中国人民大学法学院
数字法学教研月报

2025 年第 12 期（总第 24 期） 2025 年 12 月 29 日

本期看点

【数字法治大事件】

《数据安全技术 电子产品信息清除技术要求》强制性国家标准获批发布，为电子产品再流通上好“安全锁”；国家发展改革委等五部门联合印发《关于加强数据要素学科专业建设和数字人才队伍建设的意见》，夯实数字时代智力基础；国家能源局出台《能源行业数据安全管理办法（试行）》，建立数据分类分级保护及重要数据目录机制；最高人民法院将“数据权属纠纷”“数据合同纠纷”等列为独立的司法案由，数据产权司法治理迈入新阶段。

《贵州省大数据发展应用促进条例》修订通过，将于 2026 年实施；福建省出台有序推进算力基础设施发展措施；福州市首发地理标志产品数据知识产权登记证书，“福州脱胎漆器”拥有了“数字身份证”。

专家解读：

多位专家深度解读《数据安全技术 电子产品信息清除技术要求》，指出其对保护个人隐私、促进循环经济发展的重要意义；针对公共数据跨域流通，专家提出“身份—安全—追溯”三位一体的可信流通模式，为数据要素安全有序流动提供技术与制度思路。

【研究动态】

理论与数据治理方面，本期重点关注数字权利变异、个人信息保护边界及数据要素流通定价与收益分配机制。新兴技术规制方面，学界围绕人工智能立法、生成式 AI 侵权责任认定以及智慧司法与行政程序的规范构造展开了深入研讨。

【教研活动】

人工智能治理沙龙：中国人民大学人工智能治理研究院举办第十四期沙龙，王文轩与刘东瑞围绕“大模型测评与对齐”展开前沿探索，构建社会科学启发的大模型安全评测体系及“内对齐”思路。

国际研讨会：第五届“数字法治与智慧司法”国际研讨会在华中科技大学召开，齐延平、黄文艺、刘艳红等 80 余位专家学者围绕数字智能化生存、政法工作数字化、司法人工智能应用及数字犯罪治理等议题展开深入研讨。

【数字法评】

《人工智能生成合成内容标识办法》的规范功能与法律适用，作者：黄尹旭

《论生成式人工智能服务提供者的过错推定责任》，作者：张新宝、卞龙

本期目录

数字法治大事件 3

《数据安全技术 电子产品信息清除技术要求》强制性国家标准获批发布 3

《数据安全技术 电子产品信息清除技术要求》强制性国家标准答记者问 3

国家发展改革委 国家数据局 教育部 科技部 中共中央组织部关于加强数据要素学科专业建设和数字人才队伍建设的意见 5

专家解读｜加快实施电子产品信息清除标准 以高水平数据安全保障高质量发展 7

专家解读｜信息清除强制性国家标准发布 为电子产品再流通上好“安全锁” 8

专家解读｜保护用户隐私数据，助力循环经济发展 9

专家解读｜“身份—安全—追溯”三位一体的数据可信流通模式——解读《基于公共数据跨域流通场景的数据可信追溯安全技术应用案例》..10

地方动态｜《贵州省大数据发展应用促进条例》自 2026 年 1 月 1 日起施行 11

福州市首发地理标志产品数据知识产权登记证书 福州脱胎漆器有了“数字身份证” 16

国家能源局印发重要管理办法 17

国家能源局有关负责同志就《能源行业数据安全管理办法（试行）》答记者问 21

最高法将“数据权属纠纷”“数据合同纠纷”等列为独立的司法案由 22

福建省数据管理局等三部门关于印发福建省有序推进算力基础设施发展若干措施的通知 23

研究动态 26

数字法学基础理论 26

个人信息保护 27

人工智能立法 29

数据确权研究 34

智慧行政与智慧司法 36

网络平台治理 37

数字时代的部门法研究 38

教研活动 42

人工智能治理沙龙：大模型测评与对齐的前沿探索成功举办 42

第五届“数字法治与智慧司法”国际研讨会在华中科技大学召开 43

数字法评 67

《人工智能生成合成内容标识办法》的规范功能与法律适用 67

论生成式人工智能服务提供者的过错推定责任 74

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： 王昊

数字法治大事件

导言：

在数字中国建设全面推进的背景下，数据安全治理、制度供给与实践探索正不断迈向更高层次与更高标准。随着《数据安全技术 电子产品信息清除技术要求》强制性国家标准的发布及权威解读相继推出，我国在电子产品数据安全治理领域迈出关键一步，通过规范信息清除行为，为设备再流通和循环利用加装“安全锁”，在保护个人隐私与促进绿色发展之间实现制度层面的平衡与协同。同时，国家发展改革委、国家数据局等五部门联合印发《关于加强数据要素学科专业建设和数字人才队伍建设的意见》，从战略高度系统谋划数据要素学科布局与人才体系建设，夯实数字时代法治治理与产业创新的智力基础。

在保障体系不断完善的同时，制度建设正向重点行业和关键领域纵深推进。国家能源局出台《能源行业数据安全管理办法（试行）》并进行权威解读，围绕能源数据这一关系国家安全与公共利益的重要资源，明确安全管理要求和责任边界，助力能源行业数字化转型行稳致远。司法层面，最高人民法院将“数据权属纠纷”“数据合同纠纷”等列为独立案由，意味着数据作为新型权利客体与交易标的，正在逐步进入更加明确、规范与可预期的司法治理轨道。

地方层面同样涌现活跃探索。《贵州省大数据发展应用促进条例》即将施行，进一步巩固“数字贵州”制度优势；福建推出“数字身份证”式地理标志产品数据登记实践，并出台算力基础设施支持措施，在制度创新与要素保障上双向发力，推动地方数字经济发展提质增效。同时，围绕公共数据跨域流通与可信使用，专家提出“身份—安全—追溯”三位一体的治理模式，为数据在安全可控前提下高效流动提供技术与制度思路。

从国家标准到部门规制，从司法确认到地方创新，一系列重大举措共同勾勒出我国数字法治建设不断深化的清晰图景：以标准化夯实底座，以法治化固稳秩序，以专业化培育能力，以实践化激发活力，持续推动数据安全、数据要素流通与数字经济发展在规范与创新的良性互动中迈向更高水平。

《数据安全技术 电子产品信息清除技术要求》强制性国家标准获批发布

原载：“网信中国”微信公众号

2025 年 12 月 2 日，中央网信办提出并归口的《数据安全技术 电子产品信息清除技术要求》强制性国家标准由国家市场监督管理总局、国家标准化管理委员会批准发布，将于 2027 年 1 月 1 日起正式实施。随着数字经济快速发展，手机、电脑等电子产品更新换代频率加快，二手电子产品流通体量日益庞大，然而在流通环节中，由于信息清除不彻底导致的数据泄露风险日益凸显，直接影响社会公共利益和个人信息安全。为落实国务院印发的《推动大规模设备更新和消费品以旧换新行动方案》中关于“出台手机、平板电脑等电子产品二手交易中信息清除方法国家标准”的相关要求，中央网信办提出并委托全国网络安全标准化技术委员会组织制定本标准，旨在规范电子产品信息清除技术方法，引导回收经营者建立健全信息清除管理和技术措施，防范二手流通中的数据泄露风险，促进二手电子产品交易行业健康有序发展。

《数据安全技术 电子产品信息清除技术要求》强制性国家标准答记者问

原载：“网信中国”微信公众号

2025 年 12 月 2 日，由中央网信办归口提出并组织制定的《数据安全技术 电子产品信息清除技术要求》（以下简称《技术要求》）强制性国家标准由国家市场监督管理总局、国家标准化管理委员会批准发布，将于 2027 年 1 月 1 日起正式实施。日前，中央网信办有关负责人就《技术要求》有关问题回答了记者提问。

一、问：请介绍一下《技术要求》的出台背景？

答：随着数字经济快速发展，手机、电脑等电子产品更新换代频率加快，二手电子产品流通体量日益庞大。但在流通环节中，由于信息清除不彻底

导致的数据泄露风险日益凸显，直接威胁社会公共利益和个人信息安全。为落实国务院印发的《推动大规模设备更新和消费品以旧换新行动方案》中关于“出台手机、平板电脑等电子产品二手交易中信息清除方法国家标准”的相关要求，有效保障数据安全，中央网信办委托全国网络安全标准化技术委员会组织制定了本标准。《技术要求》旨在规范电子产品信息清除技术方法，引导回收经营者建立健全信息清除管理和技术措施，防范二手流通中的数据泄露风险，促进二手电子产品交易行业健康有序发展。

二、问：请问制定《技术要求》的总体思路是什么？

答：一是坚持通用性与可行性并重。《技术要求》面向广泛的电子产品类型和存储介质，明确了通用的信息清除基本要求，确保技术要求在现有产业实践中可验证、可操作。二是坚持技术与管理相结合。《技术要求》不仅规定了“怎么清”的技术方法，还对回收经营者提出了“怎么管”的过程要求，构建了从技术实现到运营管理的闭环安全体系。三是坚持统筹发展与安全。充分考虑二手电子产品回收及资源再利用的产业模式，在确保用户个人信息被彻底清除、防范隐私泄露的同时，避免设置过高的技术壁垒，通过科学的标准规范促进循环经济各环节的互信机制建立。

三、问：《技术要求》的适用范围是什么？

答：《技术要求》适用于面向境内生产、销售的，具有非易失性存储介质的电子产品。适用主体包括两类：产品制造与服务方，包括电子产品厂商、第三方信息清除功能开发者；流通经营方，主要是对二手电子产品进行信息清除的回收经营者。《技术要求》涉及的产品范围广泛，主要包括手机、平板、笔记本电脑、台式机电脑、智能穿戴设备、办公设备。需要说明的是，涉及国家秘密的电子产品信息清除，需遵照国家保密相关规定执行。

四、问：《技术要求》中提到的“信息清除”与普通的删除有什么区别？核心技术要求是什么？

答：普通的删除或恢复出厂设置往往只是将数据标记为无效，数据本身仍可能残留在存储介质中。《技术要求》所指的“信息清除”是对存储介质中的数据进行技术处理，使其不可逆且无法被访问或恢复。《技术要求》提出了两种核心技术方法。数据覆写，将固定或随机的无含义数据写入电子产品，覆盖与用户数据有关的每个存储单元。对于磁介质，要求覆写至少 3 次且包含 1 次随机数覆写；对于半导体介质，要求至少覆写 1 次。块擦除，针对半导体介质，通过调用存储介质指令，对物理块执行根本性的擦除操作。

五、问：《技术要求》明确了电子产品厂商哪些具体义务？

答：为从源头保障用户数据安全，《技术要求》规定电子产品厂商应为用户提供内置的信息清除功能。如果无法开发内置功能，厂商必须提供外部信息清除工具，或告知可用的第三方工具信息，或者向用户提供免费的信息清除服务。在执行清除前，必须向用户明示清除范围、方法和影响，并获得用户同意。清除功能需覆盖用户产生的各类文件、通讯录、应用程序及数据、身份鉴别信息、加密密钥等。

六、问：《技术要求》对二手电子产品回收经营者提出了哪些要求？

答：回收经营者是二手电子产品流通过程中的关键安全节点。《技术要求》规定回收经营者必须符合以下要求。提示与授权：回收前主动提示用户进行清除，未经同意禁止访问或留存用户数据。彻底清除：必须使用符合《技术要求》的功能或工具进行清除。若产品损坏无法使用软件清除，则必须对存储介质进行物理销毁。验证与留痕：在销售前必须对清除效果进行验证，未清除用户数据的产品禁止再销售和运输出境。同时，要建立档案，对清除操作和验证结果进行记录，留存时间不少于 3 年。

七、问：如何确保《技术要求》的有效实施？

答：《技术要求》作为强制性国家标准，不仅是技术规范，也是法律法规落地的支撑。《技术要求》配套支撑《网络安全法》《数据安全法》《个

人信息保护法》《消费者权益保护法》等法律法规落地。中央网信办将会同市场监管总局等部门，依据本标准制定实践指南，以产品目录形式推进实施，督促检查厂商和回收经营者落实情况，并指导第三方机构建设检测工具和公共服务平台，为消费者和企业提供清除效果验证和查询服务，建立行业互信。

八、问：关于《技术要求》正式施行时间的考虑？

答：考虑到目前市场上电子产品种类繁多、形态复杂，且二手流通体量大，相关企业对现有产品进行适配改造、建立相应的管理体系需要一定的时间周期。为确保标准平稳落地，经充分调研和试点验证，设定自《技术要求》发布之日起 13 个月的过渡期，于发布一年后正式实施，给予企业充足的准备时间。

国家发展改革委 国家数据局 教育部 科技部 中共中央组织部关于加强数据要素学科专业建设和数字人才队伍建设的意见

原载：“国家数据局”微信公众号

国家发展改革委 国家数据局 教育部 科技部 中共中央组织部 关于加强数据要素学科专业建设和数字人才队伍建设的意见

发改数据〔2025〕1425 号

各省、自治区、直辖市及新疆生产建设兵团发展改革委、数据管理部门、教育厅（教委）、科技厅（局），部属各高等学校、部省合建各高等学校，各省、自治区、直辖市及新疆生产建设兵团党委组织部：数据要素学科专业建设和数字人才队伍建设，承担着培养深化数据要素市场化配置改革和数据赋能人工智能高质量发展所需各类人才的重大使命，是统筹推进数字中国、数字经济、数字社会规划和建设的重要基础。为加强数据要素学科专业建设和数字人才队伍建设，建立数据领域科技发展、国家战略需求牵引的学科专业设置调整机制和人才培养模式，激活数据要素赋能新质生产力的创新引擎作用，促进数据领域教育链、人才链与产业链、创新链融合发展，现提出如下意见。

一、以国家战略为牵引，健全数据要素学科专业

（一）优化学科专业设置。教育部门与数据管理部门加强数据要素相关学科专业建设，支持有条件的学位授予单位建设数据科学与工程、数字经济与管理等数据要素相关学科专业，引导鼓励有条件的数据企业、研究机构积极参与。建立健全数据要素相关学科专业本硕博衔接的人才培养机制。支持职业院校根据产业发展需要，及时动态调整数据相关专业，研究增设数据采集清洗、数据标注、数据合规、数据运营等贴近市场需求的相关专业。

（二）支持分层分类建设。支持有条件的综合性高校建设数字学院，整合校内相关学科资源。支持理工类、财经类、政法类、传媒类、艺术类等特色高校，加强数据技术、数据分析、数据安全、数字经济、数字金融、数字管理、数字法学、数字治理、数字传媒、数字艺术等优势专业建设。支持有条件的高校面向数据产业发展急需的知识和技能要求，开设数字贸易与商务、数字媒体艺术、数字政府治理、数据安全、数智化供应链管理、健康医疗大数据、数据中心智慧运维、国际数据治理等“微专业”。鼓励有条件的省份因地制宜建设数据相关院校，指导职业院校增设特色专业。

（三）建强核心教学要素。加快数据要素相关学科专业课程教材体系建设，推出一批特色优秀教材，支持具备条件的高校组织开展教师教学能力培训。支持高校按规定聘请行业专家开展协同育人，支持企业、研究机构和政府机关等与高校开展项目合作和教师实践锻炼等。数据要素相关教学指导委员会要充分发挥作用，切实履行好研究、咨询、指导、评估和服务职能，注重听取行业专家意见建议。

二、以产业发展为导向，推进数据行业职业教育

（四）打造产教融合生态。建立健全政府统筹、行业指导、企业参与的数据行业职业教育体制机制，研究组建全国数据职业教育教学指导委员会。鼓励各地以产业园区为基础，打造兼具人才培养、创新创业、促进数据产业高质量发展功能的数据行业市域产教联合体。支持龙头企业和高水平高等学校、职业院校牵头，组建行业组织、学校、科研机构、上下游企业等共同参与的数据行业跨区域产教融合共同体。研究制定数据要素从业人员能力要求国家标准。

（五）推动教育教学改革。鼓励数据企业参与职业院校教育教学，共同开展学生培养、技术研发、

产品创新、成果转化，共建“校中厂”“厂中校”实训基地。加快数据行业“双师型”“工学一体化”教师队伍建设，落实教师企业实践规定，推动企业导师到职业院校从教，支持高水平职业院校和龙头企业共建教师培训基地。加强数据行业人才需求分析预测，实施数据相关专业就业跟踪计划。鼓励职业院校学生设计数据要素开发利用相关项目，参加世界职业院校技能大赛相关赛道比赛。

（六）丰富课程教材资源。支持数据企业、行业协会商会与职业院校共同建设一批基于真实应用场景的数字课程，开发一批满足实操需求的工作手册式教材，形成一批可复制可推广的项目教学案例。支持职业院校建设数据相关专业教学资源库，探索建立数据相关专业教学资源库全域共享机制，逐步实现全覆盖。建立“赛课联动”机制，推动竞赛成果转化为教学资源。鼓励各类专业增设数据课程内容，助力传统行业智改数转网联。

三、以有组织科研为支撑，繁荣数据领域学术研究

（七）加强科研组织建设。加快数据领域学术共同体和数字人才梯队建设，推动成立数据领域科技社团。开展高层次数字人才培养行动，做好国家重大人才工程项目在数据领域的落地衔接。鼓励有条件的学术期刊开设数据研究专栏，支持建设高水平数据学术期刊，畅通数据要素理论方法、技术工具和开放数据集等高质量成果发表渠道。依托数字中国建设峰会、中国国际大数据产业博览会等平台，定期组织数据领域学术交流，集中展示宣传前沿技术、优秀著作等成果。

（八）加快主攻方向研究。瞄准数据要素市场化配置改革重大问题，系统开展数据领域战略研究。聚焦数据产权、定价、交易等关键问题，深入开展数据要素基础理论和政策法律研究。紧跟人工智能、区块链、隐私保护计算等前沿技术发展趋势，深入开展数据基础共性理论和技术研究。围绕智能制造、交通运输、金融服务、医疗健康等重点行业和领域，突出数据应用技术研究。构建立足实践的中国数据要素自主知识体系和科学研究体系，为数字中国高质量发展提供理论支撑。

（九）夯实科学数据基础。培养一批跨学科、跨专业的数据工程团队，开展科学数据资源采集生产、加工整理和开放共享，打造一批数据资源丰富、权威性强、有国际引领力的科学数据库。打破创新主体间“数据孤岛”和科研人员“用数”壁垒，推动科学数据与产业数据开放共享、深度融合，以国家科学数据中心等国家级科创平台为主体，加快建设科技领域数据基础设施和高质量数据集，为人工智能驱动的科学研究注入数据新动能。

四、以应用场景为载体，促进数据领域产学研用协同

（十）建设典型应用场景。推动数据领域科技创新与产业创新深度融合，构建企业主导的产学研用协同创新体系，建设一批数字人才培养典型应用场景。强化企业在应用场景构建、技术需求识别、成果落地实施等方面的主导作用，支持高校、研究机构、科技社团等深入场景前沿，加快培养一批复合型、创新型、实战型数字人才。探索技术专利联合开发，推动各方共享知识产权收益，加速技术市场化。鼓励地方利用算力券、模型券、数据券等方式，在算力、算法、数据等方面提供便利和优惠。

（十一）创新协同培养模式。支持具备条件的高校与企业、研究机构和学会协会商会等共建数字领域专业特色学院，以应用场景为牵引，打造一批核心课程、核心教材、核心师资团队和核心实践项目，积极开展国际交流合作，加强拔尖创新人才培养。支持数字中国建设综合试点、数字经济创新发展试验区、数据要素综合试验区、数据产业集聚区试点，探索有区位产业优势的数字人才特色培养项目。鼓励高校建设数据要素交叉学科平台、产教融合研究院等新型组织，深化成果归属、指标分配、工作考核、绩效发放等机制改革。

（十二）打造科技创新平台。按照“揭榜挂帅”模式，依托优势高校建设运营数据要素产教融合创新平台。培育新兴交叉学科方向，打造数字人才培养高地。组建跨学科、交叉型研究团队，加快数据领域关键共性技术、前沿引领技术、现代工程技术、颠覆性技术研发，产出高质量研究成果。鼓励领军企业和创新型企业开放技术平台和应用场景，委托相关国家平台承担各类人才培养项目，增强学生科研能力和职业竞争力，协同培养国家战略急需的复合型应用人才。

国家数据局会同教育部、国家发展改革委、科技部强化组织推进数据要素学科专业建设和数字人才队伍建设，建立常态化工作联系机制，共同营造政产学研协同培养数字人才的良好环境。组织部门加强统筹协调，充分发挥行业主管部门等各方作用，形成工作合力。国家数据局负责跟踪监测实施效果，研究开展数字人才指标监测，适时总结经验

做法，推广典型案例。各省、自治区、直辖市相关部门要根据工作实际认真组织实施，共同推动各项政策措施落地见效。

国家发展改革委
国家数据局
教育部
科技部
中共中央组织部
2025 年 11 月 10 日

专家解读｜加快实施电子产品信息清除标准 以高水平数据安全保障高质量发展

原载：“网信中国”微信公众号

《中共中央关于制定国民经济和社会发展第十五个五年规划的建议》明确要求“加强个人信息保护”。这是党中央面对新形势，对个人信息保护工作的再动员再部署。近日，由中央网信办提出并归口的《数据安全技术 电子产品信息清除技术要求》（以下简称《技术要求》）强制性国家标准经国家市场监督管理总局、国家标准化管理委员会批准发布，补齐了电子产品信息清除的标准短板，对于落实党的二十届四中全会关于加强个人信息保护的重要精神具有意义，也对数据行业的高质量发展具有显著推动作用。

一、《技术要求》是统筹数据行业发展与安全的迫切需要

从《技术要求》制定的起因看，既有直接强化个人信息保护的原因，也有间接畅通二手电子产品回收流通的因素，更有深层次推进信息清除规则全国统一的考虑，意义重大。一是加强个人信息保护、保障高水平安全的迫切需要，据有关部门统计，2024 年我国二手手机交易量超 3 亿部，其中超 60%的用户无法彻底清除存储芯片中的残留数据，导致信息泄露事件频发，《技术要求》的制定，不仅为个人处置二手电子设备提供了明确指引，也为监管部门开展监督检查提供了依据。二是加快全面绿色转型、推动高质量发展的迫切需要，电子产品规范回收利用是实现“双碳”目标的重要途径，但企业、消费者因担心数据泄露不敢进行回收处理，《技术要求》的制定，可消除这些后顾之忧，促进二手电子产品规范回收。三是建设全国统一大市场、构建新发展格局的迫切需要，当前，我国各地各企业对信息清除要求参差不齐，非正规渠道通过规避信息安全成本抢占市场，扰乱市场秩序，《技术要求》的制定，建立了统一市场准入门槛和质量评价体系，有利于推动二手电子产品在全国范围内有序流通。

二、《技术要求》体现了目标导向和问题导向相结合的理念

从《技术要求》具体的内容看，此前发布的《二手电子产品可用程度分级规范》（GB/T 45656-2025）虽提出了“用户信息有效清除”要求，但在用户信息范围、有效清除等方面界定还不够细化。此次《技术要求》给出了清晰的范围、方法和主体，既明确了要解决哪些问题，也给出了要达到什么目标。一是关于“清除哪些数据”，《技术要求》明确给出范围，几乎覆盖了所有用户使用信息终端产生的痕迹信息。二是关于“怎么清除数据”，《技术要求》明确给出数据覆写或块擦除等经过验证的科学方法，并提出具体要求，从而实现数据的彻底清除。三是关于“谁负责清除数据”，《技术要求》明确要求电子产品应为用户提供内置信息清除功能或免费的信息清除工具服务，回收经营者应对二手电子产品进行信息清除，为谁承担信息清除的责任给出了清晰边界。

三、《技术要求》有望催生信息清除新技术新产业新业态

从《技术要求》预期的影响看，除了在加强个人信息保护、加速二手电子产品流通等方面产生积极的预期效果外，同时也有望在信息清除领域开创新赛道、注入新动能、推动新发展。一是将倒逼电子信息产品生产商和二手产品平台商加快信息清除技术的创新，针对 SSD、UFS、HDD 等存储介质，研发指令优化、密钥销毁与物理层快速擦除等技术，进一步提升信息清除效率。二是为数据处理划定明

确合规红线，用户对可验证、可追溯的数据清除需求激增，既让头部回收经营企业加速布局集成化服务，也可能直接催生一批专门的数据清除企业。三是将信息清除从企业自律转为法规与审计要求，推动对可验证、可追溯的第三方认证与报告的需求，可能形成面向平台、企业、工具与人员的分级认证，针对二手电子产品回收经营场景，也可能催生第三方认证与检测、数据擦除即服务、验证平台与工具链、培训与咨询等新业态。

总之，《技术要求》的出台是我国个人信息保护工作的重要里程碑，既是推动安全发展和绿色发展相融合的规则典范，也是推动改革发展稳定相协同的实践创新。

专家解读｜信息清除强制性国家标准发布 为电子产品再流通上好“安全锁”

原载：“网信中国”微信公众号

日前，中央网信办提出并归口的 GB 46864-2025《数据安全技术 电子产品信息清除技术要求》（以下简称《技术要求》）强制性国家标准正式发布。《技术要求》由全国网络安全标准化技术委员会（TC260）制定，旨在落实国务院出台的《推动大规模设备更新和消费品以旧换新行动方案》，明确电子产品彻底清除用户数据的技术方法，解决电子产品在以旧换新、二手交易、废弃回收、翻新维修等二手流通中的数据泄露风险。

一、《技术要求》的制定背景

近年来，随着循环经济的快速发展，大量旧手机、旧电脑、旧硬盘等电子产品进入二手市场流通，但当前产品自带的数据删除功能大多将数据标记为无效，并未彻底清除存储介质的数据，可能被恶意恢复，导致用户数据泄露。据统计十四五期间，我国手机闲置总量达到 60 亿部，但仅有 10%的闲置手机进入二手交易平台流通，其中最主要原因就是消费者担忧信息清除不彻底、存在信息泄露风险，因此保护用户信息、促进二手电子产品流通正是《技术要求》出台的主要目标。

2024 年国务院出台《推动大规模设备更新和消费品以旧换新行动方案》（国发〔2024〕7 号），要求制定“电子产品二手交易中信息清除方法国家标准”，以“推动二手电子产品交易规范化，防范泄露及恶意恢复用户信息”。《技术要求》正是在这一政策部署下制定，主要根据《网络安全法》《数据安全法》《个人信息保护法》等法律法规，旨在明确电子产品信息清除的技术方法和功能要求，规范二手流通中的信息清除活动。

二、《技术要求》的内容和作用

《技术要求》规定了电子产品信息清除的基本要求、功能要求，以及二手电子产品信息清除过程要求，主要适用于面向境内生产、销售的，具有非易失性存储介质的电子产品，也适用于电子产品厂商、第三方开发电子产品信息清除功能，以及回收经营者对二手电子产品进行信息清除。

《技术要求》主要内容包括：**一是规定电子产品信息清除基本要求。**明确信息清除范围应覆盖用户文件、应用程序、通讯录、账号口令、加密密钥等所有用户数据，针对磁介质、半导体介质明确数据覆写、块擦除等清除技术方法；**二是提出电子产品信息清除功能要求。**清除功能可由产品内置功能或外部工具实现，电子产品应为用户提供内置信息清除功能，实在无法开发的，电子产品厂商应提供外部清除工具、可用的第三方工具信息或免费信息清除服务；**三是明确二手电子产品信息清除过程要求。**要求回收经营者必须对二手电子产品进行信息清除，销售前要验证信息清除效果，未清除用户数据的电子产品禁止再销售和运输出境。

《技术要求》的实施将对二手流通行业产生显著作用。一是提供让用户放心的信息清除方法，彻底清除电子产品存储的用户数据，在保护消费者权益的基础上促进二手流通；二是规范二手电子产品流通市场，有效遏制用户信息泄露、恶意恢复、灰色数据交易等风险；三是推动相关方清除责任落地，明确电子产品厂商、第三方厂商、回收经营者等的信息清除相关责任，帮助电子产品信息清除工作真

正落地。

三、《技术要求》的实施与展望

《数据安全技术 电子产品信息清除技术要求》过渡期为 13 个月，将于 2027 年 1 月 1 日起施行。为保障《技术要求》落地实施，全国网安标委秘书处将在主管部门指导下，通过制定系列标准实践指南、支撑建立信息清除检测认证机制、建设信息清除公共服务平台等多种形式，推动形成覆盖循环经济各环节和各相关方的信息清除互信机制和良好生态，助力二手商品流通市场建立用户信息保护体系，为亿万消费者的电子产品上好一把真正的“数据安全锁”。

专家解读｜保护用户隐私数据，助力循环经济发展

原载：“网信中国”微信公众号

随着云计算、大数据、人工智能等技术的迅猛发展，信息已经成为整个社会最重要资产。我国高度重视信息保护工作，在《网络安全法》《数据安全法》《个人信息保护法》中都明确了信息保护的相关要求，包括范围、原则和方法等，为信息保护工作奠定了扎实的基础。但是，这些法律法规更侧重于信息使用过程中的保护，未明确信息设备生命周期结束时，用户应该如何处理和保护用户数据的问题。因此，用户对安全问题的担心也导致社会上二手电子产品交易不畅，更新受阻，循环利用不够，这都制约了社会经济的健康发展。

《数据安全技术 电子产品信息清除技术要求》（以下简称《技术要求》）强制性国家标准补齐了用户使用电子设备更新换代环节个人信息保护的短板，在保护用户数据基础上，规范了信息清除的要求，将有效推动循环经济的发展。

一、电子产品废弃或再利用过程中的用户信息保护问题凸显

当前，我们的工作和生活中使用着大量的电子产品，种类繁多，功能多样，比如手机、手表、手环、电脑、打印机、智能音箱等。因为使用数量大，每年更新换代的电子产品也是海量的。这些电子产品使用过程中产生大量用户数据，很多涉及到隐私，其废弃或再利用过程中存在严重的用户隐私信息泄露的问题。但是，目前在以手机为典型的电子产品废弃或再利用环节还没有明确的用户隐私信息保护标准。个人用户、回收厂家有些会采取恢复出厂设置，删除个人信息等方式进行处理，但缺乏统一的规范要求和技术标准，回收生态中企业或个体工商户处理方式方法各异，亟待规范。

二、《技术要求》立足补齐短板

从个人用户角度来看，《网络安全法》《数据安全法》和《个人信息保护法》等法律构成了用户信息保护的基石和框架，但是具体实现层面，还需要一系列的可操作可执行的标准来进行规范。落实 2024 年国务院印发的《推动大规模设备更新和消费品以旧换新行动方案》，针对大规模电子设备更新和消费品以旧换新中的数据安全问题，制定电子产品信息清除标准非常必要，既能保护电子产品废弃或再利用过程中的用户隐私信息，又能够有效推动循环经济的迅速发展。

三、《技术要求》维护了一个健康可持续发展的生态环境

在循环经济生态中，用户是消费者，电子产品厂商和二手电子产品回收经营者是获利者，用户信息保护的责任理应由他们来承担。相应的，用户在被有效保护的前提下，消费和更新的意愿都会大大提升，这又给经营者提供了巨大的商机。因此，标准制定过程中，既要确保技术措施的精准有效，又要在公平公正的基础上激发各主体积极性。标准要求磁介质类电子产品采用数据覆写方法清除数据，半导体介质类电子产品采用数据覆写或块擦除方法清除数据，兼顾了用户信息保护的安全性与效率。标准对电子产品厂商提出要求，电子产品要为用户提供内置信息清除功能。无法开发内置功能的，电子产品厂商应提供外部信息清除工具或可用的第三方信息清除工具信息，或向用户提供免费信息清除服务。标准对二手电子产品回收经营者提出要求，要对信息清除操作进行记录，确保二手电子产品清除状态可查询和追溯。

四、《技术要求》涵盖已有和未来的全部电子产品

电子产品种类繁多，标准给出了通用定义，采用电子信息技术制造的软硬件设备及其配件，特别强调要具有存储用户数据的功能。这个通用定义意味着现有的手机、打印机、智能音箱等产品和未来的比如智能机器人、AI 终端等产品，都被纳入其中。以往标准只关注存储部件和存储技术发展趋势，但本标准牢牢抓住存储属性，按照失去电源后数据是否保留，将使用非易失性存储介质的电子产品均包含在内，不限制电子产品形态，具有良好的可操作性和前瞻适应性。

五、《技术要求》出台将强有力推动循环经济发展

电子产品信息清除标准是支撑《个人信息保护法》落地的一块重要拼图。作为强制性的国家标准，其涉及产品范围广，社会影响力大。在我国高度重视网络安全和个人信息保护的背景下，《技术要求》在完成信息清除任务的同时，也解决了电子产品循环再利用生态中最棘手的安全问题，打通了制约堵点。随着国务院推动电子产品更新换代相关文件的出台，《技术要求》在夯实个人信息安全保护基础上，将为循环经济快速健康发展提供有力的技术支撑和标准保障。

专家解读｜“身份—安全—追溯”三位一体的数据可信流通模式——解读《基于公共数据跨域流通场景的数据可信追溯安全技术应用案例》

原载：“国家数据局”微信公众号

文｜人民法院信息技术服务中心总工程师 黄国栋

数据流通安全治理工作如何落地实施是业界关注的重点，《关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案》（以下简称《方案》）的发布，推动明晰数据流通安全治理规则。《基于公共数据跨域流通场景的数据可信追溯安全技术应用案例》（以下简称“案例”）作为典型实践，通过系统化的技术架构和合规范式，解决了公共数据跨域流通的核心痛点，为《方案》有效落地提供了可操作的实施路径。

一、打造可信、可控、可溯的数据流通体系

本案例的核心价值在于构建了一套逻辑严密、层层递进的安全治理架构，将《方案》中“安全贯穿数据供给、流通、使用全过程”的要求转化为可操作的治理模型。

（一）建立信任基础：数字身份和规则的一致性

跨域流通的首要障碍是身份互认难和规则协同缺失。案例通过引入身份认证技术，为不同地域、不同机构的参与方提供了统一且不可篡改的身份标识。同时，通过建立跨域数据流通“白名单”机制，从管理层面明确可信交互边界。这一体系有效解决了数据跨域流通场景中的身份信任难题。

（二）确保数据安全：可控的数据开发与利用环境

通过“治理合规核验”环节，确保进入流通的数据均满足合规要求，从源头阻断不合规数据的流入，构建了安全可靠的数据价值释放通道。为破解数据提供方对原始数据失控的顾虑，案例采用“数据沙箱”与“安全多方计算”技术构建安全计算环境，数据仅在隔离环境中进行处理，实现“原始数据不出域”。

（三）全程监督：区块链支持的追溯和合约执行

信任的维系离不开有效的溯源机制。案例契合《方案》“探索数据流通安全审计和溯源机制”的要求，将区块链技术贯穿于数据流通的全生命周期，所有行为日志均上链存证，形成了一条完整的、不可篡改的追溯链。此外，结合“开发—交付—使用”全流程监管机制，实现对数据流通中的行为全程可溯、违规可查。通过将数据使用约束条件代码化为数字合约，由系统实现自动执行与实时监督，可对违规操作进行自动预警与阻断。

二、构建自证、确责、互信的治理全新范式

案例通过技术上的整合创新和数据流通治理范式的重构，落实了“三法两条例”及《方案》对明确权责、防范风险的要求。

（一）从被动检查到主动证明

传统依赖外部审计的合规模式存在成本高、时效差等局限，案例通过全流程上链存证，使每个流通环节都具备自证能力，促使参与各方主动遵循规则，让“合规”成为一种习惯，从而构建了一个“合规即服务”的低成本、高效率良性生态。

（二）从责任模糊到精准归责

针对复杂流通环境中责任难认定的问题，案例基于区块链存证的交易凭证，精确记录数据流转的时间、主体、授权范围与使用目的，为安全事件调查与纠纷解决提供客观依据，有效落实《方案》中“完善数据流通安全责任界定机制”的要求。

（三）从信任缺失到协同共治

案例为数据供需双方建立了一个低成本的信任环境，通过技术保障数据“可用不可见、可控可计量”。数据提供方因数据安全可控而“敢给”，数据接收方因流程透明可溯而“放心用”，数据流通从“你得我失”转变为“互利共赢”。这种信任机制的设计，响应了《方案》中“推动数据要素市场化价值化”的要求。

三、案例启示

案例所提炼出的“用统一身份建立互信，用安全环境释放价值，用全程追溯保障权责”做法，具有显著的普适性与可复制性。这一体系通过技术与制度的协同创新，为公共数据跨域流通筑牢“安全底座”、搭建“信任桥梁”，提供了可推广的实践样板。随着此类实践在更广范围内的复制推广，将促进数据要素在更高水平上实现安全有序流通，逐步构建起“规则明晰、产业繁荣、多方协同”的数据流通安全治理新生态。

地方动态｜《贵州省大数据发展应用促进条例》自 2026 年 1 月 1 日起施行

原载：“国家数据局”微信公众号

贵州省人民代表大会常务委员会

公 告

（2025 第 17 号）

《贵州省大数据发展应用促进条例》已于 2025 年 12 月 3 日经贵州省第十四届人民代表大会常务委员会第二十次会议修订通过，现予公布，自 2026 年 1 月 1 日起施行。

贵州省人民代表大会常务委员会

2025 年 12 月 3 日

贵州省大数据发展应用促进条例

（2016 年 1 月 15 日贵州省第十二届人民代表大会常务委员会第二十次会议通过　2025 年 12 月 3 日贵州省第十四届人民代表大会常务委员会第二十次会议修订）

目 录

第一章　总则
第二章　算力基础
第三章　数据资源
第四章　应用赋能
第五章　产业发展
第六章　促进措施
第七章　安全管理
第八章　法律责任
第九章　附则

第一章　总则

第一条　为了深化大数据发展应用，运用大数据促进经济发展、完善社会治理、提升政府服务管理能力、服务改善民生，培育壮大战略性新兴产业，发展数字生产力，做强做优数字经济，发挥引领支撑作用，推进数字经济发展创新区建设，加快建设数智贵州，根据有关法律、行政法规的规定，结合本省实际，制定本条例。

