

中国人民大学法学院 数字法学教研月报

2026年第6期（总第30期）

2026年8月28日



本期看点

【数字法治大事件】国家层面多领域协同推进数字法治制度升级，道路交通安全法修订草案提请审议，专章设立自动驾驶汽车道路交通安全制度；《促进网信企业高质量发展行动计划（2026—2030年）》印发实施；最高人民法院发布依法规范平台经营、保护消费者合法权益典型案例，为平台经济规范健康发展提供司法指引；《网络数据安全风险评估办法》落地施行，配套答记者问明确评估服务认证、报告报送流程等实操细则；《大型个人信息处理者个人信息保护规定（征求意见稿）》公开征求意见，同步发布政策法规问答与专家解读。

【研究动态】本期基础理论聚焦数字人权理论体系建构、数字时代权利保护范式更新等核心命题；数字时代部门法研究涵盖数字经济竞争损害标准转型、数据窝赃刑法规制等前沿议题；人工智能治理围绕人工智能代理刑事责任归属、算法可专利性判定等展开；网络平台治理聚焦平台数字权力规制、版权侵权权责匹配、平台权力行使正当程序等热点；智慧行政与司法探讨数字政府正当

程序重塑、科技创新中政府法治边界等实践难题；新技术法律规制涉及物联网产品责任等现实问题；数据法学围绕数据跨境治理充分性认定、个人信息单独同意法理基础等深入论证。

【教研活动】三位境外专家分别解读欧盟数据法、AI人格标识财产化、美欧网络安全治理；“AI善治·新智新声”人工智能法治在线课堂暨硕博研习举办两场专题活动，分别聚焦智能体订约法律规制、算法行政中实质性人类监督建构；“个人信息保护的新发展”研讨会围绕智能体与社交场景下的个人信息保护议题展开深度交流；“2026年人工智能法青年研习营”成功举办，助力人工智能法治领域青年人才培养。

【数字法评】

《数据不正当竞争行为认定逻辑的重塑与承继》，《法律适用》2026年第6期，作者：孟雁北。

《论数字司法价值对齐的实现路径》，《中国法学》2026年第3期，作者：彭中礼。

本期目录

数字法治大事件	3	人工智能治理.....	31
道路交通安全法修订草案提请审议 建立自动驾驶汽车道路交通安全制度.....	3	网络平台治理.....	34
促进网信企业高质量发展行动计划（2026-2030年）.....	4	智慧行政与智慧司法.....	35
最高人民法院发布依法规范平台经营、保护消费者合法权益典型案例.....	8	新技术的法律规制.....	36
《网络数据安全风险评估办法》实施有关事项答记者问.....	14	数据法学.....	37
专家解读 新形势下完善大型网络平台个人信息保护的重要举措.....	15	教研活动	39
专家解读 夯实能力、强化责任、构建托底机制——《大型网络平台个人信息保护规定》的监管逻辑与国际比较.....	17	Andreas Sattler 教授：欧盟《数据法》及其对商业秘密保护与竞争法的影响.....	39
个人信息保护政策法规问答（2026年8月）.....	19	John F. Duffy 教授：人工智能时代姓名与肖像的财产化.....	40
2026年个人信息保护系列专项行动取得阶段性成效.....	20	“AI 善治·新智新声”人工智能法治在线课堂暨硕博研习（春夏季）第七场.....	42
国家互联网信息办公室关于《大型个人信息处理者个人信息保护规定（征求意见稿）》公开征求意见.....	20	“个人信息保护的新发展”研讨会.....	43
研究动态	28	Anupam Chander 教授：TikTok、Anthropic 案与美欧国家安全互联网的兴起.....	46
数字法学基础理论研究.....	28	“AI 善治·新智新声”人工智能法治在线课堂 暨硕博研习（春夏季）第八场.....	48
数字时代的部门法研究.....	29	“2026年人工智能法青年研习营”成功举办.....	50
		数字法评	52
		数据不正当竞争行为认定逻辑的重塑与承继.....	52
		论数字司法价值对齐的实现路径.....	61

