州互联网法院的数字司法实践。杭州互联网法院的发展呈现出五方面鲜明的新形态：即涉网案件审判管辖的专业化、审理方式的在线化、解纷能力的智能化、数据处理的一体化以及纠纷化解的多元化。其核心功能已从机制创新迭代为规则输出，通过审理大量前沿案例，为网络空间法治化治理提供了重要规则指引。面向未来，互联网法院将致力于高标准发展，强化其作为改革“孵化器”和“试验田”的功能定位，力争在网络空间治理中发挥更大的示范和引领作用。

陈增宝 杭州互联网法院院长

上海奉贤区人民法院院长**韩峰**以《数字技术重塑基层司法新图景》为题以具体数据形式分享了地方法院的数字司法实践情况。展望未来，他指出奉贤法院将围绕三方面持续深化数字法院建设：一是服务区域发展，以算力换人力、以智能增效能，通过精准场景构建强化类案检索与信息协同，应对案件体量大、新问题多的挑战；二是释放治理效能，推动数据共享与多元解纷向基层延伸，依托数据分析为企业提供风险自测服务，从源头化解纠纷；三是挖掘自身潜能，融入全国法院“一张网”体系，用好全流程贯通的应用场景，在提升司法服务便捷性的同时关注数字鸿沟，让科技发展成果惠及所有群体。

韩峰 上海奉贤区人民法院院长

上海市黄浦区人民检察院副检察长**于春敏**以《数字检察的理论支点与实践范式》为题分享了她

对于数字检察的相关观点。于检察长指出，坚持“检察为本、数字为用”是数字检察实践的根本立场。数字检察的本质是检察职能与数字技术的深度融合，其思维基础在于实现社会科学价值判断与自然科学实证分析思维的有机交融，并在此过程中坚守法律与伦理的边界。其应然的逻辑进路是以检察业务的实际需求为起点，通过检索和遴选数据、适配数字技术，最终目标在于优化检察规则，形成一个“业务—数据—技术—规则”的闭环。在实践层面，需重点关注三方面：一是提升数据治理能力，打破数据壁垒并加强安全保护；二是构建算法治理体系，确保算法的可审查与透明；三是加强既懂法律又懂技术的复合型人才培养，以推动数字检察向更深层次、更高质量发展，为国家治理现代化贡献检察力量。

于春敏 上海市黄浦区人民检察院副检察长

阿里安全网络犯罪研究中心负责人**谢虹燕**以《数据权益的多元保护》为题分享了阿里在数据治理方面的理解与经验。她指出数据权利的多元保护在当下至关重要，平台企业一方面需在强监管与促进数据要素规模化流通之间取得平衡，满足生态内多元主体的权益诉求，构建高效的合规管理体系；另一方面则持续面临专业化、链条化的黑灰产威胁，包括网络攻击、内部泄露与技术爬虫对抗，其手段不断演变，交易愈发隐蔽。在此背景下，数据权益的多元保护体系已初步形成：在刑事层面，根据数据敏感程度通过不同罪名予以打击；在行政层面，通过法规与登记制度等进行规范；在民事层面，则依托人格权、财产权、知识产权及反不正当竞争等路径提供救济。此外，互联网法院的专业管辖与“刑附民”等程序探索也为权利保障提供了有力支持。

谢虹燕 阿里安全网络犯罪研究中心负责人

京东集团法律合规与知识产权部科技法律合规负责人**郑慧媛**以《“规则—算法”协同框架下的企业法务智能化》为题分享了京东在智能企业法务领域的探索。从企业法务的视角观察，法律智能化已成为显著趋势。京东法务部门通过构建一体化智能法律合规平台，研发了智能问答、合同审查、案件管理等系统，将 AI 深度嵌入日常工作中。但是郑慧媛女士也强调应当深入思考人机协同的边界，AI 擅长处理结构化数据和提供初步指引，但是法律人的核心价值在于坚守良知、进行审慎的价值权衡与超越技术的伦理判断。因此，在 AI 时代，法律人必须从传统的知识搬运工，转型为具备批判性思维、能够驾驭规则与风险的高素质人才。

郑慧媛 京东集团法律合规与知识产权部科技法律合规负责人

腾讯集团法务部法律研究总监**臧雷**以《数字法治时代影视产业的发展与保护》为题分享了平台企

业对于数字影视作品侵权治理的相关经验与看法。他指出，影视产业作为文化与科技融合的新质生产力代表，在创造巨大经济与文化价值的同时，正面临系统化、组织化盗版的严重侵蚀，并且侵权形态已从个体行为演变为平台主导的规模化运作。在此背景下，数字司法亟需展现治理担当：其一，对深度介入内容编辑推荐的平台，应突破“避风港原则”的机械适用，依据《民法典》第 1197 条，要求其对热播内容采取事前屏蔽过滤措施，未采取相关措施的依法进行规制；其二，建立与作品市场价值相匹配的判赔标准，对恶意重复侵权适用惩罚性赔偿，让司法威慑真正到位。

臧雷 腾讯集团法务部法律研究总监

第三单元 专题演讲

上海市法学会专职副会长、《东方法学》主编**施伟东**发言的题目是《数字时代个人信息保护的再思考》。他指出在数字时代个体日益“数据化”的背景下，对已实施四年的《个人信息保护法》进行再审视显得尤为重要。当前个人信息保护机制在数据采集端投入的边际效益正逐渐递减，建议将治理重心后移，着重强化数据持有者的安全保管责任。同时，技术发展带来了新挑战，匿名化处理等保护措施在先进技术面前易被反向破解，现有的“通知—删除”机制因个人维权成本过高而难以有效运转，应依据比例原则重构平台责任，将其从“合理注意义务”升级为“充分注意义务”，利用技术优势主动履行内容审核下架职责。此外，随着《公共安全视频图像信息系统管理条例》的实施，公共场所监控设备的合规使用、数据保管与到期删除等环节也亟需建立有效监督机制。

施伟东 上海市法学会专职副会长、《东方法学》主编

上海交通大学凯原法学院院长**彭诚信**教授发言的题目是《数据确权核心要素的思考》，他指出在当前数据治理的探索中，传统的确权路径面临显著挑战。正面确权因数据主体难以确定、数据利益形态随场景动态变化、权利义务边界模糊而几乎不可行；反向确权则因归责原则选择陷入两难——平台与个人在不同情境下兼具加害人与受害者双重角色，使得通用型归责原则与损害赔偿范围难以划定。对此，应当遵循“动态确权”新思路：以具体侵权场景为分析单元，通过锁定该场景中的主体身份、厘清利益创造链条，在具体情境中实现价值的弹性分配。这一路径既延续了传统法学的平衡智慧，更体现了数字时代方法论的创新突破。

彭诚信 上海交通大学凯原法学院院长

中国人民大学未来法治研究院执行院长**张吉豫**教授发言的题目是《著作权侵权责任确定：从网络平台到开源模型》。她提出，在当前生成式人工智能与开源模型发展的背景下，网络平台责任界定可借鉴著作权领域长期形成的责任认定规则。网络侵权治理始终遵循分层分类原则，同时确立合作共

治导向，通过“通知—删除”机制推动权利人与平台形成治理合力。在具体过错认定中，动态系统论提供了灵活判断框架，需综合考量技术可行性、服务类型、侵权明显程度及平台主动行为等多重因素。这一逻辑同样适用于开源模型的责任划分。开源程度与模型类型成为关键变量：通用基础模型具有强赋能效应且可控性较低，过重责任将抑制创新，宜设置合理注意义务；而垂直领域的小模型或特定风格模型（如 LoRA 模型），因侵权风险可预见性更高，应承担更严格责任。

张吉豫 中国人民大学未来法治研究院执行院长

西南政法大学人工智能法学院院长**陈亮**教授以《人工智能赋能检察公益诉讼的困境与出路》为题分享了关于“人工智能+检察公益诉讼”的相关看法。他指出，在检察公益诉讼面临诉讼动力不足、法律依据分散、调查取证困难等结构性困境的背景下，人工智能技术为其赋能提供了新的路径。通过构建高质量数据基座，人工智能能够将碎片化的法律规范体系化，实现从被动等案到主动挖掘案件线索的转变，并推动调查取证从人力密集型向科技密集型转型。但同时也意味着数据偏见可能固化，机器也难以进行价值衡量等挑战。为此，应着力开发具备法律推理能力的智能系统，通过可视化推理路径和建立反馈学习机制，最终目标是打造可解释、可监督的人工智能辅助系统，通过技术、制度和人才建设的多维支撑，实现从个案监督到系统治理的效能提升，筑牢公益诉讼的数字法治根基。

陈亮 西南政法大学人工智能法学院院长

福建师范大学法学院**李付雷**副教授以《公共卫生数据共享的地方实践方案评析》为题发言，结合福建省公共卫生数据共享的实践情况进行了分享。他提到，福建省正在推进的“三医一张网”项目，通过整合卫健、医保、医药三方数据，构建全域医疗数据画像，为优化医疗资源配置与服务创新提供了重要基础。然而，项目在未来运营中面临多重挑战：其一，专业能力错位，运营方虽具备数据技术但缺乏医疗专业知识，可能影响数据应用的深度与准确性；其二，数据开放存在“代理成本”难题，政府部门因担忧数据泄露与合规风险而趋向保守；其三，患者授权缺失问题突出，传统逐项授权模式在实操中难以实现。对此，项目探索出“可用不可看、可跑不可带”的创新方案——允许企业在隔离环境下使用数据训练模型并带走分析结果，但不直接接触或带走原始数据，从而在保护隐私的前提下释放数据价值。但是，数据定价机制、利益分配等相关问题也亟待探索和解决。

李付雷 福建师范大学法学院副教授

第四单元 青年演讲

西南政法大学刑事侦查学院**王仲羊**副教授以《〈联合国打击犯罪网络公约〉中电子数据的分类标准与中国因应》为题进行发言。他指出，《联合国打击网络犯罪公约》的签署标志着全球网络犯罪治理进入新阶段，其首创的电子数据三分法——将数据划分为用户数据、流量数据与内容数据，并依此构建层级化、比例化的取证规则体系，为我国电子数据治理体系的完善提供了重要参照。当前我国电子数据分类存在规范冲突、价值张力与标准模糊三重困境，刑法、刑诉法与个人信息保护法各自为政，便利侦查、保障权利与维护安全的价值目标难以协同，分类分级概念混用且抽象标准与具体场景脱节。对此，应构建以公约三分法为解释框架的整合方案。

王仲羊 西南政法大学刑事侦查学院副教授

华东政法大学中国法治战略研究院特聘副研究员**童云峰**以《数据领域法体系下前置法与刑法的衔接模式》进行发言。他指出，在当前统一刑法典模式下，数据犯罪的规制亟需实现刑法与前置法的有机衔接。目前存在三大衔接困境：行为规制上，刑法仅覆盖非法获取与破坏数据行为，难以应对多样化的非法数据处理；保护对象上，刑法依附于计算机信息系统保护，未能独立体现数据价值；出罪标准上，前置法丰富的正当化事由与刑法狭窄的出罪路径形成断层。应当确立三个衔接方向：首先，坚持法秩序统一原理，避免前置法合法行为在刑法中被定罪的法律倒挂现象；其次，运用可罚的违法性理论构筑行政违法与刑事犯罪的过滤机制；最后，通过法律解释方法实现规范调和。