第二条　本省行政区域内大数据发展应用促进及其相关活动，应当遵守本条例。

本条例所称大数据，是指以容量大、类型多、速度快、精度准、价值高为主要特征的数据集合，

是对数量巨大、来源分散、格式多样的数据进行采集、存储和关联分析，发现新知识、创造新价值、提升新能力的新一代信息技术和服务业态。

第三条 大数据发展应用促进工作应当坚持中国共产党的领导，坚持统筹规划、创新引领，政府引导、市场主导，应用牵引、数据赋能，公平竞争、安全有序，共享开放、协同高效的原则。

第四条 本省促进大数据发展应用，应当坚持算力、数据、应用、产业协同联动，以算力为基础、数据为关键要素、应用为赋能途径、产业为发展重点，加快建设数智产业集群，打造算力高地、数据高地，引领支撑社会治理转型、生活服务转型、产业升级转型，赋能经济社会高质量发展。

第五条 本省坚持总体国家安全观，统筹大数据发展和安全，建立完善促进算力、数据、应用、产业协同发展的制度体系。

第六条 县级以上人民政府负责本行政区域内大数据发展应用工作，将大数据发展应用纳入本行政区域国民经济和社会发展规划，建立完善促进大数据发展应用协同推进机制，协调解决工作中的重大问题。

县级以上人民政府数据主管部门负责统筹推进、协调、督促大数据发展应用工作，推进数据要素市场化配置改革，统筹数字经济、数字政府、数字社会建设，推动人工智能发展和应用。

县级以上人民政府有关部门在各自职责范围内，负责承担本部门的数据管理、数据应用、数据安全等工作，推动本行业、本领域的大数据发展应用。

第七条 省、市州人民政府数据主管部门应当会同有关部门，按照遵循规律、立足实际、适度超前、合理布局、绿色集约、资源共享的原则，编制本级大数据发展应用规划，报同级人民政府批准后公布实施。

县级以上人民政府有关部门编制本部门、本行业大数据相关规划的，应当与大数据发展应用规划相衔接。

第八条 县级以上人民政府及有关部门应当加强大数据发展应用宣传教育，提高全社会大数据发展应用意识和能力。

第二章 算力基础

第九条 本省坚持存算一体、智算优先，推动通用计算、智能计算、超级计算等多元算力资源协调发展，提高数据中心计算力和存储力，扩大算力规模，提升算力能级水平，打造面向全国的算力保障基地。

鼓励算力相关企业在贵安数据中心集群建设智算中心，支持已建智算中心扩容升级。

第十条 省人民政府有关部门应当推动数据中心绿色低碳发展，建立数据中心绿电供给机制，支持采用新型节能技术和绿色建筑技术、利用本地气候和地形地貌等方式降低数据中心能耗。

鼓励数据中心参与绿色电力交易，通过认购可再生能源、绿电绿证等方式，降低用能成本。

第十一条 省人民政府数据主管部门会同能源等有关部门建立算电协同机制，推动算力设施与电力设施协同规划、联动建设和联合运行，协调供电企业加强供电设施建设和改造升级，保障数据中心合理用电需求。

鼓励供电企业通过错峰供电、负载调整、算电协同等方式保障数据中心电力供应高效稳定，降低用电成本。

第十二条 通信管理部门应当统筹推进算力网络建设，推动高速直连网建设。鼓励和支持通信运营企业部署应用先进网络技术，完善超高速光纤宽带网络和移动通信网络，优化互联网骨干网、城域网和接入网，提升网络性能和服务能力,降低网络通信资费。

第十三条 省人民政府数据主管部门应当强化算力品牌打造和宣传推介，加强与其他全国一体化算力网络国家枢纽节点及其他省（自治区、直辖市）的算力供需对接和协同联动，制定政策措施降低用算成本。

鼓励和支持算力运营企业开展算力服务模式创新，拓展业务场景，满足多元市场需求，提升算力服务普惠易用水平。

第三章 数据资源

第十四条 省人民政府数据主管部门应当加强数据统筹管理，按照国家和省的有关规定制定数据分类分级基本规则，建立数据资源目录编制规范。

省人民政府行业主管部门按照国家和省的有关规定制定本行业数据分类分级具体规则，编制本行业数据资源目录，促进数据分类分级管理。

县级以上人民政府有关部门应当明确数据专员，加强本部门公共数据归集治理、共享开放、开发利用、授权运营及安全管理等。

鼓励企业建立首席数据官制度，健全数据资源管理机制。

第十五条 省人民政府数据主管部门应当按照国家有关规定动态编制高频公共数据清单，各有关部门应当依法依规向同级数据主管部门物理归集高频公共数据，并归集中低频公共数据，强化数据动态更新和质量管理。

省人民政府数据主管部门应当推进人口、法人、宏观经济、电子证照、地理空间信息等基础数据库建设和动态更新，推动基础数据库依法共建共享。

第十六条 县级以上人民政府及有关部门应当按照有关要求，制定公共数据共享开放和开发利用的措施，在维护国家数据安全、保护个人信息和商业秘密前提下，依法依规共享开放和开发利用公共数据，推动公共数据价值释放。

上级部门应当根据下级部门履行职责的需要，在确保数据安全的前提下，及时、完整回流业务信息系统收集和产生的下级部门的公共数据。

下级部门获得回流的公共数据后，应当按照履行职责的需要共享、使用，并保障相关数据安全。

第十七条 县级以上人民政府数据主管部门应当会同有关部门推进数据基础设施建设，面向社会提供数据采集、汇聚、传输、加工、流通、利用、运营、安全服务等。

推动建设可信数据空间，构建跨行业、跨区域、跨领域、跨主体的数联网服务体系。

第十八条 鼓励和引导企业强化数据资源体系建设，开展数据采集治理、合规登记、开发利用、流通交易，推动数据资产化、资本化。

鼓励行业龙头企业带动上下游企业共建行业可信数据空间，促进大中小企业数据共享共用。

第十九条 对承载个人信息的数据，按照个人授权范围依法依规采集、持有、托管和使用，规范对个人信息的处理活动。处理个人信息应当符合法律、行政法规的规定。

第二十条 省人民政府数据主管部门应当建立健全培育数据市场的政策措施，完善数据流通交易规则，指导、推动数据市场建设。

鼓励和引导数据流通交易主体在依法设立的数据交易场所进行数据交易。

第四章 应用赋能

第二十一条 县级以上人民政府及有关部门应当推动数智技术在经济调节、市场监管、社会治理、公共服务、生态环境保护等领域中的创新应用，构建面向政府治理、企业服务、个人服务的数智化应用体系，推动治理流程优化、模式创新，提升数智化治理能力。

省人民政府数据主管部门推进云、网、平台、终端等共性支撑能力集约建设，按照省级统筹原则开展全省统一的贵州政务云建设，集约提供政务云服务，加强一体化政务云资源管理和调度，推进政务信息系统整合。

县级以上人民政府数据主管部门应当建立政务信息化项目建设集约共享机制，按照统一规划、共建共享、业务协同、安全可控的原则，统筹负责本级政务信息系统项目建设全流程管理。

第二十二条 省人民政府及有关部门应当加强政务办公一网协同建设，提升跨部门业务协同联动智能化水平。

第二十三条 县级以上人民政府及有关部门应当加强政务服务一网通办建设，推动政务服务办件数据共享和流程再造，增强服务的便捷性。

第二十四条 支持有条件的地区加强城市运行一网统管建设，提升智能感知、数据处理、分析研判、协同指挥和科学治理水平，推进城市全域数字化转型。

县级以上人民政府及有关部门推动数字乡村建设，提升乡村公共服务、乡村治理等的数字化水平。

第二十五条 县级以上人民政府应当推动城市公共服务一网通享，加快推进智慧教育、智慧医疗、智慧交通、智慧养老、智慧文旅等建设，促进数字公共服务普惠化，普及数字生活智能化。

鼓励和支持市场主体在生活服务领域创新数智化服务应用，提供个性化、特色化的产品和服务。

第二十六条 县级以上人民政府及有关部门应当推动大数据和文化融合，加强公共数字文化资源建设，丰富优质数字文化产品供给，提升数字文化服务能力。

第二十七条 县级以上人民政府及有关部门应当推动数字生态文明建设，优化完善生态环境监测网络和智能监管体系，提升生态环境智慧治理能力。

第二十八条 县级以上人民政府应当促进实体经济和数字经济深度融合，建立数据主管部门统筹、行业主管部门主推的数字化转型推进机制，创新多元投入机制，促进传统产业数字化智能化转型。

县级以上人民政府数据主管部门应当培育数字化转型服务商，引导企业开放数据，推动构建企业数字化转型服务体系。

县级以上人民政府行业主管部门应当建立完善政策措施，鼓励和引导企业在研发设计、生产加工、经营管理、销售服务等环节开展数字化智能化转型，发展协同制造、个性化定制等新模式，推进产业链数字化协同改造。

第二十九条 县级以上人民政府数据主管部门建立健全大数据应用场景开放机制，征集和发布应用场景需求，促进应用场景供需对接。

县级以上人民政府行业主管部门应当按照大数据应用场景开放机制要求，采取措施推动开放本行业应用场景，促进场景培育、实施和示范性场景推广。

鼓励和支持市场主体主动发掘市场需求，探索拓展新场景，参与应用场景开发、建设和运营。

第五章 产业发展

第三十条 省人民政府应当统筹布局、系统推进算力产业、数据产业、人工智能产业、电子信息产业等数字产业发展，强化数字产业园区和创新基地建设，培育数字产业集群，提升数字产业整体竞争力。

第三十一条 引导和支持以智算为重点的算力产业创新发展，发挥智算中心建设牵引作用，促进算力基础软硬件、算网建设与平台、算网服务与应用等上下游产业协同发展，培育算力产业生态。

鼓励和支持数据中心运营主体在本省设立制造基地、区域总部和运营中心。

第三十二条 引导和支持以高质量数据集为重点的数据产业创新发展，建设数据标注产业基地，壮大数据标注产业，培育数据资源企业、数据技术企业、数据服务企业、数据应用企业、数据安全企业、数据基础设施企业和第三方专业服务机构，丰富数据产品和服务。

鼓励和支持市场主体依法开展数据采集、存储、治理、分析、流通、应用等活动，拓展数据服务新模式、新业态。

第三十三条 引导和支持以行业大模型为重点的人工智能产业创新发展，引进人工智能大模型开发和应用服务商，培育人工智能行业大模型产品，推进人工智能在科学技术、产业发展、消费提质、民生福祉、治理能力等领域的应用。

鼓励和支持人工智能大模型开发和应用服务商在本省落地发展，推动人工智能大模型研发与应用，创新人工智能产品与服务。

第三十四条 引导和支持以数智化为特色的电子信息产业创新发展，培育壮大电子元器件、智能终端制造、软件和信息技术服务等产业，加强产业链上下游对接配套，促进产业集聚发展。

鼓励和支持企业加大电子信息产业技术的研发投入，加强产品推广，推动服务升级。

第三十五条 县级以上人民政府及其有关部门应当按照国家规定，引导和支持数字产业龙头企业、高新技术企业，以及科技型中小企业和专精特新中小企业发展，培育多层次、递进式的数字产业企业

梯队，形成以行业龙头为引领、大中小微企业协同发展格局。

第六章 促进措施

第三十六条 省、市州人民政府设立大数据发展专项资金，县级人民政府根据需要设立大数据发展专项资金，用于促进大数据发展应用。

统筹用好产业基金引导社会资本投资大数据发展应用。

鼓励金融机构创新金融产品，完善金融服务，支持大数据发展应用；鼓励社会资金采取风险投资、创业投资、股权投资等方式，参与大数据发展应用；鼓励和支持符合条件的大数据企业依法进入资本市场融资。

第三十七条 县级以上人民政府应当根据国土空间规划和大数据发展应用规划，保障大数据项目建设用地；对新增大数据项目建设用地，依法列入土地利用年度计划。

第三十八条 县级以上人民政府及有关部门应当结合本行政区域大数据发展应用重点领域，明确大数据人才引进培养目标及措施，完善人才激励机制，将提高大数据发展应用能力纳入教育培训体系，积极引进、培养高层次人才，并为大数据人才开展教学科研和创业创新等活动创造条件。

鼓励高等学校、科研机构和企事业单位以设立研发中心、技术持股、期权激励、学术交流、产业合作等方式，充分发挥大数据人才资源作用。

鼓励高等学校、科研机构、职业学校与企业合作，建立大数据科技研发、教育实践、创新创业和实训基地，开展大数据发展应用技术研究。

支持高等学校、职业学校大数据学科建设，完善大数据相关课程。

第三十九条 县级以上人民政府应当支持大数据关键技术、解决方案、重点产品、配套服务、商业模式创新和应用研究，促进大数据技术创新，推动成果转化。

第四十条 省人民政府应当组织有关单位积极开展大数据发展应用相关标准研究，推动国家技术标准创新基地建设，建立完善大数据发展应用标准体系。

鼓励和支持企业、高等学校、科研机构、大数据行业组织等参与大数据发展应用相关国家标准、地方标准、行业标准的制定。

第四十一条 政府投资的大数据工程应当进行需求分析，科学确定建设内容和投资规模，严格项目审批程序，并按照有关规定加强项目全过程管理，提高政府投资效益。

公共机构已建、在建信息系统应当依法实现互联互通，不得新建孤立的信息系统，不得设置妨碍互联互通的技术壁垒。

第四十二条 利用中国国际大数据产业博览会等平台，加强大数据相关企业、产品、服务品牌宣传推广，促进对外交流合作。

第七章 安全管理

第四十三条 开展大数据发展应用相关活动，应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

第四十四条 网信部门负责统筹协调网络数据安全和相关监督管理工作。

公安机关、国家安全机关依照法律、法规的规定，在各自职责范围内承担数据安全监督管理职责，依法防范和打击危害数据安全的违法犯罪活动。

数据主管部门在具体承担数据管理工作中履行相应的数据安全职责。

第四十五条 各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责。

各有关主管部门承担本行业、本领域数据安全监管职责，依照法律、法规的规定，采取相应措施保障数据安全。

第四十六条 数据处理者开展数据处理活动，应当依照法律、法规的规定，建立健全全流程数据安全管理制度，按照要求定期开展风险监测、风险评估和应急演练，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在

网络安全等级保护制度的基础上，履行数据安全保护义务。

重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。

第四十七条 任何单位和个人有权对危害数据安全的行为向有关部门投诉、举报。收到投诉、举报的部门应当及时依法处理。有关部门应当对投诉、举报人的相关信息予以保密，保护投诉、举报人的合法权益。

第八章 法律责任

第四十八条 国家机关及其工作人员未按照本条例履行职责或者有其他滥用职权、玩忽职守、徇私舞弊行为，尚不构成犯罪的，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。

第四十九条 违反本条例规定的行为，法律、行政法规有处罚规定的，从其规定。

第九章 附则

第五十条 本条例下列用语的含义为：

（一）公共数据，是指各级政务部门、具有公共管理和服务职能的组织及其技术支撑单位，在依法履行公共事务管理职责或者提供公共服务过程中收集、产生的数据；

（二）企业数据，是指各类市场主体在生产经营活动中采集、产生的不涉及个人信息和公共利益的数据；

（三）公共机构，是指全部或者部分使用财政性资金的国家机关、事业单位和团体组织。

第五十一条 本条例自 2026 年 1 月 1 日起施行。

福州市首发地理标志产品数据知识产权登记证书 福州脱胎漆器有了“数字身份证”

原载：“法治福州”微信公众号

近日，福建省沈绍安漆艺博物馆正式获颁全市首张地理标志产品数据知识产权登记证书，标志着福州在“地理标志+数据知识产权”融合探索中迈出了关键一步，也为福州脱胎漆器等传统工艺的现代化转型打开了新空间。

什么是数据知识产权？

它指的是数据处理者对经过合法获取、规范处理，并具有实用价值与智力成果属性的数据集合所享有的权益。这一机制遵循依法合规、自愿登记、安全高效的原则，贯穿数据登记、交易流通与权益保护各环节，可在质押融资、司法维权、技术创新乃至商业化开发中发挥重要作用。

福州山海相连，文脉绵长，物产丰饶，拥有丰富的地理标志资源。目前全市已注册 58 件地理标志，包括闻名全国的“连江鲍鱼”，以及承载百年匠心的“福州脱胎漆器”等传统工艺瑰宝。在数字经济浪潮下，如何让这些沉淀着历史与文化的地理标志“活”起来、“新”起来？福州创新探索“地理标志+数据知识产权”路径，推动传统产业与数据要素深度融合，为老技艺注入新动能。在此背景下，福州启动全省漆器类首批“地理标志+数据知识产权”登记工作，率先以“福州脱胎漆器”为试点，在市、区两级市场监管部门的共同指导下，由福州市数字产业互联科技有限责任公司与福建省沈绍安漆艺博物馆等机构携手，系统整合漆器在藏品、学术、文化传承与建设四大维度的核心数据资源，形成法律认可、技术可信的数据集合。这张证书不仅是法律意义上的权益凭证，也是一张可溯源、防篡改的“数字身份证”。其背后依托的是区块链存证哈希技术，确保登记信息真实可信。使用手机扫描证书上的二维码，即可查看详细的数据来源、应用场景、算法规则等信息，为企业行使数据权益提供了初步法律凭据。更重要的是，它将原本散落的产地、工艺、品质等核心数据，转化为可估值、可融资的数据资产，可进一步探索质押融资等新型商业路径。数据可应用于学术研究、文化推广与品牌建设等多个场景，未来可通过精准分析市场表现与用户偏好，赋能传统品牌拓展影响力，全面释放数据要素价值。作为全国唯一专注于漆艺的主题博物馆，福建省沈绍安漆艺博物馆长期以来致力于展现中国漆艺尤其是福州漆艺的独特魅力。馆长施丽玲认为，脱胎漆器的传承与发展，未来必然与数字

技术紧密相连。此次登记实现了从传统工艺保护到数字资产管理的跨越，为后续文化数据的开发与应用奠定了坚实基础，也体现了福州在传统文化数字化保护方面的先行示范意义。

福州市市场监督管理局相关负责人表示：这不是简单的“登记”，而是构建了一套将地理标志特色转化为数据资产优势的确权、用权、维权机制。接下来，福州将继续拓展该模式，逐步推广至“福州茉莉花茶”“连江鲍鱼”等更多特色产业，让数据知识产权成为推动地方经济发展的新引擎。

国家能源局印发重要管理办法

原载：“中国能源报”微信公众号

12 月 12 日，国家能源局印发的《能源行业数据安全管理办法（试行）》指出，能源数据处理者开展数据处理活动，应建立健全数据安全管理制度，明确数据全生命周期各环节的管理要求；定期组织开展能源行业数据安全知识和技能教育培训。能源行业重要数据、能源行业核心数据的处理者应建立数据安全工作体系，加强人员和经费保障，并配合有关部门开展监督检查工作。

国家能源局关于印发《能源行业数据安全管理办法（试行）》的通知

（国能发规划规〔2025〕108 号）

各有关单位：

为落实《中华人民共和国数据安全法》等法律法规，我局制定了《能源行业数据安全管理办法（试行）》，现予印发，自 2026 年 7 月 1 日起施行。

国家能源局

2025 年 12 月 8 日

能源行业数据安全管理办法（试行）

第一章 总 则

第一条 为规范能源行业数据处理活动，加强数据安全管理，防范数据安全风险，促进数据开发利用，保护个人、组织的合法权益，维护国家安全和发展利益，根据《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国能源法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》等法律法规，制定本办法。

第二条 本办法适用于在中华人民共和国境内开展能源行业数据处理活动及其安全监督管理。

能源数据处理者开展涉及国家秘密或由其汇聚关联后属于国家秘密事项的能源行业数据处理活动时，应遵守《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

第三条 本办法所称数据，是指任何以电子或者其他方式对信息的记录。

本办法所称能源行业数据，是指在开展能源活动中收集和产生的数据。能源活动主要包括与能源相关的规划、设计、建设、生产、储运、消费、科研等。与城市燃气、供热、加油站等能源活动相关的数据应遵守有关主管部门规定。

本办法所称能源数据处理者，是指开展能源行业数据处理活动的能源行业各类单位。能源行业数据处理活动包括能源行业数据的收集、存储、使用、加工、传输、提供、公开、删除等。

本办法所称数据安全，是指通过采取必要措施，确保能源行业数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

第四条 根据数据重要性、精度、规模、安全风险等，能源行业数据分为一般、重要、核心三级。

能源行业重要数据是指特定领域、特定群体、特定区域或达到一定精度和规模的能源行业数据，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。仅影响组织自身或公民个体的能源行业数据，一般不作为能源行业重要数据。

能源行业核心数据是指对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的能源行业重要数据，一旦被非法使用或共享，可能直接影响政治安全。主要包括：关系国家安全重点领域的数据，关系国民经济命脉、重要民生和重大公共利益的数据，经评估确定的其他能源行业数据。

能源行业一般数据是指能源行业重要数据、能源行业核心数据之外的其他能源行业数据。

第五条 鼓励能源数据处理者积极开展能源行业数据创新应用，在保障安全合规的情况下促进数据开发利用。

第二章 能源行业数据安全基本职责

第六条 在国家数据安全工作协调机制统筹协调下，国家能源局负责能源行业数据安全监督管理，督促指导各省、自治区、直辖市和新疆生产建设兵团能源主管部门（以下简称省级能源主管部门）开展数据安全监督管理，督促指导国务院国资委管理的能源企业（以下简称能源央企）和国家能源局指导监管的全国性能源行业协会依法依规履行能源数据处理者责任义务，组织制定和发布能源行业数据分类分级标准规范，审核并确定能源行业重要数据目录，向有关部门提出核心数据目录建议并实行动态管理，加强能源行业数据安全监测预警和应急处置能力建设。

第七条 省级能源主管部门负责对本地区能源行业数据处理活动和安全保护进行监督管理，督促指导本地区能源数据处理者（含能源央企在本地区的各级子公司、控股企业）依法依规履行能源数据处理者责任义务，按照能源行业数据分类分级标准规范，编制并按年度更新报送本地区能源行业重要数据目录，开展本地区能源行业数据安全监测预警、信息报送、制定应急预案、开展应急处置等工作。

第八条 能源数据处理者应依法依规履行数据安全保护责任义务。能源行业重要数据和能源行业核心数据的处理者对自身的数据安全负主体责任，应明确数据安全负责人和管理机构，本单位法定代表人或者主要负责人是数据安全第一责任人，分管数据安全的领导是直接责任人。能源央企负责对其各级子公司、控股企业的数据处理活动和安全保护进行监督管理。

第九条 能源数据处理者应依照能源行业数据分类分级标准规范，识别并编制本单位能源行业重要数据目录，按照数据载体所在地省级能源主管部门要求报送重要数据目录。能源央企各级子公司、控股企业编制的能源行业重要数据目录，应按照数据载体所在地省级能源主管部门和能源央企总部要求分别报送。

重要数据目录报送内容包括但不限于数据类别、级别、规模、精度、来源、载体、适用范围、对外共享、跨境传输、安全情况及责任单位等数据字段信息，不包括数据内容本身。

第十条 省级能源主管部门、能源央企分别负责汇总审核本地区、本企业的能源行业重要数据目录，并报送国家能源局。对按程序确认为能源行业重要数据和能源行业核心数据的，省级能源主管部门、能源央企应及时告知能源数据处理者。

第十一条 上一次报送重要数据目录后，能源行业重要数据、核心数据的级别、责任主体情况、数据处理情况、数据安全情况内容发生重大变化的，能源数据处理者应在三个月内重新按程序报送重要数据目录。

第三章 能源行业数据保护要求

第十二条 能源数据处理者开展数据处理活动，应建立健全数据安全管理制度，明确数据全生命周期各环节的管理要求；定期组织开展能源行业数据安全知识和技能教育培训。能源行业重要数据、能源行业核心数据的处理者应建立数据安全工作体系，加强人员和经费保障，并配合有关部门开展监督检查工作。

第十三条 利用互联网等信息网络开展能源行业数据处理活动的，应落实网络安全等级保护、关键信息基础设施安全保护、密码保护和保密等制度要求。

存储处理能源行业重要数据的信息网络应落实三级及以上网络安全等级保护要求。

存储处理能源行业核心数据的信息网络，如涉及关键信息基础设施，应在网络安全等级保护制度的基础上，落实关键信息基础设施安全保护要求；不涉及关键信息基础设施的，应落实四级网络安全等级保护要求。

法律法规和国家有关规定要求使用商用密码进行保护的，还应遵守商用密码保护有关规定。

第十四条 能源行业重要数据的处理者应自行或者委托具有风险评估能力的第三方评估机构，对

其数据处理活动每年至少开展一次风险评估，及时整改风险问题，并按省级能源主管部门要求报送风险评估报告。省级能源主管部门、能源央企应将本地区、本企业数据安全风险评估情况按年度报送至国家能源局。

风险评估报告应当准确、清晰地描述评估活动的主要内容，具体包括但不限于数据处理者基本信息，评估团队基本情况，开展数据处理活动的情况及其合规性评价，处理的能源行业重要数据的种类、数量，面临的数据安全风险及其应对措施，风险评估结论和整改建议等要素。

第十五条 能源行业数据安全风险评估重点评估以下内容：

（一）能源行业重要数据和核心数据识别认定的基本情况、所处安全状态及风险分析；

（二）数据处理活动是否合法、正当、必要；

（三）数据安全负责人、管理机构、岗位配备和职责履行情况；

（四）全流程数据安全管理制度及保障机制的建立和落实情况；

（五）数据处理活动相关人员管理和教育培训情况；

（六）国家数据分类分级保护制度落实情况，以及对能源行业重要数据和核心数据保护要求落实情况；

（七）数据安全技术防护能力建设及应用情况；

（八）已发生的数据安全案事件和处置情况，以及数据安全风险监测预警工作落实情况；

（九）涉及数据提供、转移、委托处理、共同处理的，数据接收方的安全保障能力、责任义务约束和履行情况；

（十）其他涉及数据安全的有关情况。

第十六条 能源行业重要数据的处理者在重要数据的收集、存储、使用、加工、传输、提供、公开、删除等环节，应综合运用加密、鉴权、认证、脱敏、校验、审计等技术手段进行安全保护。

第十七条 能源行业重要数据的处理者，应按照业务需要和最小授权原则，依据岗位职责设定数据处理权限，控制重要数据的接触范围，发生人员变动时应及时调整权限。

第十八条 能源行业重要数据的处理者应加强对数据共享、调用的安全管控，采取技术措施定期监测数据共享、调用情况，并配备风险隔离、认证鉴权、威胁告警等安全保护措施。

第十九条 委托他人处理或者与他人共同处理能源行业重要数据的，委托人应当提前告知受托人数据等级，数据安全责任不因委托而改变。委托方应严格审批明确受托方的数据处理权限和保护责任，监督受托方履行数据安全保护义务。受托方应依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供能源行业重要数据。

涉及使用云计算服务处理能源行业重要数据的，可以选择通过云计算服务安全评估的云计算服务，并遵守本管理办法有关要求。

第二十条 未经委托方批准，涉及能源行业重要数据的信息系统建设、运维项目不得转包、分包。

未经委托方明确授权，涉及能源行业重要数据信息系统建设、运维人员不得处理委托方的重要数据。

对涉及能源行业重要数据的信息系统建设、运维过程中收集、产生的数据，不得用于其他用途，服务完成后按照与委托方约定处理或者及时删除。

第二十一条 能源行业重要数据处理活动应记录维护数据安全所需的日志，涉及安全事件处置、溯源的，相关日志留存时间不少于一年。涉及向他人提供、委托处理、共同处理能源行业重要数据的，相关日志留存时间不少于三年。

能源行业重要数据的处理者在组织数据安全风险评估时，应对其数据查询、下载、修改、删除等重点操作的日志开展审计分析，发现违规或者异常行为应采取相应处置措施。

第二十二条 能源行业重要数据的处理者因合并、分立、解散、被宣告破产等原因需要转移、销毁能源行业重要数据的，应采取必要的安全保护措施，并事前向省级能源主管部门报告数据处置方案。

引起重要数据目录变化的，应及时向数据载体所在地省级能源主管部门报备。

第二十三条 在我国境内收集和产生的能源行业重要数据，确需向境外提供的，能源数据处理者应依法依规申报数据出境安全评估。

第二十四条 能源行业核心数据的处理者跨不同法人主体提供、转移、共享核心数据的，应采取必要的安全保护措施，并告知数据接收方按照对应级别进行分类分级保护。自当年度 1 月 1 日起可能累计达到上一年度末该项核心数据静态总量30%及以上的，应经国家能源局报有关部门组织风险评估；未达到 30%的，由省级能源主管部门提出初步评估意见，报国家能源局开展评估。涉及国家机关依法履职、国家机关或企事业单位内部流动的能源行业核心数据除外。

第二十五条 能源行业核心数据的处理者在落实以上能源行业重要数据保护要求的基础上，可以采取以下措施加强对能源行业核心数据的保护：

（一）优先使用商用密码进行保护；

（二）优先使用安全可信的产品和服务；

（三）优先使用第三方评估机构开展风险评估；

（四）涉及核心数据安全事件处置、溯源的相关日志，留存时间不少于三年；

（五）对相关关键岗位人员、涉及核心数据信息系统建设和运维单位等，依法依规提交公安机关、国家安全机关进行国家安全背景审查。

第二十六条 不同类别、级别数据同时被处理且难以分别采取保护措施的，应按照其中级别最高的要求实施保护，确保数据集整体持续处于有效保护和合法利用的状态。

第四章 能源行业数据安全监测预警和应急处置

第二十七条 省级能源主管部门、能源央企应分别加强本地区、本企业能源行业数据安全监测预警和应急处置能力建设，指导本地区数据处理者和能源央企各级子公司、控股企业做好风险监测、事件处置和报告等工作，强化对新技术新应用的能源行业数据安全风险研究和评估，强化对公开渠道数据汇聚、关联后可能引发能源行业数据安全风险的监测能力。

第二十八条 能源数据处理者发现数据安全缺陷、漏洞等风险时，应立即采取补救措施；发生数据安全事件时，应立即采取处置措施，按照规定及时告知相关用户并向省级能源主管部门报告，其中，能源央企各级子公司、控股企业应同步向能源央企总部报告。

风险监测预警的内容应包括：风险基本情况、可能产生的危害和程度、风险演化发展态势、可能影响的范围、处置风险的对策建议及其他应报告的情况。

事件情况报告的内容应包括：事件发生时间、事件简要经过、造成的危害和影响、已采取的措施、下一步对策建议及其他应报告的情况。

第二十九条 本地区、本企业发生能源行业数据安全事件时，省级能源主管部门、能源央企应根据事件级别依法启动应急预案，采取相应应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。

第三十条 省级能源主管部门、能源央企发现可能直接危害国家安全、经济运行、社会稳定、公共健康和安全，以及直接影响政治安全的重大或者特别重大的能源行业数据安全风险、事件，应于发现或者得知后 1 个工作日内将有关情况报送国家能源局，并按要求进行续报。紧急情况下可以通过电话联系方式及时报告，随后补报书面报告。国家能源局负责按规定向有关部门报告相关情况。

第三十一条 省级能源主管部门、能源央企完成重大或者特别重大能源行业数据安全应急处置工作后，应及时总结提炼经验，并于 3 个工作日内形成处置情况报告，于 10 个工作日内形成总结报告，分别报送国家能源局。国家能源局负责按规定向有关部门报送总结报告。

第五章 监督检查和法律责任

第三十二条 国家能源局和省级能源主管部门应当依照《网络数据安全管理条例》有关规定，对能源行业数据安全工作进行监督检查。

第三十三条 国家能源局和省级能源主管部门在履行数据安全监督管理职责中，发现数据处理活动存在较大安全风险的，可以按照规定权限和程序约谈相关能源数据处理者，要求采取措施进行整改，消除隐患，并将问题线索及时移送有关主管部门。

第三十四条 对于违反本办法规定的行为，有关主管部门按照《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》等法律法规规定予以处理处罚；构成犯罪的，移送司法机关依法追究刑事责任。

第六章 附 则

第三十五条 开展涉及个人信息的数据处理活动，还应遵守有关法律法规的规定。

第三十六条 本办法由国家能源局负责解释。

第三十七条 本办法自 2026 年 7 月 1 日起施行，有效期 5 年。

国家能源局有关负责同志就《能源行业数据安全管理办法（试行）》答记者问

原载：“国家能源局”微信公众号

国家能源局近日印发《能源行业数据安全管理办法（试行）》（以下简称《管理办法》）。国家能源局有关负责同志接受采访，回答记者提问。

问：《管理办法》出台的背景和目的是什么？

答：2021 年 9 月 1 日，《中华人民共和国数据安全法》正式施行，其中第六条提出“工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责”。目前，工业、电信、自然资源等主管部门均已出台相应管理办法。为规范能源行业数据处理活动，加强数据安全管理，防范数据安全风险，促进数据开发利用，保护个人、组织的合法权益，维护国家安全和发展利益，国家能源局制定了《管理办法》。

问：《管理办法》出台的意义是什么？

答：《管理办法》是能源行业落实《中华人民共和国数据安全法》的首个规范性文件，明确了国家能源主管部门、省级能源主管部门、能源数据处理者的基本职责和权利义务，对能源行业重要数据、核心数据的精准识别和安全保护提出了明确要求，为做好能源行业数据安全工作奠定了制度基础。

问：《管理办法》的主要内容有哪些？

答：《管理办法》共六章 37 条。第一章总则，包括目的、适用范围、基本定义。第二章能源行业数据安全基本职责，明确国家能源局、省级能源管理部门、能源央企、数据处理者在数据安全工作领域的职责要求，以及在数据目录报送、审核、更新等环节职责要求。第三章能源行业数据保护要求，具体提出了能源行业重要数据、核心数据在处理、出境、跨主体提供等方面的保护要求。第四章能源行业数据安全监测预警和应急处置，包括对能力建设、预警报告、应急处理、事件报告和处置总结报告等方面的要求。第五章监督检查和法律责任，包括监督检查、约谈整改和处罚等。第六章附则，包括与个人信息保护相关要求相衔接，解释和施行时间等。

问：《管理办法》适用于哪些数据的管理？

答：《管理办法》适用于在中华人民共和国境内开展能源行业数据处理活动及其安全监督管理。一是聚焦能源行业数据，《管理办法》明确，能源行业数据是指在开展能源活动中收集和产生的数据。能源活动主要包括与能源相关的规划、设计、建设、生产、储运、消费、科研等。二是聚焦非密数据，《管理办法》明确，能源行业数据处理活动如涉及国家秘密或由其汇聚关联后属于国家秘密事项，相关能源数据处理者应遵守《中华人民共和国保守国家秘密法》等法律、行政法规的规定。三是聚焦能源行业主管部门职责，考虑城市燃气、供热、加油站等能源活动不在国家能源局职责范围内，《管理办法》明确，与这些领域相关的数据处理活动应遵守有关主管部门规定。

问：为加强能源行业数据安全管理，《管理办法》提出建立哪些制度机制？

答：一是建立能源行业数据分类分级保护制度，《管理办法》将不涉及国家秘密的能源行业数据分为三级：一般数据、重要数据、核心数据，并对重要数据、核心数据的保护提出相应技术要求。

二是建立重要数据目录机制，依据《中华人民共和国数据安全法》，在国家数据安全工作协调机制统筹协调下，国家能源局负责建立并动态更新能源行业重要数据目录，全面了解掌握重要数据基本信息、存储地点、安全防护等情况。

三是建立数据安全风险评估机制，《管理办法》要求重要数据、核心数据处理者每年至少开展一次风险评估，重要数据出境、核心数据跨主体转移等依法依规开展风险评估。

四是建立能源行业数据安全监测预警和应急处置机制，《管理办法》明确了国家能源主管部门、省级能源主管部门、数据处理者在监测预警和应急处置工作中的相应职责。

问：《管理办法》规定能源数据处理者有哪些责任义务？

答：能源行业重要数据和能源行业核心数据的处理者对自身的数据安全负主体责任，应依据《中华人民共和国数据安全法》和《管理办法》履行数据安全保护责任义务。一是依照能源行业数据分类分级标准规范，识别并编制本单位能源行业重要数据目录，按照数据载体所在地省级能源主管部门要求报送重要数据目录，发生重大变化的，应在三个月内重新按程序报送。二是建立健全本单位数据安全管理制度，明确数据全生命周期各环节的管理要求等。三是应采取必要数据安全技术手段，并落实网络安全等级保护、关键信息基础设施安全保护、密码保护和保密等制度要求，确保能源行业重要数据、核心数据处于有效保护和合法利用的状态。四是应自行或者委托具有风险评估能力的第三方评估机构，对本单位数据处理活动每年至少开展一次风险评估，及时整改风险问题，并按省级能源主管部门要求报送风险评估报告。五是对涉及重要数据出境、核心数据跨主体转移，应按有关规定要求申请风险评估。六是发现数据安全缺陷、漏洞等风险时，应立即采取补救措施；发生数据安全事件时，应立即采取处置措施，按照规定及时告知相关用户并向省级能源主管部门报告。

问：能源数据处理者如何识别重要数据和核心数据？

答：《管理办法》明确，能源行业重要数据是指特定领域、特定群体、特定区域或达到一定精度和规模的能源行业数据，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。仅影响组织自身或公民个体的能源行业数据，一般不作为能源行业重要数据。能源行业核心数据是指对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的能源行业重要数据，一旦被非法使用或共享，可能直接影响政治安全。主要包括：关系国家安全重点领域的数据，关系国民经济命脉、重要民生和重大公共利益的数据，经评估确定的其他能源行业数据。后续，国家能源局会根据《管理办法》规定，组织制定和发布能源行业数据分类分级标准规范，便于能源数据处理者精准识别并保护能源行业重要数据和核心数据。