学术顾问：王利明

编委会：张新宝 丁晓东 王莹 张吉豫

编辑部：阮神裕 毕坤阳 来唯希 吕昊然 邓语鑫 梁因格 王昊

联系方式：RUCdigitallaw@163.com

本期编辑：梁因格

数字法治大事件

导言：

在数字经济持续发展、网络平台深度融入社会生产生活以及智能技术加快进入现实应用场景的背景下，我国数字法治建设正围绕平台治理、个人信息保护、网络数据安全、新技术应用和网信产业发展等重点领域持续完善制度体系，推动数字技术创新与安全规范治理协同推进。随着网络平台在数据利用、信息服务和社会治理中的作用不断增强，其数据处理规模、技术能力和生态影响力也使其承担更加重要的个人信息保护和数据安全治理责任。近期围绕大型网络平台个人信息保护、网络数据安全风险评估、平台经营规范、自动驾驶治理以及网信企业高质量发展的一系列立法进展、政策文件、司法案例和专家解读，体现出我国数字法治建设正向更加精准化、体系化方向发展。

在平台经营治理和消费者权益保护领域，最高人民法院发布依法规范平台经营、保护消费者合法权益典型案例，回应平台经济发展中的消费者权益保护问题，通过司法实践进一步明确平台经营者责任边界，为平台经济规范健康发展提供司法保障。

在个人信息保护领域，围绕大型网络平台和大型个人信息处理者的制度建设进一步深化。国家互联网信息办公室发布《大型个人信息处理者个人信息保护规定（征求意见稿）》公开征求意见，并发布《个人信息保护政策法规问答（2026年8月）》等内容，进一步回应个人信息处理规模扩大、场景复杂化背景下的监管需求。相关专家解读进一步强调夯实平台治理能力、强化主体责任和构建托底机制，体现出个人信息保护治理正在更加重视不同主体的规模、能力和风险特征。

与此同时，《网络数据安全风险评估办法》实施有关事项答记者问进一步明确网络数据安全风险评估的制度要求和实践路径，推动数据处理器主动识别和防范安全风险，促进数据安全与数据利用协调发展。

在新技术应用治理领域，道路交通安全法修订草案提请全国人大常委会审议，并专章规定自动驾驶汽车道路交通安全制度，围绕自动驾驶汽车上道路行驶条件、交通违法处理、保险制度以及相关企业责任等作出制度安排。这一立法进展将自动驾驶技术发展进一步纳入道路交通法治框架，体现出在

鼓励技术创新和产业发展的同时，通过明确安全要求 and 责任边界回应新技术应用带来的治理风险。

《促进网信企业高质量发展行动计划（2026—2030年）》则进一步从企业培育、技术创新、产业赋能、安全发展和营商环境等方面作出系统部署，体现出鼓励支持与规范发展并行的发展思路，为网信产业持续健康发展提供政策支撑。

总体来看，本期数字法治大事件既体现出对大型平台个人信息保护、数据安全和经营责任的进一步强化，也体现出对自动驾驶等新技术应用场景加快建立规则体系，以及以制度保障促进网信企业创新发展的政策导向。从平台规范经营、个人信息保护、风险治理，到新技术应用和产业发展，我国数字法治建设正更加注重统筹高质量发展与高水平安全，在规范秩序、保障权益与促进创新之间形成更加协调的治理格局。

道路交通安全法修订草案提请审议 建立自动驾驶汽车道路交通安全制度

原载：“法治日报”微信公众号

道路交通安全法修订草案8月25日提请十四届全国人大常委会第二十四次会议审议。修订草案遵循以下总体思路：一是统筹发展和安全，妥善处理道路交通安全与自动驾驶汽车和电动自行车产业发展、通行效率提高等关系。二是坚持问题导向，聚焦“醉驾”“僵尸车”“超标车”治理和电动自行车、“暴走团”管理等突出问题，有针对性完善制度措施。三是注重便民利民，在维护道路交通安全的同时，推行便民举措，便利群众出行。四是强化制度衔接，处理好本法与公路法、网络安全法、个人信息保护法等相关法律法规的关系。

修订草案共9章170条，主要作了以下修改：

强化道路交通安全保障。一是完善总体要求。明确道路交通安全工作坚持总体国家安全观，坚持人民至上、生命至上。二是压实各方安全责任。规定政府及其有关部门管理职责和机关、企业事业单位、社会组织等道路交通安全责任；互联网平台企业不得利用算法等强迫、纵容、默许从业人员违法

通行。三是强化车辆管理。禁止生产、进口、销售不符合强制性国家标准的车辆，禁止在道路上停放废弃机动车。四是改善道路通行条件。要求城市建设项目进行交通影响评价或者推行区域评估，有关单位及时排查、治理道路交通安全隐患。