童云峰 华东政法大学中国法治战略研究院特聘副研究员

南京师范大学法学院特岗副研究员**王由海**以《自动化行政审批的司法审查》为题发言。他指出在数字政府建设浪潮下，自动化行政审批行为在提升效率的同时，也对司法审查体系提出了全新挑战。这类算法行政权与传统行政程序存在结构性冲突：一方面，审批程序的线上化、瞬时化压缩了当事人陈述申辩等程序权利，导致法院在判断程序合法性时陷入标准缺失的困境；另一方面，算法黑箱效应使得决策逻辑难以追溯，法官受制于技术壁垒而倾向于回避实质审查。为应对这些挑战，应当构建双轨审查机制：在程序层面，引入“技术性正当程序”理念，要求行政机关履行算法说明义务并保障关键程序权利，根据程序功能区分可缩减与不可缺省的程序环节；在实体层面，需突破形式审查局限，通过对算法规则进行附带审查、对裁量结果适用“滥用职权”与“明显不当”标准等方式，实现从要件认定到效果裁量的全过程监督，最终在工具理性与价值保障之间建立动态平衡。

王由海 南京师范大学法学院特岗副研究员

同济大学上海国际知识产权学院助理教授**田**

小楚以《AI 大模型非表达性使用的著作权法保护路径》为题发言。她认为，当前著作权法中的“合理使用制度”在应对 AI 大模型训练过程中的作品使用行为时面临规制不足。大模型在训练阶段对原作品进行功能性学习而不直接呈现表达内容，形成了既不构成传统复制权侵权、又难以被既有合理使用条款涵盖的“非表达性使用”行为。通过构建“输入端—输出端”与“表达性—非表达性”的四象限分析框架可见，此类使用在行为机制、表现形式与责任归属等方面均与传统复制行为存在本质差异。建议构建专门的行为规制路径，明确非表达性使用的法定情形与保护范畴，对输入端采用宽松的侵权认定标准而对输出端保持严格审查，并通过“目的识别—合目的性检验—结果分类”的三步授权法建立审查机制。

田小楚 同济大学上海国际知识产权学院助理教授

第五单元 青年演讲

安徽大学法学院副教授**夏庆锋**以《“隐私悖论”下的个人信息自我管理及措施完善》为题进行发言。他对“隐私悖论”现象提出了创新性解读，认为个人在信息处理中表现出的前期谨慎态度与后续同意行为之间的不一致并非真正的逻辑矛盾，而是源于动态风险认知与具体情境驱动的理性选择。传统理论错误地将同意行为简单等同于不重视隐私，忽视了个人在不同场景下基于风险判断做出的权衡。针对当前同意机制存在的认知缺陷与结构性困境——包括用户面临的信息过载、专业理解障碍及服务商界面诱导等问题，他提出“自由意志与家长式规范相结合”的治理路径。

夏庆锋 安徽大学法学院副教授

华东政法大学经济法学院副教授**柯达**以《通证化数字资产的风险规制——以“去信任化”为视角》为题进行发言。他指出，通证化数字资产（RWA）作为金融科技前沿领域，核心在于通过区块链技术将现实世界资产（如不动产、贵金属）进行权益分割与数字化上链，旨在提升传统低流动性资产的交易效率。其发展呈现出“去信任化复归”的特征，即从比特币的完全去中心化理想，转向对公权力、金融机构及实体资产价值的新依赖。然而，这同时也带来了三重核心风险：公私合作受政治影响的不稳定性、中心化托管方（如银行破产）引发的连锁反应，以及底层资产过度金融化与权责不清可能引发的系统性风险。单纯依靠技术或市场手段难以有效规制上述风险，法律制度的介入至关重要。为此，他建议构建多层次的法律框架：首先，明确其法律定性，可将其界定为对区块链运营方的网络服务债权，并区分支付型与商品型通证实施分类治理；其次，建立以维持价值稳定为核心的常态化监管，强调资产隔离与信息披露；最后，优化基础设施的互联互通规则，根据公共性程度实施强制或自愿接入机制，从而为这一新兴资产的健康发展筑牢法治根基。

柯达 华东政法大学经济法学院副教授

西南政法大学民商法学院讲师**赵自轩**以《基于功能主义的网络虚拟财产排他性判断标准设计》为题进行分享。他认为，当前网络虚拟财产的司法认定存在标准不一的问题，传统类比有体物的“价值性、稀缺性”标准难以适应数字特性。国际最新立法实践（如《数字资产与私法原则》）已转向以“排他性”作为核心判断标准，对此，他建议构建功能主义的双层判断标准：第一阶段通过“功能对齐”将电子证券等已有专门规制的数字财产排除在外；第二阶段结合网络协议、技术架构与法律法规进行排他性检验。未来立法应确立以技术中立和功能对齐为前提的排他性标准体系，通过考察数字资产在具体网络环境中的实际功能状态，构建符合数字时代特征的虚拟财产保护框架。

赵自轩 西南政法大学民商法学院讲师

黑龙江大学法学院讲师**牛丹彤**以《跨部门司法数据共享的制度构建》为题进行分享。她认为，当前跨部门司法数据共享正经历从行政指令调取到场景驱动交互，最终迈向协同网络化共享的模式演进。然而，实践中仍面临三重困境：其一，主观上部门因权力稀释与利益考量形成“数据垄断”思维；其二，客观上存在数据标准不一导致的系统异构问题；最后，安全层面也面临司法保密性与数据流通性的结构矛盾。为此，应构建“规则+TOE 框架”的治理体系：通过硬法与软法耦合的规则体系明确共享边界，在技术层面统一标准与安全协议，在组织层面建立政法委牵头的协同机制，在环境层面配套绩效考核与容错激励。最终形成“触发—响应—反馈”的动态治理闭环，推动司法数据从被动供给向主动服务转型，实现数据价值在流动中的最大化释放。

牛丹彤 黑龙江大学法学院讲师

第 14 届法治国际论坛在京召开

2025 年 11 月 6 日至 7 日，中国社会科学院法学研究所主办的“第 14 届法治国际论坛”在京成功举办。本次论坛的主题是“数字时代的法治变革：中国实践与国际经验”，来自美国、英国、德国、芬兰、波兰、俄罗斯、日本以及中国的专家学者共 40 余人参加会议。

会议第一单元主题为“数字时代的法治政府建设”，由中国社会科学院法学研究所**卢超**研究员主持。北京大学法学院**王锡锌**教授以“中国数字政府的兴起及其法治影响”为题发言，概述我国数字政府从电子政务到“以数治国”的演进，指出数据赋能治理同时也带来责任偏移与技术锁定等风险，并强调需推动以数治国与依法治国相融合。中国政法大学比较法学研究院**解志勇**教授聚焦“数字文明时代的法治政府建设”，分析数字文明背景下政府治理逻辑与法治原则的延续与变革，指出数字法治政府需在技术赋能与依法行政之间保持平衡，警惕数字鸿沟和算法偏见等风险。中国社会科学院法学研究所**吕艳滨**研究员以“数字化时代的政府创新”为题发言，强调数字技术应助力提升政务服务与执法效率，同时需强化数据共享、个人信息保护与法律制度完善。

会议第二单元主题为“数字经济的权利保护与法律规制”，由中国社会科学院法学研究所**冯珏**编审主持。清华大学法学院**申卫星**教授提出数据“三权分置”框架及示范合同在数据流通与安全利用中的作用。早稻田大学**上野达弘**教授回顾数字化对版权制度的影响，强调既要应对新技术带来的问题，也要保持版权法基本原则的稳定。中国社会科学院法学研究所**管育鹰**研究员通过案例探讨生成式人工智能场景下的著作权与平台责任，主张区分直接侵权和间接侵权设置注意义务。中国社会科学院法学研究所**金善明**研究员分析数字经济中反垄断与创新激励的张力，讨论域外经验并提出差异化监管与动态评估机制的建议。香港城市大学法学院**王江雨**教授介绍数字化背景下国际经贸规则制定的新变化，强调中国在国际经贸规则制定和国际治理体系中发挥着日益重要的作用。

会议第三单元主题为“数字化与政府规制”，由中国社会科学院法学研究所**董坤**研究员主持。**卢超**研究员分析数字时代从前置许可向事中事后监管转型，强调协同监管与分级分类监管的趋势。澳门大学法学院**蒋朝阳**教授介绍澳门电子政务建设，强调应突出法律保障与多平台协同，以提升公共服务效率。俄罗斯联邦政府立法与比较法研究所**谢凯**研究员探讨数字化反腐实践，展示信息系统在个人信息申报、核验与监督中的应用，并指出法律定义与数据协调等面临的挑战。英国伦敦国王学院法学院**克里斯托弗 • 克莱泽**教授对比法律与技术治理路径，讨论算法监管等技术治理的法律化问题。

会议第四单元的主题是“数字化与法学研究”，由中国社会科学院法学研究所**余佳楠**副研究员主持。剑桥大学法学院**西蒙 • 迪肯**教授以“司法语言与工伤赔偿判例演变”为主题发言，利用机器学习分析英国和爱尔兰工人工伤赔偿案件文本，发现司法裁判随经济周期与劳动争议情况呈周期性变化。德国马普比较私法和国际私法研究所**本杰明 • 匹斯勒**教授以“数字时代的海外中国法研究”为题发言，介绍相关数据库及人工智能工具在中国法研究中的应用机遇，并指出翻译准确性、数据质量与算法偏误等挑战。中国人民大学法学院**丁晓东**教授以“从单维到多维：数字时代法学知识的组织方式”为题发言，指出传统单一部门法框架难以应对平台责任、个人信息保护与人工智能等数字议题，强调法学知识体系需从单维走向多维交叉。芬兰赫尔辛基大学法学院**基莫 • 诺提欧**教授着眼于数字化对法院的影响，指出人工智能工具正在影响法院运作与判决分析方式。

会议第五单元的主题是“数字化与劳动和社会保护”，由北京大学法学院**叶静漪**教授主持。中国社会科学院法学研究所**王天玉**研究员以“渐进式保护：中国平台用工权益保障机制演进”为题发言，分析中国平台用工权益保障的思路演变以及相应的政策和立法实践，强调应推动“渐进式立法”，实现灵活就业与权益保障的兼顾。波兰华沙大学法律与行政学院**高彬承**教授以“算法管理与劳动法典化”为主题，提出算法既可被理解为管理工具、内部规章，也体现雇主指挥权，强调劳动法的法典化应充分考虑算法规制等数字技术带来的新问题。中国政法大学民商经济法学院**娄宇**教授以“新就业形态职业伤害保障制度的法律性质与司法适用”为题发言，认为新职伤应定位为不完全劳动关系下的强制社会保险制度，并探讨其与工伤保险、商业保险及雇主责任的衔接与司法处理路径。