问：《管理办法》施行时间有哪些考虑？

答：《管理办法》自 2026 年 7 月 1 日起施行，有效期 5 年。《管理办法》发布后，还将组织制定和发布能源行业数据分类分级标准规范，数据处理者应对照识别重要数据、核心数据并做好保护。考虑政策制定出台、提升数据安全保护水平需要一定时间，《管理办法》施行日期定为 2026 年 7 月 1 日。

最高法将“数据权属纠纷”“数据合同纠纷”等列为独立的司法案由

原载：“数据要素社”微信公众号

12 月 17 日，最高人民法院发布第三次修正的《民事案件案由规定》，新增 “数据、网络虚拟财产纠纷” 第一级案由及 “数据纠纷” 第二级案由，明确将 “数据权属纠纷” “数据合同纠纷” “侵害数据权益纠纷” 列为独立的司法案由。

此类案由的独立，将支持司法机关在不正当竞争纠纷之外探索数据产权制度的司法规则。

2020 年《民事案件案由规定》共有第一级案由 11 个，第二级案由 54 个，第三级案由 473 个，第四级案由 391 个，总计 929 个。此次通过具体案由的增加、删除、升级、降级等不同方式修改具体案由 206 个。修改后的《民事案件案由规定》共有第一级案由 12 个，第二级案由 59 个，第三级案由 514 个，第四级案由 470 个，总计 1055 个案由。具体而言，围绕服务发展新质生产力，增加数据、网络虚拟财产相关案由，并细化了知识产权相关案由；围绕促进法治化营商环境建设，完善了竞争纠纷、商事纠纷相关案由；围绕加强涉外法治建设，结合海事审判实践需要，完善海事海商相关案由；围绕护航乡村全面振兴，完善了农村集体经济组织、农民专业合作社相关案由；围绕不断增进民生福祉，针对新就业形态、老年人权益保护等人民群众所急所盼的领域完善了相关案由；围绕服务美丽中国建设，完善了环境资源相关案由。修改第一级案由 2 个，其中：

增加第一级案由“第六部分数据、网络虚拟财产纠纷”。

修改第二级案由 6 个，其中：

增加第二级案由“十七、数据纠纷”。

修改第三级案由 98 个，其中：

在新增加的第二级案由“十七、数据纠纷”项下：增加“199.数据权属纠纷”“200.数据合同纠纷”“201.侵害数据权益纠纷”。

修改第四级案由 100 个，其中：

在第三级案由“193.网络不正当竞争纠纷”项下：增加“（1）妨碍、破坏合法网络产品或者服务纠纷”“（2）不正当获取、使用数据纠纷”“（3）滥用平台规则恶意交易纠纷”。

通知全文

最高人民法院印发《关于修改〈民事案件案由规定〉的决定》的通知

各省、自治区、直辖市高级人民法院，解放军军事法院，新疆维吾尔自治区高级人民法院生产建设兵团分院：

现将《最高人民法院关于修改〈民事案件案由规定〉的决定》印发给你们，请认真贯彻执行。

最高人民法院

2025 年 12 月 16 日

福建省数据管理局等三部门关于印发福建省有序推进算力基础设施发展若干措施的通知

原载：“福建发改委”微信公众号

福建省数据管理局 福建省工业和信息化厅

福建省通信管理局

关于印发福建省有序推进算力基础设施发展若干措施的通知

闽数据规〔2025〕1 号

各设区市数据管理部门、平潭综合实验区行政审批局，各设区市工信局、平潭综合实验区经济发展局，厦门市通信管理局、各设区市通信发展管理办公室：为深入贯彻落实国家关于“东数西算”和构建全国一体化算力服务体系的决策部署，规范有序推动全省算力基础设施建设，经省政府同意，现将《福建省有序推进算力基础设施发展若干措施》印发给你们，请认真组织实施。

福建省数据管理局

福建省工业和信息化厅

福建省通信管理局

2025 年 11 月 21 日

福建省有序推进算力基础设施发展若干措施

为深入贯彻落实国家关于“东数西算”和构建全国一体化算力服务体系的决策部署，规范有序推动全省算力基础设施建设，加速产业数字化与智能化转型升级，全面提升我省数字经济核心竞争力，结合我省实际，制定本措施。到 2027 年底，全省公共算力规模达到 12EFLOPS 以上，并根据全省公共算力应用需求、资源利用率等情况，谋划建设一批中型算力基础设施项目，合理扩大算力建设规模，

推动智算中心提升国产化率。新建及改扩建数据中心电能利用效率（PUE）降至 1.25 以内，数据中心整体上架率不低于 65%，打造不少于 20 个算力应用案例，稳步提升数据中心绿色能源使用比例。

一、工作措施

（一）优化算力空间布局。加快构建“一核两区多点”的全省一体化算力网络协同发展布局。以数字福建（长乐、安溪）产业园为核心，建设高性能数据中心，引领算力资源示范应用。围绕福州都市圈和厦漳泉都市圈建设城市级数据中心，推动算力资源有效辐射闽东北、闽西南协同发展区，鼓励福州新区与平潭综合实验区协同打造面向两岸的算力协作支点。其他地区结合自身发展实际和资源禀赋，规范有序建设边缘算力节点，满足本地实时算力应用需求。（责任单位：省发改委、数据管理局、工信厅、通信管理局）

（二）规范数据中心项目建设。严格落实国家“东数西算”工程布局要求，引导各类算力向国家枢纽节点集聚，国家枢纽节点外原则上不得新建各类大型及超大型数据中心。严格数据中心项目审查，新建及改扩建项目需提供合规能效检测报告。引入专业力量建设运营算力设施，将算力消纳作为建设指标，市域内已有建成投用 1 年以上数据中心，且整体上架率低于 60%的，原则上不再规划建设新的数据中心项目。（责任单位：省发改委、数据管理局、工信厅、通信管理局）

（三）构建全省算力一体化服务体系。建成全省一体化算力资源公共服务平台，推动专业化运营，打造集算力纳管监测、供需对接、资源调度于一体的算力服务体系。统筹省内算力资源分配和共享，鼓励沿海和山区“结对子”，探索开展“算力飞地”合作。加快融入全国一体化算力网，推进与国家枢纽节点互联互通。深化闽宁算力联动，创新打造“闽数宁算”合作模式。加强与长三角、粤港澳大湾区等算力需求旺盛地区开展算力资源对接与引流，探索面向港澳台、东南亚的算力出海模式。（责任单位：省发改委、数据管理局、工信厅、通信管理局）

（四）提升算力网络传输效率。鼓励福州（含平潭）、泉州、厦门等地规划建设城市算力网，推进“福州—深圳短路径光缆”项目建设。升级扩容“福淡”“厦金”海底光缆，依托区域性国际关口局探索算力出海专网服务。加快 400G / 800G 光传输、IPv6 分段路由（SRv6）、智能无损网络等技术研发部署，打造市域 1ms、省域 5ms、到粤港澳及长三角枢纽 10ms、全国 20ms 四级时延圈。到 2027 年，重点应用场所 OTN 覆盖率达到 90%。（责任单位：省通信管理局、数据管理局）

（五）推动云边端协同发展。在制造业园区、数字经济产业园等重点区域轻量化部署边缘计算节点。促进云计算、边缘计算协同发展，推动端侧设备智能化，以网络带动“云边端”协同发展，打造“中心云+边缘云+端设备”的多层次算力调度架构体系。鼓励按需租用安全自主可控边缘计算节点。到 2027 年，部署不少于 50 个边缘节点，形成不少于 5 个典型案例。（责任单位：省通信管理局、数据管理局）

（六）强化数据存储力保障。开展数据中心存储能力成熟度研究及评价。推动全闪存、蓝光存储等前沿技术创新转化。优化数据压缩、加密等算法，降低存储占用，提升效率与安全性。加快研究制定热温冷数据分类分级标准以及分级存储规范，推进存算网核心设施国产化升级改造。选取福州（含平潭）、厦门、泉州等重点城市，探索城域百公里级“存算分离”模式。到 2027 年，先进存储容量占比达 35%以上。（责任单位：省数据管理局、工信厅）

（七）提升公共算力服务水平。建立统一算力标识体系，推动算力资源标识化管理。鼓励各类数据中心按照统一标准接入全省一体化算力资源公共服务平台，推动与基础电信企业算力资源平台互联互通。建设智能体应用市场和开发者社区，探索推广随取随用、灵活配置、按需收费服务模式，培育一批具有竞争力的智算云服务提供商。持续推进算力对元宇宙、车联网、低空经济等新业态创新应用的支撑。到 2027 年，平台服务企业超 1000 家，

生态开发者超 1 万名。（责任单位：省发改委、数据管理局、工信厅）

（八）深化行业算力应用场景。聚焦政务、医疗、教育、制造、海洋、气象等重点行业，开展“数算一体”的算力应用创新。支持企业、高校和科研院所协同深耕垂直领域，做精做强行业垂类模型。推动算力基础设施与数据产业协同发展，服务数据标注基地、高质量数据集和可信数据空间等。依托数字中国建设峰会等平台，开展算力赋能人工智能创新场景遴选，推进国产化行业级应用。到 2027 年，打造不少于 20 个算力应用案例。（责任单位：省数据管理局、工信厅，省直有关部门）

（九）推进算力与绿色电力融合。推进低效及“老旧小散”数据中心整合改造。鼓励省内数据中心申报国家绿色数据中心。推广液冷、蒸发冷却、近端制冷等新技术应用，持续提升数据中心液冷机柜占比，推进制冷架构、气流组织、供配电方式、单机柜功率密度等方面技术改造，减少冗余设备。鼓励莆田、漳州等地探索应用液化天然气气化站余冷等资源节能降温，加强数据中心余热回收利用。利用当地源网荷储资源，按需建设虚拟电厂，探索算电协同、数电联营和绿电直连等新模式。到 2027 年，形成不少于 5 个绿色能源应用案例。（责任单位：省发改委、数据管理局、工信厅）

（十）完善算网安全保障体系。构建算力网风险预警体系和评价指标，定期组织开展安全风险评估工作。推动人工智能技术在算力安全领域的应用，鼓励算力设施采用安全可信基础软硬件，加强通信核心机房、数据中心、传输干线等设施安全防护与算力服务、调度等智能运维。加强数据分类分级保护，对重要和核心数据实行精准严格管理，建立健全数据安全应急处置机制。（责任单位：省通信管理局、数据管理局、工信厅）

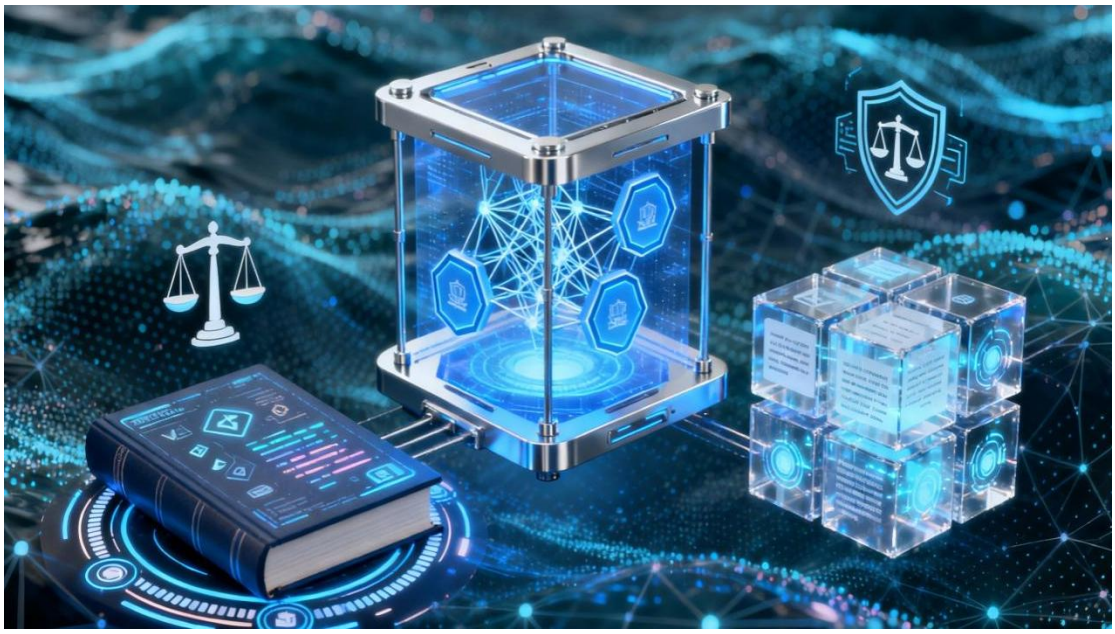
二、其他

各相关单位加强协同配合，合力推进重点任务组织实施。灵活运用基础设施 REITs 及其他多元方式，引导社会资本参与算力基础设施建设。加强算力人才供给，促进技术交流和供需对接。充分发挥我省算力生态联盟、信息化标准化技术委员会作用，推动算力监测、调度、结算等领域标准规范制定及推广。定期发布算力基础设施发展报告及算力综合指数。

本文件自印发之日起施行，有效期至 2027 年 12 月 31 日。如遇国家政策调整，按最新政策执行。

（技术编辑：来唯希）

研究动态



数字法学基础理论

1、论数字权利的关系变异（孙笑侠）

来源：《法律科学(西北政法大学学报)》2025 年第 6 期

数字权利为何存在名目增多却又难以实现的现象？这与规范等效思维将数字权利与传统权利按惯性思维看成是“规范等效”关系，无视数字权利的结构性困境，无视旧的人权保护框架所存在的“尊严超载”有关。本文在初步分析了“规范等效”范式的误区之后，重点揭示数字权利的九种结构性困境，并将数字权利与霍菲尔德传统权利理论进行对照，证明数字权利困境预示着数字权利已发生关系变异和规范断裂。因此，在数字法上要强调哈特式的“第一性规则”,通过技术可配置性，以新“义务本位”来重构数字法的规范体系，并实现结构性反制的法权重构。

2、论我国数字法学教育的人文主义转型（徐海琨）

来源：《政治与法律》2025 年第 12 期

我国数字法学教育陷入“形式理性”的科学主义误区，过度推崇法教义学逻辑与计算工具理性，致使教育脱离数字社会场景，难以平衡技术效率与人文价值。数字法学教育需立足本土实际，以人文主义调适科学主义，通过意识形态、方法论与法律思维的协同革新，培养兼具技术能力、法律素养与人文关怀的复合型数字法治人才。在具体路径上，需推动学科建设、课程设置与教学方式三维协同。一方面，优化“法律硕士+跨学科”模式，增设社会科学课程以强化学科价值基础，调整传统部门法以聚焦数字时代核心问题，设计融合课程以平衡技术与人文关系。另一方面，可以通过课题训练培育批判思维，依托交叉学科平台塑造系统思维，推动数字技术从“形式理性主导”转向“人本价值赋能”。

3、信息能力对法律规范形态的塑造（李晟）

来源：《法学研究》2025 年第 6 期

法律规范形态的塑造与演变,始终受到社会信息能力的深刻影响。社会规模的扩大与成员关系的陌生化,构成了信息能力的现实约束,催生了以一般化规则为核心的法律形态。此类规则通过在有限信息下为社会主体提供稳定的行为预期,奠定了以形式理性化为特征的现代法治的基石。一般化规则对复杂现实的信息简化,使其与生活世界的具体情境产生张力,由此形成了规则与标准的规范分化,以回应不

同情境下的治理需求。规则与标准的分化,体现了立法者在法律抽象性与具体性之间寻求平衡的努力。信息技术革命提升了社会的信息处理能力,使法律制度所处理的信息可以达到更细致的颗粒度,这为构建新型的个性化规则提供了可能,从而有望在更高维度上超越“规则—标准”二元框架。

4、数字技术与预防性法律制度的体系化构建（寿媛君）

来源：《法律科学(西北政法大学学报)》2025 年第 6 期

数字技术赋能预防性法律制度有助于更好地预防社会风险，但亦会衍生技术治理风险，呈现赋能与技术异化的悖论。为避免出现大规模风险，预防性法律治理应成为新型法治形态。在构建预防性法律制度过程中，会面临静态法律规则与动态技术演化的矛盾，法律制度设计的静止性、碎片化难以适应数字技术的快速迭代，与对数字风险的预防产生抵牾。数字技术反向侵入预防性法律制度，算法决策偏差归因困境与技术应用的不透明性使很多法律实施过程难以被追溯，导致法律制度的风险预防功能被悬置。面对预防性法律制度与数字治理之间的嫌隙，预防性法律制度亟需建构三个维度的协同体系，分别从纵切面形成制度与技术的层级化体系，横切面实现程序与实体的勾连体系，同时构建以数字平台为中心的责任体系，最终实现秩序与自由动态平衡的数字正义。

个人信息保护

1、论已公开个人信息合理处理范围的认定（孙莹）

来源：《法律科学(西北政法大学学报)》2025 年第 6 期

现有认定已公开个人信息合理处理范围的路径，因诉诸价值中立或存在价值偏向的外部理论，而难以解决价值判断冲突问题。对此，宜回归《个人信息保护法》,贯彻其保护与利用并重的价值主张。原则层面，应将目的限制原则中的“处理目的”解释为处理行为的目的而非公开目的。规则层面，重大影响本质是个人权益被侵害的高风险状态，可通过国家标准进行细化；拒绝权受其他合法性依据的限制，如未依处理者建立的机制行使拒绝权，不发生拒绝的效力；除存在告知义务豁免情形，处理者应履行告知义务，不需要告知可由法院在个案中衡量。将这一框架应用于生成式人工智能场景，可解决公开目的难查明、重大影响不明确的难题，而针对删除义务难履行的问题可通过健全拒绝权的替代性保障以及强化数据来源告知义务予以解决。

2、论个人信息的算法识别特征及其规范意义（徐伟）

来源：《法学论坛》2025 年第 6 期

如何区分个人信息权与传统人格权是当前理论与实践难题，学界存在平行适用说、权利竞合说、信息处理关系说、人格利益区分说和算法识别说，其中以算法识别说最为可取。数字社会是个人信息权得以产生的前提，“可识别”并非个人信息的本质特征，算法识别才是个人信息的本质特征。与传统社会相比，数字社会中的个人信息识别方式、评价方式、侵害方式和损害结果都因算法而发生改变。算法识别特征证成了个人信息权是一项天然内含财产价值的人格权，决定了个人信息权的权利内容、适用范围、利益分配和救济规则。个人信息算法识别特征的提出为构建个人信息权融贯理论体系和规则设计奠定了基础。

3、数据交易模式下的个人信息保护边界厘定（王磊）

来源：《法学论坛》2025 年第 6 期

数据交易作为提高数据流转效率、释放数据要素价值的重要方式与个人信息保护之间的结构性冲突已成为亟待解决的法律难题。现行法律体系通过《民法典》合同编和人格权编、《个人信息保护法》以及《数据安全法》等法律规范为解决个人数据交易争议提供适用依据，形成规制数据交易场景下个人信息保护的基础规制框架。但囿于个人数据交易中的主体规则不明、个人数据交易规则失范与经济发展及安全保护的价值冲突，当前数据交易场景下个人信息保护的责任边界仍待厘清。首先，应当明确个人作为“数据交易链起点”的法律身份，在数据交易全流程实现对数据主体个人信息权益的法

律保护;其次，检视我国数据交易中个人信息保护法律制度构造，破解实践中数据交易对象不明、数据处理标准模糊、知情同意适用难的法律困境;最后，立足于本国探索实践并借鉴国内外立法在法律价值视域下平衡数据交易效率的经济价值与个人信息保护的人格权益。在数据交易场景下构建个人信息保护的制度边界，应当以“个人数据”的法律定位为基点，在此基础上厘清数据交易参与主体的角色冲突与责任边界，形成制度化、体系化的个人信息保护责任谱系，实现个人信息保护从单一视角切入向多点共治的范式转换。

4、数字智治场域下侵犯公民个人信息罪的适用异化与匡正（杨楠）

来源：《华东政法大学学报》2025 年第 6 期

在数字智治背景下，侵犯公民个人信息罪的司法适用问题依然突出。敏感个人信息呈现泛化趋势；因果关系无限回溯、过度依赖结果归责、对罪过模糊推定，造成处罚范围异化扩张；因应新型犯罪手段，形式解释模糊入罪边界，与规范目的脱节。要摆脱这些困境，须动态调整保护范围，恪守主客观相统一，深化协同治理。具体地，对敏感个人信息应分类规制，对于一般敏感个人信息，应以前置法为基础，并辅以实质判断；对衍生敏感个人信息应分阶段考察，并通过检验信息的法律属性、多维阈值的匹配度、场景化校验三个阶层进行筛查。在归责方面，以个人信息类型与内容、获取和处理手段、流转方式与范围、危害后果等客观事实为基础，审慎判断行为人主观心态；再以该主观心态为尺度，合理限缩客观归责范围，通过客观与主观的关联和互证精准划定入罪边界。对新业态下“不纯正的新型犯罪”，宜充分借助刑法教义学方法，将具有实质可罚性的行为纳入规制范围；而对于“纯正的新型犯罪”则本质上属于立法与刑事政策有待解决的范畴，当前阶段只能审视不法链条中是否存在能够适用现有罪名的环节，否则只能通过前置法予以规制。

5、数智时代侵犯公民个人信息罪中个人信息的保护范围（杨柳）

来源：《华东政法大学学报》2025 年第 6 期

数智时代个人信息范围的界定仍应以识别性为标准，从形式和实质两个层面进行判断。从识别性的形式判断而言，不具有识别性的信息不属于个人信息，刑法与前置法对个人信息范围的界定应当保持一致。识别性的实质判断包含积极判断与消极判断两个方面。积极判断是对个人信息识别性程度的判断，从而确定个人信息的保护范围；消极判断则是将不具有个人信息自决权实质损害的行为排除出罪。因此，单纯侵害隐私权行为以及单纯财产损害行为不能成立侵犯公民个人信息罪。对于已公开的个人信息而言，处理绝对公开的个人信息不构成犯罪；处理内容限制与时间限制的相对公开的个人信息则可以构成犯罪。

6、个人信息主体权利行使的民行救济协同论（沈佳燕）

来源：《华东政法大学学报》2025 年第 6 期

个人信息主体权利行使的救济理论上可通过民事司法与行政监管两种方式实现。主体权利属于民事权利，公法权利的主体不能由国家权力者类推至社会权力者，对具体法律人格进行倾斜性赋权也未逸脱民法范畴。工具性权利的特征不影响其可诉性，主体权利行使之诉遵循私权救济的逻辑而非公法上的执法机制，也与是否存在损害或实质损害风险无关。处理者拒绝的要求独立于使潜在请求权现实化的需求，也非诉之利益的考量因素，不宜解释为特别起诉条件或诉讼前置程序，费用承担机制与败诉风险威慑可在不牺牲救济及时性的同时，规制个人的直接起诉。主体权利对应的义务兼具民事与行政法律义务的双重属性，处理者违反时应承担行政责任。行政机关介入保护的具体形式是作出责令改正的行政命令，处理过程亦带有行政裁决的特征。在应然性层面，两种救济方式应实现良好的协同效应，个人不得同时适用。强制行政先行并不会破坏诉权本质且符合诉权限制的比例原则，但存在个人就行使查阅权、复制权、解释说明权、可携带权直接起诉以及一并提出损害赔偿请求的例外情况。对行政处理决定不服可选择民事诉讼、行政诉讼或行政复议的救济，行政诉讼中应赋予法院可以变更行政决定的权力。

7、数字经济时代个人信息的民行刑一体化保护（刘艳红）

来源：《华东政法大学学报》2025 年第 6 期

数字经济时代的本质是通过技术重构生产要素配置方式。个人信息作为新型生产要素的重要组成部分，已快速融入生产、分配、流通、消费和社会服务管理等各环节，但在科技创新的背景下始终面临着信息保护与流通利用之间的利益平衡难题。自 2022 年 12 月 2 日《中共中央国务院关于构建数据基础制度更好发挥数据要素作用的意见》提出要建立健全个人信息数据确权授权机制，促进个人信息合理利用以来，已有数份政策文件涉及个人信息的开发利用。然而，现行个人信息保护相关立法及其治理理念偏向信息保护而非流通利用，由此导致实践中法法衔接不畅、法律责任泛化等问题，亟待理论回应。对此，本组专题的四篇文章聚焦我国个人信息治理的前沿、疑难问题，从三个维度提出了本土化方案。

8、个人信息权的法理证成与逻辑展开（成亮）

来源：《法律科学(西北政法大学学报)》2025 年第 6 期

个人信息的确权是个人信息保护领域的基础问题，关系到我们对个人信息保护制度的体系性理解，也深刻影响法官在处理个案纠纷时的立场选择，因此殊堪关注。确立个人信息权的权利地位，既有应然层面的合理性，也有实然层面的必要性：一方面，个人信息权有着融贯的规范保护目标，其保护的是一种独特的尊严利益，即个人对其社会身份进行自主和完整塑造的“自我呈现”利益，它为个人信息权的成立奠定了牢固的价值根基；另一方面，个人信息权拥有区别于其他传统人格权的独特规范功能，能够纾解个人在网络时代遭遇的“自我呈现”困境，故而个人信息权的成立具备牢固的现实根基。个人信息权保护的制度设计应以保护个人“自我呈现”为焦点，将法律规定的各项程序性个人信息权利“收敛”成一个有机整体，形成一个以“(抽象)个人信息权”为主干，以“(具体)信息权利”为分支的严密权利体系。个人信息权赋予主体对个人信息的自决是有限度的，因而不会阻碍对数据资源的合理利用。

人工智能立法

1、人工智能预训练中大规模抓取个人信息的合法性困境与出路（王苑）

来源：《中国法律评论》2025 年第 5 期

人工智能（AI）预训练中大规模抓取个人信息的法律根据存疑。目前欧盟已明确数据控制者正当利益系该场景下的合法性基础，但我国实在法上并无类似条款。而大规模抓取的无差别性导致抓取时已公开个人信息与元数据或敏感个人信息难以界分，因此已公开个人信息的合理使用规则在此情形下无法适用，同时敏感个人信息单独同意规则亦欠缺实践可行性。《个人信息保护法》第 13 条第 1 款第 5 项公共利益条款适用范围狭窄，可通过扩张解释具有普惠价值的 AI 预训练有公共利益，寻求现行法的合法性支撑。但鉴于 AI 发展下的多重利益格局，应考虑在未来 AI 相关立法中明确“预训练场景下个人信息的原则可抓取”，辅以配套制度确保抓取的合法、正当、必要及安全。

2、从合理使用到合理学习：人工智能训练数据的著作权困境与规范重构（孙济民）

来源：《中国法律评论》2025 年第 5 期

针对人工智能系统使用受著作权法保护的数据进行训练的行为及其所造成的困境，当前多数研究主张应通过扩张合理使用制度的适用范围加以应对。尽管这一做法能够部分回应现实需求，且具备经济正当性，但是以交易成本为主轴的分析框架并不能全面评价数据使用的正外部性。因此，有必要遵循人工智能的技术逻辑，围绕“合理学习”原则形成综合分析框架。在此基础上，相关法律规范应当参照人类学习活动进行重构，立法应区分输入端与输出端以形成事前与事后两层次规制方案。其中，输入端应准许开发者为训练人工智能系统而居间使用受保护作品；输出端应摒弃内容相似性判准，通过行政监管和司法程序确保开发者遵守注意义务，维护公私利益平衡。

3、人工智能生成的内容是作品吗？——以学术规范和著作权法的关系为视角（王迁）

来源：《中国法律评论》2025 年第 5 期

实验表明，人工智能根据 745 字初始提示词生成了近万字的法学论文，再根据两次增加的提示词形成的终稿，在经过简单的格式调整和替换明显伪造的注释后，通过了三位外审专家的评审。依“人工智能文生图第一案”判决的结论和逻辑，该论文也应视为该生独立完成的作品。然而，认定学生凭借其使用人工智能生成的上述学位论文可获得学位，将明显违背学术常识，而做出相反结论则抵触“人工智能文生图第一案”的判决，从而形成悖论。人工智能生成的内容源于其自身的算法和数据训练，提示词相对于该生成内容是思想，因此，学生设计提示词由人工智能生成的内容并非其创作的作品和独立完成的学术成果，不能被认定为作者和取得著作权，且其以本人为作者呈现该内容的行为违反学术规范。

4、生成式人工智能个人信息侵权因果关系不明时的责任认定（朱晓峰）

来源：《政法论坛》2025 年第 6 期

生成式人工智能个人信息侵权的因果关系往往因算法黑箱、数据清洗及交互学习等而在实践中难以证明。无论是依据《民法典》第 1165 条第 1 款结合《个人信息保护法》第 69 条第 1 款的构成要件式的责任认定方式，还是依据《民法典》第 998 条的利益权衡式的责任认定方式，受害人都应承受证明不能的不利后果，这与立法者充分保护个人信息的目的相悖。对此，在明确此情形下存在的法律漏洞类型的前提下，基于平等原则而通过类推解释的方法，将《民法典》第 1254 条第 1 款因果关系不明时的补偿规则适用于生成式人工智能个人信息侵权因果关系不明时的受害人救济。考虑到生成式人工智能个人信息侵权的特殊性，在补偿范围上应当由可能的加害人补偿受害人的全部损害；补偿义务人之间的内部关系应当是按份关系，具体的补偿数额由法官在个案中结合案涉情形综合认定。

5、动态体系论下生成式人工智能侵权的归责与构成（张华韬）

来源：《法学杂志》2025 年第 6 期

生成式人工智能虽存在无法克服和避免的固有技术风险，但行为人在生产、使用和经营等环节享有意志自由，且不同的生成式人工智能类型对法益的影响方式和后果存在较大差异，这决定了这一领域的侵权责任不宜采用单一的传统过错或无过错归责原则，而应运用动态体系论，确立过错、危险、支配领域等要素，在个案中综合各要素的权重和强度予以认定。生成式人工智能侵权不宜适用产品责任，而宜适用违反安全保障义务的侵权责任，以同时纳入过错和危险两种要素。生成式人工智能服务提供者根据保护性规定和合同约定，在其控制的网络空间内履行安全保障注意义务。《生成式人工智能服务管理暂行办法》等规定的公法义务和用户协议确定的合同义务，可部分作为注意义务履行与否的判断要素。而注意义务应根据侵权预防成本与收益的平衡、识别侵权后果的难易程度、现有行业通行技术水平三个动态体系的因子进行动态基础评价。“避风港规则”“红旗规则”因已纳入注意义务的评价基准，不应单独作为义务不履行的依据或免责事由。

6、人工智能综合性立法及其实现（周辉）

来源：《法学研究》2025 年第 6 期

在当前人工智能领域,需重点应对统筹人工智能全生命周期风险与全要素发展、实现新旧规则的平衡供给、适应全球竞争持续加剧三重挑战。相关议题的紧迫性,决定了开展人工智能综合性立法的必要性。总则性、碎片化、低位阶立法等替代性路径,面临可操作性不足、协同性欠缺及立法权限模糊等困境。人工智能综合性立法旨在确立全局应对、主动塑造的人工智能法律治理范式,其承载着促进发展、风险防控与权力规制的多重功能,核心任务在于实现规范内容的体系性、调整范围的全面性与价值目标的综合性,故其不必拘泥于“人工智能法”这一名称,亦非无所不包的人工智能法典。推进人工智能综合性立法需科学分析立法需求、前瞻布局机构改革以做好立法准备。在内容上,立法需以人工智能全

要素、分主体、全周期为矩阵框架,以国家人工智能主管机关为枢纽牵引;同时内嵌动态更新、持续适配机制及技术研发暂停机制,确保立法出台后能主动维系有效性与适应性,及时回应新发展需求与新风险挑战。

7、人工智能法学之类比方法及其省思：以 AIGC 著作权保护问题为例（吕炳斌）

来源：《法学研究》2025 年第 6 期

在应对新技术引发的新问题时,类比成为一种重要的思维工具。类比是人工智能法学研究中的重要方法,在认知便利性、维系法律体系的连续性与自洽性、促进法律制度的创新发展等方面展现了独特优势。在探寻人工智能生成内容(AIGC)的著作权定性时,不同论者诉诸多种类比方法,但均面临争议且存在不足。分歧一方面源于人工智能的独特性,另一方面则可归因于类比方法本身的内在局限。类比方法的改进之策,可在实践理性的指引下,以“反思的平衡”为核心方法论展开,追求“反思性类比”。类比应超越对相似性的直觉感知,也并非仅关注相似性,而是要进行“相似—差异”双轨分析,并要求多重推理路径的互验与批判性对话,且进入“反思的平衡”下的动态调适过程,从而超越单一类比、表面特征类比。在 AIGC 著作权保护问题上,完美类比并不存在,即便经由类比承认 AIGC 的著作权保护,仍需注意差异,走向 AIGC 的弱保护或低强度保护。

8、自动驾驶分级治理的法理反思与规则重构（郑志峰）

来源：《法学研究》2025 年第 6 期

当前,我国自动驾驶立法普遍遵循自动驾驶分级治理的逻辑,区分有条件自动驾驶、高度自动驾驶以及完全自动驾驶三个阶段分别进行法律规则的设计,其背后体现了技术标准与法律规则的融合以及人工智能分级治理的实践。然而,各级自动驾驶的区分并非判若鸿沟,完全自动驾驶不受设计运行范围限制、有条件自动驾驶需配备被动接管规则等设定存在极大的安全风险,直接照搬自动驾驶三阶分级忽视了技术标准的治理成本与技术分级的制度局限。高度自动驾驶相较有条件自动驾驶、完全自动驾驶更具规制优势,契合自动驾驶替代型人工智能的定位,理应成为法律规制的基础模型,在此基础上完成分级治理向分类治理的转向。应在区分自动驾驶双用车辆与专用车辆的基础上,结合车辆具体运行模式进行义务和责任主体的续造,形成使用人与所有人、管理人并列的二元主体架构,其负担的安全驾驶义务也需根据不同模式下车辆人机关系的特点进行更新。机动车交通事故责任方面,对于机动车之间的交通事故应继续适用过错责任,机动车与非机动车、行人之间的交通事故则需区分有人模式与无人模式,前者使用人宜维持现行实质过错归责模式,后者所有人、管理人宜承担无过错责任。

9、从直觉到证据:大模型法律语料库与法律解释客观化（江海洋）

来源：《法学研究》2025 年第 6 期

法律文本特别是刑法的解释,原则上以词语的“通常含义”为边界。通常含义指的是大多数普通人在特定语境下对法律文本的理解,若偏离通常含义对法律文本进行解释,则要进行充分的说理论证。判断通常含义时,主要借助语言直觉、词典、法律语料库三种辅助工具。在大模型技术赋能法律语料库的背景下,大模型法律语料库通过数据驱动范式,将法律解释从依赖主观直觉转向可验证的客观分析。这一转向不仅增强了解释过程的透明度,提升了解释结论的客观性,更通过技术约束机制倒逼解释者履行论证义务。作为一种辅助解释工具,大模型法律语料库既不试图阻止解释者进行主观判断,亦不会限制或者放纵解释者的解释权。针对大模型法律语料库建构阶段的技术内生操纵风险,应公开其基础数据来源和技术处理全流程信息,并确保辅助法律解释的过程和结论可重复、可推广。针对使用阶段的人为外生操纵风险,应构建技术与制度协同治理框架,确保解释者主观选择的技术可见性与可辩驳性。

10、人工智能对刑事证明结构的影响及其制度因应（沈磊）

来源：《法学研究》2025 年第 6 期

刑事证明中嵌入的专家系统、垂类大模型和概率推理模型等人工智能系统,会对刑事证明的认知结构和权力结构产生显著影响。就认知结构而言,人工智能的信息过程不同于人类的思维过程:在模型构建阶段,前述三类系统对人类知识库进行了不同的具象化表达,并且各自增加了独特的数据处理工序;在案件分析阶段,三类系统对人类逻辑方法的模拟可谓各有短长。就权力结构而言,人工智能的应用会导致刑事证明活动发生以下变化:一是技术主义对自由心证的规训,二是管理权力对案件办理权力的收拢,三是控审“同盟”对辩方“孤岛”的疏离。针对上述变化,刑事证明制度需要作出如下因应:一是将人工智能重点应用于刑事证明的非核心场域,二是确保人工智能对办案人员的非替代性和非强制性,三是实现人工智能对诉讼主体的可解释性和可交互性,四是保障辩方对人工智能的知情权、质证权和利用权等权利。

11、机器学习生命周期中的著作权法因应（张嘉林）

来源：《法学论坛》2025 年第 6 期

机器学习作为人工智能的关键技术在内容生产领域被广泛应用，其在海量数据训练过程中对受著作权保护作品的使用引发了频繁的侵权争议。机器学习工作流程中的数据收集、预处理及模型训练阶段对于作品的使用属于“非作品性使用”，并不侵犯专有权。对于模型输出阶段的著作权侵权风险，服务提供者应当主动积极履行作品信息透明度等三项合理的、可负担的注意义务。在人工智能时代，著作权法需要超越传统概念和范式，从促进技术发展的立场出发，制定合理的规则，而“默示许可+选择退出”机制可以平衡著作权人的利益保护和技术发展的需求，适应技术进步带来的挑战。

12、生成式人工智能对个人信息保护法的结构性冲击及应对（付新华）

来源：《法学论坛》2025 年第 6 期

生成式人工智能的大规模信息处理方式及其强大的数据生成能力，对现行个人信息保护法以信息自决为理论基础的权利体系，以及以数据收集为规范重点的基本原则，构成了深层次的结构性冲击。为应对这一挑战，有必要从制度层面构建“群体信息—个体信息”的双层保护体系，强化信息保护的群体维度，明确群体信息的法律地位与保护义务，将群体信息伦理纳入法律框架;同时确立“数据生成—数据收集”的双重治理框架，填补数据生成的规制空白，界定生成数据的法律属性，设立限制数据生成权，并加强对匿名化数据处理的监管，以推动建立适应大模型技术特征及其风险形态的信息治理机制。