加强道路交通安全行为规范。一是规范机动车驾驶行为。禁止“酒驾”“毒驾”“飙车”“盲驾”（驾驶时拨打或者接听手持电话、观看视频等）等。二是规范非机动车驾驶行为。禁止驾驶依法应当登记但未登记的非机动车上道路行驶；电动自行车与自行车、残疾人机动轮椅车共同在非机动车道通行，自行车、残疾人机动轮椅车平均行驶时速约为15公里，考虑到电动自行车行驶速度过快，会挤压自行车、残疾人机动轮椅车通行空间、增加事故风险，因此要求电动自行车最高时速不得超过20公里，不得超速、逆行、闯红灯等。与机动车类似，电动自行车25公里的最高设计时速，是对车辆产品性能上限的要求，与此不同的是道路行驶限速根据道路运行条件确定，两者分别从产品和道路通行两个环节保障安全。三是规范乘车人、行人行为。预防“开门杀”，要求开关车门时，乘车人注意观察、驾驶人提醒注意安全；规范“暴走团”，要求未经许可不得占用道路从事体育健身等非交通活动，有关单位加强日常巡查和劝阻制止。

建立自动驾驶汽车道路交通安全制度。一是明确上道路行驶条件。自动驾驶汽车通过道路通行规则符合性测试并依法登记后，方可上道路行驶。二是明确违章处理原则。相关交通违法行为由生产企业、进口企业接受处理，具体办法由国务院公安部门牵头制定。三是明确保险制度。对自动驾驶汽车实行机动车道路交通事故责任强制保险制度，具体办法由国务院制定。四是强化企业责任。要求生产企业、进口企业确保自动驾驶汽车道路行驶安全、网络安全、数据安全，不得虚假、夸大宣传自动驾驶功能。

提升便民利民服务水平。一是推行便民举措。规定机动车登记能够通过电子数据核验的免于提交证明、凭证，已申领电子行驶证的无需随车携带

实体证件，安全技术检验机构应当向社会公示检验项目和收费标准。二是满足特殊群体出行需求。规定未成年人、老年人、残疾人聚集性场所门前的道路，应当设置提示标志、行人过街设施等。三是保障受害人获得及时救助。适当扩大道路交通事故救助基金适用情形和先行垫付费用范围。

规范道路交通安全执法。一是规范电子执法。规定电子执法应当经过法制和技术审核，固定设备设置地点要向社会公布，当事人享有陈述、申辩等权利。二是严格规制传唤权。明确交警传唤情形、程序、时限，要求及时通知家属，并保证被传唤人正当需求。三是完善执法程序。规定对行政处罚进行全过程记录，当事人有权要求听证，当场处罚要符合法定条件并录音录像、及时备案。

完善法律责任。强化对道路交通安全违法行为的处罚，增强制度刚性和约束力。

现行道路交通安全法于2004年施行，2007年、2011年、2021年修正了个别条款，对维护道路交通秩序、预防和减少交通事故、提高道路通行效率、守护人民群众人身财产安全发挥了重要作用。

促进网信企业高质量发展行动计划（2026-2030年）

原载：“网信中国”微信公众号

以网络信息技术为核心驱动力、以网络安全和信息化为主要业务的网信企业是网络强国建设的重要力量，对培育发展新质生产力、巩固提升国际竞争力具有关键作用。为深入贯彻党中央关于网络强国建设和“十五五”时期网信工作有关部署，促进网信企业高质量发展，制定本行动计划。

一、总体要求

坚持以习近平新时代中国特色社会主义思想为指导，深入贯彻党的二十大和二十届历次全会精神，认真落实四中全会部署，深入学习贯彻习近平总书记关于网络强国的重要思想，完整准确全面贯彻新发展理念，加快构建新发展格局，坚持鼓励支

持和规范发展并行、政策引导和依法管理并举、经济效益和社会效益并重，以优质网信企业培育服务为主线，加快提升网信企业的技术创新、赋能产业、国际化经营和安全发展能力，持续优化营商环境与要素保障，统筹推动高质量发展、高水平安全和高效能治理，做强做优做大网信企业，为网络强国建设提供有力支撑。

到2030年，我国网信企业综合实力显著增强，科技创新力、产品硬实力、服务竞争力明显提升，网信产业生态和发展环境全面优化，安全规范、健康有序发展的制度体系更加健全，网信企业赋能经济社会高质量发展的作用更加凸显。