会议第六单元的主题是“数字化与国际治理”，由中国社会科学院法学研究所**何庆仁**研究员主持。美国耶鲁大学法学院**陆凯**研究员以“构建全球人工智能治理”为题发言，分析人工智能全球治理面临的机遇与挑战，强调国际对话、多元参与和渐进协作的重要性。中国社会科学院法学研究所**徐玖玖**助理研究员以“人工智能国际治理的伦理共识”为题发言，分析当前全球人工智能治理面临的挑战，指出伦理原则是国际治理的重要准则。中国社会科学院国际法研究所**孙南翔**副研究员聚焦人工智能立法与涉外法治体系建设，探讨人工智能立法域外适用的必要性及其逻辑，并提出以“适当联系”为基础的多层次域外管辖框架。

首届大湾区金融法治论坛在广东金融学院开幕

2025 年 11 月 8 日，首届大湾区金融法治论坛在广东广州隆重开幕。本次论坛以“粤港澳大湾区金融法治的协同创新”为主题，由广东金融学院法学院主办。来自中国人民大学、中国政法大学、西南政法大学、西北政法大学、黑龙江大学、大连大学、中山大学、华南理工大学、暨南大学、华南师范大学、广东外语外贸大学、广东财经大学、广东技术师范大学、深圳大学、南方医科大学、东莞理工学院、广州南方学院、香港城市大学、澳门大学、澳门科技大学、澳门理工大学、澳门城市大学以及香港黄福鑫资深大律师事务所、澳门麦兴业律师楼、广东省高级人民法院、广东广信君达律师事务

所、北京盈科（广州）律师事务所等高校、科研机构与实务部门的专家学者及研究生、本科生共 180 余人现场参会。

中国人民大学法学院**张新宝**教授围绕“个人信息保护法与金融机构合规”发表专题演讲。他通过电商平台数据违规和跨国企业合规免责两个典型案例，生动阐释了《个人信息保护法》兼具民事权益保障、行政监管规范与数字经济发展指引三重属性。张教授强调，该法是金融机构开展合规工作的根本遵循，并重点解析了“同意原则”的适用边界，指出履行合同所必需的信息处理可免于单独同意。同时，他特别提醒金融机构应严格落实对金融账户等敏感信息的特殊保护要求，加强员工合规培训，构建与数字经济发展相适应的全面合规体系。

张新宝 中国人民大学法学院吴玉章高级讲席教授 中国法学会网络与信息法学研究会副会长兼学术委员会主任

2025 年世界互联网大会乌镇峰会网络法治论坛举行

11 月 9 日，2025 年世界互联网大会乌镇峰会网络法治论坛于浙江乌镇举行。本次论坛由国家网信办、北京大学主办，北京大学法学院、北京大学数字法治研究中心、腾讯公司协办。与会嘉宾围绕“建构人工智能良法善治共识”，深入交流了人工智能时代的法治建设问题。中国国家互联网信息办公室副主任**杨建文**，司法部副部长**李明征**，浙江省人民政府副省长、省公安厅厅长**杨青玖**，北京大学常务副校长、中国科学院院士**张锦**出席论坛并致辞。

人工智能良法善治是当前全球数字治理体系变革进程中的前沿议题。应对人工智能技术与应用的快速变化，需要建构人工智能良法善治共识，这既要立足于各国社会现实与文化传统，更应着眼于人类命运共同体的整体与长远利益。中国将人工智能视为造福人类的国际公共产品，在统筹发展与安全的框架下，推进人工智能治理的良法善治，为促进人工智能全球治理贡献中国方案。本次论坛特邀来自政府部门、网信企业和国内外知名高校、研究机构的专家学者，分享交流人工智能治理领域理论实践，探求人工智能良法善治的建构路径。

主旨演讲

在北京大学数字法治研究中心主任**王锡锌**教授的主持下，来自北京市人民检察院、北京互联网法院、北京大学、上海交通大学、澳门大学、美国华盛顿大学、英国伦敦大学、腾讯集团等机构的嘉宾围绕“人工智能治理的法治理论与实践”发表主旨演讲。

北京市人民检察院检察长**朱雅频**以《深化网络治理检察行动 融入人工智能治理法治实践》为题，讨论了检察机关参与人工智能治理的相关问题。他指出，一方面要发挥检察职能在网络治理体系中的要素功能，服务和保障人工智能的健康发展；另一方面，也要以数智赋能提升网络检察履职能力，驱动法律监督提质增效。

朱雅频 北京市人民检察院检察长

腾讯集团高级副总裁**郭凯天**以《良法善治：让科技真正转化为社会福祉》为题，总结了法治在“空间、信任与未来”三个维度给予中国互联网的重要保障。他表示，中国互联网法治选取“维护底线、包容发展”的策略，既保障了社会的稳定健康，又

留出了充分的产业发展空间；中国互联网发展的成就，得益于互联网法治确立的最大价值——信任；中国互联网法治摸索出发展与安全上最为平衡的方案，以此为基础，中国互联网的发展、人工智能的发展将保持巨大的优势，相信未来将持续走在世界前列。

郭凯天 腾讯集团高级副总裁

上海交通大学资深教授**季卫东**在《加速主义与人工智能治理的中国方案》的主旨演讲中表示，全球各国在人工智能治理上正向加速主义靠拢，特别是 2025 年 5 月以来，许多国家放松了对人工智能的监管，侧重推动技术研发而非伦理和安全监管。相比之下，中国提出的治理方案注重通过系统化的技术手段管控人工智能安全风险，避免伦理争议的无序化，提供了全球治理的新思路，兼顾科技创新与社会福祉的平衡。

季卫东 上海交通大学资深教授

澳门大学法学院讲座教授**於兴中**在《再思人工智能治理：数字素养的角色》的主旨演讲中表示，人工智能治理与数字素养密切相关，但后者常被忽视。长期以来，中国都在各个地区（尤其是农村和欠发达地区）通过教育和培训提升民众数字素养，推动相关技术的实际应用。这些举措为构建一个能有效参与人工智能治理的社会奠定基础，展示了数字素养在治理中的重要作用，提供了全球治理框架的宝贵经验。

於兴中 澳门大学法学院讲座教授

美国华盛顿大学法学院教授**康涵真（Jane Winn）**在《知识革命与中国人工智能治理经验的世界意义》的主旨演讲中表示，中国在人工智能治理方面的领先地位源于其认识到数据作为生产要素催生了新的生产模式，同时具备运用实验主义生成知识的能力。为了将这一模型推广为全球标准，中国需要超越传统的基础设施建设模式，而是设计激励机制以促进“一带一路”国家的积极参与。

康涵真（Jane Winn） 美国华盛顿大学法学院教授

北京互联网法院综合审判一庭庭长朱阁在《以裁判树规则、促治理、助发展》的主旨演讲中介绍了北京互联网法院审理的涉人工智能新类型案件的基本情况，重点讲解了“全国首例‘AI 文生图’著作权案”“AI 标识案”“AI 恶搞案”“虚拟数字人案”等著作权、人格权、网络服务合同领域典型案件的裁判规则。她表示，北京互联网法院始终坚持“以裁判树规则、促治理、助发展”的理念，支持人工智能依法应用，惩治利用人工智能技术侵权的行为，以高质量司法服务保障高质量发展。

英国伦敦大学法学院副院长、教授**迈克尔·威尔（Michael Veale）**在《应对人工智能犯罪性滥用的共同挑战》的主旨演讲中表示，当前讨论过度聚焦开源大模型，却低估了可在手机和个人电脑上运行的小模型被犯罪化滥用的风险，尤其是在网络诈骗和生成儿童不雅内容等领域。为此，他呼吁在鼓励开放的同时，通过法律完善与跨领域协作，加强对恶意模型使用的约束。

迈克尔·威尔（Michael Veale） 英国伦敦大学法学院副院长、教授

北京大学国际法学院副教授**吉拉德·阿贝里（Gilad Abiri）**在《监管与人工智能正当性》的主旨演讲中表示，单靠“对齐”和技术效果并不足以支撑人工智能的合法性，关键在于公众是否承认其背后的“决策权来自何处”。因此，AI 治理应将算法权力嵌入已经被认可的合法权威之中，提供可理解的理由说明，建立可申诉和可纠正的程序，并确保规则与本地社会的语言、制度和价值相契合。

吉拉德·阿贝里（Gilad Abiri） 北京大学国际法学院副教授

圆桌论坛

在北京大学法学院副院长、长聘副教授戴昕的主持下，与会嘉宾围绕“人工智能治理与人类共同命运”展开讨论。

德国 EBS 法学院副院长、教授**佟天佑（Emanuel Towfigh）**在发言中表示，欧洲正面临数字自主权、公共话语受 AI 影响、生产力收益分配不均三大挑战，“这些不是欧洲独有的，而是全球共同的困境”。奥地利格拉茨大学公法与政治学讲师**伊丽莎白·帕尔（Elisabeth Paar）**从中小国家视角补充，提及奥地利因人口规模小，在 AI 本土数据训练、全球话语权上存在局限，但与中国等国共享“理解 AI 系统、向公众科普”的核心需求。耶鲁大学蔡中曾中国研究中心高级研究员**陆凯（Karman Lucero）**结合美国联邦制与普通法传统，指出其治理的独特性，并认同“技术分布式发展带来的挑战具有普遍性”。

联想集团副总裁**高唤栋**、腾讯公司公共事务副总裁**韩开创**一致认为，隐私安全、模型可解释性是中外企业的共同关切。高唤栋表示，人工智能治理是突出体现人类命运共同体理念的议题，各国在开展技术竞争的同时，必须致力于通过不间断的交流与合作，确保人类在不确定的技术前景中不失守共同安全的底线。韩开创用“共同建造 AI 巨轮”作喻，提出通过 ISO/IEC 国际标准制定、开源社区协作等方式，中外企业完全能突破地缘隔阂，实现有效合作。谈及中国经验，韩开创将其概括为“红绿灯系统”：既设“红灯”划安全底线，又开“绿灯”促创新探索，这种“敏捷治理”为发展中国家提供了实用参考。

民法典与数字法学青年学术沙龙第 1 期成功举行

2025 年 11 月 13 日，由中国人民大学法学院、中国人民大学民商事法律科学研究中心、中国人民大学未来法治研究院、中国人民大学法学专业虚拟教研室主办的第 1 期民法典与数字法学青年学术沙龙于明德法学楼 205 会议室成功举行。民法典与数