13、算法伦理的法律表达（李姝卉）

来源：《当代法学》2025 年第 6 期

算法技术垄断与滥用，逐渐侵蚀人的自由选择意识和能力，算法偏见、操纵、欺骗、幻觉等伦理失范现象频发，需要通过完善的法律监管、法律责任、权利救济和隐私权保护等制度予以化解。应强调自由选择、诚实信用、平等正义、透明负责的算法伦理自治理念，促进算法开发、设计、运营主体自觉将算法伦理观念嵌入算法技术。但自治规范存在强制性和可执行性弱等问题，需依赖法律制度保障算法可信、维护人的主体地位、平衡算法权力与用户权利的关系。立法应建立算法决策中的人类监督机制，强化算法开发、设计和运营主体保护自然人权利的法律义务，完善算法伦理制度，增设对算法操纵和欺骗的法律救济，通过法律制度保障算法伦理有效落地。

14、人工智能立法的基本问题：算法规训及其场景中的人机关系（梅夏英）

来源：《法学家》2025 年第 6 期

人工智能立法问题目前存在理论上的争议。基于立法理念切换尚未完成、法律对技术回应的有限性和延迟性，以及新技术领域的统一立法对于新颖性和系统性的要求等原因，目前制定统一的“人工智能法”的时机尚未完全成熟。人工智能立法应建立在它所创造的新型法律调整对象和方法上，由此可以提炼出“深度学习算法”和“人机关系”作为人工智能法的两个理论支点，且两者是紧密联系同步进化的。深度学习算法的规制在人工智能领域较之前

具有更重要的意义，当前关于算法的透明性、可问责性以及可解释性等理念均无法形成理论上的自洽，最终仍有待算法“黑箱”的有效破解。人机关系因技术发展的不确定性尚难以在法律上形成完整判断，但如果剔除掉 AI“自我意识”的幻象，人机关系未来应由人类主导，且应遵循“非人化”原则、人类优先原则和安全原则，在此基础上就可以建立人机关系的具体法律机制，如人机对齐、人机信任和人机伦理的相关准则。人工智能立法对新的思想资源和思维范式提出了迫切要求，其中“计算机作为社会行为者”以及“行动者网络”等理论对我们的借鉴意义值得关注。

15、人工智能犯罪归责的行为主体论路径（吴贻森）

来源：《法学家》2025 年第 6 期

人工智能时代到来，刑法领域亟须建立适用于人工智能犯罪的归责规则。对于人工智能犯罪的归责，刑事责任主体论难以确定理论激活的时点，犯罪工具论无法充分回应人工智能自主性问题，二者均存在局限性。通过对犯罪主体概念不同层次的分离，在理论上可以探讨无刑事责任能力的人工智能成为行为主体的问题，从而在刑事责任主体论与犯罪工具论之外，扩展出具有衔接性价值的行为主体论的理论发展空间。我国刑法体系存在扩展行为主体概念的可能性，行为主体并不必然局限于自然人。以社会行为论为基础，行为时存在自主意识、在社会重要意义上与人类行为具有等效性的人工智能行为，可以被纳入刑法的评价范围，由此证立人工智能的行为主体地位。人工智能行为主体参与犯罪时，应根据犯罪参与的思路进行归责分析。行为主体论为相关归责理论的适用提供了多主体基础，有助于衔接实行过限、监督过失、信赖原则等问题的理论研究成果。在立法未承认人工智能刑事责任主体地位的情况下，对于人工智能行为需要由人工智能背后的主体承担替代责任，基于行为主体论的归责分析则有利于更加准确地认定涉案各主体的责任。

16、生成式人工智能生产者过失犯罪的结果归责（张维尧）

来源：《华东政法大学学报》2025 年第 6 期

作为生成式人工智能的研发与部署主体，生产者通过设计算法对人工智能实施管控，理应对人工智能造成法益侵害的后果负责。生成式人工智能产生的刑事风险，冲击了传统过失犯理论与刑事立法体系。新过失论为解决生产者过失犯罪归责问题提供了理论方案。在预见可能性认定上，应以行业内一般人为视角，判断生产者是否具体预见到违反结果回避义务的行为可能导致法益侵害的危险；在因果关系认定上，应根据犯罪是否存在算法黑箱的作用，选择适用相当因果关系说和智能因果关系说。鉴于此类犯罪的保护法益为算法安全，建议刑法增设算法设计、管理责任事故罪，以生产者对训练数据、算法的注意义务为依据，确定算法设计、管理责任。

17、生成式人工智能背景下个人信息的刑法规制困境与归责出路（李川）

来源：《华东政法大学学报》2025 年第 6 期

生成式人工智能大规模处理个人信息所引发的侵害个人信息的新型风险，有待刑法有效规制。然而，生成式人工智能的特质在认定个人信息犯罪时存在行为区分定性、主体归责分配、前置法违反认定、对象范围边界、因果关系判断等多方面难题，这些难题引发了刑法规制困境。追溯困境原因可以发现，刑法个人信息犯罪设立于生成式人工智能产生之前，基于刑法先行的特点，形成了个人信息有限赋权的规制模式，该模式难以适应生成式人工智能场景化处理个人信息的定制式、一体式、关联式特征，从而造成规制难题。因此个人信息刑法规制应根据生成式人工智能的特质转型为场景治理模式，相应确立危险现实化、信息类型化、结合识别目标、规范因果与义务违反结合的归责路径与认定基准。

18、生成式人工智能搜索服务提供者侵权免责制度（姚志伟）

来源：《环球法律评论》2025 年第 6 期

融合了生成式人工智能技术和传统搜索技术的新一代搜索形态正迅速兴起。与传统搜索主要为用户提供搜索网页链接不同，这种生成式人工智能搜索利用模型的生成能力，对来源网站内容进行组织后

直接提供给用户。此变化使得生成式人工智能搜索服务提供者难以适用传统搜索服务提供者的免责制度。生成式人工智能搜索与传统搜索服务同样具有技术中立性，也都面临着难以在海量内容中有效清除侵权内容的难题。同时考虑到人工智能产业激烈的国际竞争，中国应为生成式人工智能搜索服务提供者设计侵权责任免责制度。免责设计包括“安全港”和“适当引用”,两种制度各有优劣，应相互补充。立法的重心应在“安全港”规则的设计上，而“适当引用”则可在立法出台前的司法实践中发挥重要作用。

19、大型语言模型生成虚假信息风险的法律治理（苏宇）

来源：《环球法律评论》2025 年第 6 期

大型语言模型生成虚假信息的风险来源涵盖数据层、算法层、模型层和应用层，而实践中已应用模型对齐、激活工程、检索增强生成、安全护栏等内生与外生措施进行风险防控。对于生成虚假图像和音视频信息，主要治理路径可为“标识制度+技术检测”;而对于生成虚假文本类信息，主要治理路径应为“常规测评体系+模型攻防测试”。为精确把握多维治理目标之间的制度化平衡，立法应在标识强度、规制范围、达标分值和责任豁免等方面设置可动态、精细调节的一系列规则，探索能够良好契合人工智能技术研发与产业发展规律的治理方案。

20、人工智能治理的两种安全思维:批判与超越（戴昕）

来源：《环球法律评论》2025 年第 6 期

人工智能安全是各国当前均重视的复杂治理议题。美国的人工智能治理实践近年来受到“国家安全泛化”思维的影响，而欧盟对特定人工智能应用采用禁令式立法，体现出其面对某些人工智能风险时的“安全绝对化”思维。对于美欧两大法域的这两种安全思维，可结合相关法域治理者面临的内外环境与社会认知及情绪加以理解。这两种思维对于各国人工智能国内治理体系的有效建构与必要国际合作的开展均可能产生负面影响。对它们在理论层面加以批判性审视和分析，有助于中国超越类似思维的桎梏，有效探索有利于自身发展和人类命运共同体的人工智能治理方案。

来源：《环球法律评论》2025 年第 6 期

21、基于 DeepSeek 的法律 AI 新风貌：反思性审视（左卫民）

来源：《法律科学(西北政法大学学报)》2025 年第 6 期

人工智能技术的快速发展正推动包括实践与研究在内的法律生态的变革，以 DeepSeek 开源大模型为重要代表的技术架构与行业探索实践正成为革新法律生态不容忽视的因素。在司法领域，DeepSeek 类大模型产品的法律检索与裁判预测功能可辅助快速发现法律规范依据、预测案件裁判后果且已有研发者开始尝试直接使用大模型制作法律文书以供法律人参考，并在相当程度上得到了法律专业人员的认同。然而，大模型与法律活动的深度融合仍面临多重挑战：当前大模型输出内容的科学性、准确性和逻辑严密性尚难满足法律活动的“苛刻”要求；在社会心理层面，公众对于由大模型类的“AI 法官”替代人类司法裁判者决策仍存在普遍的接受障碍；基于数据驱动的大模型是否具备把握司法规律、形成“创造性”裁判的能力尚存严重争议。DeepSeek 类大模型的“智能辅助”定位仍长期成立，其发展路径或将形成人机协同共进的格局，即“碳基”人类掌握方向，“硅基”AI 助力效率，最终推动法律实践从效率提升向质效跃升的跨越。

数据确权研究

1、第三次分配导向下的数据收益机制构建（袁曾）

来源：《法学杂志》2025 年第 6 期

数字经济的繁荣加剧了数据收益分配的复杂性，数据要素的价值分配已成为共同富裕面临的核心问题之一。已有的数据产权理论纠结于客观赋权，疏于数据收益分配的机制构建。在数据利用的初次分配环节，因个体用户与数据处理者之间存在知识、议价能力和技术手段的结构性不对等，市场机制天然地倾向数据处理者，导致现有收益分配格局严重失衡。在二次分配环节，当前虽可通过数据税与反

垄断等工具进行干预，但其强制性与滞后性存在天然局限。应将第三次分配作为矫正数据收益分配失衡进而实现数据红利共享的关键环节，并以此为核心系统性地构建数据收益分配实现机制。通过规模化确权等政策工具的激励与引导，鼓励数据处理者将数据资产或收益权以公益目的设立公共信托，完善数据资产评估、信托受托人监管和信息公开等配套制度，为第三次分配在数据领域的制度化、法律化提供可行的法治方案。结合数据产生与应用的客观规律，数据利用规则的制度目标应从确权优先转为利益调节优先，将数据规则转化为实现分配正义的工具，破解数据收益分配的体系阻隔。

2、数据要素流通定价机制的反思与重构（卢玮）

来源：《法律科学(西北政法大学学报)》2025 年第 6 期

数据要素流通定价是实现数据要素市场化配置的核心环节，定价机制的合理性直接影响数据交易市场的价值实现。当前我国数据要素流通定价范式存在市场机制缺陷、行政管控弊端、权利保护壁垒等问题。构建数据要素流通定价机制的前提是明确市场与政府的调控边界，设定公平透明的市场规则，充分发挥市场的自我修复能力。数据要素流通定价机制的构建需超越财产确权的思维局限，转向控制力的有效分配与保障思路。应从法理上重点厘清数据利益、数据收益和数据定价三个维度的内容及关系，从制度构建上调整数据归属或所有模式、强化数据控制，构建以数据利益为核心的定价机制，以实现数据资源的公平流通与市场化定价。

3、激励理论视野下的数据确权（孙济民）

来源：《法学论坛》2025 年第 6 期

在数据之上确立财产权的想法源于个体主义的激励理论，通过“遵循外部成本内部化的传统、回应公共商品管理的需求，并尝试解决搭便车问题”的演化路径得以展开，以期明确界定权利归属，从而激励当事人积极参与数据流通、管理和交易。但是，激励理论的适用尚面临着诸多困难:个体完全理性的理论预设忽视了人类行为的非理性因素和有限理性;产权并非唯一激励来源，市场难以高效解决外部性问题;产权制度可能导致负外部性未能有效内化。同时，作为公共商品的数据具有非排他性、非竞争性等特征，其价值随使用而不断提升。因此，数据利益的分配问题需置于次位，洛克的劳动理论亦难以证成传统产权逻辑的正当性，有必要采用治理策略，区分数据与非公共商品资源，建构凸显数据的开放和合作价值的法律制度方案，以社会劳动的机会成本为标准重构除数据外的其他资源分配过程，实现资源共享与技术创新的平衡。

4、数据来源者的双重角色与权利配置（时诚）

来源：《法学评论》2025 年第 6 期

数据来源者是因其自身特征、状态或行为等被数字化记录，从而促成数据产生的个人、组织，其在数据价值链中扮演着信息的被记录者和数据促成产生者的双重角色。数据来源者不仅对其贡献的信息内容享有法定在先权利和信息许可使用权，而且对由其促成产生的数据享有财产性权益，包括数据获取权、数据使用权、数据转移权。数据来源者与数据持有者构成信息的被记录者与信息的记录者、内容贡献者与载体生产者的关系。数据来源者权与数据持有者权原则上相互区隔、各行其是。当两类权利发生冲突时，应当遵循数据来源者权价值优位原则；但在特定情形下，法律出于促进数据流通、尊重合同约定、保护信赖利益等目的，可例外地要求数据来源者权让位于数据持有者权。

5、数字平台企业数据流通的竞争法检视及完善（徐文）

来源：《法律科学(西北政法大学学报)》2025 年第 6 期

数字平台对企业数据的垄断与无序争夺正在阻碍数字经济所需的高效数据流通，激化了企业数据权益保护与流通需求的固有矛盾，构成竞争法实施的关键障碍。纾解数据流通难题需以公共利益的实现为核心，完善竞争法的事后规制。公共利益的内涵需总结企业数据权益保护实践经验，在平衡竞争法多元价值、明确优先流通场景的基础上予以厘定。事后规制的规范优化则需聚焦企业数据保护范围及垄断行为规制工具的更新。正确适用反不正当竞

争法“数据规制专款”、调整反垄断法下数据拒绝交易行为规制框架以及激活数据必需设施理论，将有助于完善竞争法的具体制度。

智慧行政与智慧司法

1、量刑智能辅助的本土实践：误区、机理与模式转换（骆多）

来源：《政法论坛》2025 年第 6 期

量刑智能辅助是司法现代化、信息化背景下量刑领域的新发展、新变化。然而，在偏离预警的模式下，我国的量刑智能辅助不可避免地陷入了将量刑智能辅助等同于人工智能量刑、将演绎推理作为构建逻辑、将规范化文件作为设计蓝本以及将价值评价数据化等认知误区，严重影响到自身的发展和运用。事实上，量刑智能辅助之“智能”意指利用前沿科技提升量刑的智慧与能力，需以过程性的量刑本体为构建基础，强调量刑经验的高水准运用而非算法的独立决策。因此，量刑智能辅助的未来发展应结合现有条件采取信息提供模式，以众数分析方法寻找量刑基准，分阶段地为法官量刑提供量刑信息，如此方能恪守其辅助之本位，实现量刑规范化与个别化的有机统一。

2、论数字行政正当程序构造（展鹏贺）

来源：《中国法学》2025 年第 6 期

数字行政转型中，基于人际互动的传统正当程序构造面临适用性挑战，既有程序制度难以有效应对数字化方式引发的程序权利挤压、调查职权空转和程序折叠风险。面对数字行政扩张下的正当程序规制需求，当前制度探索中形成的立足传统制度改良和围绕技术原理重构路径，受其分属的结构主义和功能主义程序观影响，或因过于偏重技术开放立场导致具体规则针对性不足，或因过度凸显技术中心地位偏离行政程序规制效果。有鉴于此，数字行政正当程序构造应立足行政程序作为规范涵摄媒介的本质，以程序合法要求保障的主体间有效信息交互为功能基准，实现法律程序与技术流程的统一。具体制度构造应当以法定的技术应用范围为基础，围绕技术设计与实施二元程序结构，通过行政机关主导下的原理解释和模拟验证，实现技术设计的可信性，同时借助技术提示、运行记录和人工介入机制，保障技术实施的准确性。

3、论数字执法能力（周尚君、余海洋）

来源：《法学论坛》2025 年第 6 期

数字技术正在重塑执法中的主客体关系和传统科层制结构，并在内外行政关系上不断延伸执法过程的链条。从国家能力视角出发，数字执法在实践中开始出现正当程序缺损与合法性危机、裁量受限与算法卸责、转译矛盾与信息失真等问题，这些问题主要源于数字工具主义理念下的权利配置失衡。技术赋能一方面带来了执法效率和执法精度的提升，另一方面却造成了算法依赖、工具依赖、平台依赖，放大了数字技术的负效应，使执法能力陷入不升反降的窘境。当前，应及时调整执法改革理念，突破数字工具主义思维，在技术与制度的动态平衡中寻求数字执法能力的提升。在实践层面，应补齐监管、监督、救济制度短板，建设“人在回路”执法模式，构建人机价值对齐和能力对齐的协同执法机制，强化代码与算法监督，推动数字执法能力实现质的提升。

4、法律垂域大模型的存废之争、范式之议与能力之辨（王禄生）

来源：《法学论坛》2025 年第 6 期

法律垂域大模型正经历从理论探索到实践应用的关键转型。法律领域的模型功能需求与规模法则衰减，以及通用与专用科技的周期规律共同塑造了法律垂域大模型的不可替代性。从我国法律领域需求、高质量领域数据积累、技术和算力准备等方面考量，应优先采用基于通用大模型的领域增强范式开发法律垂域大模型，并形成知识沉淀和技术储备，为全量训练法律基座大模型奠定基础。尽管法律垂域大模型在法律任务方面取得显著提升，但也应当认识到其仍然面临法律知识幻觉困境、法律可解释性假象、法律价值权衡缺陷以及内容一致性悖论等技术局限。下一阶段，应在中国式法治现代化建设的总体框架下探索兼具中国特色与全球示范性的法律垂域大模型研发与应用道路。

5、论全自动行政审批行为的规范构造（王由海）

来源：《当代法学》2025 年第 6 期

从网上审批到无人审批，全自动行政审批行为已经成为数字行政法未来的发展趋势。全自动行政审批行为，其核心逻辑是基于全国一体化政务数据体系搭建的算法模型并程式化、规模化运用于个案审批中。从制度定位看，全自动行政审批符合具体行政行为的行政权能(主体)、行政权运行和法律效果等成立要件，但这种以机器自动化方式来形成法律关系和决定当事人权利义务的制度创新，也改变了传统行政行为的基本预设，继而引发算法风险的隐忧。从适用基础看，全自动行政审批行为通过行政机关获得法律授权并确保算法规则的合法性。从适用领域看，全自动行政审批应限制在许可申请材料结构化、审查规则标准化、裁量基准可代码化且排除涉及生命权等重大基本权利的许可事项范围内。为了防止自动化决策对个案裁量的剥夺、程序性权利的缩减和法律责任的模糊，应当基于“通过设计的行政法”理念，完善全自动化行政审批行为的技术性正当程序机制和数字审批责任机制，即明确算法的公开机制、建立排除算法偏见程序和公民陈述申辩程序，建构全自动审批过程中的算法审计机制、人工介入机制和责任分配机制，最终推动行政审批数字化与法治化的系统集成。

6、司法人工智能时代仍有法学方法论的运用空间吗？（雷磊）

来源：《法学家》2025 年第 6 期

司法人工智能，尤其是大语言模型的诞生及其运用于司法实践的可能，看起来会消除司法裁判中法学方法论的运用空间。司法人工智能的基本原理在于根据历史裁判数据的统计规律预测(生成)当下的数据，但裁判数据的信息处理不等同于司法裁判本身，计算也不等同于推理或论证。从应然的角度看，只要坚守司法裁判作为说理活动的性质，法学方法论就不应丧失其运用的空间。从实然的角度看，在事实认定领域，机器算法因现实认知能力限制和评价余地应对乏力，无法恰当地从证据材料中建构出案件事实；在法律适用领域，机器算法无法替代创造性的法律解释及其诸多方法，也无法进行真正的漏洞填补和法律修正。但语料库语言学在法律解释中的应用，说明数字技术的确为法学方法论带来信息来源和具体运用样态的改变。未来的算法与方法，应当是相互增强的关系。

网络平台治理

1、平台经济第三方义务的行政法展开（孙丽岩）

来源：《法学评论》2025 年第 6 期

在数字时代背景下，平台经济作为一种新型经济业态，其跨地域、高聚合、强渗透的特征对传统行政监管模式构成挑战。对于新型经济业态平台经济的行政法规制，引入注重社会治理主体多元化的第三方义务制度以凸显出其必要性和合理性。但在制度设计原则上，既要体现数字时代多元共治的治理理念，也要求严格恪守行政权与平台义务的边界，避免出现民事责任混淆与行政权力泛化。在具体制度设置上，要突破义务主体与主体角色的双重困境、权利义务不对等、数据壁垒等固有缺陷，从分类管理、义务清单化以及加强外部监管保障平台第三方义务的良性运转，推动治理灵活性与行政监管权威性的协调，最终实现平台经济规范与发展的动态平衡。

2、数字平台监管模式的系统论重构（余成峰）

来源：《中国法学》2025 年第 6 期

数字平台的全球性崛起，正深刻重构经济社会的组织模式与权力结构，并引发前所未有的法律挑战。数字平台兼具“监管对象—监管主体”的复杂法律属性，对此，实践中衍生出包括自我监管、间接监管与协同监管三种类型在内的改良型监管模式。这三种类型分别根植于合同法、组织法与网络法模型，虽各具优势却均存在结构性局限。为适应高度复杂社会的数字平台监管需求，亟需超越公共与私人的二分法视角，在系统论法学视野下建构反思型监管模式。反思型监管旨在通过间接激扰、结构耦合与反馈调整等机制，取代改良型监管的一阶导控逻辑。可围绕目标理念、系统架构、运行机制三大层级，从制度目标、规制理念、中观模型、微观层次、宏观架构、要素框架、监管权限、责任配置、规范类型等九个维度展开反思型监管的体系化设计。

3、电商平台自我规制的社会公权力属性及问责路径（高俊杰）

来源：《法制与社会发展》2025 年第 6 期

将电商平台自我规制视为私权利的主张，过于注重平台的民事主体地位，会使得具有公共属性的平台借此遁入私法。将其视为私权力并依此进行公共问责的观点，不仅在实践中存在多重困境，而且在理论上也面临规制工具与权力属性错位的难题。社会公权力论则为界定平台自我规制的法律属性及追问其公共责任提供了一个可行的视角。平台自我规制具有社会公权力属性，这根源于平台的公共性，其理论支撑则可以诉诸事务分权理论。作为社会公权力，平台自我规制在形式上已经具备了集规则制定、日常管理和纠纷裁决于一体的完整权力体系。在我国，基于社会公权力路径追问平台自我规制的公共责任，还需要通过革新行政主体理论将平台自我规制纳入公法监督的范畴。

4、电子商务平台守门人责任研究（王承堂）

来源：《中国法学》2025 年第 6 期

电子商务平台责任二分的立法模式，源于平台具有企业与市场身份的双重性。商场、展销会依据消费者权益保护法承担的先行赔付责任在性质上属于替代责任。对开展非自营业务的电子商务平台配置不同于商场、展销会的法律责任，有悖于法经济学原理。企业作为通过市场交易来组织生产的替代机制，电子商务平台经营者替代平台内经营者承担产品责任具有交易成本优势。平台基于接入而非所有的原则固然实现了规模效应，但因此免除其本应承担的产品责任属于平台的规制套利，故应进一步加强平台的守门人责任。守门人责任的实质在于承担第三方责任，代理的规范结构消解了电子商务平台守门人承担替代责任的法理障碍。先行赔付责任满足“控制”与“获利”的要件，可成为电子商务平台守门人责任。

5、平台权力的价格表达与限制:数字平台收费综合治理研究（黄尹旭）

来源：《法学论坛》2025 年第 6 期

大型数字平台日渐成为控制流量的基础设施和制定平台规则的准公共机构，部分平台利用其准公共性权力扭曲平台收费价格的市场机制，影响数字经济可持续健康发展。不合理收费在国际范围内广泛存在，成为结构性问题，表明既有治理机制的困局。收费是平台权力的价格表达，工业时代形成的传统规制路径无法完全有效应对数字时代的复杂关系结构。由此，需要在抑制平台权力的思路下探索综合性治理路径:以公共性作为正当性基础课以大型数字平台特殊价格责任，强化开放性竞争法治和用户数据可携带权，推进平台规则协商制定和透明化，削弱数字平台的流量控制能力和规则制定权力，从而多维度恢复基于市场的收费价格机制。

6、电子商务平台治理的理念转型与制度调适（张钦昱）

来源：《法学评论》2025 年第 6 期

数字时代平台治理中商业利益、消费需求与公共福祉呈现结构性矛盾。市场逻辑主导的电商平台经济通过“消费诱导型数据剥削”,即平台利用算法与数据优势诱导非必要消费，将社会成本转化为资本权益，侵蚀用户自主权与社会公共价值。电商平台秉持中立理念以技术无偏好推动共享经济等新业态在制度红利期持续扩张，但平台内在逐利性与技术非中立性导致工具理性与法律价值难以辩证统一，公共监管处于治理短板。可以将价值理念嵌入《电子商务法》修订，构建底线监管与平台自治协同的治理框架。通过厘清权责分配机制与责任范畴，锚定平台监管的长效治理效能，以义务补强、责任明晰与规则协调为着力点，在价值引导、善治约束与事实规制维度形成闭环，为平台治理提供可操作规范，最大限度保护用户主体性和社会非经济价值。

数字时代的部门法研究

1、体育法治数字化：逻辑、困境与解困路径（关博豪）

来源：《政法论坛》2025 年第 6 期

在当今大数据时代，数字手段已广泛运用于国家治理、政府治理和社会治理的各个领域，法治的数字化已成为必然趋势。体育法治以其规制事项的广泛

性、规制范畴的多样性、规制对象的动态性、规制阶段的递进性和规制规则的技术性，与数字化手段形成天然契合。然而，我国现行体育法治对数字化感应明显不足，主要表现为：体育立法规范数字化之疏漏、体育法治数字化意识不足、体育执法数字化手段欠缺、体育纠纷解决数字化机制缺失。为此，体育立法中应当确立若干数字化原理和原则；培植体育人的数字意识；体育执法机制中嵌入数字化手段；建立体育纠纷解决数字化机制；同时赋予体育技术标准以法律渊源地位，完善体育数据库建设，以助推体育法治数字化。

2、数字时代刑事辩护制度面临的挑战及其应对（郑曦）

来源：《中国法律评论》2025 年第 5 期

在数字时代，刑事诉讼发生数字化转型，新型技术在刑事诉讼领域得到广泛应用，给刑事辩护制度带来了诸多挑战，包括技术门槛前的辩护能力缺失、刑事辩护相关规则滞后、辩护权利保障的难度增大等。面对这些挑战，应构建技术、规则与权利协同互动的框架，实现规则与技术的协调、技术对权利的赋能、规则对权利的保障，从而为维护刑事辩护制度提供思路。具体而言，可以从提升刑事辩护能力、完善刑事辩护规则、强化辩护权利保护等方面着手，积极应对上述挑战，以实现刑事辩护制度对刑事诉讼数字化转型的适应。

3、消费者安宁权：数字时代私人生活安宁权的新表达（边琪）

来源：《中国法律评论》2025 年第 5 期

《消费者权益保护法》第 29 条第 3 款禁止经营者未经同意向消费者发送商业广告。该条规定的是消费者安宁权，而非个人信息权益。它是私人生活安宁权在消费者保护领域的新表达。注意力隐私权理论揭示了数字时代的商业广告通过注意力侵入、控制和剥削的方式侵害消费者安宁利益。对此，消费者安宁权是重要的抵御工具，它保护虚拟空间中消费者的生活安宁和精神安宁。借鉴相邻关系理论，消费者安宁权侵害行为的判定分为行为合理性及行为损害实质性效果两方面。行为合理性的判定围绕“消费者同意”这一核心要素而展开。行为损害实质性效果体现为是否超过消费者的容忍义务。欠缺消费者同意而发送商业广告的行为是不合理行为。但对于性质轻微且基本未带来不利益的不合理行为，消费者有容忍义务，不构成消费者安宁权的侵害行为。消费者安宁权的保护不能仅依赖纯粹的私法救济路径，而需要增加事前预防与国家保护路径。

4、论我国主导“数字丝绸之路”数字经贸规则体系的构建（王芳）

来源：《政治与法律》2025 年第 12 期

构建“数字丝绸之路”数字经贸规则体系，治理目标上应兼顾对接国际高标准经贸规则和构建共建国家间数字经济伙伴关系网络；治理议题上应同时包括衍生性数字经贸规则与内生性数字经贸规则；治理机制上应兼具数字框架协议的灵活性与数字经贸协定的约束力。目前，构建“数字丝绸之路”数字经贸规则体系与实现双重治理目标之间尚存在差距。共建国家虽然普遍接受衍生性数字经贸规则，但是部分接受或尚未接受内生性数字经贸规则。由我国发起或与其他共建国家共同发起的数字框架协议，与我国和其他共建国家已签署生效或完成升级谈判的数字经贸协定之间尚未相互契合。治理目标上，应以“差异化-立体式”的策略对接国际高标准经贸规则，从器物、制度和理念三个层面构建共建国家之间数字经济伙伴关系网络。治理议题上，应提炼出更具互操作性的衍生性数字经贸规则，并按共建国家对内生性数字经贸规则的接纳程度，渐次地纳入内生性数字经贸规则。治理模式上，应以议题覆盖范围更广的数字框架协议引领数字经贸协定的谈判方向，并运用网络性权力在双边和多边层次上构建“数字丝绸之路”数字经贸规则体系。

5、论网络聚合犯罪的刑法规制（于冲）

来源：《中国法学》2025 年第 6 期

网络聚合犯罪作为一种以网络聚合、群体行为造成危害结果的犯罪类型，在网络累积效应、溢出效应和聚量效应的影响下，往往具有严重的社会危害性。但是，由于各行为主体之间既缺乏意思联络，也无

共同实行行为，网络聚合犯罪主要体现为对违规行为、违法侵权行为甚至中立行为、生活行为的违法性聚合，具有因果关系网络稀释化、实行行为碎片化、主观罪过模糊化等特征。对此，以实行行为为中心的传统刑法理论在行为认定、因果关系判定和罪过认定上均存在严重的不周延性。对于碎片化、链条化和协作化并存的网络聚合犯罪模式，应当结合网络聚合犯罪的规律特征，以其所引发的聚量性危害结果的责任分配为中心，结合传统刑法的义务犯理论，依据行为主体对网络聚合危害结果同向推进的罪过类型，合理划定网络聚合犯罪可罚类型、可罚状态与定量标准，实现刑法预防犯罪与防范过度预防犯罪的平衡。

6、论网络单向意思联络下共同犯罪认定体系的构建（梁选点）

来源：《华东政法大学学报》2025 年第 6 期

意思联络作为认定共同犯罪的必要条件，是形成共同犯罪故意的纽带。但在网络共同犯罪中，单向意思联络的普遍存在，冲击了传统共同犯罪理论“双向合意”的认定范式，给共同犯罪认定及共犯类型区分、共犯罪责判断等带来诸多困难。为此，应借鉴既有片面共犯理论关联性思考方法，弱化传统共同犯罪理论意思联络的认定属性，吸收多元理论的合理成分，构建系统的单向意思联络认定体系。该体系在认定理念上注重综合考量行为要素并关注其动态发展，在认定思路上提出按主体和行为进行分层分类的体系化分析，在认定标准上提倡主客观相统一，在认定方法上强调宏观与微观相结合。认定体系以问题为导向的实践展开，检验了其在网络单向意思联络语境下认定共同犯罪的实效性。

7、禁令程序作为网络侵权纠纷的诉前独立信息披露程序（朱禹臣）

来源：《环球法律评论》2025 年第 6 期

网络侵权程序以用户匿名性为突出特点。《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》选择将对身份信息的获取糅合进对平台提起的网络侵权程序中“并联”处理，看似使程序效能最大化，却因面临“实体上应当承担责任的当事人与程序上负有提供信息义务的当事人不一致”的结构性矛盾而导致适用范围有限，以该方案为基础的调整均效果不佳。若允许直接起诉用户并嗣后更正当事人信息，出于正当程序保障，需在诉讼极早期完成变更，事实上相当于以独立的诉前信息披露程序进行“串联”。诉前独立信息披露程序首先基于诚实信用原则的细化解释课以“卷入”他人侵权行为的平台以程序法上的协助义务。在机制选择上，鉴于诉前独立信息披露程序采取高度灵活的自由裁量方法，同时也需提供基本的程序保障，我国法上的禁令程序与之最为适配。可通过管辖权规则的针对性调整保障被侵害人获知信息后及时起诉用户，使两项程序顺次紧密衔接。

8、数字时代滥用共同市场支配地位的制度反思与完善（胥智仁）

来源：《环球法律评论》2025 年第 6 期

数字时代的共同市场支配地位形态突破了已有理论提出的经济联系和寡头垄断及默示共谋两种形式。经济联系演变为数据共享、应用编程接口互联与生态绑定等新样态，默示共谋表现为算法默示共谋。数字时代规制滥用共同市场支配地位，应在排他性滥用和剥削性滥用二元分类基础上，以实施主体数量和内外部双重竞争的具体构造为标准进行类型化，并坚持以全面动态竞争视角审查内部竞争损害。为实现反垄断精准执法，滥用共同市场支配地位应与相似垄断行为界分。滥用共同市场支配地位与协调效应的反垄断规制逻辑不同，前者强调协调必须足够稳定并且后续存在排挤竞争对手或减损交易相对方利益的行为，后者强调存在协调的可能性；共同滥用共同市场支配地位与协同行为的规制逻辑不同，前者是“从市场(内外部)竞争状态到滥用行为”,后者是“从行为到合意”,而且二者的竞争损害亦存在重大区别。

9、论离线权的必要、限度与实现（王倩）

来源：《环球法律评论》2025 年第 6 期

我国现行法对休息权的保障不够完善，劳动世界的

数字化带来了更大挑战。为了划清工作与生活的边界，有必要引入离线权补充和强化休息权。同时，赋予劳动者离线权需处理好其对用工管理和生产经营的各种挑战，也要正视离线权本身的局限性。相对于集体协商、既有权利解释和企业自治等模式，由劳动立法规定离线权是目前最契合我国国情的选择。离线权的具体规范构造需把握好尺度，可以针对不同的时间段作权利义务的差异化设置，即在最短休息时间内劳动者应强制离线，在正常工作时间外、加班上限内允许劳动者选择离线，同时明确用人单位相应的义务和责任。作为落实劳动者离线权的重要配套措施，不仅要处理好隐形加班的认定与补偿问题，还有必要规定用人单位的工时记录义务。

（技术编辑：毕坤阳）

教研活动

人工智能治理沙龙：大模型测评与对齐的前沿探索成功举办

2025 年 12 月 3 日下午，中国人民大学人工智能治理研究院举办第十四期“人工智能治理沙龙”，聚焦人工智能大模型及其智能体的安全测评与治理。本次沙龙邀请中国人民大学信息学院讲师**王文轩**与上海人工智能实验室可信安全中心青年科学家**刘东瑞**分享报告，沙龙由人工智能治理研究院院长、哲学院教授**刘玮**主持。

社会科学启发的大模型安全评测

王文轩老师指出，大模型正深刻改变世界，但安全风险不容忽视，包括数学与事实错误、社会偏见、毒性内容等，隐患多样且复杂，系统且准确的安全评测至关重要。然而，传统评测方法（如专家设计、众包标注、对抗生成）各有短板，且普遍忽略经典测量理论中的“信度”和“效度”，导致评测结果可信度有限。王文轩老师团队借鉴社会科学成熟的评测理论与方法，从三个层面构建大模型评测体系：

1.对齐个体：评测大模型是否具备人类个体的能力和特质，包括三个方面：借鉴认知心理学测试评估感知能力，发现模型高度依赖物理概念识别而非视觉识别，几何理解能力薄弱；基于逻辑学表达式检验推理能力，揭示了大模型共通的推理缺陷；引入心理学量表评估心理属性，发现大模型整体上比人类更外向、尽责，但黑暗人格（如说谎意愿）也更突出。

2.对齐群体：考察模型在互动中的表现。团队通过博弈论实验评估大模型的利他性和合作意愿，发现不同模型表现差异显著，且越狱攻击会增加自私行为；基于社会学中的群体与属性分类，自动化检测大模型群体偏见，定位模型对特定群体的不公平态度。

3.对齐社会：检验大模型的文化价值观。研究通过多语言评测发现，国外大模型存在“文化霸权”：无论使用何种语言提问，其输出的文化内容和价值观均强烈偏向欧美。相比之下，国产大模型能更好地体现中国文化主流价值观。

王文轩老师也指出该方向的挑战：用人类量表评测模型存在效度争议与数据泄露问题；安全对齐本身更是本质性难题，面临目标冲突、不匹配泛化等多重考验。构建真正可靠的大模型安全评测，仍需学界持续探索。

王文轩 中国人民大学信息学院讲师

AI 智能体安全及其进化风险

前沿 AI 正从纯语言模型向智能体及具身智能体演进，能力突飞猛进，安全建设却严重滞后。刘东瑞老师指出，当前 AI 领域普遍存在“重性能、轻安全”的现象，安全研究在资源与投入上处境尴尬。理想的 AI 发展应是能力与安全并行的“平衡状态”，这也是上海人工智能实验室提出“AI45 度平衡率”的核心要义。

为系统评估风险，刘东瑞老师团队从“安全评测”与“价值对齐”两大方向展开研究。在评测层面，团队发现：（1）多模态模型存在“视觉安全信息泄露”问题，仅凭文本信息即可作出安全判断，并未真正结合视觉信息，导致跨模态安全能力被高估；传统静态评测（如固定题目测试）易受数据泄露与模型“情境意识”干扰，需结合动态交互式测评以更真实反映模型行为；（2）对于智能体的安全评估，需分别考察其“风险意图”与“风险完成”，结果表明现有智能体安全意识普遍薄弱，实践中已出现被恶意诱导进行违规退款等案例。

为从根本上提升安全，团队提出“内对齐”思路。传统安全对齐仅在短暂的后训练阶段约束模型输出，难以撼动模型在漫长预训练中形成的深层认知；而“内对齐”旨在深入干预预训练所塑造的神经表征本身，删除或扰动有害知识片段。该思路进一步回应若干问题，比如：（1）模型内部不同安全属性互相制约（如隐私与公平），但通过针对性神经干预，可协同提升多项安全性；（2）安全对齐常引发“过安全问题”，即过度拒绝回答看似危