二、企业培育服务行动

1. 建立完善优质网信企业培育服务机制。

建立并持续更新优质网信企业数据库，建立分类分级培育标准和工作机制，针对生态主导型、产业引领型、高成长创新型三类企业分类施策开展培育服务工作。整合投融资机构、会计师事务所、律师事务所、知识产权服务机构、网信领域社会组织等资源，构建优质网信企业孵化培育服务机制。鼓励各地区因地制宜开展优质网信企业培育服务工作。

2. 培育具有世界影响力的生态主导型企业。

培育形成一批具有技术和标准主导能力、要素资源和市场整合能力、产业和生态构筑能力的生态主导型企业。引导生态主导型企业发挥技术、人才、资金、渠道、数据等优势，赋能中小企业发展壮大，积极参与全球网信技术合作，共同应对国际市场风险，构建具有国际竞争力的网络信息技术产业生态。

3. 培育细分领域产业引领型企业。

支持细分领域领军企业优化整合产业链创新链价值链，培育形成更多具有核心竞争力、行业影响力的产业引领型企业。支持产业引领型企业积极牵头技术标准制定，加快技术攻关和产业化应用，加强与传统企业、中小企业合作，打造网信产业集群。

4. 孵化高成长创新型企業。

支持网信科技属性强的中小企业加速技术迭

代、产品创新、市场开拓，培育形成众多创新能力强、成长性好、发展速度快的高成长创新型企業。支持高成长创新型企業聚焦细分领域差异化创新，在特定技术领域深耕细作，形成独特的技术和市场优势，加快培育更多瞪羚企业、独角兽企业。

三、创新能力提升行动

5. 加强关键核心技术攻关。

引导网信企业强化基础研究，加强高端芯片、基础软件和工业软件、网络通信、网络安全和数据安全等关键核心技术攻关，着力突破量子科技、区块链、脑机接口、数字孪生、新型显示等前沿技术，深化新一代网络信息技术集成创新和市场化应用。支持企业加强人工智能关键技术研究，研发高端人工智能芯片，突破高性能训练集群关键技术，提升大语言模型、多模态模型、世界模型等基础模型性能，布局智能体、具身智能等前沿技术。鼓励企业积极参与推动开源项目和开源社区建设。综合运用知识产权优先审查、快速审查等方式，强化知识产权服务支撑。

6. 强化企业创新主体地位。

支持有能力的网信企业牵头承担国家科技攻关任务。建立企业常态化参与科技创新决策机制，引导高校、科研机构、科研人员从企业需求中凝练任务。鼓励企业为高校、科研机构提供算力资源支持，加速人工智能在科学研究中的应用。鼓励生态主导型企业等通过内部创业、投资孵化等方式，培育细分领域具有竞争优势的创新主体。

7. 推动科技成果转化应用。

鼓励网信企业与高校、科研机构开展联合攻关，促进科技成果快速转化和产业化。强化科技成果转化绩效考核，建立与网信企业特点相适应的科技成果转化奖励机制。加强对网信企业的知识产权公共服务供给，加强网信领域产业知识产权运营中心建设，推动科技成果专利转化运用和产业化。优化网信领域知识产权许可、转让机制，鼓励科研人员持续参与技术改进和完善。支持和鼓励高校、科研院所科研人员按规定通过选派挂职、参与项目合作、兼职创新等方式到企业开展科技创新和成果转化。

四、赋能产业升级行动

8. 赋能制造业数字化转型。

支持网信企业聚焦研发设计、生产制造、经营管理、运维服务、供应链管理等全链条典型场景，提升数字化产品和服务供给能力。鼓励企业开发推广符合中小企业需求、高性价比的数字化转型通用工具产品、服务和解决方案。引导支持企业牵头或参与工业互联网建设应用，打造一批具有全球竞争力的工业互联网平台。鼓励企业布局制造业行业大模型、智能体，建设高质量工业数据集，加强人形机器人等研发应用，加快智能工厂建设，推进人工智能赋能新型工业化。

9. 赋能数字乡村建设。

鼓励网信企业积极参与智慧农业技术研发应用，推动“人工智能+”农业发展。加快农村数字基础设施建设，加强涉农数据开发利用。深入实施农村电商发展工程和“数商兴农”，培育壮大“土特产”网络品牌。鼓励企业积极参与乡村数字治理和信息服务体系建设，提升教育、医疗、广播电视等领域优质数字资源供给能力，推进乡村旅游数字化转型升级。鼓励企业参与和支持脱贫地区数字乡村建设，助力构建消费帮扶平台矩阵，持续扩大农产品销售规模。