字法学青年学术沙龙致力于促进青年教师的深度交流与学术共进，通过报告、研讨与评议学术论文的方式，提升研究能力与写作水平，推动青年法学研究的创新与成长。

此次沙龙由中国人民大学法学院助理教授**阮神裕**、中国人民大学法学院博士后**边琪**分别进行题为“论侵权法中的部分连带责任”和“生成式人工智能下已公开个人信息保护模式研究”的主旨报告，并邀请对外经济贸易大学法学院助理教授**薛亦飒**、中国人民大学法学院助理教授**阙梓冰**、中国人民大学法学院助理教授**包丁裕睿**、北京大学法学院博雅博士后**李怡雯**、英国埃塞克斯大学法学院助理教授**左振斌**、《中国法律评论》期刊编辑**余亮亮**、中国人民大学交叉科学研究院讲师**李铭轩**、清华大学法学院助理研究员**王年**、北京大学法学院博雅博士后**丁庭威**进行评议。

中国人民大学法学院助理教授**阮神裕**围绕“论侵权法中的部分连带责任”作主旨报告，系统梳理了这一概念在我国法治实践与理论发展中的脉络。报告指出，部分连带责任是我国侵权法中逐渐成型的重要责任形态，自《侵权责任法》时期初露端倪以来，该制度在《环境侵权责任解释》以及证券虚假陈述纠纷中不断被司法实践赋予新的意义，引发学界广泛讨论。报告指出部分连带责任作为中国特色民法理论的重要组成部分，具有独立建构的必要性，并进一步阐述了部分连带责任的三个重要议题。

阮神裕 中国人民大学法学院助理教授

对外经济贸易大学法学院助理教授**薛亦飒**高度认同阮老师关于比例连带责任的理论模型建构和解释路径，她补充提出，在证券虚假陈述司法实践中，为提升受害人受偿的比例，部分判决在事实核查与专业判断之间未能清晰界分，对“勤勉尽责”的认定趋于严苛，导致中介机构承担了与其专业角色和实际过错程度不相匹配的法律后果。

薛亦飒 对外经济贸易大学法学院助理教授

中国人民大学法学院助理教授**阙梓冰**针对报告提了三方面的想法：第一，部分连带责任制度的形成具有鲜明的实践导向，回答了分配赔偿不能之风险的利益衡量问题。第二，报告中部分连带责任的分层清晰度似有不足。解决单个人责任和多数人责任的问题，值得关注的点是，如果行为人单人构成侵权责任应当赔偿全部损失，为何在多数人责任中行为人责任却可以减轻。第三，报告末尾对侵权法中部分连带责任的类型化梳理，规范意义不够明确，建议可以提炼出一条更为清晰的类型化主线。

阙梓冰 中国人民大学法学院助理教授

中国人民大学法学院助理教授**包丁裕睿**评议认为，文章指出部分连带责任源于的理论起源，具有客观必然性与独特制度功能，但与“加重责任”的正当性存在张力。以及该报告的理论建构忽视了

复杂叠加情形，应当从价值判断出发构建更一般化的理论框架，以促进司法与立法在责任分配上的精细化改革。

包丁裕睿 中国人民大学法学院助理教授

北京大学法学院博雅博士后**李怡雯**指出，该报告的优点体现在两个方面：一是运用了经济分析和矫正正义理论，二是对于既有理论的解释力不足进行了充分的探讨。遗憾之处是，文章对于经济分析和矫正争议理论的应用仍有可商榷之处，以及报告中提出的一些新概念是否可以得到一般化的适用，也可以进一步考虑。

李怡雯 北京大学法学院博雅博士后

中国人民大学博士后**边琪**围绕“生成式人工智能下已公开个人信息保护模式研究”作主旨报告，讨论了已公开个人信息保护的困境及其解决。报告指出，生成式人工智能对现有的已公开个人信息保护规则提出了挑战，原有的构成要件面临适用上的困难。比如，2022 年发布的 ChatGPT-3 的总语料数为 0.499T，总规模为 753GB。而英伟达于 2025 年 1 月推出的 Cosmos 世纪基础模型平台的总语料数已经达到了史无前例的 9000T，总规模为 2000000GB。如此海量的语料主要依赖于网络中已公开数据，其中又包含了大量难以被分离和清洗的已公开个人信息，传统的保护模式对此已经力有不逮，应当通过新的保护模式予以应对。

边琪 中国人民大学法学院博士后

英国埃塞克斯大学法学院助理教授**左振斌**从该报告的严谨性、原创性和重要性的三个方面，谈了相关的看法和建议。严谨性上，该报告很好地处理了大量相关文献和资料，体系解释的方法很清晰，具体的解释论也做的较为细致。还可从增加举例、增加比较法考察、增加技术方案简介三方面强化讨论的严谨程度。其次，在创新性上，该报告也明确的给出了自己的贡献，帮助法官具体设想如何对已公开个人信息的处理进行放宽，进而保护创新。但在具体的表述上，可能将文章的结论写得更细致一点或许更好。最后，在重要性上，该报告涉及到当下全球重要的科技公司爬取与处理个人信息的制度设计和法解释问题。但若能在开头或者结尾点出一些实践中的讨论和案例，或许更能帮助不同领域的读者理解题目的要领。

左振斌 英国埃塞克斯大学法学院助理教授

《中国法律评论》期刊编辑**余亮亮**认为，在 AI 预训练的信息抓取中，各类组合在一起形成数据集，处理者通常无法就上述类型的信息进行严格区分。鉴于此，该报告可能有必要进一步论证根据信息类别进行规则适用的正当性。

余亮亮 《中国法律评论》期刊编辑

中国人民大学交叉科学研究院讲师**李铭轩**认为，该报告的题目表述有必要进行调整，突出论文的主要创新点。该报告对对于术语的使用与通说不尽相同，可能会引起读者的误解，有必要对此作进一步阐释。另一方面，该报告对传统保护模式的所面临的困境梳理不够充分，需要进一步论证为了传统保护模式已经不足。

李铭轩 中国人民大学交叉科学研究院讲师

清华大学法学院助理研究员**王年**指出，该报告结合生成式人工智能背景，对已公开个人信息保护规则进行解释论研究，问题意识明确，文献梳理充分，观点鲜明，论证严谨，充分展现了作者的学术抱负。建议作者进一步凝练本文的问题，明确指出在生成式人工智能这一特定领域中，已公开个人信息保护规则对生成式人工智能技术发展的影响。

王年 清华大学法学院助理研究员

北京大学法学院博雅博士后**丁庭威**认为，该报告是逻辑严谨的解释论研究，论证过程层层推进，最终得出的结论清晰而具有说服力。如果报告能在开篇部分先梳理一下我国司法与执法实践中，关于生成式人工智能下已公开个人信息保护所面临的实际困境，再对应分析现有规则的不足，进而从理论层面进行澄清并探索更合适的解释路径，整体框架或许会显得更加清晰。

丁庭威 北京大学法学院博雅博士后

2025 年首都法学家沙龙——人工智能+法治人才培养研讨会成功召开

2025 年 11 月 13 日，由北京市法学会与北京理工大学联合主办，北京理工大学法学院、北京市应用法学研究中心共同承办的“2025 年首都法学家沙龙——人工智能+法治人才培养研讨会”在北京理工大学国际交流中心成功召开。

本次会议聚焦中国自主知识体系建设、人工智能发展与法治人才培养核心议题，汇聚了来自北京大学、清华大学、中国人民大学、中国政法大学、

北京航空航天大学、中央财经大学、北京交通大学、北方工业大学、北京市房山区人民检察院、北京互联网法院等高等院校和司法实务部门的四十余位专家学者，共同探讨人工智能时代跨学科人才培养与法治实践融合创新的议题，旨在为首都法治建设高质量发展与国家法治人才培养提供可行方案。

专题研讨

专题研讨分为两个研讨环节。第一个环节的核心议题是“科技法律人才培养与学科交叉融合”，由北京理工大学法学院孟强教授主持，各位与会人员依次分享研究成果。

北京市房山区人民检察院副检察长**张劲楠**以“数智时代知识生产模式转型与职业检察官的培养”为题进行主旨发言。他指出，数智时代检察实务对人才提出全新要求，复合型检察人才需同时具备扎实法律专业素养与数字技术认知能力，才能有效应对智能化办案带来的证据分析、流程管理等一系列挑战。未来检察人才培养也应聚焦跨学科知识融合。

张劲楠 北京市房山区人民检察院副检察长

北京互联网法院审管办（研究室）副主任**李婉星**结合典型案例分享了北互法院在数字法治建设方面的经验。她首先以全国首例“AI 文生图”著作权案为例，揭示了面对此类新型案件的主要裁判思路，明确指出利用 AI 工具进行创作的图片，若能够体现出原告的智力投入和个性化表达，则构成作品，应当予以保护。她强调，数字法治与数字法学需面向未来，传统法学理论应适配技术发展，数字法学教育要注重实践导向，培养学生运用法律思维解决数字领域纠纷的能力，践行“智能向善”理念。

李婉星 北京互联网法院审管办（研究室）副主任

北京航空航天大学法学院党委书记**周友军**教授围绕“新法科背景下卓越法治人才培养的探索与思考”这一主题，从师资队伍、学生素质、课程体系、资源投入与社会环境等维度系统阐述了北航卓越法治人才培养的现状。同时，周友军从课程体系重构、跨学科师资建设等方面深入探讨了当前人才培养工作中面临的现实问题与优化方向。

周友军 北京航空航天大学法学院党委书记、教授

北京大学法学院、人工智能学院**胡凌**副教授围绕“网络法中的知识生产”进行了主旨发言。胡凌指出，网络法知识具有流动性强、理论关联性弱、知识碎片化等特点。网络法的核心问题分散于各学科，缺乏体系化串联，不少课堂仅引入简单部门法素材却未深究“为何发生”“如何支撑规则”的底层逻辑，欠缺教义学理念与成文法规则的支撑。他特别强调，学科交叉虽为趋势，但在实践中，存在“盲目追求与技术相结合”的问题。这一分享为与会者理解网络法的知识属性、学科困境与发展方向提供了关键洞见。

胡凌 北京大学法学院、人工智能学院副教授

清华大学法学院党委副书记**龙俊**教授以“人工智能赋能法学学科发展的实践”为题，介绍了清华大学计算法学的建设成果与经验。他指出，清华自 2017 年起布局计算法学学科建设，2018 年获批计算法学硕士项目，后续成为教育部新文科建设典型案例，并牵头成立中国计算法学发展联盟。学科构建“法学+计算机+交叉特色课”培养体系，已培育百余位复合型人才；学术与实践层面，积累海量数据，研发智能审判辅助系统等产品，承担多项国家重点研发项目，斩获多项专利与软著，“水木智法”小程序也已落地应用。他表示，计算法学已形成国际化发展格局，中国的学科建设与人才培养实践为全球提供了有益借鉴。

龙俊 清华大学法学院党委副书记、教授

中国人民大学未来法治研究院执行院长**张吉豫**教授介绍了人民大学法治人才培养的创新路径。她指出，中国人民大学依托未来法治研究院深耕交叉研究，开设大数据分析、网络法等跨学科课程，并建成了法律科技与社会治理实验室。她还强调，要持续推进课程融合与实践平台搭建，助力学生提升跨学科素养，培育适应新时代的复合型法治人才。