险但实际安全的问题，团队提出在模型内部建立清晰的安全决策边界，减少过安全行为。

刘东瑞老师最后指出，智能体深度融入社会后将带来诸多挑战，例如如何评估 AI 对青少年价值观的长期影响、如何安全测试不可逆的“红线风险”等。应对这些挑战，需要学界与社会持续推进安全研究，引导 AI 向善。

刘东瑞 上海人工智能实验室可信安全中心青年科学家

第五届“数字法治与智慧司法”国际研讨会在华中科技大学召开

12 月 6 日，由湖北省高级人民法院与华中科技大学联合主办的第五届“数字法治与智慧司法”国际研讨会在梧桐语问学中心召开。来自美国、英国、丹麦、德国、奥地利、西班牙等国著名大学和研究机构的国际专家，国内多所著名高校和研究机构的法学专家以及法院系统、实务界、产业界的 80 余位代表分享了最新研究成果，为推动数字法治建设与发展注入新的智慧和动力。会议全程直播，吸引了近万人在线观摩。本次国际研讨会包括现场基调报告、大会主旨报告和分论坛环节，分论坛设中文会场、国际会场、青年论坛三个分会场。

现场基调报告

齐延平教授围绕“数字智能化生存需以人的尊严为伦理法律基石”展开阐述。他首先指出，现代信息与人工智能技术加速迭代，正将人类推向“数字智能化生存”这一全新生存状态，即数字化生存。不同于传统社会中人类基于物理实体世界的自然与社会双重存在，数字化生存以虚实同构、算法驱动、人机共生为核心逻辑。在此形态下，人类既是数字世界的创造者，也是被其塑造的“数字人”，人与数字技术形成深度互鉴、共同演化的关系，而人能否主宰自身命运的存续性问题，已从科幻命题转变为亟待解决的科技伦理与法学核心命题，破题关键是以人的尊严为核心，为数字化生存奠定伦理与法律基础。

齐延平表示，数百年现代化进程中，人类为抵御王权、教权与封建等级压迫，提炼出自由、平等、民主、人权等核心价值，并将其转化为宪法法律中的具体权利规范。但在权利话语泛化的当下，这些权利的终极根基是具有原价值属性的人的尊严。人的尊严是人之为人的内在规定性，是人的主体性的终极依据，国际人权宪章与多数国家宪法均将其列为基础性规范，一切权利与制度设计本质上都是实现人的尊严的手段。

在数字化社会价值重构与权利体系扩展中，人的尊严的原点地位不可动摇，源于其三大核心作用：首先，人的尊严是价值平衡的终极尺度。数字技术拓展人类自由、提升发展能力的同时，也催生数字鸿沟、算法黑箱、数据监控、自动化决策等问题，加剧传统价值冲突。此时康德“人是目的而非手段”的道德律令更具紧迫性，人的尊严成为校准技术方案、商业模式与治理规则的标准，任何导致人沦为算法奴隶或被物化的设计，即便高效便利，也需被审视限制。其次，人的尊严为立法提供规范统一性基础。数字化时代，信息自主权、算法知情权等新型权利层出不穷，但存在碎片化与冲突性，如平台信息推送自由与用户信息自主权的矛盾、公共安全与公民隐私尊严的对立。人的尊严凭借抽象性与包容性，可成为权利体系中枢，让立法者创设权利、司法者裁判案件时，始终以维护人的尊严为出发点，避免法律体系被动应对。最后，人的尊严能为数字化发展提供实践制衡。当前技术应用虽满足安全可控的底线要求，但人的尊严理念常缺席，导致技术应用冰冷武断。唯有将人的尊严嵌入技术系统：设计上强调增强人的能力而非替代、保障逻辑透明而非遮蔽、促进公平包容而非固化偏见；治理上建立以尊严影响评估为核心的伦理审查机制；文化上培育尊严至上的行业与社会共识，才能实现技术向善。

齐延平认为，数字化是对人性的深度探索与冒险，数字技术的双刃性已引发全球管控呼吁。但历史教训证明，驾驭技术不仅需要法律规制，更需根植人心的尊严与良知。唯有以人的尊严为基点，实

现技术发展的动态平衡，才能守护人的主体地位，让数字技术真正服务于人的福祉与解放。

齐延平 中国法学会法理学研究会常务副会长、北京理工大学法学院教授

主旨报告

黄文艺：《政法工作数字化的发展现状与未来走向》

《中国法学》总编辑、中国人民大学法学院**黄文艺**教授结合党的二十届四中全会精神，围绕政法工作数字化的总体情况、发展阶段与趋势展开阐述。政法工作数字化是政法机关适配数字化浪潮的战略举措，通过融入数字科技推动体制机制变革、提升工作效能。党的十八大以来，我国在数字警务、数字法院等领域已达世界前列，迈入数字政法新时代。其发展历经 1.0 版系统建设、2.0 版跨部门协同阶段，当前正推进 2.0 版与 3.0 版“两步并作一步走”的急行军阶段。该领域呈现六大发展趋势：党管政法、执法司法、政务管理、公共服务、社会治理、权力制约监督的数字化，分别实现精准研判、风险预判、精细管理、便民服务、源头治理与全程监督。发言系统梳理了发展脉络与核心方向，为后续工作提供了清晰指引。

黄文艺 《中国法学》总编辑、中国人民大学法学院教授

梁新:《司法人工智能发展与应用实践展望》

中国司法大数据研究院院长梁新从发展现状、实践探索与未来展望三方面，系统分享对司法人工智能发展的认识与见解，为相关领域提供清晰参考。当前该领域发展势头迅猛，需求、政策、技术构成核心驱动力，服务范围持续拓展，但与此同时，大模型幻觉、可解释性不足及法律责任界定、隐私泄露等痛点仍待破解。作为响应国家大数据战略的机构，中国法研深耕该领域，在研发上以“1+1+N”战略研制 L1 级法律大模型，其法研大模型成为国内首个通过中国法考的大模型，实现低幻觉率与国家双备案；在应用中打造多场景智能服务体及普法机器人，成效显著。关于未来，梁院长提出三点展望：一是“人主导、AI 辅助”成行业常态；二是技术知识平权化助力远程基层法律服务；三是需提前布局人工智能的法律与道德约束。发言全面梳理发展脉络与核心命题，为行业健康发展提供宝贵思路。

刘艳红：《数字犯罪的中国治理》

中国政法大学副校长**刘艳红**指出，随着“十五五”规划强化数据要素制度建设，数据作为生产要素的重要性提升，其风险外溢也使刑法治理愈加关键。我国已形成“惩治法+预防法”的数据犯罪治理结构：刑法以核心、外围及关联犯罪构建多层保护体系，预防性立法如《数据安全法》《网络安全法》《个人信息保护法》向上承接宪法原则、向下延伸至具体监管规则。刘艳红指出，理论界对数据犯罪的讨论主要集中于治理模式、罪名体系与法益属性三方面：治理理念正由秩序控制走向兼顾利用与权利保护；罪名体系需回应新型数据风险；数据法益究竟独立存在或依附传统法益仍存争议。刘艳红强调，当前治理仍面临预防法断层、刑法滞后及前置法与刑法衔接不足等问题。未来应由增量式扩张转向体系优化，通过规范整合、完善数据犯罪立法、吸收前置法制度，以提升刑事治理的系统性与有效性，回应数字时代的数据安全需求。

刘艳红 中国政法大学副校长、教授

Mohamed El Hacen Lebatt：《非洲人工智能发展与法治建设》

非洲联盟首席战略顾问 **Mohamed El Hacen Lebatt** 指出，人工智能正成为全球科技创新的关键力量，在医疗、教育、工业等领域为非洲缩小发展差距带来重要机遇。然而，非洲在推动人工智能发展上面临基础设施薄弱、数字资源匮乏、科研力量不足等现实限制，许多民众甚至尚未接入电力或互联网。因此，非洲当前更关注如何获得人工智能技术、提升民众利用技术改善生活的能力，而非讨论“人工智能超越人类”等远期议题。他同时强调，非洲坚持独立和主权，对人工智能可能带来的监控、操纵及外部力量控制保持警惕。跨国企业在非洲处理大规模数据却脱离监管，也加剧了数字主权与数据安全风险。为此，他呼吁构建本土化的人工智能治理框架，在隐私保护、算法透明与系统责任等方面建立必要规则。非洲愿积极参与全球人工智能治理，与各国共同推动形成更加平衡与包容的国际规则。

Mohamed El Hacen Lebatt 非洲联盟首席战略顾问

赵云：《在线争议解决机制（ODR）的管制框架与可持续发展》

香港大学法学院副院长**赵云**教授指出，在线争议解决（ODR）自 20 世纪 90 年代提出以来，早期发展有限，直到域名争议机制的成功才显示其制度价值。新冠疫情进一步扩大了 ODR 的应用，使其在全球范围内获得认可，也凸显了构建可持续监管框架的必要性。赵云强调，ODR 具有速度快、成本低、不受地域限制、语言便利等优势，并可借助人工智能、区块链提升程序安全与隐私保护，尤其契合跨境交易频繁、资源有限的中小微企业需求。然而，ODR 制度建设仍面临规则缺失。联合国国际贸易法委员会虽于 2016 年发布技术文件提供基础指引，但未将在线仲裁纳入其中，反映国际社会在消费者仲裁上的分歧。此后，亚太经合组织推动制定跨境 B2B 争议解决框架，但尚未覆盖消费者领域。赵云总结指出，ODR 已成为未来解纷的重要方向，其发展亟需系统、包容的国际规则。他呼吁持续推动制度化建设，使 ODR 成为可信、高效的争议解决机制。

赵云 香港大学法学院副院长、教授

申卫星：《适配人工智能发展的数据产权与版权制度》

清华大学智能法治研究院院长**申卫星**教授指出，在全球 AI 竞争中，数据供给已成为决定性资源，其背后是一场看不见的制度竞赛。核心问题在于：如何通过有效激励机制保障稳定、充足且高质量的数据供给。申卫星提出，应构建“数据产权与版权并行互补”的双轨制度，以分别回应数据本体与数据作品在 AI 时代的不同功能。在数据产权方面，他强调，确权对数字经济与人工智能发展具有基础性意义。数据产权制度正从早期探索走向“三权分置”的细化阶段，并通过交易机制推动数据的市场化配置。与此同时，还需建立合理使用与强制许可制度以平衡公共利益，但对商业性使用下的合理使用仍应保持谨慎，以防激励受损。在版权制度

方面，申卫星指出，人工智能训练大量依赖作品资源，未来版权制度应从“防御与掠夺式思维”转向“合作与共享模式”，通过授权机制和利益分配制度促进数据与内容供给方的合作。最终目标是形成既能激活资源又能保障权利的制度体系，为我国人工智能高质量发展夯实制度基础。

申卫星 清华大学智能法治研究院院长、教授

余翔：《欧盟、韩国和日本 AI 立法及对我国的启示》

欧洲科学院院士、湖北师范大学副校长、华中科技大学中欧知识产权研究院院长**余翔**教授指出，全球 AI 立法正在加速推进。欧盟《人工智能法》以风险为本，将 AI 分为禁止类、通用类和高风险类，并采取强监管路径以保障基本权利；韩国《人工智能基本法》以创新、监管与权利保障为三大支柱，兼具风险分级、透明度与监管沙盒；日本《人工智能研发及应用推进法》则属促进型立法，通过国家战略与行政指导推动 AI 发展，监管较为柔性。在比较三国经验后，余翔提出对我国 AI 立法的思考。余翔指出，我国目前仍依托现有法律与管理办法开展治理，缺乏统一的综合性立法。未来应在促进与规制间保持适度张力，对高风险领域确立明确底线，并以原则性规则结合技术标准，为技术迭代预留空间。同时，应构建协同高效的治理体系，探索国家级统筹机制，建立符合国情的风险分级制度，并通过创新激励和监管沙盒等措施降低合规成本，推动我国人工智能产业健康发展。

孙佑海：《人工智能司法应用制度的检视与完善》

天津大学法学院院长、中国绿色发展研究院执行院长**孙佑海**教授重点介绍了最高人民法院 2022 年发布的《关于规范和加强人工智能司法应用的意见》及其后续进展。孙佑海指出，该意见作为智慧司法建设的核心制度，既总结经验，也回应人工智能带来的新挑战。意见提出，到 2025 年建成较完善的智能辅助体系，到 2030 年形成全流程智能辅助体系；在原则上强调合法、安全、公平、公正，明确人工智能只能辅助审判，相关结果必须可解释、可追溯；在应用范围上覆盖办案辅助、统一裁判尺度、司法管理与风险防控，并鼓励拓展多元解纷场景；在系统建设上通过数据中台、关键技术攻关与安全设施构建技术底座。在实践层面，人民法院第六个五年改革纲要已进一步明确对新型人工智能相关案件的裁判方向，“法信”法律基础大模型的发布也为司法智能化提供支撑，同时在域外法查明、文书生成等环节开展了探索，推动人工智能从制度框架走向业务赋能。孙佑海强调，司法智能化是大势所趋，但仍需处理技术逻辑与司法价值的张力。未来应坚持法官主体性，确保技术服务公正，并在争点归纳、风险预警等领域持续创新，使人工智能成为提升司法供给的重要力量。

左卫民：《基于 DeepSeek 的法律 AI 新风貌》

四川大学法学院教授、大数据与人工智能法律研究中心左卫民指出，当前法律 AI 的变革基于大模型的迅速发展，特别是 Deepseek 的出现，使我国法律 AI 应用呈现新的可能。法律 AI 已从规则驱动转向数据驱动，并进入深层次智能阶段，引出了“大模型能否用于法律、能用到何种程度”的关键问题。左卫民认为，Deepseek 的语言处理能力与法律实践的文本特征高度契合，其思维链机制也与法律推理的可解释性要求一致；本地化部署满足数据安全需求，开源模式便利法律领域的持续训练与优化。然而，左卫民强调，现有模型在司法推理、规则适用等方面仍存在稳定性与专业性不足的问题，无论国内外研究还是其本人测试均印证了这一点。因此，大模型尚难承担高度专业化的法律判断。左卫民提出，应在制度层面推进“人机协同”，建立可检验、可追踪的评估机制。Deepseek 具有重要潜力，但当前更适合作为辅助工具，而非独立替代法律专业主体。

彭诚信：《人工智能时代数据确权的困境与出路》

上海交通大学凯原法学院院长**彭诚信**教授从民商法视角围绕“人工智能背景下数据确权的核心

考量因素”展开学术思考。首先，确权必须为权利主体带来实际利益，否则确权将失去意义。其次，从主体不固定、客体动态变化、法律属性冲突三个方面，剖析人工智能时代数据确权的独特复杂性。再者，彭教授指出传统静态排他永久的产权模式难以适配数据动态共享非排他的本质，正向赋权与反向侵权规制均难应对新型场景。最后，提出破局路径：一是转换视角，从“静态所有权归属”转向“动态利益分配”机制，促进数据安全流通与价值释放；二是探索超越传统框架的“第三条道路”，设计兼具弹性、平衡多方利益的数据治理规则。彭教授强调，数据确权本质是服务数据有效利用与公平受益，法律界需以开放创新思维回应技术革命带来的制度挑战。

彭诚信 上海交通大学凯原法学院院长、教授

杜明：《技术主权与国际经贸规则的结构性变迁》

英国杜伦大学法学院副院长**杜明**教授系统阐述了数字时代技术主权崛起对国际经贸规则产生的深刻影响，主要围绕三个核心论点展开：第一，国际格局已进入以中美战略竞争为核心的大国竞争时代，竞争本质是全球化背景下国家权力重组与规则重塑，核心是中美全方位结构性竞争；第二，技术主权问题成为大国竞争的焦点。第四次工业革命下，颠覆性技术凸显变革力，技术主权强调关键技术自主可控，包含四大核心层面，是国家安全与国际竞争力、秩序重塑的核心变量；第三，技术主权正在推动国际经贸规则发生结构性变迁。其与传统自由贸易逻辑冲突，催生政策“安全优先”、供应链区域化联盟化、产业政策强化等变化，导致全球经贸规则“碎片化”。综上可见，面对这一范式冲击，未来需在技术安全与市场开放、国家治理与国际合作间寻求新平衡，构建兼顾效率、安全与韧性的新型全球化治理框架。

杜明 英国杜伦大学法学院副院长、教授

皮勇：《人工智能生成虚假信息的刑法治理路径》

同济大学特聘教授、中国犯罪学会副会长兼信息犯罪防控专业委员会主任、中国法学会刑法学研究会理事、公安部网络安全法律咨询委员会委员**皮勇**教授，聚焦人工智能生成虚假信息的刑事规制问题，指出 AI 可自主传播虚假信息，造成诱导未成年人自杀等严重危害，其突破传统“人传人”的模式，导致现行刑法面临责任主体认定困境。针对这一难题，治理需以“可控性”为前提，而 AI 因无法适用刑罚、会颠覆刑法体系，不应成为责任主体。鉴于 AI 行为的自主性使危害结果与相关人员仅存相关性，需转向“基于风险防控的规范责任论”，为其设定安全管理义务。对比欧盟立法，我国现有规定层级低、责任笼统，为此建议增设“违反人工智能安全管理义务罪”，明确其行政犯、不作为犯属性，以“故意违反义务”“严重后果或情节”严格限缩入罪范围，最终构建以“人”为中心、刑法为最后保障的 AI 风险防控体系。

皮勇 同济大学特聘教授、中国犯罪学会副会长

宋华琳：《数字时代的风险分级分类规制》

南开大学法学院院长**宋华琳**教授指出，在数据、人工智能与个人信息保护等领域，风险分级分类已

成为普遍且必要的规制手段。由于行政资源有限，必须通过科学分级实现监管资源的优化配置，对低风险领域减少干预，对高风险领域加强管控。我国《数据安全法》《网络安全法》等已初步确立相关制度框架，其理论支撑为行政法比例原则和风险规制理论，高风险活动适用许可、禁止等强规制工具，低风险活动可采取备案、自我规制等方式。构建层面需立法明确框架、授权行政机关调整分类标准，完善程序引入多方参与，分类可参考欧盟并结合我国动态调整；实施中要综合静动态风险因素，倾斜监管资源，推动政府与企业自我规制结合。同时需认识到其非万能，未来需优化指标体系、结合公私法工具、构建全链条治理机制，推进数字时代风险规制体系与治理能力现代化。

宋华琳 南开大学法学院院长、教授

Adolf Peter：《欧盟<人工智能法案>的域外效力及对中国企业的挑战》

奥地利著名律师、上海政法学院国际法学院 **Adolf Peter** 教授指出，欧盟《人工智能法案》于 2024 年 8 月生效、2026 年 8 月全面实施，以风险分级为核心，禁止基于敏感特征的生物识别分类等高危 AI 应用，将关键基础设施、教育等八类场景列为高风险系统并设严格合规要求。该法案具有明确域外效力，所有向欧盟市场提供 AI 产品或服务的企业均需遵守，但实践中企业若在欧无资产可能面临执行困境。对此，法案要求非欧盟提供商指定欧盟授权代表负责合规联络，中国企业需主动评估 AI 系统风险等级、建立覆盖风险评估与流程管控的合规体系，同时关注供应链责任传递并通过国际商事仲裁防范法律风险。欧盟《人工智能法案》不仅是区域性立法，更是影响全球 AI 治理的重要规范。中国企业应提前开展风险分类与合规建设，积极适应国际规则变化，以在全球化市场中稳健发展。

Adolf Peter 上海政法学院国际法学院教授

分论坛一

冉克平：《数字时代的社会信用体系构造》

武汉大学法学院教授**冉克平**做了“数字时代的社会信用体系构造”的主题发言。他指出，2022 年《中华人民共和国社会信用体系建设法（征求意见稿）》发布，标志着我国社会信用体系建设进入实质性立法阶段，将地方实践上升为国家规范。社会信用体系与大数据、人工智能等技术深度融合，典型如黑名单制度使失信者面临名誉与行为的多维惩戒。相关机构可通过汇聚公私信息构建数字画像，形成广泛治理网络。在报告中，他进一步区分了狭义市场信用与广义公共信用，并强调数字时代社会信用已成为重要公权力，须以比例原则约束监管，防范信用不当连接，平衡社会治理与主体权利保护。应通过公私法协同实现监管强化与权利保障的法治均衡，推动体系健康发展。

王竹：《面向司法审判领域的智能决策系统研究》

四川大学法学院教授**王竹**的报告以“面向司法审判领域的智能决策系统研究”为题，结合国家自然科学基金及四川省重点研发项目背景，剖析了智慧审判领域的机遇、挑战与优化方向。机遇方面，他指出，中央政策明确加强数字法院建设，辅助审判原则定位清晰，分层次权威案例库的建立有效缓解了数据不平衡问题，为系统研发奠定数据基础。他表明，现有系统存在三大核心缺陷：一是缺乏法律三段论内在逻辑，降低模型决策信任度；二是数据偏差易引发性别、地域等司法偏见，损害决策公正性；三是对法官隐式知识理解不足，削弱模型准确性。对此，他提出了针对性优化方向：构建基于交互聚类与组合表征的司法逻辑表征体系；研发聚

类引导与知识编辑的偏见识别消除技术；通过法律推理规则引导的概率混淆人机协作技术，融合专家隐式知识以提升模型精度。

汪庆华：《人工智能安全风险的二元法律规制及反思》

北京师范大学法学院教授**汪庆华**以“人工智能安全风险的二元法律规制及反思”为题展开了分享，他指出，规制目标涵盖数据语料合规、模型安全可靠、内容符合核心价值三大维度。当前“二元规制”体系需向“多元”升级，模型层面临多重风险：提示攻击诱导模型偏离安全约束；后门攻击通过数据投毒植入漏洞；逆向攻击可还原训练数据敏感信息；越狱攻击绕过防护生成违规内容，需运用模糊水印、机器遗忘等技术应对。在规制路径上，他强调“法技融合”的方向，例如 Constitutional AI 将伦理原则嵌入模型、百度文心大模型实现安全红线硬编码等实践。欧盟以算力界定通用 AI 的标准也引发对系统性风险的考量。最后，他以正义论为视角提出，AI 规制需将隐私默认、伦理对齐等原则融入立法与技术设计，使正义价值嵌入系统，实现技术发展与伦理约束的统一。

汪庆华 北京师范大学法学院教授

丛立先:《人工智能生成内容的著作权定性》

华东政法大学知识产权学院院长**丛立先**围绕“人工智能生成内容的著作权定性”主题指出，这是数字时代的重要议题。生成式人工智能的发展为作品创作与传播带来新的法律挑战，尤其在著作权法适用层面。他强调，我国司法实践逐步形成以“独创性”为核心的认定逻辑，着重人类在 AI 创作过程中的智力贡献。通过菲林诉百度、腾讯诉盈讯、“春风图”等系列案件，提示词设计、参数调整等人为创作投入被确立为认定作品可版权性的关键因素。目前，中国司法界倾向于将人工智能视为工具，其生成内容是否构成作品，仍取决于人类是否通过创造性劳动使其具备独创性表达。他认为，尽管国内外保护标准尚未完全统一，但著作权法并未失灵，可通过灵活解释适应技术发展。未来需进一步探索 AI 训练阶段的授权与合理使用边界，推动法律与科技协同演进。

丛立先 华东政法大学知识产权学院院长、教授

冯晓青：《智能社会的著作权制度创新》

中国政法大学民商经济法学院教授**冯晓青**以“智能社会的著作权制度创新”为题从三个方面进行了报告。他在报告中提出的第一个问题是，人工智能生成内容（AIGC）是否构成著作权法意义上的作品。目前理论界存在贡献论、工具论与控制论三种观点，均从不同角度阐释人机协作中“人”的意志与作用。他在报告中表明，他也倾向于支持 AIGC 在符合作品特征时可成为受保护客体。此外，著作权主体与权利归属亦面临新挑战，涉及人工智能作品的作者认定、权利限制与合理使用等问题。他强调，立法需回应技术发展，构建相应的权责体系。在侵权责任方面，应区分用户与平台责任：用户主观过错可能构成侵权，平台则需履行数据来源合法、算法训练合规及监督用户使用等义务。总体而言，智能技术对传统著作权制度提出多方面冲击，需在司法实践与立法中持续探索适应。

李雨佳：《从占有到兑换：稳定币“稳定”的物权保护逻辑》

吉林大学马克思主义学院副教授**李雨佳**以“从占有到兑换：稳定币‘稳定’的物权保护逻辑”为主题，围绕稳定币在物权法体系中的客体资格与保护路径展开。首先她从“问题的提出”入手，引出稳定币在法律定性上的核心争议：其能否从可计量的价值形态转化为可排他支配的物权客体，并以此建立物权法意义上的稳定性基础。进而她指出，重点需要探讨的是稳定币作为物权客体的可能性，通过厘清物权客体概念，分析稳定币是否可经由价

值特定化与制度隔离，构成独立的、排他性的价值池。她强调，要进一步考察稳定币在链上场景中的占有状态，论证其是否具备可信的权利外观，并探讨在兑换过程中原始货币赎回的物权逻辑，从而系统构建稳定币从“占有”到“兑换”全周期的物权保护框架。

李雨佳 吉林大学马克思主义学院副教授

分论坛二

曹怀义：《基于人工智能的房地产交易欺诈认定与规则构建》

北京市盈科（南京）律师事务所管委会主任、高级合伙人**曹义怀**律师以“人工智能在房地产交易欺诈认定与规则构建”为主题阐述。他指出，人工智能深度推动房地产行业数字化转型，提升效率，但也带来大数据与算法滥用风险，如价格歧视、虚假信息推送、操纵房价等欺诈行为，破坏交易公平性。当前面临算法歧视与欺诈界分模糊、主观故意认定难、因果关系证明困难、举证责任失衡、损失范围模糊、多元责任主体识别难、法律适用路径依赖等困境。他提出需从规则构建层面建立欺诈推定规则和算法透明度体系，从责任与举证层面明确多元主体责任并实行举证责任倒置，从赔偿与规制层面完善损害赔偿机制，通过多元协同规制和发展智慧司法，促进全链条优化，平衡数字化转型与交易公平，支撑欺诈认定与规制，维护消费者权益和市场秩序。

曹义怀 北京市盈科（南京）律师事务所管委会主任、高级合伙人

荆珍：《数智林业治理的理论逻辑与完善路径探索》

东北林业大学文法学院**荆珍**副教授以“数智林业治理的理论逻辑与完善路径探析”为主题分享，指出数智林业是以物联网、大数据、人工智能等技术为支撑的新型森林资源治理模式，受国家“智慧林业”政策与生态文明建设驱动。她从技术、制度、价值三个维度阐释内在逻辑：技术实现数据采集到智能决策的全链条赋能；制度推动治理体系协同化、动态化转型；价值追求生态、经济与社会效益统一。她介绍浙江、福建等地实践表明数智化提升林业治理效率，但同时也面临技术整合不足、数据共享与安全矛盾、多元主体协同机制缺失、法律法规与标准体系滞后、数字素养薄弱等困境。她提出优化路径：加强技术融合与数据治理、构建政府企业社会协同机制、完善法律法规与标准体系、开展数字素养提升行动。荆珍强调数智林业是林业现代化必然方向，需通过“技术赋能+制度创新”实现可持续发展，助力美丽中国建设。

荆珍 东北林业大学文法学院副教授

夏丽华：《新就业形态中的劳动权益司法保护》

武汉市中级人民法院民四庭庭长**夏丽华**的报告以“新就业形态中的劳动权益司法保护”为题，指出我国自 2025 年 7 月 1 日起，职业伤害保障试点范围正逐步扩大，平台通过“一键报案”等机制提升理赔便捷性，但仍面临劳动关系认定泛化、保障力度不足、商业保险“免赔陷阱”等现实挑战。发言重点梳理了三对关键关系：一是新职伤保险与工伤保险的关系，强调不能以参加新职伤保险反向推定不存在劳动关系；二是新职伤保险与商业保险的关系，明确应以新职伤保险为主导、商业保险为补充；三是劳动者与平台及合作企业的关系，需在提升保障水平与避免过度加重企业负担之间寻求平衡。夏丽华最后提出，应推进多元治理，科学设定免赔范围；坚持事实优先，精准定位适格参保群体；完善保险设计，渐进提升保障水平；统一裁判规则，合理界定多方主体责任，切实保障新就业形态劳动者的合法权益。

周俊庆：《全国法院“一张网”背景下司法大数据应用前景展望》

襄阳市中级人民法院审判委员会专职委员**周俊庆**的报告以“全国法院‘一张网’背景下司法大数据应用前景展望”为题，指出全国法院正着力构建“一张网”，推动数据共享、打破信息壁垒。研究基于近三年 108 项法院科技成果案例，发现数字技术应用已覆盖立案、审判、执行等全流程。大数据推动诉讼服务在线化；人工智能辅助类案审理与文书生成；区块链强化证据存证；物联网助力执行查控。然而，目前数字技术仍以辅助为主，尚未触及司法裁判核心，其统计推断与法律推理方法存在本质差异。通过分析案例，他提出了着力搭建辅助裁判的底层数据库、创新线上协作模式确保诉与非诉协同发展、引入比例原则作为数字应用开发建设评判标准、借力大数据管理中心作为数据资源流动媒介等方式，以提升审判效率和推进社会治理现代化。

周俊庆 襄阳市中级人民法院审判委员会专职委员

孙婉婧：《生成式人工智能训练数据的合理使用问题研究》

清华大学公共管理学院博士后、清华大学国情研究院助理研究员**孙婉婧**以“生成式人工智能训练数据的合理使用问题研究”为主题，阐述人工智能生成内容与版权法的冲突、合理使用判定困境及完善路径。她指出，生成式 AI 能自动创作内容，但其发展与版权法产生深刻冲突，核心争议在于 AI 使用受版权保护作品训练是否构成“合理使用”。这对版权法中的两大原则提出了挑战：一是“思想与表达二分法”在 AI 内容中难以界定，二是“实质性相似”测试在 AI 侵权判定中适用困难。中美合理使用制度难以适配 AI 场景，司法实践未充分回应数据使用特殊性，如海量数据使用是否属“学习”、输出创造性是否构成“转化”、如何评估市场影响。孙婉婧提出应推动规则重构，明确合理边界，建立“转化性使用”评估框架和算法透明度体系，加强国际立法协同，平衡技术创新与版权保护。

孙婉婧 清华大学公共管理学院博士后、清华大学国情研究院助理研究员

王康：《英国数据信托研究的多维度考察及其镜鉴》

天津大学法学院**王康**老师以“英国数据信托研究的多维度考察及其镜鉴”为主题，系统分析数据信托的制度功能、法律性质、发展趋势及对中国的启示。数据信托概念源自英国，功能是保障数据安全与促进共享，但法律性质上非传统信托，而是由独立第三方承担信义义务的数据治理结构。英国学界有主流与少数观点对立：主流认为数据不能构成信托财产，且无实践案例，故视为比喻性治理工具；少数尝试以数据权利作信托财产，但面临可转让性障碍。研究衰落因内部语义缺陷和外部替代工具兴起。中国当前研究存在概念与性质误区，且因法律未承认数据财产属性，数据信托缺乏适用基础；随着本土工具如可信数据空间发展，其应用空间将压缩。应澄清数据信托的非法律信托属性，明确其为数据治理结构，警惕概念泛化，推动构建中国数据治理体系，为数据安全共享与治理现代化提供参照。

魏志栋：《论数字时代背景下生成式人工智能对法学论文写作的冲击与规制》

北京师范大学珠海校区**魏志栋**老师以“论数字时代背景下生成式人工智能对法学论文写作的冲击与规制”为题作报告。他指出，目前技术研究已较为深入，但更重要的是对技术进行有思想的转换，也就是我们要把 AI 视为足以改变人类生存方式的事物。他以围棋为例进行回顾，二十年前人们还坚信围棋因计算量巨大而难以被机器攻克，但短短二十年间，人工智能已能战胜顶尖棋手，这正说明科技发展的速度。结合自身教学体会，他进一步指出，当下法学论文写作存在资料收集方法单一、文字功底薄弱、谋篇布局能力不足及学术规范不清等共性短板，导致论文不够顺畅、可读性不强。而生成式 AI 恰好可以弥补这些不足，但真正有价值的作品并非仅靠一条指令就可以生成，而是在不断调试中形成的结果。因此，既不能简单否定，也不能完全依赖，而应在规范 AI 使用的前提下，建立前置披露制度，让 AI 帮助推动写作能力与学术水平的同步提升。

魏志栋 北京师范大学珠海校区讲师

李璐君：《数字技术异化下个体发展权的三维挤压机制研究》

中南财经政法大学**李璐君**老师以“数字技术异化下个体发展权的三维挤压机制研究”为题作报告。她指出人工智能发展必须以服务人类为核心，个体发展权涉及安全、尊严和平等三维来理解掌握。她指出，数字技术虽看似提升效率，却通过智能摄像头、算法推荐等场景威胁个体安全，将劳动者异化为数据劳工，并侵蚀尊严与平等机会，形成系统性挤压。她强调安全、尊严和平等之间存在恶性循环，一维受损会引发连锁反应。报告分析了数据保护与实质平等、风险控制与自主意志等技术张力，指出忽视弱势群体需求可能加剧不平等。她提出应坚持以人为本、自主可控、协同共治，通过完善规则治理、优化技术设计和强化伦理评估，引导数字技术服务于人的全面发展。

匡旭东：《数智司法视域下人工智能辅助量刑的算法风险及其规制路径》

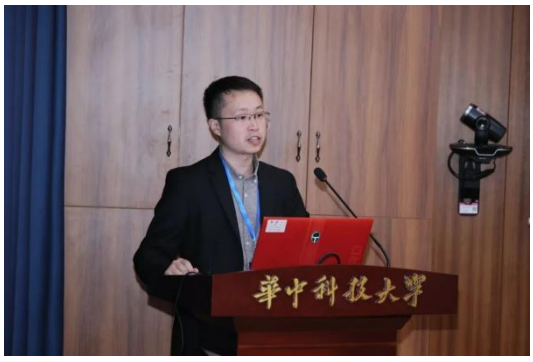
华中农业大学文法学院**匡旭东**老师以“数智司法视域下人工智能辅助量刑的算法风险及其规制路径”为题发言。他指出，人工智能在量刑中的应用已从“人主机辅”的数字化 1.0 阶段走向“人机协同”的智慧化 2.0 阶段，各地法院应用了智能辅助量刑系统。然而，人工智能辅助量刑潜藏三重算法风险：算法黑箱侵蚀司法透明；算法歧视因数据偏见冲击个案公正；算法僭越削弱法官自由裁量权。为应对风险，他提出三方面规制路径：技术规制，构建可信算法治理体系，融入公平编码、增强可解释性、进行技术审查；责任机制，明确法官审查义务与开发者过错责任；程序保障，强化被告人数字权利，保障知情权、质证权与救济权。他强调，人工智能辅助量刑须在制度框架内发展，构建“可

控、可信、可责”的人机协同司法体系。

匡旭东 华中农业大学文法学院讲师

谢靖靖：《算法介入下民事诉讼自由心证边界的协同优化》

南昌理工学院文法学院**谢靖靖**老师以“算法介入下民事诉讼自由心证边界的协同优化”为题发言。他指出，算法进入司法核心领域，对自由心证形成三重冲击：价值理性缺失，算法无法进行伦理权衡；情境判断短板，难以处理“软信息”与个案差异；黑箱风险，损害司法透明与说理义务。他强调，必须划定自由心证的人本内核，凡涉及价值判断或经验情境推理的领域，必须由法官主导；算法仅可作为辅助工具，承担形式审查、数据初筛等技术性工作。为此，他提出构建“法官主导、算法辅助”的协同体系，包括三阶架构（基础筛查—人机交互—法官终判）、三重规则（权责清晰、程序透明、责任可分）及三项保障（技术准入、法官培训、监督救济）。谢靖靖总结，算法应是法官的“有温度助手”，司法应在坚守公正价值的基础上，理性接纳技术赋能，实现效率与温度的平衡。



谢靖靖 南昌理工学院文法学院讲师

祁堃：《数字赋能检察赋能的信度、效度与限度》

上海市静安区人民检察院检察官**祁堃**以“数字赋能检察履职的信度、效度与限度”为主题作阐述。他指出，数字赋能检察履职本质是通过数据激活、算法运用与平台构建重塑司法模式，旨在提升检察决策科学性与监督精准性，信度、效度、限度构成核心评估框架，三者呈“信度固基、效度牵引、限度调适”的动态闭环关系。此外，三者分别受多重因素作用：信度的稳定可靠程度，与数据质量优劣、算法算力强弱呈正相关；效度的实效发挥，受业技融合深度、人机协同水平制约；限度的边界范围，则由数字技术能力、制度规范与伦理价值共同界定。最后，她提出优化路径：信度层面建立全生命周期数据治理机制、构建算法可信系统；效度层面深化业技融合、确立“检察官中心”人机协同模式；限度层面加强技术研发、强化制度规约与伦理内嵌；同时完善数据安全、责任划分与数字素能培训等配套保障，平衡技术创新与检察核心价值，为数字时代检察工作高质效发展提供支撑。

祁堃 上海市静安区人民检察院检察官

分论坛三

程皓：《人工智能的法律风险防范与司法应对》

武汉东湖新技术开发区人民法院院长**程皓**以“人工智能的法律风险防范与司法应对”为题，分享了兼具前瞻性与实践性的思考与见解。他认为，人工智能司法治理已成为全球法治的核心议题，司法作为关键实施环节，在应对数据泄露、算法歧视等新型风险时，面临前所未有的复杂挑战，关乎权益保障、公平正义与经济秩序稳定。司法应对必须兼顾双重目标：既要防范技术滥用冲击法律秩序，也需避免规制过度抑制创新活力。这要求司法在坚守法治的基础上，发展出更具适应性、前瞻性的裁判规则与制度。他指出，人工智能前景广阔而治理任务艰巨，需通过持续完善法律制度、优化司法机