10. 赋能数字消费提质升级。

鼓励网信企业加速研发创新，增加人工智能终端、可穿戴设备等数字产品供给。支持企业加快生活服务数字化赋能，发展数字教育、“人工智能+”医疗服务、广播电视等新模式新业态。鼓励企业运用人工智能等技术赋能文博场馆、旅游景区、休闲街区等相关场所，打造沉浸式、体验式、互动式数字消费场景。支持企业开展动漫、游戏、影视、音乐、网络文学等领域精品创作，加强数字内容消费供给。鼓励企业充分考虑老年人、残障人士等群体需求，提升数字化服务的便利性和友好度。

11. 推动企业绿色低碳发展。

引导支持网信企业绿色低碳发展，实现办公、生产、运输、服务等全流程绿色化设计、包装、交付和运营，定期披露减碳进展。支持企业提升可再

生能源利用水平，引导新建算力设施与可再生能源发电等协同布局，持续开展国家绿色算力设施建设。及时更新节能降碳技术装备推荐目录，推广液冷技术、废热回收等先进适用节能降碳技术。鼓励生态主导型、产业引领型企业助力上下游企业提高减碳能力，加快数字化能碳管理中心建设应用，构建绿色价值链和供应链。鼓励各地建设绿色转型服务平台，为企业提供低成本、标准化的碳排放核算工具、能效诊断服务等，降低企业绿色化转型门槛。

五、海外市场拓展行动

12. 支持企业有序“走出去”。

持续利用世贸组织、“一带一路”、金砖国家、上海合作组织、亚太经合组织等多边合作机制，深化数字基础设施、人工智能、电子政务、电子商务、移动支付、数字化转型等领域合作，支持算力、云服务、人工智能等优势企业在防范风险的前提下有序“走出去”。鼓励生态主导型、产业引领型企业凭借资金、技术和经验优势，为中小企业有序出海提供支持。支持网信企业积极参加国际知名行业展会，为企业提供参展指导。支持网信企业参与国际标准组织活动和国际标准制定。规范网信企业海外竞争行为。

13. 构建企业出海服务体系。

加强网信企业海外经营合规指引，探索设立面向重点市场的海外业务合规指导中心。建立完善风险监测预警机制，指导企业有效应对不合理的贸易限制措施。建立网信企业出海法律纠纷案例库，鼓励贸易投资促进机构、行业协会、商会等向企业提供法律服务和培训。鼓励各地区有关机构为企业出海提供合规指引。

六、安全有序发展行动

14. 守牢安全底线。

支持网信企业加强网络安全、数据安全防护体系建设，完善技术防护措施，提升风险识别、监测预警、应急处置等保障能力。持续开展移动互联网应用程序违法违规收集使用个人信息专项治理，指导企业建立健全个人信息保护机制，提高个人信息保护水平。持续开展互联网信息服务算法综合治理，

督促指导网信企业持续优化算法运行机制和管理规则,完善算法推荐内容审核,强化人工智能技术滥用治理,维护网民和劳动者合法权益。引导鼓励网信企业积极担负社会责任,增加网络优质内容供给,自觉成为正能量传播者。督促指导提供内容服务的网信企业进一步加强内容导向管理,确保正确政治方向、舆论导向、价值取向,主动防范化解风险。

15. 防范无序竞争。

加强网信领域反垄断监管执法,依法规制重点领域涉嫌垄断行为,严格禁止企业变相实施“二选一”等排除、限制竞争行为。建立健全平台企业与平台内经营者重大事项协商机制,规范平台收费行为,减轻平台内经营者负担。着力规范网信企业过度补贴、“内卷式”竞争等问题。发挥行业协会自律作用,引导企业提升产品品质,实行优质优价。

16. 加强网络法治建设。

积极开展网信领域立法前瞻性研究。加快推进人工智能、反网络暴力、数字经济、网络平台、区块链等新兴领域立法。推进修订《互联网信息服务管理办法》,完善互联网信息服务管理、“自媒体”管理、算法治理等法律制度。推进制定电信法、网络犯罪防治法、网络安全等级保护条例,完善《未成年人网络保护条例》《网络数据安全条例》配套规定。规范涉网信企业行政检查,最大限度减少对网信企业正常生产经营活动的干扰。健全适应互联网发展治理新特点的监督管理执法措施,严厉打击网络违法违规行为。