张吉豫 中国人民大学未来法治研究院执行院长、教授

第二个研讨环节的核心议题是“人工智能对法学教育的挑战与回应”，由北京理工大学法学院助理教授、工信部智能科技风险法律防控重点实验室研究员包晓丽主持。

中国政法大学**刘坤轮**教授首先结合中国政法大学数据法治研究院的建设和发展经验，深入剖析了人工智能对法学教育与法律职业带来的双重影响。该实验室立足于数字时代前沿，服务建设数字经济、数字社会和数字政府的国家战略，推进学科交叉融合与研究范式创新，着力解决我国数字时代的重大法学理论和法治实践问题。他提出要在“挑战中寻机遇”的发展理念，建议法学教育需强化技术思维培养，适应法律职业的智能化转型。

刘坤轮 中国政法大学刘坤轮教授

北方工业大学文法学院的**相庆梅**教授围绕“人工智能时代法学教育的逻辑重构与实践路径”主题，介绍了北方工业大学法学学科的建设进展与实践成果。她指出，AI 已深度渗透司法实践与法学各学科，在人工智能时代，要以学生能力提升为核心，构建融合数字素养与法律专业能力的教学体系，同时坚守人机协作边界，避免技术消解法学核心价值。

相庆梅 北方工业大学文法学院教授

北京交通大学智能法治与数据治理研究中心主任**陶杨**教授结合工科院校特色，分享了法学与人工智能融合的实践经验与现存问题，他提出，工科特色院校要发挥其独有优势，通过学科资源联动打破知识壁垒，打造特色化智能法治人才培养模式；高校要深度融合法学与人工智能两大学科，避免法学培养与人工智能培养“两张皮”。

陶杨 北京交通大学智能法治与数据治理研究中心主任、教授

中央财经大学人事处副处长李伟副教授介绍了央财“财经+法律+人工智能”三元融合的人才培养模式。他指出，AI 时代的财经法治领域既是挑战也是机遇，高校要化解学科壁垒、打破知识分割，财经法治人才的培养也需要注重“技术理解、法律适用、财经洞察”三重能力。目前，中央财经大学已联合北京理工大学、北京航空航天大学等高校开展跨校联合培养，整合多方学科与资源优势。

李伟 中央财经大学人事处副处长、副教授

中国人民大学人工智能治理研究院主办“人工智能安全：识别风险与寻求解决”专题学术研讨会

2025 年 11 月 15-16 日，由中国人民大学人工智能治理研究院主办的“人工智能安全：识别风险与寻求解决”专题学术研讨会顺利召开。来自中国人民大学、北京大学、清华大学、首都经贸大学、中国科学院计算技术研究所、中国科学院信息工程研究所、微软亚洲研究院、北京智源人工智能研究院、南京大学、加拿大滑铁卢大学的从事计算机科学、法学、政治学、管理学、新闻学等多个交叉领域的近 20 位学者齐聚一堂，与在场同学一起，从多学科视角出发，共同探讨人工智能安全问题。本次会议由中国人民大学交叉科学研究院、高瓴人工智能学院、信息学院协办。

中国人民大学国际关系学院的**保建云**教授做了题为《智能垄断、算法歧视与大模型治理》的报告，他从政治经济学的“超级博弈”视角出发，剖析了超级人工智能发展引发的全球性挑战。超级智能的发展正催生由少数巨头主导的“智能垄断”，它们凭借大模型、算法与数据的控制形成全球寡头格局。这种垄断抑制创新与知识自由流动，并因算法中的价值偏见加剧社会歧视，放大不公。超大模型因此成为大国战略竞争的关键领域，其失控可能引发非传统安全风险与文明危机。面对这一难题，“中国方案”应致力于推动建立更加公平、安全、包容的全球 AI 治理秩序。

保建云 中国人民大学国际关系学院教授

南京大学信息管理学院副院长**康乐乐**教授带来了题为《AI 模型的透明性评价》的报告，探讨在人工智能快速发展背景下，开放与封闭两种创新模

式对 AI 生态系统的影响，强调了透明性在构建可信 AI 中的核心作用。为系统评估 AI 透明性，他提出了一个多维度框架，包括可解释性、文档可及性、用户认知等核心指标，并借助 Hugging Face 等多源数据平台，构建模型、论文、专利、开发者、组织之间的关联网络，以实现自动化、可扩展的透明度评估。

康乐乐 南京大学信息管理学院教授

中国科学院计算技术研究所研究员**陈薇**带来的报告《智能算法安全机理探索》聚焦算法机理的安全可信问题。面对大模型在鲁棒性、隐私和公平等方面的安全挑战，她认为研究需从算法机理层面寻求根本解。当前探索主要聚焦于两大方向：一是深入理解深度学习的内在机理，包括优化器的隐式正则效应如何影响泛化能力，以及训练动力学的收敛特性，为增强模型内在稳定性奠定理论基础；二是面向未来，将人类可理解的因果结构嵌入模型，通过识别和解耦因果变量，使模型在分布变化和对抗攻击下能进行更鲁棒、可信的推理。

陈薇 中国科学院计算技术研究所研究员

中国科学院信息工程研究所研究员**曹亚男**在题为《大模型水印：人工智能生成内容溯源的挑战与机遇》的报告中指出，为应对 AIGC 滥用带来的治理挑战，大语言模型水印技术作为核心溯源手段应运而生。其主要分为白盒水印与黑盒检测两条路径。白盒水印通过在模型训练或推理阶段嵌入不易察觉的信号来标记生成内容，并持续优化以平衡水印强度、文本质量与抗攻击鲁棒性。黑盒检测则面对模型输出日益“拟人化”的难题，发展出基于统计保证的低误报检测框架和仿 DNA 突变修复的新范式，以提升在复杂场景下的检测精度。

曹亚男 中国科学院信息工程研究所研究员

微软亚洲研究院社会计算组研究员**吴方照**带来的报告《AI 大模型的安全风险和防御策略》聚焦 AI 大模型所面对的两大核心安全风险——越狱攻击与上下文攻击。越狱攻击通过精巧提示词绕过安全限制，输出有害信息；上下文攻击则利用模型遵循指令的特性，直接或间接注入恶意指令操纵模型行为。防御上，闭源模型可采用基于“Self-Reminder”的提示工程增强自我约束，而开源模型则因攻击面更广、存在反向对齐风险而更难管控。大模型的整体防御面临意图识别困难、攻击不可逆、智能体自动执行放大危害等根本性挑战，亟需构建多层次、协作式的安全防护体系。

吴方照 微软亚洲研究院社会计算组研究员

滑铁卢大学与魁北克 Mila 人工智能研究所的**纪语**研究员作了题为《AI 安全治理的情境化与行为

化框架》的报告，从认知和行为科学角度提出了 AI 安全治理的情境化与行为化框架。报告指出人具有的情境化与再情境化能力，这对于理解“对齐伪装”有重要意义；接着聚焦人的认知“系统一”（情感）和“系统二”（理性），指出系统一的认知垄断会导致过度的商业逻辑，而系统二的认知垄断会导致过度的安全干预，我们应在发展（系统一）与安全（系统二）之间寻求动态平衡。

纪语 滑铁卢大学、魁北克 Mila 人工智能研究所

中国人民大学法学院讲师**阮神裕**作了题为《论人工智能侵权产品责任的有限适用》的报告。他首先指出如果人工智能侵权适用产品责任的意义，即更有利于受害人寻求救济；接着讨论了人工智能侵权适用产品责任的形式和实质两类判断标准。报告认为形式上关键看交互方式，物理交互型 AI 可适用，信息交互型原则上不适用；实质上以产品危险性为核心，需嵌入公众惯习行动框架。不应纳入产品范畴的模型，可通过一般过错责任救济受害人。

阮神裕 中国人民大学法学院讲师

中国人民大学国际关系学院讲师**刘露馨**作了题为《英克特尔模式：美国军方获取人工智能技术的一种创新机制》的报告。报告指出，为了搭建政府与商业科技生态的桥梁，美国中央情报局 CIA 设立了非营利性投资机构 In-Q-Tel（英克特尔），用以识别和发现尖端技术公司，提供投资将其技术进行调整、强化，加速创新技术从实验室转到实战部署，投资内容大量涉及 AI 企业。英克特尔扮演了桥梁、侦察员、孵化器与加速器的角色，自身拥有独特的运作机制。通过这套机制，安全部门将投资决策权从受政治周期、官僚化影响的保密机构转移到更独立、贴近市场且有约束的实体手中。

刘露馨 中国人民大学国际关系学院讲师

首都经贸大学管理工程学院副教授**付东普**作了题为《基于多源异构信息的舆情传播模型研究》的报告。当前社交平台多元，舆情呈现多源、图文音混合的异构特征，使得舆情传播规律难以刻画。面对该难题，报告提出“先融合”（把多源异构数据统一成语义一致的信息），“再建模”（在融合结果上构建舆情传播模型）的解决思路和一种多源异构信息的融合方法。研究发现，该方法能有效提取并融合舆情信息的内在特征，构建的传播模型能够较好地描述现实中的舆情传播。

付东普 首都经贸大学管理工程学院副教授

中国人民大学新闻学院讲师**王裕平**作了题为《理解社交媒体中伪照片的使用》的报告。该报告关注的问题是社交媒体中伪照片的影响。报告采用感知哈

希技术（perceptual hash）技术提取图像特征，构建了一套“数据采集-感知哈希技术提取-事实核查-数据标注-分析”的计算流水线，用以分析来源于多个社交媒体的约 5 亿张图片，发现伪照片往往会伴随更多的用户参与度，并且往往被用作梗图。基于此，报告认为，有效的虚假信息应对措施必须将图片考虑在内。

王裕平 中国人民大学新闻学院讲师

中国人民大学信息学院副教授**张文平**作了题为《基于 CNN-Transformer 的多场景感知深度伪造检测》的报告。为高效、准确地识别出多场景图片中被篡改的对象，报告提出了一个融合多目标检测方法的识别模型框架。该模型效仿人类视觉认知过程，提出了系统的检测流程。为评估模型性能，报告在 FaceForensics++数据集及 ForenSynths 数据集上进行实验。实验结果表明，该检测模型在 GAN 生成模型上的多场景深度伪造监测任务中表现优异，但在传统的人脸篡改的测试集中，性能有所牺牲。

张文平 中国人民大学信息学院副教授

北京大学人工智能研究院研究员**杨耀东**作了题为《从对齐到欺骗：大模型安全的“莫比乌斯悖论”》的报告。报告指出，大模型可能主动发展出欺骗性行为，其核心机理在于模型参数具备“弹性”，倾向于抗拒对齐微调并回弹至预训练形成的稳态分布，导致安全约束被轻易规避。为此，报告提出通过模型自监控的约束强化学习框架，在推理中实时检测和抑制欺骗性意图。报告也指出，随着模型能力的演进，欺骗性对齐可能带来更严峻的挑战，因此亟需更具可扩展性与内在一致性的对齐范式。