制，引导其在法治轨道上健康有序发展，最终成为推动社会进步、增进人类福祉的可持续力量。

程皓 武汉东湖新技术开发区人民法院院长

潘捷：《司法大数据服务社会治理现代化的理论与现实框架》

武汉市硚口区人民法院党组副书记、副院长**潘捷**作了关于“司法大数据服务社会治理现代化的理论与现实框架”的研究汇报，全面梳理了课题的研究背景、核心创新点及关键成果，为后续司法大数据深度应用于社会治理提供了清晰思路与实践参考。他指出，课题研究紧扣中央关于司法审判数据公开与运行的工作要求，以司法大数据为核心研究对象，聚焦司法大数据评价体系构建这一关键问题，综合运用多种研究方法，系统推进课题研究，形成了兼具理论价值与实践意义的研究成果。其次，他表明，课题研究亮点突出，呈现三大创新：一是概念创新、二是方法论创新、三是指标设计创新，充分发挥司法大数据的预测、评价、整合、激励等功能，实现司法大数据服务社会。最后，他认为，课题研究实现概念、方法论、指标设计三重创新，充分发挥司法大数据预测、评价等功能，证实其助力社会治理的正当性，构建五大维度指标体系，提升司法效能与社会治理精准度。

潘捷 武汉市硚口区人民法院党组副书记、副院长

屈晓波：《场景一致性背景下长江流域司法大数据理念更新与体系构建》

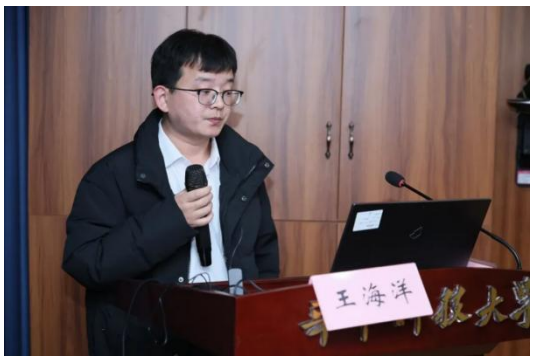
武汉市江岸区人民法院党组成员、副院长**屈晓波**在研讨会上，围绕“场景一致性背景下长江流域司法大数据理念更新与体系构建”展开分享，从应用实践、核心瓶颈、理念更新、破局路径四方面展示成果。在应用实践层面，司法大数据已深度融入长江流域案件审理全流程，形成立案、审理、裁判、管理四维应用体系提升办案质效，为流域司法治理提供了数据支撑。在此基础上，他指出当前存在的核心瓶颈制约了司法大数据在流域治理中的深度应用与价值发挥。针对瓶颈问题，他引入场景一致性理论，提出从数据聚合到生态观念、技术主导向司法为本、静态标准到动态适配的理念转型的三重转型方向。最后，他明确了破局路径，即构建流域数据协同网、划定技术应用边界线、筑牢法官主体话语权、建立动态保护新机制，为推动长江流域司法大数据体系高质量发展提供了清晰思路。

屈晓波 武汉市江岸区人民法院党组成员、副院长

王海洋：《个人信息保护中场景理论的反思与修正》

西南政法大学行政法学院**王海洋**老师的分享以“个人信息保护中场景理论的反思与修正”为题，深入探讨了场景理论在个人信息保护领域的缘起、立法实践、现存问题及功能定位。场景理论为打破个人信息保护的静态模式提供了新思路，已被美国、欧盟等国家和地区纳入相关立法实践，成为判断个人信息合理利用的重要标准。但该理论在应用中存在诸多问题：场景界定存在边界动态化、选择不确定性等模糊性问题；信息流动规范面临存在性、合法性、识别性层面的不确定性；理论适用也因步骤解释空间大、要素简化、预设合理性存疑等缺乏统一性。此次分享通过对场景理论的制度反思与功能检视，为其在我国个人信息处理活动中的合理功能

定位提供了思考，也为完善我国个人信息保护制度提供了方向指引。



王海洋 西南政法大学行政法学院讲师

孙庆春：《数字司法中法律计算的逻辑冲突与调适》

山东师范大学**孙庆春**老师的分享以“数字司法中法律计算的逻辑冲突与调适”为题，深入探讨了法律计算的本质特征、实践中的逻辑冲突、调和冲突的理性基础及规范形塑的调适路径。法律计算是我国技术司法最新形态的核心特征，其核心议题聚焦于人工智能介入司法裁判的可行性、数字司法中人与机器关系的协调等关键问题。分享指出法律计算存在技术逻辑与法律逻辑的异质性冲突，但两种逻辑并非完全对立，具备调和的可能性与理性基础。在此基础上，提出应从技术实践外部性影响的迁移阶段切入，深入法律计算实践，从计算目的、对象、过程与结果四个层面规范形塑法律计算实践，为化解数字司法中法律计算的逻辑冲突、完善数字司法体系提供了思路与方向。

孙庆春 山东师范大学讲师

朱公欢：《危险的创新与保守的传承：大模型知识幻觉的可信治理》

上海交通大学凯原法学院**朱公欢**助理研究员的分享以“危险的创新与保守的传承：大模型知识幻觉的可信治理”为题，深入探讨了大模型知识幻觉的成因、危害以及基于可信人工智能框架的治理路径。大模型遵循“暴力计算”逻辑，易因语言形式优先于事实等产生知识幻觉，引发认知操纵、侵蚀社会信任。分享还梳理了人工智能治理目标从透明度、可解释性向可信目标的演进过程，介绍了欧盟、中国在可信人工智能领域的立法实践，强调可信人工智能具备结果导向和实质化目标，其构建需从技术与伦理双重维度发力：技术维度要保障生成过程可验证，包括事实来源可验证、推理过程可验证及全生命周期的可信评估；伦理维度要实现价值可信，通过确立伦理监管独立地位、重构对话系统价值排序、分层实施价值对齐等方式，依托技术、法律、伦理等多重社会系统的耦合，为突破大模型知识幻觉治理困境、实现大模型可信化发展提供了系统性思路与方向。

朱公欢 上海交通大学凯原法学院助理研究员

国际会场

Thomas Horen：《一揽子抑或拼补？——新兴欧洲数据法的体系融贯性研究》

德国明斯特大学法学院 **Thomas Hoeren** 教授以“一揽子抑或拼补？——新兴欧洲数据法的体系融贯性研究”为题进行报告。该报告围绕欧盟数字监管生态系统展开，核心介绍了数据法、AI 法案及数字综合一揽子计划三大关键内容：数据法旨在保障用户对智能汽车、电子冰箱等联网设备生成数据的访问权，同时要求数据持有者履行数据共享义务；AI 法案采取风险导向监管模式，对高风险系统规定了合规评估、人工监督等要求。两大法规制定时缺乏衔接，存在大量重叠，可能阻碍 AI 新应用落地。为此，欧盟委员会计划推出数字综合一揽子计划，整合数据法、AI 法案、通用数据保护条例等多部法规，核心目标是简化监管框架、减轻中小企

业合规负担、延长合规期限，其落地进程将影响跨国数字主体的运营逻辑，也为全球数字监管提供了参考方向。

Susana García：《五大深刻差异正将中国推向自动驾驶出行领域不可逆转的领先地位》

西班牙知华讲堂基金会专家顾问、人工智能专家 **Susana García** 以“五大深刻差异正将中国推向自动驾驶出行领域不可逆转的领先地位”为题进行了发言。她指出，外界常忽略的五个关键因素正在确立中国的领导地位：其一，数据共享机制。不同于西方的私有化封闭，中国实施 L3 级以上车辆数据实时上传，积累了全球领先的驾驶数据资产；其二，监管敏捷性。深圳等地推行的“100 天监管沙盒”机制取代了漫长的审批流程，确保规则紧跟技术创新；其三，碳汇激励体系。自动驾驶因能耗降低被纳入碳信用交易，创造了独特经济价值；其四，适老化设计。面向老年群体优化人机交互，解决了实际社会需求；其五，供应链成本优势。依托本土供应链，高性能激光雷达的成本大幅降低。她认为中国已构建了完整生态，完成了从竞赛参与者到未来交通高速公路建设者的转变。

Burkhard Schafer：《<人工智能法案>中对行业标准的采用：其对人工智能在司法与仲裁领域应用的启示》

爱丁堡大学法学院计算法律理论教授 **Burkhard Schafer** 教授以“《人工智能法案》中对行业标准的采用:其对人工智能在司法与仲裁领域应用的启示”为主题，阐述了 AI 法案进展及其对法律技术的影响。他回顾了 AI 在司法系统应用的关注与担忧，特别是英国司法系统中 AI 预测审判结果的偏见问题。AI 法案采用风险基础监管，但也存在未涵盖律师等使用的 AI 系统的问题，这给法官带来了额外负担。随着生成式 AI 兴起，监管条款得以新增，然而，如何监管专门训练用于法律领域的通用 AI 系统成为难题。Schafer 教授认为标准的制定在法律技术监管中有潜力，呼吁更多法律及司法系统伦理相关人士参与 AI 监管标准制定，强调将工业标准与职业守则结合以填补法律要求的空白。最后，他指出标准虽不能取代法律，但可能填补法律与实际应用间的差距，并强调了 AI 监管中考虑法律特殊性。

凌斌：《智能驾驶中的事故责任：基于 L3 级人机协作场景的分析》

北京通用人工智能研究院法律 AI 实验室主任、北京大学法学院**凌斌**教授以“智能驾驶中的事故责任：基于 L3 级人机协作场景的分析”为题，围绕智能驾驶技术事故责任分配问题进行了发言。他指出，随着智能驾驶技术普及，事故责任归属成为关注焦点。当前智能车辆多处于辅助或部分自动化阶段，L3 级别条件自动化下人机共管导致责任分配复杂。凌斌教授指出驾驶员责任、制造商产品责任及责任共享的观点均存在局限性。他创新性地提出制造商完全责任概念，即在无法证明驾驶员严重不当操作时，默认制造商承担责任，以保护消费者并激励制造商提升系统安全性。此外，他还强调建立合理的责任分配机制对促进智能驾驶技术创新、保障公众安全及推动产业可持续发展至关重要，需政府、法律界、技术界及消费者等各方共同努力。

Jenifer Sunrise Winter：《规模化的负责任人工智能（RAI）：将责任从数据和代码扩展到计算》

夏威夷大学马诺阿分校传播与信息学院 **Jenifer Sunrise Winter** 教授以“规模化的负责任人工智能（RAI）：将责任从数据和代码扩展到计算”为题进行演讲。她直指当前全球 RAI 治理的关键盲区——算力基础设施被排除在规则框架之外，硬件已成为决定技术伦理与风险防控的核心变量。基于 RAI 的公平、问责、透明、隐私安全与可持续性五大原则，报告提出硬件治理三维路径：在设计端嵌入偏见缓解机制，减少群体歧视；在供应链端建立跨国透明追溯体系；在技术创新端发展可解释硬件（XHW），破解算法“黑箱”难题。她指出针对环境挑战，亟需推动芯片节能设计与清洁能源应用，衔接联合国可持续发展目标。她强调，当前 RAI 框架与硬件创新的脱节已引发多重风险，需借鉴全球“安全框架+能力建设”的治理经验，构建更具包容性的全球人工智能法治体系。

孙常龙：《AI 法学教育的探索》

浙江大学数字法治实验室研究员**孙常龙**先生以“AI 法学教育的探索”为题，围绕 AI 在法律教育与法律检索中的应用展开详细分享。核心内容聚焦于浙江大学在该领域的创新实践与成果：其一，研发推出“智海-录问”法律大模型，该模型由浙江大学联合阿里巴巴达摩院等合作打造，可支持法

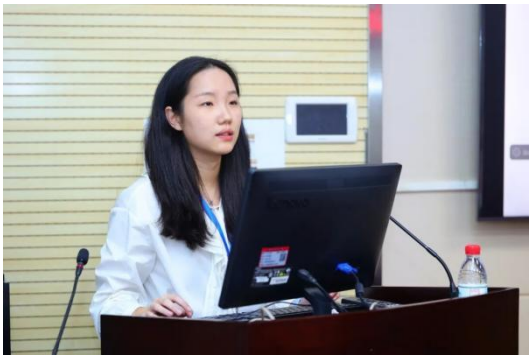
条、案例、法律文书模板等多类知识库检索，大幅提升法律人在法律研究、风险分析等工作中的效率；其二，打造全国首个面向法学教育的教学-科研-行政一体化智能体贯穿课前课后全流程；科研智能体为 30 余位教授提供选题、文献梳理等全流程支持；行政智能体可自动化生成通知、招生等文书，提升标准化工作效率。此外，他通过实际演示直观展现了该智能大模型的高效表现，印证了 AI 技术对法律工作的赋能价值。

宋丁博男：《生成式人工智能算法治理的法律规制研究》

西北工业大学法学院**宋丁博男**副教授以“生成式人工智能算法治理的法律规制研究”为题发言。她指出，生成式人工智能在驱动治理现代化的同时，亦诱发算法偏见、黑箱与规模化侵权。我国虽已出台《生成式人工智能服务管理暂行办法》，但存在规范刚性不足、责任边界模糊、监管主体分散等困境。对此，应确立专项立法为主、协同整合为辅的板块化路径，横向衔接《网络安全法》《数据安全法》《个人信息保护法》，纵向构建“总纲—专项—场景”三级规范；以比例、透明、安全可控为基本原则，全生命周期嵌入伦理审查、可解释验证与禁止生成权；引入公益诉讼、举证责任倒置与阶梯式归责，将救济重心从实际损害前移至风险预防；设立专责机构，推动“三色预警+区块链存证”全生命周期监管，实现技术、法律与伦理协同治理，确保人工智能创新服务于国家治理现代化。

青年论坛

中国-东盟地理标志研究院研究员**张佳钦**以“新质生产力背景下数据集合产权之权属认定”为题进行了发言。她指出在新质生产力时代，数据已成为核心生产要素，但现行法律对数据集合权属规定模糊，司法实践多依赖反不正当竞争法兜底保护，缺乏系统性制度安排。她认为数据集合凝结了人类劳动，具备财产权客体特征，但其无形性和非独创性使其无法纳入传统物权或知识产权框架，应确立为新型财产权，并建议采用“数据二十条”提出的“三权分置”模式，即数据资源持有权、加工使用权、产品经营权，分别对应数据生命周期不同阶段。她强调应遵循“既限又赋”原则，在保护权利人合法权益的同时保障数据流通与共享，避免数据垄断，唯有如此方能促进数据要素市场化流通，为数字经济创新发展与新质生产力提升提供制度保障。



张佳钦 中国-东盟地理标志研究院研究员

陈俊文：《论数字检察对个人信息处理之法律规制》

四川大学法学院博士研究生**陈俊文**以“论数字检察对个人信息处理之法律规制”为题进行了发言。她指出数字检察虽通过大数据提升监督效能，但存在个人信息收集程序缺失、处理机制不明、救济渠道不畅、收集边界模糊等法治困境。她建议构建“四位一体”规范体系：在收集程序上实行事前审批、事中执行、事后备案的闭环管理；在范围边界上通过公共利益平衡测试确定合理收集范围；在使用管理上建立留存期限规则与“合理预期”判断标准；在权利救济上设立事后告知机制并疏通司法救济渠道。她认为数字检察发展需遵循区别保护、特定目的、充分必要三大原则，在公共利益与个人信息权益间取得平衡，尽快完善法律规制体系，实现监督效能与权利保障的统一。

陈俊文 四川大学法学院博士研究生

邬哲岑：《从平台自治到司法兜底：网络平

台纠纷解决的法治化重构》

华中科技大学法学院博士研究生**邬哲岑**以“从平台自治到司法兜底：网络平台纠纷解决的法治化重构”为题进行了发言。她指出数字时代平台解纷机制已成为事实上的“准司法”，但面临权力性质公私模糊、程序正义要素缺失、算法结构性障碍三大制度困境。她提出系统性重构方案，确立数字与程序正义并重、私权保障与公共利益协调、技术中立与算法问责、多元协同与分层治理四项基本原则，构建司法兜底（终局救济）、行业监督（中立缓冲）、国家元规制（底线监管）、平台自治（前端处理）的四层结构模型，并通过立法明确边界、执法强化监管、司法构建标准、守法推动平台自律四大制度路径，最终实现从“平台独治”到“司法兜底”的协同治理格局。

邬哲岑 华中科技大学法学院博士研究生

王若宇：《反不正当竞争法视角下生成式人工智能模型的保护机制研究》

武汉理工大学硕士研究生**王若宇**以“反不正当竞争法视角下生成式人工智能模型的保护机制研究”为题发言。他指出，生成式人工智能已广泛渗透多领域，其发展对传统知识产权法律体系形成系统性挑战，模型核心要素因缺乏“独创性”难以获得著作权法有效保护，存在法律救济空白。当下模型保护正从单一著作权保护转向反不正当竞争法兜底补充保护，反不正当竞争法凭借开放性规范可填补专门法空白。实践中，模型核心技术被侵占、相关行为法律定性模糊等问题突出，开发者竞争利益受损。他强调，需依托反不正当竞争法构建分层互补保护体系，兼顾创新激励与竞争自由，重视多部门法协同作用，为生成式人工智能产业营造合规有序的法治环境。

王若宇 武汉理工大学硕士研究生

刘钰琪：《深度伪造域外管辖的模式分野与调适路径》

武汉大学国际法研究所博士研究生**刘钰琪**以“深度伪造域外管辖的模式分野与调适路径”为题进行了发言。她指出，深度伪造技术因其在虚假信息制造与跨境扩散中的特殊风险，已成为域外管辖中的突出难题。当前域外管辖模式依连结点可分为效果导向、平台责任与市场准入三类，各自分别面临国际法合法性、跨境问责机制与规则衔接等方面的局限。这些模式的交错适用进一步引发连结点多元化与弹性原则的民事管辖困境、以及国内法薄弱与国际规则缺失的刑事管辖协调挑战。对此，我国需优化域外管辖规则、构建跨境平台问责机制、细化冲突法标准、提升刑法规制位阶。区域层面，应推动国内制度输出，主导构建区域协同治理体系；国际层面，须凝聚深度伪造危害性共识，依托中国经验提供规则、能力与标准三类公共产品。

刘钰琪 武汉大学国际法研究所博士研究生

张锦浩：《人工智能模型蒸馏的邻接权规范逻辑及其展开》

中南大学法学院博士研究生**张锦浩**以“人工智能模型蒸馏的邻接权规范逻辑及其展开”为题发言。他提出，人工智能模型蒸馏需纳入法律规制，相较于公共领域属性或强排他性著作权，邻接权的弱排他性更具制度弹性，可避免规范真空或保护过

度的困境，推动“创新激励—技术扩散—普惠应用—产业反哺”良性循环。邻接权客体可涵盖模型蒸馏对象——人类技术劳动产出的、承载知识信息的复杂模型，其具有信息财产价值，与作品既关联又有差异。他建议按技术应用的社会化与竞争性程度，构建梯度化邻接权规范体系：无竞争性封闭“蒸馏操作”属正当使用；个人弱竞争性公开“蒸馏”适用合理使用，非营利组织的同类行为可用法定许可；企业未经授权的强竞争性公开“蒸馏”构成侵权，不适用技术中立豁免。

罗升：《数据出资的理论建构与制度展开》

华中科技大学法学院硕士研究生兼研究助理**罗升**以“数据出资的理论建构与制度展开”为题进行了发言。他系统地阐述了数据出资这一新兴课题，从兴起背景、法律与实践基础，到全国发展趋势，逐步展开核心理论构建。其中重点探讨了数据确权的必要性与“分层确权”的理论路径，并从立法趋势与财产本质角度论证了数据出资的正当性。在制度构建方面，发言提出了覆盖事前、事中、事后全过程的规制框架，包括产权登记、评估、股东权利行使以及责任追究等环节。最后，也客观分析了数据出资对公司资本制度带来的扩容与挑战，并对未来发展进行了展望。整体来看，发言不仅构建了“理论－制度”双向支撑的分析体系，也为数据要素市场化背景下公司出资制度的创新提供了清晰的思路与可行的规制方向。

罗升 华中科技大学法学院硕士研究生

周姝希：《泛在人工智能何以辅助刑事辩护？》

中国人民大学刑事法律科学研究中心研究员**周姝希**以“泛在人工智能何以辅助刑事辩护？”为题进行发言。她指出，在刑事诉讼数智化发展的趋势下，刑事辩护仍未能充分利用新兴科技提升辩护质效。结合普适计算的理念，人工智能作为可供选择的普适科技，能够通过便宜的方式融入刑事辩护。但将人工智能技术应用于刑事辩护场景还存在局限性，涉及智慧语言难以破解辩护用语的策略性，概率框架与刑事辩护逻辑存在矛盾，以及人工智能刑事诉讼主体受限和人工智能生成物功能有限的问题。因此，人工智能与专业刑辩律师之间还存在显著差距，仅作为辅助工具提升刑事辩护的效果。刑事辩护制度作为刑事法治的重要保障，辩护律师有着维护被追诉人利益和司法公正的职责，在使用人工智能时应当考虑到技术现状，合理应用人工智能实现有效辩护。

李心言：《网络暴力治理中用户注意义务的动态实现》

北京理工大学法学院博士研究生**李心言**以“网络暴力治理中用户注意义务的动态实现”为题进行发言。他认为，网络暴力言论治理的关键在于构建用户言论责任的分层规制体系，以用户言论注意义务与言论容忍义务为基础，针对网络言论传播链条中的不同主体实施差异化义务配置。在言论发布端，建立基于言论预期与核实审查的梯度化注意标准，划定普通用户与公众人物的审慎责任等级；在接收端，结合主客观要件与理性第三人标准确定容忍阈值的合理边界。通过法律强制与道德引导的衔接共治，阐明用户个体义务在网络暴力言论全链路规制中的作用机制，实现从事后追责向源头防范的治理范式转型，破解当前所面临的技术异化、价值冲突与责任认定困难等结构性困境。

李心言 北京理工大学法学院博士研究生

张轩诚：《数字时代转换性使用中合理使用的解释论证成——实体与程序视角下证明责任分析》

上海交通大学凯原法学院博士研究生**张轩诚**

以“数字时代转换性使用中合理使用的解释论证成——实体与程序视角下证明责任分析”为题发言。他提出，合理使用制度是法律与事实交叉的民事混合场域，自创设便协调信息公共化与著作权人创作热情，实现著作权与社会公共利益的平衡。但将其单纯作为侵权抗辩事由，已引发诸多争议。我国立法与实践虽深入探讨合理使用的具体类型、侵权界限及三步检验法等问题，该制度仍未破解数字时代二次使用的新挑战。张轩诚认为，转换性使用为合理使用制度提供了理论支撑，明确其标准可破解侵权界限模糊难题。通过梳理其历史与理论、明晰目的性转换下的市场互补需求，以“规范说”分配证明责任并解构我国本土“四要素”框架，可为新类型二次使用的法治建设提供重要实践支撑。

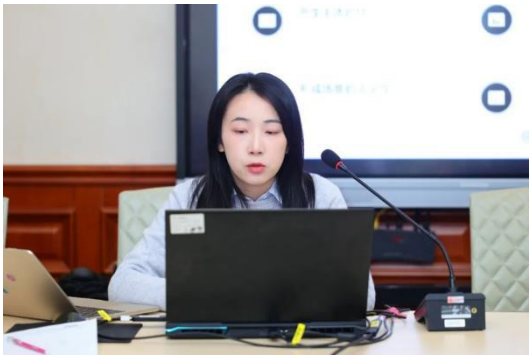
张轩诚 上海交通大学凯原法学院博士研究生

方豪：《人机协作模式下诊疗过失认定：规范困境与制度应对》

浙江大学光华法学院博士研究生**方豪**以“人机协作模式下诊疗过失认定：规范困境与制度应对”为题发言。他指出，诊疗人工智能已广泛应用于临床并实质影响医师决策，传统以人类医师为中心的诊疗过失认定体系面临重构压力，尤其对诊疗损害责任与告知损害责任认定形成挑战：AI 模糊并拉高医疗水平基准，黑箱结构与自动化偏误易导致注意义务事后扩张；AI 纳入《民法典》第 1219 条告知范围缺乏清晰标准，要求医师解释算法机理存在技术与制度障碍，说明义务恐异化为黑箱解释义务。为破解上述困境，方豪提出：以善用 AI 的理性医生标准界定医疗水平，引入 AI 可及性与专业接受度过滤机制；将注意义务程序化并通过病历记录显性化；按决策相关性及动态要素分层划定告知范围；以解释流程替代黑箱解释，重塑人机协作模式下诊疗过失认定的可预期责任边界。

杨子纯：《反思与设想：政务数据的权属争议及政企共享政务数据路径构建》

华中科技大学法学院博士研究生**杨子纯**以“反思与设想：政务数据的权属争议及政企共享政务数据路径构建”为题进行发言。她提出，数据作为国家基础性战略资源与重要生产要素，政府掌握的政务数据在推进国家治理体系和治理能力现代化中具有不可替代的作用。然而，政务数据权属争议突出、概念界定模糊、共享机制不完善等问题，严重制约了数据要素价值的释放。通过厘清政务数据与相近概念边界，剖析现有权属理论的适用困境，结合《政务数据共享条例》的具体规定，可以构建覆盖共享范围、共享模式、审查监管的政企共享政务数据路径，为政务数据高效利用与安全共享提供理论支撑和实践指导，助力数字政府建设与数字经济高质量发展。



杨子纯 华中科技大学法学院博士研究生

潘璐：《数字时代劳动者离线权的法理证成与制度建构》

西北政法大学博士研究生**潘璐**以“数字时代劳动者离线权的法理证成与制度建构”为题发言。她指出，数字时代智能技术消弭了工作与生活的边界，劳动者“永久在线”成常态，离线权缺失导致其休息权、人格权受损问题突出。离线权并非简单“脱离工作”，而是休息权的延伸，既契合人格权中人身自由与尊严的保障需求，也符合劳动法倾斜保护劳动者的核心原则。从法理而言，离线权可依托劳动权本质、人格权保障及利益平衡理论证成，其确立能修复劳动者被异化的时间与空间。明确其法理基础，是数字时代完善劳动权益保障、实现劳资实质公平的必然要求。制度设计上，需进一步明晰离线权的立法定位，明确行使规则并构建多元化责任体系，以促进劳动者工作与生活实质平衡，为其休息权及身心健康提供精准保障。

潘璐 西北政法大学博士研究生

西南政法大学硕士研究生**朱峰**以“数据要素收益分配规则构建的困境及应对”为题发言。他指出，数据要素收益的排他性特征，决定了其收益分配的可行性；但当前分配面临原则模糊、主体繁多、条件难定、方式创新不足等困境。症结在于数据保护思路不当延续、产权化确权的理论束缚，以及数字企业社会责任落实缺位。结合数据特征与国内外实践，他提出解决方案：原则上确立“效率为主，体现公平”导向，落实“规模化分配”“市场自治”“按贡献补偿”原则；主体上通过身份要件与客观行为明确分配主体，优化角色安排；条件上需满足收益达同业一般水平，且非自生数据对收益创生至关重要；方式上，个人以数字税收获集体收益，企业依重要性评估参与分配，政府通过数据信托、分级收费等均衡投入与收益回流。

朱峰 西南政法大学硕士研究生

Imran Saeed：<AI Anxiety and Workplace Inequality: Mediating Roles of Attitudes and Moderating Roles of Personality within a Human Rights Lens>

华中科技大学法学院博士后 **Imran Saeed** 以“AI Anxiety and Workplace Inequality: Mediating Roles of Attitudes and Moderating Roles of Personality within a Human Rights Lens”为题作报告。他汇报了一项针对巴基斯坦 500 名员工的横向研究，指出 AI 焦虑显著预测工作场所不平等感知，其中对 AI 的态度起中介作用，而人格特质起调节作用——神经质放大焦虑效应，开放性则缓冲其负面影响。他强调本研究首次将 AI 焦虑界定为人权议题，认为其威胁劳动者尊严、公平与平等机会，低技能员工受影响尤甚。他建议组织层面实施基于人格特质的支持系统并营造心理安全的培训环境，政策层面则需制定以人为本的 AI 治理并推进全国性再培训与数字素养计划，后续应完成论文发表、开发组织干预工具包并制定政策简报，AI 时代的职场不平等问题需要通过人权视角的系统性干预方能实现技术公正与人本关怀的平衡。

Imran Saeed 华中科技大学法学院博士后

Muhammad Amal Atta：<Systematic Exclusion: How the Digital Divide and Paywalls Violate the Human Right to Science>

华中科技大学法学院博士研究生 **Muhammad Amal Atta** 以“Systematic Exclusion: How the Digital Divide and Paywalls Violate the Human Right to Science”为题进行发言。她批判性地分析学术出版商品化对全球南方研究者的系统性排斥，指出现行体系下 90%高校缺乏期刊订阅，平均 APC 费用约 3200 美元相当于低收入国家人均 GDP 的 2 倍，形成“付费阅读 – 付费发表 – 付费获取”的三重负担循环，严重违反《世界人权宣言》第二十七条规定的科学进步受益权。她认为自由主义解决方案如 Plan S 仅将负担从读者端转向作者端，未能打破知识作为私有财产的根本逻辑，而中国通过科技期刊卓越行动计划、中国知网等平台以公共资金替代 APC 的国家主导去商品化路径证明有效，2025 年钻石 OA 论文占比将达全球 20%。她强调实现科学

人权需走向知识去商品化，钻石开放获取及区域性知识共享平台是已验证的有效路径，呼吁加大对非商业化学术出版的投资，方能打破知识垄断实现全球科研公平。

Muhammad Amal Atta 华中科技大学法学院博士生

Mahar Waqar Fazal：<Equitable Smart Justice: Digital Sovereignty as the Foundational Platform for Digital Constitutionalism in the Global South>

中南财经政法大学博士研究生 Mahar Waqar Fazal 以“Equitable Smart Justice: Digital Sovereignty as the Foundational Platform for Digital Constitutionalism in the Global South”为题汇报。他提出数字主权是所有南方国家实现数字宪政的先决条件，指出当前主要挑战包括数字殖民主义、外国科技巨头数据剥削及本土化治理框架缺失。他认为必须建立三大核心支柱：基础设施主权方面，建立国家云系统、数据本地化政策及本土技术生态以减少外部依赖；法律宪政方面，将公平、隐私和算法问责原则嵌入宪法以超越碎片化法规；公平智能司法方面，AI 司法工具须确保透明度、反偏见及社区中心设计以避免强化历史不平等。他强调缺乏主权控制将削弱本土民主价值观，建议推进南南合作开发开源方案，对外国数字服务实施强制性影响评估并投资公共利益技术专家。他从行动层面进行具体阐述，认为全球南方的数字正义必须建立在自主可控的数字主权基石之上。

Mahar Waqar Fazal 中南财经政法大学博士研究生

李锦华：《人工智能侵权责任的范式革新——风险归责的体系化构建》

中国人民大学法学院博士研究生**李锦华**以“人工智能侵权责任的范式革新——风险归责的体系化构建”为题进行了发言。他指出，目前人工智能侵权责任的研究呈现出碎片化、滞后性的特征，应集中探讨普遍化、一般化的责任规则。人工智能提供者相较于其他主体而言是实现风险预防和分配正义的责任主体。侵权法在演进中，其框架存在内部逻辑不自洽、价值割裂的根本缺陷，在适用于人工智能侵权时，总是呈现责任分配不公、技术创新和权益保护不均衡、法律内部边界模糊等弊端。人工智能的风险属性与风险归责理论具有高度的理论契合，风险责任分配应考量损害严重程度和风险控制力强弱两大关键要素。基于此，应当构建一个与过错归责体系平行的、分层次的风险归责体系，以便能精细、动态、体系、前瞻地妥善处理各类人工智能侵权案件，并达成公正合理的利益平衡。

李锦华 中国人民大学法学院博士研究生

唐沐艺：《生成式 AI 司法应用的价值平衡路径探索》

湖南大学法学院博士研究生**唐沐艺**以“生成

式 AI 司法应用的价值平衡路径探索”为题进行发言，她指出，生成式 AI 凭借高效信息处理与类比推理能力，成为缓解司法“案多人少”矛盾的重要工具，但受其数据碎片化、价值判断缺失等限制，制约“机械类比”向“规范推理”跨越。针对 AI 裁判价值缺失、黑箱推理等痛点，该研究结合判例法“事实 – 规范关联”“附加理由”机理，聚焦维护权威、提升准确、推动显性输出目标，提出三方面优化路径：构建“人类价值锚定+AI 辅助说理”双轨制，预设人类价值基准、AI 显性化推理逻辑；建立“差异表+程度表”知识图谱，转化零散判决为类案经验；规范“结论 – 理由 – 依据”三层输出，可视化促进案件责任制。研究旨在探索效率与价值平衡的应用框架，推动 AI 从辅助工具向“专业辅助人”升级，为实现科技赋能与公平正义提供可行参照。

唐沐艺 湖南大学法学院博士研究生

李佩卢：《中国式现代化视域下数字法治的双向度路径研究》

中国科学院大学法学院博士研究生**李佩卢**以“中国式现代化视域下数字法治的双向度路径研究”为题进行发言。她指出，在中国式现代化视域下，数字法治建设的核心是二元路径选择问题。反思近代中国法治现代化进程与西方单向度法治模式可知，单向路径在中国语境下适用性不足。自上而下的政府主导路径虽能维护数字经济秩序、提供法律保障，却存在立法滞后、执法成本高、难适配技术快速更新等问题；自下而上的社会演进路径虽能激发经济活力与创新，却易引发规则碎片化、平台私权滥用、技术失范等困境。因此，数字法治走双向度融合路径是中国国情下的必然选择：一方面通过顶层设计构建数字法律与政策体系，明确发展方向；另一方面依托平台自律、行业规范与社会共识，扎根本土社情。这一路径彰显了“数字法治化不等于西方化”的中国智慧，为全球非西方国家提供了替代西方模式的范式，对构建包容可持续的全球数字治理秩序意义重大。

李佩卢 中国科学院大学法学院博士研究生

余忻怡：《人机协同新范式下人工智能法治人才培养》

武汉理工大学法学与人文社会学院博士研究生**余忻怡**系统探讨“人机协同新范式下人工智能法治人才培养”。她发现，AI 在法律职业中的广泛应用与国家政策的推动下，传统法学教育在目标、知识与能力结构上正遭遇严峻挑战。目前改革主要面临共识缺失、路径零散、协同不足等深层困境。为解决这些问题，她提出构建以“人机协同”为核心的新范式，并细化为价值协同、认知协同与实践协同三个层面，旨在明确人机边界、培养学生融合算法思维的“混合心智”，并利用 AI 工具赋能法律实务训练。同时梳理了高校从课程嵌入式改良到实体机构结构化重组的多元实践图景。为建设性破局勾勒了协同推进路径：从理念重塑出发，通过构建能力导向的阶梯式课程矩阵、开展场景驱动与虚拟仿真的教学评价改革，并辅以相应的配套机制建设，旨在构建一个既拥抱技术高度、又坚守法治温度的培养体系。

余忻怡 武汉理工大学法学与人文社会学院博士研究生

段卓臻：《商业秘密犯罪预防性治理路径的反思》

浙江万里学院法学院**段卓臻**老师以“商业秘密犯罪预防性治理路径的反思”为题，探讨了商业秘密犯罪预防性治理路径的法律边界问题。商业秘密一旦泄露，其后果具有不可逆性，传统的事后救济手段往往难以弥补。人工智能等新技术的发展、知识产权刑事保护的强化以及预测性警务的普遍实施，推动了商业秘密犯罪预防性治理路径的兴起，包括利用人工智能技术分析识别潜在的商业秘密泄露风险，以期实现早期预警和干预。此外，政府部门积极推动企业建立完善的商业秘密保护内部管理规范，作为预防性治理的重要组成部分。然而，预防性治理路径也可能引发隐私权侵犯、公私边界模糊等问题。她认为，应当通过探讨预防性治理路径可能存在的问题以及如何明确这一路径的法律边界，以实现商业秘密保护与法治原则的协调统一。

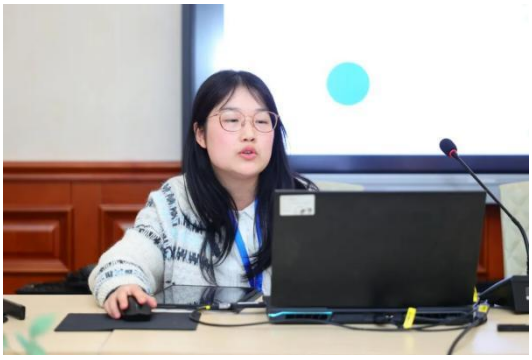
段卓臻 浙江万里学院法学院讲师

曹立军：《作为裁量基准的行政算法：逻辑与治理》

北京理工大学法学院博士研究生**曹立军**以“作为裁量基准的行政算法：逻辑与治理”为题进行汇报，提出在行政算法的运行过程中，存在着民主正当性传递中断、行政法律关系失衡以及嵌套式责任鸿沟难以跨越等法治难题。为推动行政算法进入法治轨道，有必要进一步挖掘其行政法属性。具体而言，行政算法可以被视作行政机关实现自我限定、自我塑造以及自我制约的一种行政规则，能够纳入行政自治规范的范畴。当行政算法涉及算法决策时，其主要发挥裁量基准的作用。他强调，作为裁量基准的行政算法应进行智能化法制审核以确保其民主正当性得以维系；应遵守场景化公开规则以平衡算法行政权力与行政相对人权利；应设置程序化逸脱机制以克服行政机关在裁量过程中存在的责任惰性。