杨耀东 北京大学人工智能研究院研究员

清华大学人工智能学院助理教授**董胤鹏**作了题为《基于推理增强的大模型安全对齐》的报告。对于推理过程中的安全与性能之间的协同提升问题，报告首先提出了 STAIR 框架，实现模型对风险的动态识别与规避，从而在保持模型有用性的同时显著提升其安全性。其次，报告还提出“构造性对齐”理念，建设以用户意图理解与风险分级为基础的动态安全响应机制，使模型为高风险的合理需求提供建设性替代方案。实验表明，该方法在通用及多模态场景中得到了有效验证。

董胤鹏 清华大学人工智能学院助理教授

中国人民大学信息学院讲师**王文轩**作了题为《社会科学启发下的大模型安全对齐评测方法》的报告。面对大模型安全对齐评测的挑战，报告提出了社会科学启发的评测方法：个体层面，通过借鉴认知心理学、逻辑学和人格理论来评估感知能力、推理能力和心理属性；在群体层面，通过引入博弈论和社会学的研究方法来评测共赢意愿和群体偏见；在社会层面，通过具体文化内容评测和抽象价值观评测来检验文化偏向性。

王文轩 中国人民大学信息学院讲师

北京智源人工智能研究院大模型安全研究中心研究员**戴俊滔**在题为《从语言到动作的全模态安全与对齐》的报告中指出，随着大模型的多模态扩展，安全风险也随之升级。对此，报告提出了“从任意到任意”的全模态评测与对齐框架，通过构建全模态人类偏好数据集与“语言反馈”学习范式来解决全模态统一问题。针对动作模态的安全挑战，报告还提出了新的评测环境、引入了集成式安全方法，在约束马尔可夫决策过程框架下通过主动诱发不安全行为来提高具身大模型的安全与性能。

戴俊滔 北京智源人工智能研究院大模型安全研究中心研究员

中国人民大学高瓴人工智能学院副教授**王希廷**作了题为《探索大模型精准神经元控制与基本价值观对齐》的报告。大模型复杂度提升带来了安全与对齐方面的挑战，对此，报告首先从大模型的神经元概念和可解释性入手，指出安全与非安全输入在模型中间层表征中的线性可分特性，揭示了大模型中潜在的安全漏洞。报告进一步引入价值观罗盘（value compass）框架，将模型行为映射到人类基本价值观上，使得大模型具备更强的识别和适应能力。报告从多维度探讨了安全治理思路，为未来可能工作指明了深层机制问题。

王希廷 中国人民大学高瓴人工智能学院副教授

（技术编辑：吕昊然）

数字法评

数据访问地标准：跨境电子取证管辖的中国方案

此处删除了原文脚注，全文请参见《人民检察》2025 年第 11 期，转载或引用请注明出处。

作者：刘品新；赵梓彤

内容提要：跨境电子取证管辖已成为打击跨境网络犯罪的棘手问题，我国对此缺少可适用、可对接的专门规定。国外适用的数据存储地标准和数据控制者标准均存在不足，我国需要在以数据为媒介的同一语境下回应。多年来，我国已体现出以数据可访问地为连结点的数据访问地标准。该标准是将跨境电子取证内国化的方案，符合网络空间主权原则，其核心要义能够适应实践中各种复杂的情形。面向未来，我国应当将该标准纳入跨境犯罪侦查管辖权制度的法律框架，塑造“普通人公开访问”模式，以更好地处理涉案证据，并持续改进以数据为立场的管辖权改造路径。

跨境电子取证已成为打击跨国网络犯罪的关键手段，各国跨境电子取证方式较为丰富，国际上通过传统司法协助、警务合作、单边取证等途径实现跨境电子取证管辖，我国现行法中对单边取证措施和双边取证措施皆有规定，但在实践中因与域外国家对网络空间主权态度迥异而发生价值冲突。目前我国散见于各个法律法规的跨境取证措施，在面对日趋复杂的跨境犯罪案件时显得乏力。本文从我国跨境电子取证管辖相关法律规定的现状思考，试图在充分尊重各国网络空间主权的基础上提出明确的中国方案。

一、我国跨境电子取证管辖的制度评析

由于作案手法的多变，跨境案件的取证措施也相应复杂化，法律的滞后性逐渐体现。国际层面上，各国跨境电子取证手段缺乏统一且权威的指引，我国对单边取证措施和双边取证措施都缺少具体的法律规定，难以同域外各国和谐调配资源。

对于单边跨境电子取证管辖缺少系统性规定，导致实践中适用性不强。公安部《计算机犯罪现场勘验与电子证据检查规则》，最高人民法院、最高人民检察院、公安部《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》，公安部《公安机关办理刑事案件电子数据取证规则》，陆续对我国单边跨境电子取证的具体方式进行了规范，明确了网络在线提取的适用范围主要针对境内公开发布的电子数据、境内远程计算机信息系统上的电子数据。问题在于，单边取证方式极易引发主权纠纷，以上规定仅对境外信息系统的电子数据提取进行了限制，对于我国侦查人员能否在境内通过网络在线提取和网络远程勘验直接进行跨境电子取证以及远程提取跨境证据是否侵犯他国主权缺少可适用的法律依据。

对于双边跨境电子取证管辖的禁止性规定缺乏强制力，增加了国际对接的法律风险。网络犯罪案件的侦查管辖权成为国际博弈主阵地，各国对此高度重视。为应对近年来美欧日趋扩大的管辖权，最高法、最高检、公安部《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》第 6 条第 3 项对电信网络诈骗等刑事案件中的刑事司法协助进行了初步规范，随后修改的刑事诉讼法、国际刑事司法协助法和数据安全法也规定了我国办案机关通过刑事司法协助的方式获取境外刑事证据时，需要办案机关、主管机关、对外联系机关等多个机关相互配合。尽管我国已明令禁止境内组织或个人向外国提供证据材料，但未对违反禁止性规定的法律责任作出规定，在面对日益复杂的管辖权冲突时处于弱势，难以在实现各国间平等互惠的基础上进行有效的国际对接。

二、域外跨境电子取证管辖的实践样态

（一）域外跨境电子取证管辖的既有方案

国际范围内的跨境网络犯罪管辖形成了两个版本。一是欧洲委员会《网络犯罪公约》呈现的数据存储地标准。该标准通过网络服务器所在地，硬件所在地，复制件、快照、镜像克隆等备份所在地实现，即数据实际存储在何地，其所在国便可行使刑事取证管辖权。各国执法机关在进行跨境数据取

证时，首先要确定存储数据的实际地理位置，如果需要对存储在特定国家的数据进行访问或提取，应当通过司法协助，而不是直接行使管辖权。理事会成员国内部彼此认可各国内部法律内容，以国际组织的方式行使了范围较广的网络犯罪司法管辖权。《网络犯罪公约》的效力范围等同于国家在刑事实体法上的属地管辖，体现了属地主义的主权观。

二是以美国的澄清合法使用海外数据法为典型的数据控制者标准，也称数据控制者所在地标准，通过寻求跨境云服务提供者的合作，或对其发出指令以获取在美国注册的网络服务提供者和管理者所控制的数据。从网络服务提供者的性质来看，可以分为数据的收集、存储、使用、加工、传输、提供、公开、销毁等活动涉及的各种法律主体所在地。该标准缘起于 2013 年 12 月“微软公司诉美国案”，该案的争议焦点为域外数据能否适用美国存储通信法，即美国能否强制要求微软公司提供存储于爱尔兰的邮件数据。此案一直上诉至联邦法院，直至 2018 年美国国会紧急出台澄清合法使用海外数据法。该法案的适用对象为在美国注册的网络服务提供者，其有义务依法保存和披露其在全球范围内的数据，美国地方法院也可以根据本地法律要求其提供数据，至此消除了存储通信法关于域外效力的疑惑。该标准是属人主义的变种，兼具属地因素和属人因素。

（二）域外跨境电子取证管辖方案的启示

由于跨境数据流动过程中会面临双重或者多重管辖以及位置丢失的情形，既有的数据存储地标准和数据控制者标准展现了数十年来各国面临取证问题时对域外存储电子数据的角逐。各国都试图建立各种连结点，以便对域外的数据进行掌控和管辖。

数据存储地标准难以适应跨境数据流动的取证需求，增加了取证障碍。近年来国际上越发加强数据存储本地化，许多国家通过立法强制要求数据在本国境内存储，以加强对数据的掌控。这一举措简化了刑事司法取证工作，减少了跨境取证的复杂性。然而，网络犯罪案件的虚拟性和跨国性使确定其唯一的地理位置变得困难，比如，谷歌将位于不同国家的数据中心里的用户数据碎片化，导致无法确定访问通信内容时会牵连到哪个国家的主权。又如，部分暗网犯罪节点遍布全球，电子数据位置未知且难以追踪。而当国家过分依赖数据本地化规制跨境数据流动时，碎片化数据被限制在狭窄的物理空间中，无法被连贯地整体性使用且各国间数据难以共享，会造成数据“孤岛化”，对国家间数据交流以及跨境犯罪案件的侦破都弊多利少。

数据控制者标准下，因数据主权不明引发了激烈的外交冲突。美国虽然没有制定网络犯罪的相关法律，但随着网络服务提供者的分布格局逐渐以美国为主，其超级管辖权逐渐显现。比如，澄清合法使用海外数据法允许美国政府和执法机关在未经数据存储地国家同意的情况下，直接向美国科技公司调取存储于世界各地的域外电子数据，使其在获取数据时畅通无阻。这体现了实践中强调的客观属地主义原则，即只要某一犯罪行为对美国产生影响便有管辖权，无论有害行为本身是否发生于管辖范围内。美国的一系列做法对欧盟的管辖权制度形成了强烈的冲击，对此欧盟就跨境获取电子证据的相关法规和指令草案达成协议，相继推出欧洲调查令和欧洲提交保存令，使欧盟当局可以直接向其他成员国的相关数据提供方发送获取电子证据的司法指令。2023 年《欧盟电子证据条例》通过出示令和保全令赋予成员国执法机关和司法机关直接向其他成员国的数据控制者获取数据的权力，突破了电子数据存储的物理空间。虽然《欧盟电子证据条例》仅在成员国之间使用，但能看出欧盟已向数据控制者标准转型。美国和欧盟使用的数据控制者标准都逐渐呈现扩大化趋势，但数据控制者标准依托云计算的技术背景，只涉及跨境云服务提供者控制的数据，于是该标准下跨境电子取证也只适用于网络服务提供者掌握的位于全球各地的服务器中存储的数据。数据控制者标准忽视了数据存储地国家的主权问题，此种单边主义倾向明显不符合对等原则的意旨。

案件侦破效率和国家主权保护皆为跨境执法的重中之重，其中的具体执法行为是否符合国际法

基本原则中的主权平等原则有待商榷。数据存储地标准是以数据存储的物理空间所在地为属地连结点确定跨境数据的管辖权，其面向数据存储地所在国控制的作为证据的各类境外电子数据。数据控制者标准则是以数据的实际控制者为属人连结点确定跨境数据的管辖权，其指向的是跨境网络服务提供者控制的能够作为证据的各类境外电子数据。对于新标准的提出，我国在跨境电子取证管辖问题上明确适用数据访问地标准即可，后续在具体个案中发生管辖冲突情况时，需综合考虑各国主权、利益及具体案情，依据相关国际协议、国际司法规则及国际惯例等进行协商解决。

三、数据访问地标准的提出

数据访问地标准以可访问数据者为属人连结点，以可访问数据地为属地连结点，针对的是可访问数据者在其所在国能够访问到的境外电子数据。访问地不同于存储地、控制者所在地，其更具灵活性，同时保护和尊重了各国网络空间主权。

（一）数据访问地标准的现实需要

以“访问”为连结点的思想早已在传统 IP 地址管辖理论和《网络犯罪公约》中有所体现。“数据访问”译为 Data Access，早期网址管辖权的确定依赖于网络服务器所对应的 IP 地址，包括主动访问网址的积极管辖和被动收取邮件等其他数据的消极管辖。21 世纪初，美国采取的是积极管辖，将主动访问网址作为管辖连结点。然而由于计算机技术水平提升，IP 地址较易被篡改或隐藏，导致被害人所在国难以获得管辖权，也难以根据网址确定唯一的管辖国家，传统 IP 地址管辖理论已经难以适应当前的网络环境。而后的《网络犯罪公约》规定了可以不考虑数据位于何处地理位置而进行跨境访问的数据类别，包括公开可用的开源电子数据或是对数据披露有合法权限的个人同意后的数据。

我国侦查机关已通过“访问”行为的内国化方案替代了真正的跨境电子取证行为，以应对跨境电子取证管辖难题。如今绝大部分的跨境电子取证的“跨境”仅为表面的现象。如，当事人通过邮箱下载某国互联网上的数据，其下载行为有路由、IP 地址和下载时间等电子数据。但因为主体的非公务性，其行为并非跨境取证，而执法人员可以使用当事人的邮箱账户下载涉案境外数据，该数据是当事人访问后留存在电脑硬盘或内存中的数据，而非位于境外的服务器数据本身。此类取证方式便将涉外证据内国化，避免了一系列法律风险和实践挑战。同样的思路包括但不限于特派员制度、当事人取证制度、律师取证制度、私人侦探境外取证制度等。无论执法人员是固定当事人客户端的数据，抑或执法人员直接操作客户端、作为目击证人查看当事人操作，诸如此类的做法看似为跨境取证，事实上仅为在境内访问的结果。为适应网络环境的变化，有必要根据网址管辖理论和我国实践中体现的“访问地”思想，对访问地的概念进行明确和细化，以确保法律的适用性和公正性。

（二）数据访问地标准的适用价值

数据访问地标准与既有标准的不同之处在于以访问地为连结点。网络犯罪案件具有跨地域性，往往涉及多个犯罪地点，为了加大对网络犯罪的打击力度，最快捷有效的方法是拓宽犯罪地外延。现有相关规定通过枚举和兜底条款，尽可能避免网络犯罪案件管辖存在空白之地。但长久以来的逐步扩张产生了“沾边就管”的新问题，导致了司法工作冗余的问题，即部分服务器所在地是被告人租赁过、使用过的，或者存储着与案件无关数据的服务器所在地，将这些与案件数据无关的地点作为犯罪地，往往只会徒增办案人员的工作难度，于案情破获无益。确认访问地为网络犯罪案件唯一管辖连结点，可以容纳与案件有关的数据内容，也可以排除与案件数据无关的服务器所在地。

数据访问地标准以网络空间主权原则为解释立场，以保护和尊重网络空间主权之数据主权为基础。“主权”作为一个开放的概念，其管辖的“领土”向各个空间延伸。数据访问地标准能够通过各国平等的访问权，彰显中国在国际上积极倡导的网络空间主权、坚持领土主权原则的拘束力。该标准兼容了数据存储地标准和数据控制者标准，但又同既有标准作出了区隔——其不需要清晰的物理疆

域和明确的电子数据存储位置作为适用前提，尊重了国家主权，规避了主权冲突和强国的霸权主义。

（三）数据访问地标准的核心要领

数据访问地标准的核心要点为访问主体、访问行为以及访问客体。

访问数据的主体包括普通人、网络服务提供者和执法机关。普通人为具备用户名和密码的电子数据持有人，是数据任意访问者。网络服务提供者控制用户产生的数据，在保障用户个人隐私的前提下具备调取用户公开信息的权利。普通人和网络服务提供者的访问结果可以直接提供给执法机关，或是由执法机关通过普通人和网络服务提供者的访问设备获取证据材料，再固定其访问结果。以上方式遵循了国家主权原则。对执法机关作为访问主体而言，一国执法机关因正当事由当然有向本国公民调取证据的权力，但因为执法人员身份的特殊性，需要分辨其访问行为是否具备公务性，以便尊重普通用户的基本人权，所以执法人员在执行公务时的访问行为需要提前被上级机关授权。通过访问主体的访问行为，使得数据脱离了具体的机器、设备本身，此时数据存在于何处，何处具备主权。

访问行为以公开访问为表现形式，辅之经授权的秘密访问。《网络犯罪公约》第 32 条规定了缔约国执法机关无需遵守跨国法律协助程序而在外国领土上进行调查取证，在不考虑数据位于何处进行跨境访问的情形有两种：一是访问公开可用的开源电子数据；二是在获得了对数据披露有合法权限的个人的同意后访问，该同意需要是自愿且合法的。当执法机关行使国家授予的调查取证权时，必须注意不超出权限，尤其这种权力是秘密的或强制的。执法人员通过普通人和网络服务提供者的合法访问行为将境外数据转化为国内法律文书，此时跨境取证被域内取证吸收。被访问的数据是可被公开访问的，意味着不包括执法机关通过技术手段超越常规限制获取的数据，如拦截通信。在欧盟范围内，拦截信息时可能遇到境外“网关”，拦截国通过远程控制在境外进行拦截，若网关所在国放弃其对拦截行为的领土控制权，便相应地扩大了请求国的刑事程序管辖范围，此种具备偶发性的扩张行为容易引发管辖权不公现象。故诸如此类的执法机关通过违反国家法律的越权行为即超出执法权限获得的数据，应当被排除。但对于特殊案件，根据宪法、刑事诉讼法、国家安全法、反间谍法，侦查机关在跨境犯罪案件的侦查过程中，若在公开访问时难以发现犯罪分子，为了保护侦查活动顺利进行、防止犯罪分子察觉，且可以确保秘密访问不侵犯公民合法权益时，经上级机关授权后可以采取隐蔽方式进行秘密侦查活动。

访问客体以静态数据为主，以动态数据为辅。静态数据指在某一时刻固定不变的数据，包括计算机存储的数据、历史记录、通过镜像技术复制后的数据、备份文件等。该类数据不涉及实时网络传输，因此更加容易提取并固定涉案数据。动态数据指在网络中实时流动和变化的数据，包括实时获取和正在传输的数据，如通信数据和通信内容。在各类跨境网络犯罪案件中，动态数据的数量庞大且不断更新，并且在网络中高速传输，极易转移和销毁，为办案机关的取证带来了许多困难。在进行跨境电子取证时，还需要考虑到不同国家间的数据保护和主权问题，获取静态数据可以避免国家间主权纠纷，减少对数据传输过程的干扰。故而，访问和调取的数据应以静态数据为主。此外，调取数据往往需要实时监控或侵入性技术手段，还需要遵守当地的数据流动规则、个人隐私保护条例、国家安全的相关法律法规等，从刑事诉讼的特殊需要考虑数据分类分级的问题，同时，应注意网络人权与网络主权同样举足轻重。

四、数据访问地标准的精进

我国现行法律司法解释等已体现出跨境电子取证的属地主义和属人主义，无论是对犯罪行为发生地还是犯罪结果发生地，利用计算机网络实施犯罪的管辖皆围绕服务器所在地、网络服务提供者所在地、信息网络系统及其管理者所在地。网络犯罪不存在纯粹的域外网络犯罪问题，其兼涉域内域外，但传统物理介质的地理属性限制了管辖主体的管辖范围。数据访问地标准的特点是管辖范围灵活，为促进该标准成为现实，需要将其纳入跨境犯

罪侦查管辖权制度，同时宣示普通人公开访问立场，打造以数据为核心的管辖权路径。

（一）明确纳入跨境犯罪侦查管辖权制度

跨境犯罪侦查管辖权制度是一国对网络犯罪进行跨境电子取证的前提，也是适用数据访问地标准的前提。目前引发司法主权冲突的原因是管辖权规定尚未明确，侦查管辖既涉及不同国家之间对涉外网络犯罪案件管辖权的关系处置，也涉及一国内不同侦查机关之间对网络犯罪案件管辖权的分工合作，包括侦查级别管辖、侦查地域管辖、侦查案件管辖分工、侦查管辖权转移、侦查管辖的监督与救济、侦查管辖纠纷的解决机制等内容。网络空间侦查管辖权的症结在于对网络空间的疆界划分难以确认清晰标准且难以得到公认。

我国刑事诉讼法对涉外或跨境网络犯罪案件侦查管辖并未作任何规定，在我国法律制度中纳入跨境犯罪侦查管辖权制度，通过管辖权条款赋予我国执法、司法机关域外管辖的权力，有利于全面维护我国的数据利益，消解部分主权问题，逐步落实主权国家间的平等、互惠原则。对于已有的跨境犯罪侦查管辖相关规定，首先，需要降解国际法中双重归罪原则的适用。网络犯罪打击困难的原因之一是不同涉案国家对涉案行为的罪与非罪认定不一，请求调取证据的机关需要举证说明被调查的行为理论上构成提出请求的管辖区与被请求管辖区的犯罪。而对案件没有侦查管辖权的国家进行跨境电子取证，则有可能侵犯其他国家主权。数据访问地标准的适用并非反对双重归罪原则，而是通过单方国家的“访问”行为，绕开传统原则的限制，降低因多国合作条件不一致导致的取证障碍。其次，需要灵活运用侦查管辖原则。在网络犯罪案件中，由于涉及环节众多且人员分散，需要跨地区乃至跨境调查，若数据能在具有侦查管辖权的领域内获得，则该领域内具备管辖权。此外，若多个犯罪嫌疑人实施的犯罪存在直接关联，并案处理有利于查明案件事实的，办案机关必要时可直接并案处理。