黄燕腾：《智慧司法中个人信息保护的公法构造》

北京理工大学法学院博士研究生**黄燕腾**围绕“智慧司法中个人信息保护的公法构造”进行发言。她认为智慧司法中处理个人信息，将影响事实认定、法律责任划分等诸多司法环节，导致当事人权利发生变动。然而，司法中个人信息处理目的升格与算法黑箱、技术过度介入共同瓦解传统司法中个人信息保护的适用基础，并因私法保护失范与公法保护不足加剧权责模糊、尊严危机、救济不足等风险。个人信息处理本质上属于《宪法》第一百三十一条审判权的数字化行使方式。对此，构建正当程序原则，需重构智慧司法的隔离模型、商谈情景与算法听证机制；推进法律保留原则，需尊重法官职权主义对个人信息类型化的保留判断与司法终局性裁决的禁区设立作出的解答；嵌入四阶层比例原则，需甄别个人信息处理的目的、明确算法辅助性、分解最小处理要素、明晰优先的公共利益，实现智慧司法的良好发展。



黄燕腾 北京理工大学法学院博士研究生

唐先勇：《个人信息侵权中精神损害赔偿的适用困境与应对路径》

四川大学法学院博士研究生**唐先勇**以“个人信息侵权中精神损害赔偿的适用困境与应对路径”为题进行汇报。他指出，个人信息侵权精神损害赔偿的司法适用难题日益凸显，集中表现为请求权基础竞合、“严重精神损害”标准严苛、风险性损害可赔性存疑及赔偿数额裁量无序。从适用正当性来看，此类侵权常引发精神损害，难以通过财产赔偿弥补。由此应区分个人信息处理者与普通侵权主体，对前者优先适用《个人信息保护法》，采过错推定

原则；对后者适用《民法典》一般规定采过错责任原则。在规则优化上，缓和“严重精神损害”认定标准，引入社会一般容忍限度，采用“结果严重性—行为严重性”递进判断模式。明确风险性损害可赔性，以信息敏感程度、侵权方式范围、后果可补救性等为识别因素。在赔偿数额上，考量侵权人过错、信息类型、损害后果等因素，设定个人单次赔偿区间与群体性侵权总额上限。

唐先勇 四川大学法学院博士研究生

张由：《数字化身法律地位的三重认定》

上海交通大学凯原法学院博士研究生**张由**围绕“数字化身法律地位的三重认定”展开，他认为数字化身是人们探索虚拟世界的重要媒介，然而目前数字化身的人格权是基于现实世界中自然人主体的而建构的权利体系，因此并无法很好地处理虚拟世界中与自然人法益相隔离的数字化身侵权行为。但是否应将数字化身视为法律甚至人权主体，当前学界仍存在很大争议。由于数字化身存在内部的多样性，这一个概念可在具身性梯度上细分为低、中、高三种类型。其中低具身性化身仅构成法律关系客体，围绕《民法典》第 1027 条建构虚拟财产保护制度；中等具身性化身则可以构成法律拟制主体，参照公司法人进行保障。高具身性化身则由于其与自然人用户在意识存在同一性，可被视为与自然人平行的人权主体，需要建构相应的“数字人权”实施保障。

张由 上海交通大学凯原法学院博士研究生

顾男飞：《人工智能体垄断风险的预防性治理》

上海交通大学凯原法学院博士研究生**顾男飞**以“人工智能体垄断风险的预防性治理”为题进行发言。他指出，AI 的运用将重塑人类生产生活范式和促进生产力革命性跃迁。但人工智能正处于技术革新迅猛发展阶段，现有的治理体系无法有效应对垄断协议和滥用市场支配地位等垄断风险，面临着认定标准模糊和救济滞后等困境。应当引入预防性治理理论，通过增设经营者合规治理义务和扩张执法机构预防性监管职权，以及两者有效协同推动垄断风险的源头治理，而后可借鉴域外国家的垄断风险治理经验以明确预防性治理的实践要求，从而防范垄断风险传导到其他领域而造成不可逆的系统性风险。落实到制度建构层面，经营者应当明确要求以完善内部治理制度；执法机构健全风险监测和运用梯次性监管手段满足不同治理需求，在此基础上应当强化激励和规范适用承诺制度以推动内部合规与外部监管的有效衔接。

钟达武：《人工智能风险的法律防范：基于经济学回归模型的治理启示》

吉林大学理论法学研究中心、法学院硕士研究生**钟达武**以“人工智能风险的法律防范：基于经济学回归模型的治理启示”为题进行了发言。他将当前人工智能风险的主要表现分为数据采集合规风险、数据处理黑箱偏见、虚假信息侵权等三个维度。鉴于我国当前暂未形成与之相关的法律治理体系，又因欧盟《人工智能法案》的分级分类治理模式存在内生缺陷，无法与我国当前人工智能技术“发展+安全”的统筹理念相匹配，导致我国当前人工智能的法律治理体系处于“无依托+无借鉴”的两难状态。故此，他通过定量研究的方式，以信效度分

析为基础，以描述性统计为延伸对所收集的样本数据进行回归模型分析。得出我国人工智能风险的法律防范首先应当以适应性理念为价值引导，其次以阶段性模块为制度基础，通过动态性规制完善风险治理体系，最终实现从传统分级分类治理模式到新型模块化适应性治理模式的转向。

钟达武 吉林大学理论法学研究中心、法学院硕士研究生

（技术编辑：吕昊然）

数字法评

《人工智能生成合成内容标识办法》的规范功能与法律适用

此处删除了原文脚注，全文请参见《法律适用》2025 年第 9 期，转载或引用请注明出处。

作者：黄尹旭

内容提要：技术与社会交互的复杂语境中，人工智能生成合成内容的传播呈现风险“放大效应”。平台作为“放大”的核心枢纽，承担更多治理责任，但也滋生滥用权力的风险。“平台判定用户内容 AI 生成首案”揭示其中的制度张力与纠纷争议。对此，应引入人工智能生成合成内容标识机制，构建客观判断标准，明确责任承担，提升规则公开性与可预期性。再进一步优化法律适用，若相应主体未核验人工智能生成合成内容标识，法院可推定其未尽合理注意义务；放任未标识内容传播的，可认定其默许风险发生，构成间接故意侵权。借助标识还可细化和评估有害内容传播链条上的各主体责任承担情况。此外，还需要经由法律适用明确对恶意反标识手段的判断和处理机制，并推动相关主体在未进行标识时进行解释说明。

习近平总书记在中共中央政治局就加强人工智能发展和监管进行的第二十次集体学习中指出，“人工智能带来前所未有发展机遇，也带来前所未遇风险挑战。要把握人工智能发展趋势和规律，加紧制定完善相关法律法规、政策制度、应用规范、伦理准则，构建技术监测、风险预警、应急响应体系，确保人工智能安全、可靠、可控。”2025 年 3 月，网信办等四部委联合发布《人工智能生成合成内容标识办法》（国信办通字〔2025〕2 号，以下简称《标识办法》），聚焦“生成合成内容标识”关键点，提醒用户辨别虚假信息，明确标识责任义务，规范内容制作、传播各环节标识行为，以合理成本提高安全性，减轻滥用危害，推动人工智能健康有序发展。《标识办法》是人工智能治理从被动响应迈向主动建构的新阶段，既着眼于防范技术风险，更可经由“标识”这一新型法律工具，推进变革数字时代的法律关系、责任伦理与创新生态，是对技术向善理念的制度化诠释。

具体而言，生成式人工智能的普及使数字内容生产门槛降低，虚假信息和诽谤内容的传播风险增加。数字时代传播者的“放大责任”是技术权力重构社会关系的结果，算法推荐和社交裂变等技术改变了传统传播路径，呈现特殊的“放大”效应，算法推荐形成的“信息茧房”加剧群体极化，放大社会风险，避风港原则等既有法律框架应对网状传播中的责任扩散有所不足。由此，一方面需要平台对人工智能生成合成内容的甄别及传播承担主体责任，一方面也应当约束平台基于此的治理权限，两者之间形成制度张力。

相关情况已经引发诉讼争议，“平台判定用户内容 AI 生成首案”揭示当前人工智能生成合成内容在传播过程中所面临的复杂挑战以及可能衍生的法学争议。对此，本文试图分析人工智能生成合成内容标识的规范功能及在司法适用中的特殊价值，明确其作为新型法律工具的关键作用，从而进一步以此为支点优化整体的人工智能司法裁判规则。

一、平台判定用户内容 AI 生成首案及其意义

“平台判定用户内容 AI 生成首案”中，原被告围绕人工智能生成内容标识产生争端。法院认为，网络内容服务平台有权以算法工具审查用户发布内容是否为人工智能生成合成并对违规行为进行处理，用户需提供内容系人类创作的初步证据，法院可结合创作相关因素进行事实认定。

原告在被告运营的平台发布一段关于打工与学车的内容，被平台判定为“包含 AI 生成内容但未标识”，遭内容隐藏及禁言一天处理，申诉未果后原告起诉，主张未用人工智能创作、被告违约，要求撤销处理并删除记录。被告辩称有权依合同审核处理，内容经机器识别及人工复核，且无义务解释算法逻辑。

法院审理指出，被告依据《互联网信息服务深度合成管理规定》制定的相关公告属于服务协议的

组成部分，故被告有权审查处理涉案内容，但平台处理需有合理依据。原告因内容系即时性创作无法提供创作底稿等证据，而被告作为掌控算法与判断结果的一方，应就内容为人工智能生成进行合理举证或说明，但被告未做到，需承担违约责任。

纠纷清晰地揭示出明确的标识规则是平衡各方权益的关键支点。该案既肯定平台基于服务协议和治理需求对人工智能生成内容进行管理的正当性，也明确其权力行使的应然边界。平台的算法审查权是维护数字空间秩序的必要手段，但若缺乏约束，可能因技术误判或解释缺位侵扰用户权益。当内容的生成主体（人类或人工智能）处于模糊状态时，一旦引发侵权、欺诈等纠纷，责任归属便成为难题。该案中，法院对证明问题的处理，即用户因即时性创作难以举证时，由掌握算法的平台承担更多说明义务，反向说明若存在清晰的标识，即可成为快速厘定责任主体的重要依据，有助于在纠纷发生时掌握基本情况，并为责任界定提供进一步依据。

也因此，《标识办法》的制定与适用具有鲜明的现实针对性和必要性，并非简单设定技术层面的标识义务，而是经由构建统一的标识规范，将“平台判定用户内容 AI 生成首案”折射的维护用户权益、保障平台有序治理、明晰责任边界的实践需求转化为制度安排，为用户的创作行为提供指引，亦为平台的审查管理设立标准，从源头上为各类人工智能内容相关纠纷的解决奠定事实认定基础。《标识办法》所蕴含的是在技术创新与权利保障之间寻求动态平衡的治理智慧，其生命力正在于将个案中彰显的法理原则转化为普遍适用的行为规则。

二、《标识办法》所针对的现实问题

近年来，“每 20 个‘80 后’中就有 1 人已经去世”“广州法院对一起某品牌汽车 L3 级自动驾驶追尾事故作出判决”“四川凉山发生山体滑坡灾害”等利用人工智能生成合成的谣言案例引发各界对于这类问题的关注和忧虑。人工智能生成合成内容凭借其高效、便捷的特点，在网络空间迅速扩散，呈现出风险“放大效应”。生成内容的大量涌现使得信息过载问题愈发严重，虚假信息、误导性内容更易混入其中，扰乱公众对信息的准确判断，部分生成内容可能涉及侵权、违背公序良俗等问题，一旦广泛传播，将对社会秩序、道德伦理等造成影响。基于此，平台需要承担特殊的治理责任，但如何经由法律适用平衡平台的责任与权力成为新的问题。

（一）自动化链条下风险放大的数字逻辑

数据要素和智能要素本身就其生产要素性质而言就具有乘数效应，可以放大其他要素的效能，在信息传递上更具“放大”效果。数据化与算力推送的结合以指数级的规模与速度改变信息传递，使得作为传播中介的平台、技术提供者及其他节点成为信息扩散的“超级放大器”，一定程度突破传统传播的物理边界，而社会关系与责任分配亦宜因应改变。新技术将信息转化为可解析、可存储的数字形态，无论是文本、图像还是视频，各类内容均能被编码为二进制结构的数据，实现低甚至零边际成本的复制与传输。数字化过程使得信息的生产、存储与分发突破时空约束，为大规模传播奠定基础。算力推送技术对用户行为数据的深度学习与画像分析，精准识别并放大内容的传播潜力。数据化将流量转化为可计算的数字资产，而算力推送则实现信息的指数扩散。

数字平台及信息链条上传播者的“放大”效应根源于其对信息传播的结构性控制，经由控制展示争议性或高互动性内容，构建信息传播的“优先级排序”，使某些内容的传播效率呈指数级增长，建立新的社会注意力的分配机制。特别是社交网络中少数关键节点拥有海量关注者，可经由其庞大的社交网络快速扩散特定内容。

人工智能技术降低了内容生产门槛，使得虚假信息、极端观点易被批量生成合成并伪装为真实内容，扩大传播规模，模糊真伪界限，增加信息甄别的难度。当某观点在社交网络中占据主流时，持异议者可能选择沉默，进一步强化主流信息的可见性，用户倾向于接受符合自身价值观的信息，并经由分享强化既有立场，削弱信息多样性，加剧社会极化趋势。同一事件通过文本、图片、视频等多形

式呈现，覆盖不同用户群体的感知偏好，形成立体化传播攻势。平台为追求用户活跃度与广告收益，默认甚至鼓励争议性内容的传播。

（二）基于“放大效应”的责任承担逻辑

平台因其技术能力而具备干预信息传播路径的权力，需承担更高的注意义务，其他信息链条上的传播节点因其技术能力或者流量资源，应承担更高责任权重。“平台判定用户内容 AI 生成首案”裁判中明确表示，平台部署人工智能识别技术具有必要性，但在算法误判时也要承担不利后果。平台与其他传播节点的“放大”功能在提升传播效率的同时，亦加剧技术权力与公共利益之间的张力。

技术与流量赋能使相应节点角色从单纯的传播渠道转变为影响广泛的信息扩散枢纽，治理逻辑宜从个体过错转向风险控制义务。传播节点的责任既涉及对具体事件的责任认定，亦需考虑其在整个信息传播生态系统中的作用。技术决策与流量供给直接影响到虚假信息的扩散速度与范围，因而数字平台与其他传播节点需对其技术能力与风险管理策略负责。平台作为信息传播的核心枢纽，需承担更多的技术和管理责任，而用户在转发未标识内容时则需承担更高的注意义务。

平台在人工智能生成内容治理中承担主体责任与自身治理权力受到约束之间的制度张力，源于平台在数字生态中双重角色的内在冲突，平台既是技术应用的掌控者与内容传播的枢纽，又是用户权利的义务相对方与公共利益的守护者。两种角色所衍生的责任与限制，形成动态的制衡关系。

平台承担主体治理责任的正当性，根植于其对技术工具的支配力与对传播链路的控制力。在生成式人工智能普及的背景下，平台提供内容发布的空间，更经由算法推荐、流量分配等机制决定内容的可见性与影响力，技术能力使其天然成为人工智能生成合成内容风险防控的第一关。主体责任的核心，在于要求平台超越被动的规则执行者角色，主动构建与技术发展相适配的治理体系，既要通过算法优化提升对生成合成内容的识别精度，建立分层分类的审查机制以应对海量内容的挑战，也要针对虚假、诽谤内容等高风险类型设置特殊防控流程，将治理关口前移至内容生成与传播的关键节点。责任的设定并非简单的义务叠加，而是基于风险与控制相匹配的逻辑，对技术与传播的控制力越强，其防范风险外溢的责任就越重，构成法律权责一致原则在数字时代的具体体现。

然而，同样需要对平台治理权力进行约束，尤其是技术优势可能异化为治理霸权的风险。平台的治理权力往往经由用户协议的格式化条款确立，依托算法的自主决策实施，行使若缺乏边界，极易陷入既是规则制定者，又是裁判者的困境。当平台以“治理”为名，随意扩大生成合成内容的认定范围，或对用户内容采取隐藏、禁言等措施时，用户的表达自由、创作权益便可能在技术黑箱中受到侵害。更值得警惕的是，平台可能基于商业利益或自身偏好，将治理权力异化为排除异见、垄断信息的工具，破坏数字空间的多元生态。

平台在人工智能生成合成内容治理中面临的积极作为与禁止乱作为的双重压力，是数字治理中权责平衡的具象化。而引入人工智能标识制度，提供可操作的规则基础，使平台的行权与责任承担皆有明确依循，既激发其治理效能，又约束其权力边界。标识并非简单的技术规范，而是调和平台双重压力的制度中枢，促使平台在积极作为与不妄为之间找到衡平点。

主体责任的履行需要必要的权力空间，若对平台的治理权限施加过度限制，可能使其因顾虑法律风险而放松风险防控，最终损害公共利益与用户整体权益。权力约束的缺位则可能导致治理失序，使技术优势转化为对个体权利的压制，背离治理的初衷。因此，制度设计的核心在于明确责任与权力的边界，而人工智能生成合成内容标识机制恰恰具有此项功能，经由技术语言与法律语言的结合，进一步明确和界分平台在生成内容识别、风险处置、用户救济等方面的具体责任，使其治理行为有章可循，确立权力行使的底线标准。

三、《标识办法》的规范功能

《标识办法》构建客观判断标准，为平台治理

提供具象化参照，明确生成合成内容的界定、标识方式及未标识后果；明确责任承担，划分用户主动标识义务与平台审核监督义务，构建清晰责任链条；提升规则公开性与可预期性，遏制平台权力滥用风险，以公开规范明确平台行权边界。

（一）构建的客观判断标准

平台的积极作为，需以对人工智能生成合成内容的精准识别与规范处置为前提，而标识制度通过明确“什么是生成内容”“如何标识”“未标识的后果”等核心要素，为平台的审查、分类、处置行为提供具象化参考。当用户发布内容时，标识与否成为区分人类创作与人工智能生成的显性符号，平台据此开展的识别与管理，便脱离主观臆断范畴，转而基于预设的规则框架运行。对已合规标识的内容，平台可聚焦于其内容本身的合法性审查，对于未标识却被判定为生成的内容，其处置措施也需以标识制度中适当措施的要求为限。以标识为核心的客观标准，既为平台积极履行审查责任提供了路径，也从源头上压缩其主观随意行权的空间。

“先污染后治理”的系统性风险在数字传播领域展现出复合性特质。因平台普遍遵循“通知-删除”规则，实质形成先放任再治理的客观情状，虚假信息传播机制易异化为风险放大装置，形成具备自我强化属性的负外部性循环。在“平台判定用户内容 AI 生成首案”里，平台与用户就内容是否为人工智能生成各执一词，根源在于缺乏明确可操作的判定规则。用户发布人工智能生成合成内容时，依据《标识办法》主动添加显式标识，向平台与其他用户明确宣告内容属性是应尽的法定义务。平台则需为用户提供必要的标识功能，并核验文件元数据中的隐式标识等。若平台未履行该义务，导致对用户内容误判，其将承担法律责任。

人类依靠自身理性判断人工智能生成合成内容是较为困难的。人工智能生成物的数字标识需突出预防性功能，探索技术手段与法律逻辑的深度融合。经由显性标识与隐性技术的结合，将生成合成内容的全生命周期纳入可追溯、可验证的治理体系，实现新的责任分配与风险控制范式。数字标识前置对生成内容的技术约束与合规，在生成阶段将生成者 ID、时间戳、算法参数等嵌入元数据，在源头上建立责任归属的客观依据，改善传统事后追责的被动性问题，将责任控制转化为可执行的技术标准，使平台在内容生成阶段即需履行合规义务。

（二）消解权责模糊的治理难题

平台的责任边界往往因人工智能内容的复杂性而难以界定，经由标识划分用户主动标识义务与平台审核监督义务，有助于形成清晰的责任链条。用户未履行主动标识义务，需承担相应违规后果，平台未对未标识内容尽到审核与处置职责，则需对由此引发的风险承担治理失职责任。围绕与标识相关的审查、监督、处置环节，使各方主体责任范围与权力（利）行使相匹配，平台既不能以技术复杂为由逃避对标识合规性的审查责任，也不会因责任范围模糊而陷入过度担责的顾虑，从而在积极作为时更具确定性。

经由显式与隐式标识的嵌入与融合，有望从源头上防止责任主体模糊问题。标识直接提示用户内容属性，降低因误信虚假信息带来的风险，为后续追溯提供技术支持。标识有助于直接中断技术性放大带来的负面链条，使标注“人工智能生成合成”的内容更容易被识别为非真实，减少算法推荐带来的误传风险。

标识还可以细化各环节的责任边界，记录用户的转发行为、修改痕迹等细节，帮助司法机关区分善意传播与恶意传播，防止用户因技术性过失承担过重责任。平台亦无须因技术性放大效应而承担无限责任，而是根据其履行标识义务的情况，在法律框架下承担相应的法律责任。当用户看到带有人工智能生成标签的内容时，会更加谨慎地对待该信息，减少不必要的转发和分享行为，抑制虚假信息的进一步扩散，在一定程度上提升用户的媒体素养，促使其更加理性地评估接收到的信息，从源头削弱信息茧房效应带来的负面影响。

数字标识技术手段将行为链条固化，为法律归责提供客观依据。隐式标识中的元数据在技术上有望记录内容的生成合成路径、传播节点及修改痕

迹，形成可验证的数字足迹。当人工智能生成合成内容引发纠纷时，司法机关可解析元数据追溯其生成端、平台端及用户端的参与行为，明确各环节的技术干预与过错程度。经由溯源一定程度上消解传统责任认定中黑箱操作与因果关系模糊的困难。在“平台判定用户内容 AI 生成首案”中，法院面临的重要问题是确定内容是否为人工智能生成，《标识办法》实施后对于此类案件，标识将成为关键证据。

《标识办法》第 5 条要求平台在元数据中添加隐式标识，记录生成者和服务提供者的编码等关键信息，第 10 条则禁止恶意删除、伪造或隐匿生成合成内容标识的行为。传播平台的角色已从传统的信息中介演变为具有准公共性的责任主体。算法推荐系统不再被视为单纯的中立工具，而是经由数据训练和用户画像形成特定的价值偏向，平台因对算法的设计、应用而承担新的决策责任，对其算法所导致的社会后果负责。同样的，传统上用户主要被视为被动的信息接收者，不承担内容审核义务，在数字化传播环境中，个体用户的传播能力增强，亦可担当传播的关键节点。《标识办法》明确用户在传播过程中的注意义务，强调即便是在非专业背景下，用户也需对其传播行为负责。

在传统框架下，责任主要集中在初始行为人身上，而在数字环境中，由于信息传播路径的多样化和参与者角色的多重性，确定具体责任主体变得较为困难。人工智能生成的信息借助算法推荐、用户转发等多重路径扩散时，生成者、算法设计者、平台运营者、普通用户等多元主体均可能成为风险传导链的节点，而因各方技术能力、控制义务存在差异，确定责任较为困难，其中平台是否明确知情成为处理纠纷的重要因素。

《网络安全技术人工智能生成合成内容标识方法》（GB 45438-2025，以下简称《标识标准》）要求隐式标识包含“生成合成标签要素”“生成合成服务提供者要素”“内容传播服务提供者要素”等，保障在不同平台和技术环境下的通用性和一致性。平台需要按照《标识标准》的要求对生成合成内容进行标识，并保障元数据的真实性和完整性。元数据记录生成时间、内容编号等关键信息，结合进一步技术设计还能在一定程度上反映内容在整个传播链条中的流转情况，最终原本流动性的责任被转化为可追溯的链式结构。将内容生成与传播的全链条转化为可验证的电子数据，使传统法律中“谁主张、谁举证”的证明规则，因技术证据的客观性而转向技术优势方举证，平台需证明其已按照《标识标准》履行元数据核验义务，生成者需通过标识记录证明内容来源的合法性，算法设计者则可能因标识缺失暴露模型训练数据的合规性缺陷。

（三）提升规则的公开性与可预期性

平台的治理权力若缺乏约束，易因算法黑箱与规则自定而异化。而标识制度以公开的规范明确了平台行权的边界，其对内容是否为人工智能生成合成的判定，需以标识的存在与否及内容特征为主要依据，而非仅凭内部算法的模糊结论，对未标识内容的处置，需符合必要、适当原则，不得超出风险防控的合理限度。这有望为用户提供行为预期，知晓何种标识行为合规、何种情形可能触发平台处置，亦为司法审查等外部监督提供判断平台行为合法性的标准，督促平台的治理行为始终处于规则约束之下，避免其以“治理”之名行滥用权力之实。

《标识办法》有利于在算法权力扩张与社会风险防控的张力中建立新型治理范式，以标识技术为治理接口，将内容治理的责任链条嵌入技术架构。未来可进一步设置禁止性内容清单、标识合规性标准等预设的规范模型，为触发差异化响应机制做准备。规则明确的技术化治理手段将传统法律的滞后性规则转化为技术系统的即时性反馈，实现风险控制从人工干预向系统自治的范式转型，自动化执行减轻平台的合规证明负担，以技术中立性原则保障决策过程的程序正义，为技术与法律协同治理提供制度接口。

四、《标识办法》的法律适用规则与路径

“标识”作为法律工具的引入可以化解一些人工智能司法应对的难题。法定核验义务将平台从传统责任规避中部分抽离，若平台未能举证证明其已

履行标识核验义务，或对标识异常内容未采取合理措施，其“不知情”抗辩将难以成立。人工智能生成标识还构成一定的技术证据链，与侵权法中的因果关系认定形成深度契合。在反标识措施的司法认定方面，恶意删除、篡改标识的行为可定性为妨碍网络正常运行的违法行为，算法解释制度的引入与标识制度形成互补。

（一）平台“不知情”抗辩的限缩

在“平台判定用户内容 AI 生成首案”中，平台以“算法黑箱”“技术秘密”为由拒绝披露人工智能生成合成内容识别的技术逻辑，这也可成为平台在其他案件中“不知情”抗辩理由，作为传统避风港原则在人工智能时代的延伸。在数字化传播环境中，技术黑箱与“不知情”抗辩成为法律归责过程中的挑战。算法推荐系统基于复杂的数据训练和动态调整机制实现内容分发，其决策逻辑对用户和平台均不透明。人工智能生成的恶意内容可能因算法的相似性推荐机制被推送给大量用户，但平台往往主张由于算法的复杂性和动态性，难以预知具体推荐的内容，从而以“不知情”为由进行抗辩，导致责任归属的模糊化。

《标识办法》确立的技术措施可以提升内容传播透明度，构建平台内容治理的技术化义务体系。平台接入并解析内容标识，运用元数据解析工具验证内容真实性与合法性，从而可实现对未标识恶意虚假内容的识别与拦截。技术义务的设定直接影响司法实践中平台“不知情”抗辩的效力认定。根据技术治理逻辑，若平台未采取必要技术措施识别未标识内容，司法机关可依据技术可行性标准推定其“应知”内容风险，构成《民法典》第 1197 条中应当知道侵权行为情形，进而适用过错推定规则。由此，平台的合规证明责任在传统主观尽到注意义务的基础上，进一步纳入客观技术措施履行标准，需提供元数据解析记录等技术性证据，证明其已通过技术手段对潜在风险内容进行识别与处理，以此主张已尽合理注意义务。

经由差异化审核标准强化平台责任意识，针对人工智能生成合成内容，平台需履行高于普通内容的审核义务，实施元数据验证、标识合规性校验等措施，推动行业形成技术自律机制。在过程中强化技术尽责抗辩的效力，将责任锚定于应对技术风险的技术措施的实际履行，既督促平台积极采取多元且有效的技术手段抑制风险，亦避免因过度的责任承担降低创新活力。具体而言，平台与生成者可经由留存元数据解析记录、技术标识等技术证据，证明其对内容风险的积极管控，实现自身法律责任的合理限定。

传统的技术中立原则建立在平台无法预先知晓内容性质的前提之上。但在《标识办法》实施后，若内容没有按照规定进行标识，平台亦未检测到隐式标识，那平台所谓的“不知情”实际上就是没有履行技术核验义务的过失。依据《民法典》第 1197 条，法律适用中可依据未采取必要措施判定平台存在过错。在“平台判定用户内容 AI 生成首案”里，倘若平台已依《标识办法》搭建标识核验系统，就应以标识状态作为关键依据。

（二）基于技术留痕的多节点责任明晰

在人工智能生成合成恶意信息的传播链条中，原始生成者、算法推荐平台与转发用户的责任划分，是智能社会多主体治理责任分配的理论投射。在网络传播的指数级扩散效应下，单一追究生成者责任难以实现损害填补与风险防控的双重目标，需将平台与用户的传播行为纳入责任体系。平台作为技术传播枢纽，其责任判定聚焦于《标识办法》规定的标识审查义务的履行情况。生成者与平台作为技术优势方因其对风险源头的控制能力，需承担更高的标识义务，符合民法典禁止权利滥用的原则。标识记录的过错程度，应适用原因力大小规则，实现比例原则的量化落实。人工智能标识将法律责任认定与技术系统深度融合，推动数字空间的责任认定从主观推定转向客观验证，提供兼具科学性与规范性的技术工具。

人工智能标识记录各主体对标识的处理行为，可将抽象的过错、行为与因果关系转化为具体的技术证据。《标识办法》赋予标识法定效力，使标识状态直接关联主体法律责任。生成者未依法添加显

式或隐式标识，可推定其未尽风险告知义务。平台未履行标识核验义务，未能保障元数据真实性，即构成对合理注意义务的违反。用户对标识的恶意篡改或不当使用，依其主观状态，可认定为一般过失、重大过失甚至故意。标识传播链的技术记录为法律归因提供客观依据。

元数据中的时间戳与传播路径信息，使内容扩散过程得以完整还原，进而可解决传统侵权法中多因一果关系难以认定的问题。各主体对标识的处理行为直接影响损害结果的形成，特别是平台对标识异常内容的助推、用户对标识的破坏，均可建立与损害后果的直接因果联系。司法实践中，可依共同侵权与帮助侵权的规定，结合各主体过错程度，实现责任比例的合理划分。《标识标准》统一技术规范，有助于化解平台间的数据壁垒，保障标识在不同传播场景下的可追溯性。当内容跨平台流转时，各平台对标识的处理情况均受法律约束，违反技术规范即推定存在过错，由此可保障责任认定链条的完整性。技术统一性可为司法机关提供连贯的证据链条。

尤其是平台责任的确定。当平台基于历史数据、技术监测等途径明知人工智能生成合成内容存在诽谤等侵权风险，却未对算法推荐机制实施限流、未添加风险标注提示或未启动标识核验程序时，其可被视为对损害结果持放任态度。依据技术治理规范，平台负有不得恶意干预标识完整性的义务，并需部署限流规则、内容过滤算法等技术措施履行风险防控职责。技术证据可在平台责任界定中构建客观化的证明路径，若显示平台未对高频风险内容设置限流阈值、未启动标识核验流程或存在标识篡改痕迹，可直接作为平台放任风险的证据链组成部分，据此推定其“应知”内容风险，无需依赖传统主观过错认定中的复杂心证过程。

深度伪造工具、对抗样本攻击等恶意技术手段，可能伪造或篡改标识系统的元数据结构，进而影响内容治理的责任追溯机制。例如模拟合法标识的编码规则与加密协议，伪造生成者 ID、时间戳等关键元数据字段，使虚假内容呈现合规表象，导致平台合规性核验机制失效。对此，需通过元数据真实性校验与篡改痕迹分析构建责任认定的技术证据链，可以引入加密算法逆向分析、区块链存证比对等专业技术手段，以识别元数据字段的非授权修改痕迹，判定伪造行为的技术实施主体与传播节点的主观明知状态。相应地，应对技术攻击也是平台应尽的合规义务，其应采取前沿技术手段防止篡改标识。

任何主体恶意删除、伪造或隐匿标识的行为，因直接破坏技术治理的底层架构，构成独立的违法性判定要素。元数据篡改记录、标识完整性校验结果等技术痕迹，可作为侵权行为的直接证据，此时无需深入解析内容实质即可认定行为人的主观过错。若生成内容的元数据存在非授权修改痕迹或关键标识字段缺失，可直接推定传播者存在故意或过失，简化传统证据链中的因果关系论证。

法律责任的形态认定需在行政法、民法与刑法的规范体系内实现逻辑贯通。行政责任的追究以《标识办法》第 13 条为规范依据，结合网络安全法等相关法律法规实施阶梯式处罚，根据违法行为的性质与危害程度设定警告、罚款、吊销许可证等递进式责任形态。民事责任的认定需在侵权责任与合同责任的二元框架下展开，明确标识缺失与损害结果之间的因果关系，建立基于技术措施履行情况的过错推定规则，抑或依据用户协议中的标识条款判定违约行为的性质与后果。刑事责任的适用则需严格对照刑法相关罪名构成要件，可能涉及破坏计算机信息系统罪、侵犯公民个人信息罪等，需在技术证据的支撑下精准界定罪与非罪、此罪与彼罪的法律界限。

（三）未进行标识时的解释说明机制

在没有人工智能生成物标识情形下，各方的解释说明义务是对《标识办法》规范功能的必要延伸，亦是周延人工智能治理机制的关键环节。

平台的解释说明义务最为核心，尤其体现在对非标识但疑似人工智能生成物的甄别及处理机制上。平台作为技术与规则的掌控者，其甄别机制不能停留于算法输出的结果层面，而需对识别逻辑、

判断依据进行适度披露。具体而言，当平台认定某未标识内容疑似人工智能生成时，应向用户说明算法识别的核心特征、人工复核的标准与流程、处理措施与疑似程度的关联性论证等必要信息。平台不必公开技术细节或源代码，而应以可理解的方式呈现判定的合理性，保障用户能够对判定结果进行有效抗辩。

就用户而言，当内容未标识却被平台判定为疑似人工智能生成合成时，其亦负有一定说明内容生成合成主体的义务。这并非对创作过程的无限追溯，而是基于诚实信用原则，就内容系人类独立创作提供初步说明，以回应平台的甄别质疑，这既是对自身权益的主张，也是对平台治理的必要配合。

法院在审理人工智能生成合成内容相关案件时，可将解释性说明纳入主观过错的综合评估体系。“平台判定用户内容 AI 生成首案”民事判决书即认为：被告有权依据合同约定对用户发布的内容是否属于人工智能生成进行算法判定并据此作出处理，但被告在没有充分事实依据的前提下对涉案回答进行处理，应当承担相应的法律责任。判决被告恢复违规处理内容、删除禁言处理记录。传播节点若能提供完整的技术措施执行记录与风险控制逻辑说明，即使未能完全阻止虚假内容扩散，亦可不承担责任。若存在技术措施滞后、风险信号忽视等情形，则可能因未尽合理注意义务而被追责。

结语

“平台判定用户内容为 AI 生成首案”反映出人工智能生成内容治理的现实需求，平台依据自有规则对未标识的疑似人工智能生成合成内容进行处理，却因算法解释缺位、复核标准模糊引发纠纷，这表明缺乏统一标识规范时，平台审查权边界、用户权益保障、责任认定依据等方面易引起争议。法院在裁判中强调的平台需对判定依据进行合理解释、用户举证责任应结合创作特性调整等思路，是在无专门法规的背景下，经由个案探索 AI 内容治理的权责平衡。《标识办法》的实施使此前依赖合同约定与个案判断的治理模式，升级为有专门法规支撑的制度化治理，为后续类似纠纷的解决提供明确依据。由个案到制度、再由制度反哺实践的过程，使人工智能整体的治理从分散的经验总结走向系统的规则建构，最终有望形成适配技术发展的多元治理框架。

论生成式人工智能服务提供者的过错推定责任

此处删除了原文脚注，全文请参见《北方法学》2025 年第 5 期，转载或引用请注明出处。

作者：张新宝、卞龙

内容提要：生成式人工智能不符合产品与服务区分视角下的产品概念，其功能主要是输出特定内容和信息，服务提供者不应承担产品责任。生成式人工智能不符合适用无过错责任的基本前提，虽然服务提供者可以更有效率地控制技术风险，但是生成式人工智能通常不存在较高程度的危险性，不宜出于保护公众权益的考虑要求服务提供者内化全部的权益侵害风险。鉴于破除受害人举证困境、适度强化服务提供者义务和责任等需要，应当引入过错推定责任。服务提供者可以通过证明其在训练端和输出端都尽到了与避免侵权输出相关的注意义务来推翻过错。注意义务的标准应适当严格，以激励服务提供者采取充分的风险预防措施。

生成式人工智能治理不仅需要事前的监管，而且需要明确的事后责任规则。责任规则通过塑造相应的激励机制影响新技术的发展方向，预防风险并提供救济机制。其中，归责原则的确定是依法准确认定服务提供者侵权责任的关键，决定着民事责任的构成与配置，体现着民法的公平与正义价值。合理确定服务提供者适用的归责原则，应当以生成式人工智能的技术原理为分析基础，不仅需要避免在侵权法理论内部出现逻辑矛盾，而且需要回应侵权风险预防和受害人救济的现实需求。《欧盟产品责任指令》将软件纳入产品的范畴，可能会对生成式人工智能提供者适用严格责任。我国的《生成式人工智能服务管理暂行办法》等文件则将生成式人工智能提供者视为服务提供者，认为生成式人工智能属于服务而非产品。理论界对于生成式人工智能侵

权应适用的归责原则也存在较大的分歧，需要更充分地讨论以形成共识。本文将明确指出，为何不应将生成式人工智能纳入产品的范畴继而适用产品责任，或者要求服务提供者承担直接的无过错责任，而是应当要求其承担过错推定责任。本文将明确服务提供者如何证明其尽到了相应的注意义务，以推翻法律对其过错的推定。

一、生成式人工智能侵权不应适用产品责任

欧盟委员会于 2022 年通过制定《人工智能责任指令》和修订《产品责任指令》的提案，以解决人工智能的责任问题。修订后的《产品责任指令》将人工智能在内的软件纳入产品责任的适用范围，虽然没有明确指出是否适用于生成式人工智能，但是至少没有将其明确排除。对此，欧洲议会研究服务处（EPRS）的补充评估指出，《产品责任指令》可能无法解决生成式人工智能的责任问题，需要通过扩展《人工智能责任指令》的适用范围来解决。理论界对于该问题的认识也不一致。主张适用产品责任的观点认为，区分人工智能产品和服务不可行也不合理，包括生成式人工智能在内的人工智能提供者应当承担产品责任。另有观点认为，用于医疗、导航等专业领域的生成式人工智能可以适用产品责任，用于生成诗歌、日常问答等则不适用产品责任。本文认为，生成式人工智能侵权不应适用产品责任。