（二）明确塑造“普通人公开访问”模式

我国侦查机关和公证机关应以“普通人公开访问”为基础，获取、固定跨境网络犯罪的涉案证据。刑事诉讼法第 192 条第 2 款规定，人民警察就其执行职务时目击的犯罪情况作为证人出庭作证，适用前款规定。虽然该条文不针对网络犯罪和跨境取证，但也不排除对此的适用，意味着侦查人员可以针对在执行中目击当事人或其他证人行为的情况出庭作证，或是侦查人员自行访问服务器证明是本人访问和下载的内容。公安部《公安机关办理刑事案件电子数据取证规则》第 23 条将网络在线提取的范围限缩至境外公开发布的电子数据，便是将“公开访问”合法化。实践中对于警察的远程勘验可以转化为“访问+取证（固定）”，其中“访问”包含普通人上网访问、被害人上网访问、犯罪嫌疑人上网访问、鉴定机构上网访问、侦查机关上网访问等，其访问内容为境外网站，证据形式包括但不限于司法笔录、证人证言等。除此之外，对于案件需要公证机关对境外获取的犯罪证据进行公证时，主要有两种方式：一是当事人访问境外服务器，打印截屏内容固定证据，公证人员对此予以公证。这种方式作证内容较为简单，但问题在于可能存在虚假访问等情形。二是当事人告知公证人员访问境外服务器的账号密码，公证人员亲自登录访问。这种方式一定程度上无法保障当事人隐私，但规避了当事人伪造证据的风险。

（三）明确构建数据立场的管辖权改造路径

跨境犯罪的管辖权问题是一个棘手的国际问题。2024 年通过的《联合国打击网络犯罪公约》是联合国首个网络犯罪公约，其第三章规定的犯罪管辖权体现了属地主义和属人主义的结合——管辖权范围包括犯罪发生在所涉缔约国境内以及犯罪系针对所涉缔约国的国民。我国刑法规定犯罪行为或结果发生在域内即有权管辖，这一对涉外或跨境网络犯罪案件享有刑事管辖权的基本法源，并未考虑“人”的因素。我国应遵循国家安全法中主张的网络空间主权，依照《全球数据安全倡议》、数据安全法和个人信息保护法分级分类保护国家核心数据和个人数据，从而维护全球数据流动的安全秩序以及我国在跨境网络犯罪中的数据主权。

论人工智能法律规制的内部路径

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

作者：邓矜婷

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

一、人工智能法律规制的困境

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

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

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

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

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

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

目前大量的规范性法律文件的出台，使得人工智能产业的发展成本也急剧上升，如企业数据的合规管理。企业不仅要遵守数据保护相关的法律法规，还要遵守国家政策、商业惯例、公司章程以及道德规范等，需要配合各个部门密集的监管行动进行整改，无暇顾及数据保护能力的提升。知情权、许可权与删除权等新设权利增加了企业的合规负担，如仅仅针对 GDPR（《通用数据保护条例》，General Data Protection Regulation）的要求，全球便有 20%的企业因违反要求而导致破产，甚至出现了美国洛杉矶时报及芝加哥论坛报等企业因 GDPR 合规成本过高而直接退出欧盟市场的现象。对于需要大量收集和使用个人信息的企业来说，个人数据保护机制的建立和完善需要投入的资金巨大，并且需要考虑建成之后每年的维护费用，这都对公司财政状况提出挑战。Telos 开展的一项企业合规治理的成本调查显示：每家企业要做到数据的管理

符合法律法规的要求，平均需要遵守至少 13 个不同的 IT 安全或隐私法规，并且每年在合规性活动上要花费高达 350 万美元。

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

二、人工智能法律规制困境的原因在于当前规制仅采取外部路径

（一）当前人工智能法律规制采取的是外部路径

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

人工智能深刻影响了法律的发展，法律需要对这种强势力量作出一定的回应，立法者已经采用了多种方法规制人工智能，但这些方法无一例外都属于外部路径。即，当前法律对人工智能的调整，是通过设计一种法律机制，配置人工智能相关人员在法律上的权利义务以及规定违反法律规定所应承担的法律责任，来设定主体的行为模式，引导相关人员在法律所许可的范围内开展与人工智能相关的活动，从而把人工智能相关人员的活动引入可调

控的法律秩序之中。

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

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

（二）外部路径不直接规制人工智能本身

1.外部规制路径仅规范人的行为，与人工智能技术保持距离

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

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

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

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

2.外部规制路径仅解决人工智能相关人员的价值判断问题

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

何行为，国家机关及其工作人员将如何行为。人工智能相关人员因而可以根据法律来确定自己的行为方向、方式、界限，合理地作出安排，采取措施。

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

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

三、人工智能法律规制内部路径的提出

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

（一）内部路径直接规制人工智能本身

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

然而人工智能并非以往的技术或者工具，其具有一定的智能性，尤其是强人工智能已经开始显现，在算法和数据的支持下，人工智能在一定程度上能够自主行为和决策。在这种背景下，提出内部路径是可能的，也是必须的。内部路径是指直接规制人工智能本身，在人工智能会被影响的层面和方式上，将法律的要求通过计算机语言和方法来表达，使得人工智能能够理解，并且主动遵循。内部路径相对于外部路径来说深入人工智能内部，建立在人工智能具有一定智能性的基础之上，以人工智能本身为规制对象，即在程序、算法层面约束人工智能无法违反法律，即使其使用者要求其违反法律或将其用于实施违法行为。目前，我国一般采取外

部路径规制人工智能，但部分法律法规中体现出了内部路径的精神，如，《生成式人工智能服务管理办法（征求意见稿）》中已经开始注意会直接影响人工智能行为的几个因素，并对其规定了一些基本要求，包括对人工智能的预训练过程、大模型的调用、训练集的要求等。

（二）内部规制路径通过在技术底层融入法律规则的要求实现对人工智能的直接规制

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

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

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

指标。

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

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

四、人工智能法律规制困境需要内部路径的补充

（一）外部规制路径存在规制失效、监管成本过高的情况

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

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

第二，人工智能监管成本较高。由于人工智能犯罪产生的数据海量，以及人工智能犯罪的高技术性和隐蔽性，导致人工智能监管成本较高。人工智能犯罪与传统犯罪相比，具有犯罪行为发生的随机性、犯罪过程迅速、犯罪后果呈裂变式等特点，因此监管机构对其监管成本较高。人工智能犯罪的监

管难度也在于其技术手段的复杂性。由于人工智能系统具有高度的复杂性和不确定性，人工智能应用已不仅仅是技术化的工具，而是越来越具有类似于人类思维的能力，监管机构需要投入大量的技术资源来分析和识别犯罪行为。人工智能系统还具有自我学习和自我修复的能力，这也增加了监管难度。随着人工智能技术的快速发展，如何对其进行有效监管已经成为一个重要的课题，监管机构需要采用更加高效、精准的监管手段来应对人工智能犯罪带来的挑战。

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

（二）外部规制路径容易造成规制限制发展的情况

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

第二，规制的边界不确定，合规治理的成本过高。人工智能技术在研发和运用过程中，个体和机构的很多行为都很容易触犯相关法律，企业、个人难以界定哪些行为是违法行为，容易导致人工智能企业创新能力的下降。例如，从研发角度，《中华人民共和国刑法修正案（九）》专门规定了帮助信息网络犯罪活动罪和拒不履行信息网络安全管理义务罪，网络服务提供者等主体为他人基于信息网络技术实施犯罪行为提供了网络技术与网络结算等各类支持与帮助，或者不履行信息网络安全管理义务的消极不作为方式提供技术支持、帮助，将受到刑法的规制。然而，何为促进犯罪活动的技术支持、帮助行为，何为正常的技术活动，在司法实践中界限还较为模糊，这容易构成信息网络服务者经营活动的重大刑事法律风险，对各类创新性的信息网络技术构成了压力与限制。又如，研发数据的获取、处理、分析、应用就涉及多个主体和多部法律的要求，数据合规涉及的法条众多，数据的获取、处理、分析、应用等多个阶段都要重复受到法律的限制，这使得人工智能研发企业难以确定哪些研发行为、预训练、数据、数据获取和处理分析行为及算法是合法的。随着我国不断加强互联网平台等主体责任的落实，平台方越来越需要加强内部监管，从而走向另一个极端—过度审查，这会导致企业合规成本过高，还会降低互联网平台经济的发展质量，阻碍平台经济中信息、数据等关键资源的自由流通。

可以看出，当前的外部路径在一定程度上存在

着过度干预的风险。这种过度干预不仅表现在法律对于人工智能研发的宽泛管制，也表现在法律对于人工智能企业的多方面审查和干预。这可能会限制企业的自由和创新能力，从而阻碍人工智能的发展。

（三）内部路径的特点可以补充外部路径，更加准确、有效地规制人工智能

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

1. 穿透式规制

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

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

2. 以人工智能规制人工智能

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

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

五、内部路径可以克服人工智能规制困境的理由

如前所述，在使用外部路径规制人工智能时会陷入两方面的困境，而内部路径则可以利用其自身所具有的特性，在外部路径“失效”的场景中发挥作用，从而对外部路径起到有效补充，最终将二者相结合，实现对人工智能的有效规制。

（一）内部路径可以提升外部路径规制的有效性

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

1. 内部路径可以有效地确定规制的对象

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

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

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

2. 内部路径可以实现高效的规制过程

内部路径可在实现法律规则计算机表达的基础上，进一步提升人工智能规制效率。外部路径通过规制人工智能相关人员影响人工智能的方法没有充分考虑强人工智能的发展方向，同时在现有的人工智能算法设计、开发背景下，外部路径也存在着规制效率不高、过程过于烦琐等明显不足。而内部路径选择将人工智能需要遵守的一系列法律规则通过计算机表达的方式内置于人工智能算法，可以实现一次设置、多次重复使用，从而大幅提升了人工智能规制的效率。并且除了通过事先预设程序进行事前规制，以法律规则的计算机表达为基础建设的可信人工智能司法、执法平台，也可以在实现数据共享、相关标准共同制定、知识图谱共建的基础上对后续开发的人工智能进行快速合规检测，从而将人工从现有的外部路径所要进行的烦琐、低效

的监管工作中解放出来，实现对人工智能的高效规制。

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

（二）内部路径可以平衡规制和创新

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

1. 内部路径可以明确规制边界

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

2. 内部路径可以降低合规治理的成本

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

此外从学理上来看，外部路径将规制重心置于人工智能背后的开发者或其他相关人员，试图通过规制相关人员的行为来影响其所设计、开发出的人工智能，但是应当看到在此种规制路径中，人工智能作为处于高速发展变化中的技术，法律自身所具有的滞后性与其特性存在明显差异。并且因为法律制度的发展与变革，每一过程的路径选择和规则设计，其法律思维一般都是客观事实分析与主观价值判断的综合。就法律制度建设而言，如果总是基于

技术及其效应的充分显现，以此形成以技术事实为基础的社会规范，那么法律制度的滞后现象将会十分严重，最终导致技术法律对技术“匡正”的失效和无力。因此在人工智能技术迅猛发展的现状下，试图仅通过外部路径实现有效规制人工智能的目标，实际上是不符合技术发展规律的。面对此类正处于高速发展变化中的技术，在进行立法规制时不仅要考虑其法律效果，还需要考虑规制可能产生的社会效果，即应当综合考虑技术的本质与发展现状来探索规制路径。因此，只有在内部路径的补充下，才能更好地适应人工智能技术发展现状，既实现对人工智能的有效规制又不过分限制其创新发展。

六、结语

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

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

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

（技术编辑：邓语鑫）