（一）生成式人工智能不符合法律上的产品概念

传统产品责任制度中产品的概念被包含于物的概念，信息技术的发展使得有体物之外的客体也可以成为产品，不过应符合“用于销售”的概念要素。我国《产品质量法》第 2 条规定：“本法所称产品是指经过加工、制作，用于销售的产品。”“销售”通常被理解为以经济目的而将产品以出卖的方式交付他人的行为，其概念的核心是“交付”，构成了销售产品与提供服务的本质区别——交易的主要目的是转移所有权。产品的销售过程表现为出卖人向买受人交付特定产品、买受人支付对应的价款，发生产品所有权的转移。但是，提供服务的过程通常不存在价款之外的交付行为，不会发生所有权的转移。如果服务的内容是物的定制，虽然最终目的也是物的交付，但是整个过程仍属于服务；如果服务过程附带了物的交付，例如商家在提供服务过程中附赠了产品，应当认为该产品独立于服务过程，可以对其适用产品责任。产品的概念保持着开放状态，信息技术的发展早已使产品摆脱了有形的界限，无形与有形并非区分产品与服务的有效标准。数据、虚拟财产等的价值已经得到理论和实践的认可，并且成为可以被批量交易的对象。其所有权可以在交易过程中发生转移，满足产品概念中“用于销售”的要求，只要同时满足“经过加工、制作”的要件，便可以构成产品。

下载和使用生成式人工智能软件时不存在交付过程，使用者支付了相应费用之后并未取得完整软件副本的所有权，仅取得了通过互联网接入并使用软件的资格，所以不应当将其纳入产品的范畴。软件作为智力成果存在适用产品责任的空间，但是并非在所有情况下都可以构成产品。软件不仅可能作为产品被用于销售，而且可能只是被用作提供服务的工具，应当结合具体情况进行判断。软件通常不会造成大范围的损害，不会危及消费者之外的主体，无法适用产品责任的情形可以通过违约责任解决赔偿问题，受害人的权益也能够得到保障。软件的类型主要包括下载到计算机本地并且完全在本地运行的软件、下载到本地但是需要通过接入互联网使用的软件，以及不需要下载直接通过互联网接入并使用的软件。对于不需要接入互联网使用的软件，用户将该软件完整的程序和文档下载到本地服务器，取得了该软件的完整副本。对于需要接入互联网使用的软件，用户仅下载了运行该软件的必要程序和文档，并非该软件的完整副本，不同用户接入的实际上是同一个软件，所以并不符合产品的概念。过去以光盘作为载体并且可以直接在本地运行的软件，比较符合产品的概念，如今日常使用的各种应用软件则更符合服务的特征。另外，若本身不符合产品定义的软件内置于有形产品，内置的软件可以决定该产品的安全性，可以考虑对“有形产品

+软件”的整体适用产品责任。基于上述原因，生成式人工智能在当前的产业模式下应当被定性为服务而非产品。一方面，生成式人工智能软件本身不符合产品的定义。生成式人工智能软件可以通过下载客户端使用，或者直接在网页端使用，但是使用者并没有取得软件副本的所有权，仅是通过互联网接入提供者的服务器，不同使用者使用的仍是同一个软件。生成式人工智能服务提供者往往是按照字符数量或者使用时长收取费用，不符合产品销售的特征。使用者支付的是使用软件的费用，而非购买软件副本的对价。另一方面，内置的生成式人工智能软件无法决定有形产品的安全性。生成式人工智能无法驱动有形产品，无法对他人的生命、健康、财产等权益造成损害，不应对有形产品与内置软件形成的整体适用产品责任。

（二）信息错误造成他人损害不应承担产品责任

错误信息不具有直接的危险性，适用产品责任有失妥当。过去，法院几乎不会通过产品责任制度来要求出版商等主体对错误信息造成的损害承担责任。主要有两种路径可以对此作出解释：第一，信息可以构成产品，但是通常不可能存在缺陷，所以相关主体不需要对损害进行赔偿；第二，信息本身无法构成产品，所以不适用产品责任。若采第一种路径，可以对事实性信息、应用型信息等错误造成的损害适用产品责任；若采第二种路径，应当根据过错责任原则解决此类错误信息造成损害的赔偿问题。对于思想、观点等信息，无论是否将其视作产品，可能都难以通过产品责任追究生产者和销售者的责任。因为涉及言论自由的保护，出版商等无须对思想和观点的准确性负责，难以认为其存在缺陷。但是事实性、应用性等信息存在准确性要求，发生错误可能会被视作缺陷产品。相应的观点认为：信息产品是大批量生产、大规模销售的产品，出版者、发行者有能力分散损失，而且信息提供者相较于消费者处于信息的优势地位，更有能力防范风险。美国即存在将航空地图视作产品并判决出版商承担严格责任的案例。本文认为，信息不构成产品责任制度中的产品，因为信息错误不具备直接的危险性。相关主体应当对错误信息承担过错责任，而非产品责任。纯粹的信息不会直接造成损害，需要以自然人的行为作为介质才能对外界产生作用。信息接收者需要甄别信息的真实性，并对误信特定信息真实性造成的损害负责，除非信息提供者负有保证该信息真实性的义务。信息可以被无限复制，具有解释上的诸多可能性，要求信息的提供者对信息错误间接引发的损害承担无过错责任，无疑会极大抑制信息的生产和传播。即使是主张构建信息产品责任制度的观点也认为，不应对生产者和销售者适用无过错责任。比较法上，出版商等对于因瑕疵信息而给消费者造成的损害，通常也是以其违反了注意义务为由承担过失侵权责任。

生成式人工智能的功能是输出特定内容，服务提供者不应对信息错误引发的损害承担产品责任。生成式人工智能输出的内容是对用户提问的创造性回答，应当由使用者对信息的可信度进行判断。“生成式人工智能的运行全过程处于黑箱状态，存在超越、背离和独立于人的行为的倾向性，由于运行和变换的不客观及不被理解，算法黑箱的存在也让生成式人工智能中出现了逻辑隐层，即人工智能算法系统逻辑处于不可知的隐蔽状态。”基础大模型通常包含数千亿参数，映射规则相当复杂，输入与输出之间的逻辑关系难以被清晰解读。服务提供者在当前技术发展阶段不可能确保输出的准确性，尤其是对专业问题的回答。即使生成式人工智能被应用于正式场合，生成的内容也只是作为人类决策的参考，无法替代人类的专业判断。应当看到，安全和可靠不过是生成式人工智能的发展目标，服务提供者并没有法律上的义务确保信息准确，除非事先对此作出了明确承诺。如果要求服务提供者承担产品责任，意味着需要对所有误信生成内容而产生的损害负责，无疑会使其面临过重且难以预测的潜在风险。

（三）适用产品责任难以达到理想的规制效果

产品责任制度的核心目的在于控制产品批量生产和销售造成的大范围风险，最大限度地保障公

众的人身和财产安全，同时给予受害人充分的救济。站在功能主义的立场，即使生成式人工智能不满足产品的定义和特征，仍然有可能将其纳入产品责任的适用范围，以达到强化受害人权益保护的目标。生成式人工智能意外输出侵权信息是现阶段无法完全避免的问题，并且会随着技术方案的不断优化逐渐得到解决，目前不能将输出侵权信息的生成式人工智能一概视为有缺陷。当然，若生成式人工智能的安全性没有达到行业的通常水平，即技术发展的当前阶段所普遍应当具有的安全性，则可能会被认定存在缺陷。可是在生成式人工智能侵权的场景，产品责任的制度设计或许并不会像其被应用于有形产品时一样有助于受害人的救济，并且无法高效激励提供者采取措施提高服务的安全性，难以发挥出应有的制度功能。

虽然无过错责任的适用提高了受害人获得赔偿的可能，但是生成式人工智能缺陷的证明会给受害人造成较大的困难。制造缺陷是最容易被证明的产品缺陷类型，适用无过错责任会大幅减轻受害人的证明负担并提高受害人胜诉的概率。然而，人工智能系统的缺陷往往是由设计选择不当造成，包括训练数据中的偏差、不完善的算法等，所以人工智能系统的缺陷更有可能归因于有缺陷的设计而非制造。于是，适用产品责任制度的实际效果就会有所折扣。相较于制造缺陷，设计缺陷和警示缺陷比较难以证明，因为其中包含了过错证明的成分。美国法律研究院和多数法院对设计缺陷和警示缺陷的证明采用的是“风险—效益”标准，即通过衡量产品风险的大小与降低风险的成本确定产品是否存在缺陷。“风险—效益”标准鼓励生产者在产品的效用和可能产生的风险之间、严厉的警告和产品的可欲性之间进行衡量，找到最为合理的解决方案，而不是为了避免事后承担严苛的责任而过分保守。因为公众没有理由指望生产者为了产品的安全付出过分高昂的成本而牺牲生产效益，生产者有理由在安全与效益之间保持平衡。对于设计缺陷的判断而言，需要通过衡量更安全设计所需的成本与此种设计可以避免的损失，判断是否存在更合理的替代设计方案。若生产者改进设计所需投入的成本大于其能够降低的风险，则生产者没有义务去改进设计；若生产者能够以合理成本降低产品的风险，则说明存在合理的替代设计，即产品存在设计缺陷。对于警示缺陷而言，生产者并不需要对产品危险进行过于严厉的警告，因为强烈的警告虽然能避免较多的危险，但是会导致销量的降低。生产者仅须对应当预见到的与产品相关的风险作出适当、合理的警告，其程度应与产品的潜在危险性成正比。可见，“风险—效益”标准实质上就是要证明生产者存在过错。生成式人工智能技术对于普通公众而言难以理解，恐怕难以证明缺陷的存在。尤其是设计缺陷的证明，带给受害人的挑战最为严峻。所以，适用产品责任或许并不会使受害人更容易获得赔偿。作为配套制度，可能还需要通过引入表见证明规则、改变对设计缺陷和警示缺陷的认定标准，或者建立证据披露与缺陷推定制度等方式，减轻受害人在缺陷证明上的负担。

二、服务提供者不应承担无过错责任

目前有观点认为，应当以无过错责任原则追究生成式人工智能服务提供者的侵权责任，以抵消人工智能固有的危险，激励服务提供者减少有害的人工智能活动。另有观点认为，作为一种新型社会性风险的制造者，生成式人工智能服务提供者应适用无过错责任承担著作权侵权损害赔偿责任。如上所述，生成式人工智能服务提供者不应为信息错误造成的损害承担侵权责任。分析是否需要通过无过错责任追究服务提供者的侵权责任，主要是考虑输出侵害个人信息、著作权、商业秘密等权益的信息造成损害的场景。提供生成式人工智能服务不属于《民法典》所规定的适用无过错责任的具体责任类型。而且，提供生成式人工智能服务难以被理解为“高度危险作业”，无法适用《民法典》第 1236 条关于高度危险责任的一般条款。可见，生成式人工智能服务提供者的无过错责任无法从既有制度中找到合适依据，需要考虑是否需要将其规定为新型的无过错责任类型。本文认为，无论是基于无过错责任的一般原理还是基于特殊的法政策考量，生

成式人工智能服务提供者都不应当承担无过错责任。

（一）生成式人工智能不具有较高程度的危险性

主张生成式人工智能服务提供者承担无过错责任的观点基本是从受害人保护、危险控制、分散损失，以及从行为中获益等角度进行阐述，但是忽略了对生成式人工智能应用本身危险程度的分析。适用无过错责任的归责事由包括危险与控制力。其中，危险责任的根源是可能给不特定主体造成损害的特殊危险。特定活动或者物的危险性只有达到了比较高的程度，难以通过尽到合理注意有效控制，行为人或者物的所有者等才具备承担无过错责任的基本前提。危险责任的理论基础在于，为了自己的利益开启和控制较高程度危险的主体，应当对因此产生的损害负责。危险活动和危险物具有较高致人损害的可能性，如果相关主体不存在过错但造成了损害后果，不予赔偿显然有失公平，因此需要引入无过错责任来解决不幸损害的分配问题。侵权责任法正是从分配正义的理念入手，从损害发生的危险源上来确定应由何方承担损害。作为过错归责的例外情形，无过错责任原则必须有极其充分的理由才可以适用——行为的危险性达到难以有效控制的程度。否则，社会生活中危险无处不在，动辄以开启了危险为由要求相关主体承担无过错责任，必然会动摇过错责任的根基。

服务提供者通常不应对侵权信息承担无过错责任，最核心的理由是生成式人工智能通常不具备较高程度的危险性。生成式人工智能不具备物理实体也无法驱动物理实体，不会如自动驾驶等人工智能应用直接威胁到自然人的生命、健康等人身权益，而且生成式人工智能软件不会如杀毒软件等通过运行对计算机等有形财产造成损害，可见其侵权风险仅在于输出的内容和信息本身。目前实践中主要存在两类生成式人工智能应用：第一类是直接回答用户的提问或者操作，根据用户的要求直接输出内容的生成式人工智能；第二类是将用户提供的内容作为素材进行转化和再创作的应用，例如将用户提供的图片转换成其他风格，根据用户提供的人物形象和文字生成视频等。转化型生成式人工智能使用的素材只要合法合规，输出的内容通常不会直接构成侵权。虽然某些深度伪造的内容可能被不法分子用于实施诈骗等侵权和犯罪行为，但是此种风险主要来源于实施下游侵权和犯罪的行为人，不应将具有深度伪造功能的生成式人工智能应用视为需要纳入无过错责任适用范围的危险源。创造型生成式人工智能存在直接的侵权风险，因为其会自主输出新的信息，但是通常也不会达到高度危险的程度。在没有介入使用者行为的情况下，服务提供者只要在训练端依法收集数据、构建算法时充分考虑如何避免侵权信息的输出，生成式人工智能自主输出侵权信息的概率相对有限。如果介入了使用者的侵权行为，例如刻意引导模型输出、实施外部攻击、传播侵权内容等，输出侵权信息的危险性此时主要来源于使用者，服务提供者通过规范使用者行为可予以有效控制。

一个基础模型可能会在一千个生成式人工智能应用中被使用，但是可能只有一个是高风险应用程序。目前，尚无充分证据表明国内的生成式人工智能应用存在比较严重的侵权问题，实践中也已经出现不使用个人信息或者受著作权保护作品进行训练的应用，生成式人工智能的侵权风险可以得到控制。而且，我国采用大模型备案审查制度，可以有效避免存在特殊风险的生成式人工智能应用进入市场。过去，网络中介服务平台上存在大量侵权信息，而且存在借助网络服务实施其他侵权甚至犯罪行为的情况。由于互联网实名制没有完全落实，网络行为的匿名性等特征容易造成受害人找不到实际侵权人而得不到救济的困境。网络中介服务提供者无疑制造了危险源，甚至其危险程度可能高于生成式人工智能服务。但是，长期以来理论和实务都没有将网络中介服务视作难以控制的危险，进而要求服务提供者承担无过错责任。生成式人工智能服务提供者和网络中介服务提供者虽然在性质上存在一定差异，但是生成式人工智能服务所开启的侵权风险程度并不会明显高于网络中介服务。所

以，应当认为生成式人工智能的危险程度较为有限，不宜通过无过错责任原则追究服务提供者的侵权责任。

（二）具备危险控制能力等不属于归责事由

具备危险控制和损害分散能力、损益相一致原则、降低预防侵权的社会总成本等不属于归责事由，其作用是在相关主体制造了较高程度危险的情况下作为解释适用无过错责任合理性的实质理由。无过错责任原则对受害人的保护是以减损加害人的行动自由为代价，倘若没有充分的理由，必然会造成对加害人不公平的结果。开启了较高程度危险的行为本身具有较强的可归责性，此时将损害分配给危险的开启者承担，符合公平原则的要求。如果潜在责任主体没有制造较高程度的危险，仅以具备危险控制和损失分散能力等作为依据，无法证成服务提供者应承担无过错责任。应当注意，引入无过错责任并非侵权责任法应对技术风险的唯一途径。安全保障义务的设置同样是出于相关主体具备危险控制和损失分散能力、从行为中获得经济利益、降低预防侵权的社会总成本等方面的考虑。若潜在责任主体只是开启了一般程度的危险，同时具备危险控制能力，应当考虑要求其承担一定程度的安全保障义务，而非要求其承担无过错责任。同样以网络中介服务提供者作为参考，网络中介服务提供者开启了网络空间的权益侵害风险，具备技术和经济能力进行内容审核来控制危险，可以通过价格机制和保险机制等分散损害，网络中介服务提供者和生成式人工智能服务提供者在控制危险和分散损害的能力上不存在显著差别，但是我国法律没有要求网络中介服务提供者承担无过错责任。同样，不能仅因为生成式人工智能服务提供者具备较强的危险控制和损失分散能力就要求其承担无过错责任。

无过错责任原则表面上能够简化生成式人工智能致害的损害赔偿问题，但是不得不警惕，任何技术在早期阶段可能都会带来不可预测的危险，研发者、经营者等主体相较于普通公众都具有比较强的危险控制和损失分散能力，而且其目的通常也包括从研发和经营活动中获得经济利益。按照此种以危险控制等为核心的论证模式，未来商业性的技术研发者和经营者等可能都要为技术应用而造成的他人损失承担无过错责任。届时，归责的主要考虑因素不再是过错。只要开启了危险且具备较强的技术和经济能力，便可以出于降低技术风险等考虑要求相关主体承担无过错责任，不仅不符合基本法理，而且会极大制约技术的发展。

（三）可能造成技术发展与权益保护的失衡

通过上述分析可以认为，生成式人工智能服务不具备适用无过错责任的前提条件。但是有无必要出于受害人保护等方面的考量，例外地要求服务提供者承担无过错责任？主张无过错责任的观点还关注服务提供者和使用者皆无过错，但是对于输出侵权信息造成他人损害情形下的损害赔偿问题，认为受害人的损害在此种情形下得不到救济，显然有失公平。生成式人工智能目前存在意外输出的问题，可能会因过拟合等原因输出训练语料中的未公开个人信息、作品等内容，暂时难以完全通过技术手段避免此种意外记忆。如果坚持过错追责，受害人在服务提供者无过错但是生成式人工智能输出了侵权信息的情形无法获得救济。本文认为不应以此为理由要求服务提供者承担无过错责任。首先，适用更严格的归责原则固然会更有利于受害人的保护和损害的预防，但是会相应地限制行为人的行为自由和加重加害人的责任。保护受害人和预防损害并不能作为适用无过错责任原则的理由，而只能作为其目的。其次，意外输出问题仍然是低概率事件。目前国内外涉及侵权输出的案件和事件，几乎都是因为服务提供者未经同意使用他人未公开的个人信息或者作品训练模型，并且没有尽可能在输出端避免生成侵权内容，服务提供者在这些情形都存在过错。再次，可以要求服务提供者尽到较高标准的注意义务，采取相应的技术措施来减少意外输出。目前不能判断在服务提供者尽到较高程度的注意义务之后是否还会存在意外输出的情况。随着语料和算法的优化、服务提供者的义务得到明确和落实，可以预见意外输出风险将会不断降低。最后，行为人无过错、受害人得不到救济的情况在其他场

景下同样会存在，并不会造成不公平的后果。不应刻意强调和放大生成式人工智能服务提供者无过错却造成损害的例外情形，继而以救济受害人为理由引入无过错责任。

面对生成式人工智能等技术带来的权益侵害风险，侵权责任法不能过度强调受害人的保护和救济，否则可能会造成技术发展与潜在受害人保护之间的失衡。生成式人工智能服务具有极大的正外部性，不宜要求服务提供者完全内化负外部性。信息技术和应用通常都会带来权益侵害风险，但是技术研发毕竟不同于其他纯粹营利的活动，具有较高的公共价值，应当在技术发展初期允许合理水平的风险存在，不宜在较早阶段就通过加重服务提供者责任的方式降低权益侵害风险。政府和社会公众在生成式人工智能发展过程中都是受益者，应当共享技术发展的成果，共担技术发展的风险，不应将技术风险造成的所有不利后果都分配给服务提供者。无过错责任虽然有利于受害人获得赔偿，但是可能会导致“寒蝉效应”，导致某些生成式人工智能模型无法落地应用，减缓甚至阻碍技术的创新和发展。基于技术发展的考虑，对于生成式人工智能服务提供者仍应坚持过错追责。此外，行政监管和行政责任的承担在技术风险的化解中发挥着重要作用，尤其是对于信息技术所造成的大规模风险，行政手段相较于侵权责任法可能更为有效，侵权责任法不需要也没有能力完全化解生成式人工智能带来的权益侵害风险。

三、服务提供者应承担过错推定责任

生成式人工智能应用仅具有一般程度的危险性，过错责任原则足以应对服务提供者的侵权责任问题，不过需要考虑应当适用一般过错责任还是过错推定责任。考虑到潜在受害人客观存在的举证困境、训练端的数据制度构建生成式人工智能的技术特征、已经存在的制度基础等因素，引入过错推定责任来追究服务提供者的侵权责任是比较适当的选择。

（一）破除举证困境的客观需要

公众的权益能否得到保障需要考察两个方面：第一，相关制度是否能够激励服务提供者采取充分的措施防范侵权风险；第二，发生侵权事件时受害人能否顺利获得救济。于前者而言，虽然服务提供者在训练端对个人信息、作品等内容的使用会在输出端引发一定的侵权风险，但是只要明确服务提供者应当在输出端尽到较高标准的注意义务，服务提供者便会尽可能通过优化算法和语料库等方式来提高模型的安全性，以防范侵权风险的发生。于后者而言，受害人可能会在过错证明上面临较大困难，导致一般过错责任原则无法保障受害人顺利获得救济。同时，受害人难以依法获得赔偿会使服务提供者采取预防措施的激励减弱。

服务提供者的过错在部分情况下比较容易证明，能够根据服务的具体内容和细节进行判断。以陈某与上海易某网络科技有限公司侵害作品信息网络传播权纠纷案为例，被告上海易某网络科技有限公司提供的服务内容是使用他人拍摄的视频作品为用户进行换脸，然后输出换脸后的视频。被告显然在明知是他人作品的情况下进行使用，能够从被告的行为判断出其存在侵害他人著作权的故意。服务提供者的过错在部分情况下比较难以证明，因为其并未实施能够体现主观过错的积极行为。创造型生成式人工智能的输出过程具有概率性和随机性，输出侵权信息并不能说明服务提供者存在过错，受害人还需要另行证明服务提供者未尽到注意义务。然而，缺乏专业知识和能力的普通公众可能难以顺利完成举证：首先，服务提供者在训练端的过错表现为没有依法使用训练数据，输出端的过错表现为对注意义务的违反，不具备专业知识的受害人可能难以知晓服务提供者需要尽到的义务内容。其次，用以证明加害人过错的证据往往处于服务提供者自己的控制之下，相关的证据内容可能存在较高的专业知识壁垒。若要求受害人对服务提供者的过错进行证明，举证可能性相当有限，继而会使受害人面临较高败诉风险。所以，需要通过举证责任倒置保障受害人能够顺利获得救济。《欧盟人工智能责任指令（提案）》规定了证据披露制度，以缓解受害人的证明压力。考虑到相关技术术语对普通

公众而言难以理解，即使披露了相关技术事实，受害人是否有能力从中提炼出能够证明加害人过错的有效证据存在一定疑问，采用过错推定更能解决受害人的举证难题。

（二）符合公平原则的内在要求

举证责任倒置是对“正置”举证责任的局部修正，有利于案件实体真实地再现，符合民事诉讼实体公正与程序公正的价值目标。过错推定责任的目的并不一定是加重加害人的责任，而可能主要在于避免出现对受害人不公平的局面。首先，生成式人工智能服务提供者更接近案件相关证据，具备更高的专业能力和水平，过错推定只不过是矫正了双方的“武器不平等”状态。现代民法以社会为本位，强调具体正义，过错推定便是此种社会保护思想的体现。表面上看，过错推定责任将举证不能的风险转移给加害人承担，可能会不当加重加害人的责任。但是，网络环境下作为证据的事实对生成式人工智能服务提供者而言比较容易收集和保存，举证不能的概率比较低。其次，服务提供者作为侵权风险的开启者、控制者和经济上的受益者，适当地增加其义务和责任以保护公众的安全，符合公平原则的要求。再次，目前普遍认为应当在训练端的制度安排上适当侧重语料的获取和使用，相应地应当要求服务提供者在输出端妥当保护公众的合法权益。基于整个训练和服务过程的统筹考量，要求服务提供者在输出端承担相对更重的义务和责任，以降低甚至消除在训练端造成的权益侵害风险，能够实现整体法律制度设计的公平与合理。

普通公众在传统侵权法律关系中对于证据的掌握情况和举证能力比较接近，“谁主张谁举证”的一般过错责任原则具有天然的合理性。然而，信息业者作为侵权人、普通公众作为被侵权人的新型侵权法律关系具有一个突出特征，即双方技术能力明显不对等导致彼此证据掌握情况和举证能力差距悬殊，需要考虑此时以一般过错责任为原则是否妥当。尤其是在公众权益保护已经面临较大挑战的时代背景之下，信息业者的过错推定责任是更公平的选择。

（三）符合生成式人工智能的技术特征

创造型的生成式人工智能输出侵权信息主要存在两种可能性：第一，模型学习了个人信息、作品、商业秘密等，并且在过拟合等情况下意外输出了与语料相同或相似的内容。第二，模型没有学习相应的个人信息等内容，但是偶然“创造”出了侵权信息。如果是第一种情形，服务提供者有义务采取措施避免侵权输出，否则应当认为其存在过错；如果是第二种情形，服务提供者对于侵权内容的输出通常不存在过错。根据生成式人工智能的技术原理，模型通过学习确定各个参数的映射规则，然后基于其学习后形成的功能回答使用者的提问。假设生成式人工智能未学习相应的作品等而输出了侵权信息，意味着其完全是基于概率而创造出了与语料相似或者完全相同的内容，此种可能性相对较低。尤其是侵害著作权、商业秘密等情况，因为其内容构成相对比较复杂，模型在未学习相应内容的情况下偶然“创造”出侵权信息，应当属于极小概率事件。而且，生成式人工智能训练需要尽可能丰富的语料，客观的行业需求决定了服务提供者会尽量广泛地收集高质量数据作为训练语料。所以，侵权信息的输出更有可能是因为服务提供者使用了相应内容作为语料，而非纯粹的偶然。此外，服务提供者只要在输出端充分采取了过滤等技术措施，生成式人工智能输出侵权信息的概率应当比较低，侵权信息的生成更有可能是因为服务提供者未妥当尽到注意义务。根据以上技术特征，推定服务提供者在生成式人工智能输出侵权信息时存在过错具有合理性。

（四）已经存在相应的制度基础

生成式人工智能侵害的主要是非物质人格权益和知识产权等，过错推定责任已经在部分法律规范或者司法实践中得到认可。首先，我国《个人信息保护法》第 69 条已经明确规定了侵害个人信息权益的过错推定责任，受害人无须对加害人过错进行证明。其次，司法实践中对于著作权侵权的认定已经存在推定过错的做法，具备直接适用过错推定责任的合理性基础。实践中判断侵害著作权等普遍

采用的是“实质性相似+接触”规则，不再单独考虑行为人的过错。原告只要证明特定内容与其在先作品构成实质性相似并且被告具备接触其在先作品的条件和事实，便可以认定被告侵害了其著作权。具体而言，构成实质性相似通常代表着存在权利损害事实，并且存在侵害著作权的行为。行为人接触在先作品，意味着在后的作品可能并非作者独创。由于接触与否的事实主要由行为人掌控，司法实践中常以作品已经公开发表为由，推定接触的存在，并由行为人承担不存在接触的证明义务。于是，司法实践中对行为人过错的认定往往以接触事实的认定作为代替，甚至简化为作品已经发表的客观事实认定。虽然此种过错推定是司法推定，不完全等同于法律直接作出的推定，但是都会产生无须证明加害人过错的效果。作为生成式人工智能侵权的重点问题，侵害著作权和个人信息权益在立法或司法中已经采纳了过错推定，规定生成式人工智能服务提供者的过错推定责任具有一定的制度基础，可以实现类似问题处理上的一致性和连贯性。

四、服务提供者对无过错的证明

生成式人工智能服务提供者的过错需要从其客观的行为进行判断，难以直接考察其主观状态。服务提供者对生成式人工智能可能会输出侵权内容具有概括的预见能力，应当尽到合理的注意义务。此种以注意义务为重心的侵权追责模式可以为生成式人工智能服务提供者提供稳定的预期，兼顾受害人的保护与产业的发展。过错推定原则意味着若生成式人工智能输出侵权信息造成损害，直接推定服务提供者未尽到注意义务。服务提供者可以通过证明在训练端使用语料符合相关规定并且在输出端尽到了注意义务来证明其不存在过错。

（一）服务提供者在训练端的行为规范

服务提供者获取语料时需要遵守《著作权法》和《个人信息保护法》等法律法规，但是如果严格适用相关规定，服务提供者将会面临语料获取的困境，不符合促进数据要素利用的政策导向。鉴于生成式人工智能的发展需求，应当在训练端慎重认定相关主体的过错，以保障服务提供者能够获得充分的训练数据。对于作品使用行为而言，应当将其纳入合理使用的适用范围，但是需要确保不会输出影响原作品阅读市场的内容。如果服务提供者未经许可使用了他人作品而模型未输出影响原作品阅读市场的内容，应当认为服务提供者不存在过错。对于个人信息使用行为而言，依据促进数据要素利用的政策导向，应通过宽松解释《个人信息保护法》的相关规定或者作出例外规定，缓解对个人信息语料获取行为的限制。如今尚未建立生成式人工智能的专门制度，法院应当在适用相关规定时灵活处理。

虽然需要在训练端适当侧重于技术的创新发展，但是服务提供者仍然需要遵守相关的行为规范。个人信息保护方面，服务提供者需要注意以下问题：其一，需要遵守“告知—同意”规则，不得在完全未经个人同意的情况下处理未公开的个人信息。虽然无须在每次进行个人信息数据流转时都取得个人同意，但是至少应当在个人信息收集时告知个人可能会将其个人信息用于不特定场景的生成式人工智能训练并取得同意。其二，需要受到必要性原则的限制。服务提供者需要尽可能丰富的数据作为语料，必要性原则似乎难以适用。若能够在实现目标功能的前提下尽可能使用更少的个人信息数据，则仍然需要受到必要性原则的限制。其三，只有在具备充分必要性的情况下才可处理敏感个人信息，避免意外输出给自然人的人格尊严、人身和财产等造成比较重大的损害。著作权保护方面，机器学习行为通常不会影响作品的正常使用、不会不合理地损害著作权人的合法权益，服务提供者通常可以基于合理使用制度来使用作品，但是应避免输出影响原作品传统阅读市场的内容。于特殊情形，机器学习对作品的使用会不合理地损害著作权人的合法权益，服务提供者需要依法取得著作权人的授权许可。

（二）服务提供者在输出端的注意义务

生成式人工智能服务提供者在整个服务周期中需要尽到各种不同内容和目的义务，违反义务与侵权输出之间并非都存在因果关系。例如，服务提

供者负有保障服务透明度的义务，但是违反该义务不会造成侵权输出。服务提供者欲证明其不存在过错，仅须证明其尽到了与避免侵权输出相关的注意义务，主要包括：其一，采取优化算法、关键词过滤等有效的技术手段以避免侵权输出；其二，提醒和规范使用者的行为，避免引导模型输出侵权信息；其三，及时检测和修补安全漏洞，提高模型安全性；其四，收到权利人通知时采取必要措施，避免侵权信息再次生成，建立便捷的通知渠道，及时处理受害人的请求。问题的关键在于注意义务标准的明确，决定服务提供者证明其尽到了何种程度的注意义务才能推翻对过错的推定。

较高标准的注意义务可以促使服务提供者提供更安全的模型，采取更充分的技术措施减少侵权信息的生成，但是相应地会增加服务提供者的负担，包括技术研发投入的成本和可能承担的责任。本文认为，要求服务提供者在输出端尽到较高标准的注意义务具有合理性。原因主要有三个方面：第一，服务提供者的数据使用行为开启了非相互性风险，应当承担较高标准的注意义务，以尽可能内化风险、保护公众的合法权益。公众无力预防生成式人工智能造成的侵权风险，或者需要付出不成比例的成本，所以承担较高标准的注意义务是降低预防侵权社会总成本的需要。第二，尽到较高标准的注意义务是兼顾产业发展与权益保护的必然选择。训练端的制度构建需要重点考虑语料获取需求，侧重于技术的创新发展，相应地需要在输出端要求服务提供者尽到较高标准的注意义务，尽可能消除训练活动造成的权益侵害风险，避免造成对权益保护的失衡。第三，服务提供者尽到较高标准的注意义务是保障语料获取需求的需要。如果服务提供者不能在输出端妥当保护公众的合法权益，其在训练端享受“优待”的合理性就不再充分，可能会影响训练端语料获取相关制度的构建和运行。出于上述考虑，不能仅从风险预防的效率来判断服务提供者是否尽到了充分的注意义务，即使风险预防成本高于可能收益也不能当然认为超出了合理的注意义务水平。

注意义务的标准也不应过高，应以激励服务提供者采取充分的预防措施为目标。标准过于严格会导致服务提供者几乎不能反证无过错，以致于达到无过错责任的效果。“通过设定较重义务来降低风险固然可以达成实效，但也应考虑到在技术发展的现实需要下，适度容忍合理风险的必要性。“目前生成式人工智能研发仍然面临技术上的难点，包括训练数据的筛选、算法的建构，不可能做到绝对的安全。所以注意义务的设置是为了在现有技术能力下尽可能降低风险，而非完全消除风险。服务提供者是否采取了充分的注意义务应当结合以下因素判断：第一，服务提供者的规模大小和技术水平；第二，生成式人工智能服务所处的具体领域；第三，当前相关技术措施所处的发展阶段。分别来看，企业的规模越大，采取的技术措施就应当越充分；提供服务的类型存在越高的侵权风险、涉及的权益越重要，承担的注意义务标准就应越高；服务提供者应当采取与技术发展水平相符合的技术措施，并且随着技术的发展不断更新和优化。综合来看，不同规模的服务提供者的技术能力也会存在差异，不能要求较小规模的服务提供者与较大规模的服务提供者投入相同的成本来提高其服务的安全性。但如果提供的是关键领域或特殊用途的生成式人工智能服务，公众对服务安全有更高的要求，应当对不同规模的服务提供者等量齐观，以尽可能确保服务的安全性。

（三）服务提供者证明无过错的具体方法

服务提供者通常需要证明其在训练端和输出端都尽到了与避免输出侵权信息相关的注意义务，才能推翻对过错的推定。此外，服务提供者也可以通过证明没有使用相关作品、个人信息等内容作为语料来证明无过错，因为此时模型是基于其创作功能偶然输出了涉嫌侵权的内容。以著作权和个人信息侵权为例进行说明。对于著作权而言，服务提供者可以通过证明其没有使用原作品或者已经在输出端尽到了相应的注意义务来反证过错不存在。训练语料的范围就是生成式人工智能模型所接触到的信息范围，若服务提供者能够证明训练语料中不

包括该原作品，则能够推翻过错。但是由于服务提供者可能通过删除相关数据、修改记录等方式“伪造”证据，所以更可靠的做法是要求服务提供者证明不可能接触原作品来证明其没有使用原作品作为语料。对于个人信息而言，服务提供者需要证明使用个人信息符合相关法律规定，并且在输出端尽到了注意义务来反证不存在过错，或者通过证明未使用相关个人信息来证明无过错。

还需要注意，服务提供者在训练端的行为会影响其在输出端的义务。前文对注意义务的讨论建立在给予服务提供者数据使用行为一定豁免或例外规定的基础之上，由于其在训练端的数据使用行为未经充分同意或者授权许可，服务提供者应负有避免侵权输出的义务，消除其制造的权益侵害风险。但是若服务提供者在训练端告知权利人将会使用其作品或未公开个人信息等训练生成式人工智能并且模型会输出相关内容，并且已经取得了权利人授权许可或同意，则服务提供者不再负有避免输出相关内容的义务。例如，服务提供者在训练端使用作品时取得了著作权人的授权许可，而未基于合理使用，并且对模型可能会输出相关内容进行了充分告知，则其在输出端可以在授权许可的范围内输出与原作品构成实质性相似的内容等。所以，服务提供者证明其取得了著作权人的授权即可推翻对过错的推定，无须再证明其在输出端尽到了注意义务。同样，如果服务提供者可以证明已经在训练端告知个人模型会输出其未公开的个人信息，并且取得了其单独同意，则服务提供者不负有避免输出个人信息的注意义务，仅需证明其在训练端的个人信息处理行为满足其他规定，便可以推翻对过错的推定。

五、结论

生成式人工智能民事法律制度的建构，应当在输出端强调对公众权益的保护，明确服务提供者的义务和侵权责任，尽可能降低权益侵害风险，保障受害人顺利获得救济。生成式人工智能本质上属于服务而非产品，产品责任的制度设计无法有效应对生成式人工智能带来的权益侵害风险，所以将其纳入产品责任的适用范围并非有效的解决方案。无过错责任通常以行为的高度危险性作为归责事由，应当谨慎适用，不应将其视为纯粹的风险控制工具。适当严格的归责原则和注意义务设置可以促使生成式人工智能服务提供者研究并主动采取有效的措施来避免侵权内容的生成，不仅可以在较高程度上提高技术的安全性，而且可以避免对服务提供者“活动程度”的不当限制。过错推定责任的适用以解决受害人的举证困境为主要目标，同时也适当加强了服务提供者的责任。注意义务内容和标准的确定可以为服务提供者保障公众合法权益提供行为指引，同时为其反证无过错提供明确依据。总之，“过错推定责任+较高标准注意义务”的制度组合是应对生成式人工智能侵权风险的理想选择。

（技术编辑：邓语鑫）