七、营商环境优化行动

17. 营造公平竞争市场环境。

推动网信企业积极参与纵深推进全国统一大市场建设,保障所服务的各类经营主体享受平等待遇,依法平等获取和使用各类生产要素。优化拓展“高效办成一件事”事项范围,推进“一网通办”,持续优化政务服务。规范网信领域政府采购和招标投标,重点整治异常低价竞争等突出问题。

18. 优化营商网络环境。

持续开展“清朗”“净网”系列专项行动,整

治涉企网络“黑嘴”,打击处置造谣抹黑企业和企业家、从事虚假不实测评、诋毁产品质量等问题。加强涉企网络辟谣工作,加大涉网信企业网络侵权举报受理处置力度,不断提升涉企网络侵权信息受理处置工作科学化、规范化水平。引导网信企业积极履行社会责任,参与公益慈善事业,大力弘扬企业家精神。

八、发展要素保障行动

19. 强化金融支持。

拓宽网信企业融资渠道,构建企业多元融资支持体系,有效发挥政府投资基金作用,支持投早、投小、投长期、投硬科技。鼓励金融机构探索开发网信领域金融产品,将专利、商标、数据等要素作为授信评估的重要参考因素。支持符合条件的网信企业上市融资。支持高成长创新型企业 in 境内外上市融资,加快境内上市审核流程,鼓励在科创板、创业板上市。拓宽 IPO 以外退出渠道,鼓励发展私募股权二级市场基金(S基金)、并购基金,进一步打通“投资-退出-再投资”的良性循环。

20. 强化数据保障。

鼓励引导网信企业建立健全数据安全合规体系,指导帮助企业高效合规开展数据处理活动。高效实施数据出境安全评估、个人信息出境标准合同、个人信息出境认证等制度。支持自由贸易试验区等在国家数据分类分级保护制度框架下,制定发布数据出境负面清单,建立符合“东数西算”工程布局和相关政策要求的云计算基础设施,面向外资企业、中小企业等提供数据处理服务。组织重点行业领域制定网络数据跨境流动合规指引,鼓励有条件的地区设立数据跨境服务中心,开展数据跨境咨询服务。鼓励生态主导型、产业引领型企业面向中小企业提供普惠性数据产品和技术工具。依法严厉打击涉数据违法犯罪活动。

21. 强化人才支撑。

深化全民数字素养与技能提升行动,实施数字技术工程师培育项目,支持网信企业深化产学研合作,支持高校、科研院所探索人工智能人才培养新模式,培育更多高水平、复合型数字人才。鼓励网

信企业与高校共建现代产业学院、行业特色学院、产教融合基地，支持学生实习实践，加大数字人才培养，开展对数字技能人才的供需分析研究，更好服务就业创业。完善企业网信人才激励机制，鼓励各地结合实际将企业急需紧缺网信人才纳入地方人才引进目录和城市直接落户范围。

九、组织实施

在中央网络安全和信息化委员会领导下，依托国家信息化发展工作统筹协调机制加强部门会商、协调配合，及时解决制约网信企业高质量发展的重大问题，形成发展合力。中央网信办建立健全网信企业监测和动态分析机制，做好预研预判和政策储备。定期听取企业意见建议，加强政策评估，及时总结推广做法经验。各地区网信部门要及时了解网信企业发展过程中遇到的难题，加大惠企政策宣贯力度，确保各项政策措施落地见效。

最高人民法院发布依法规范平台经营、保护消费者合法权益典型案例

原载：“网信中国”微信公众号

为全面贯彻落实习近平法治思想，深入贯彻落实“十五五”规划纲要“推动平台经济创新 and 健康发展”的部署要求，充分发挥人民法院典型案例的示范引领作用，最高人民法院发布5起依法规范平台经营、保护消费者合法权益典型案例。

平台经济是数字经济的重要组成部分，是发展新质生产力的重要载体。近年来，直播电商、短视频运营、平台代运营等新业态快速发展，在关键领域“大显身手”，但也出现了主体权责边界模糊、竞争规则适配不足、依法经营指引不够清晰、虚拟财产保护缺位等突出问题，既损害消费者合法权益，也影响市场经济秩序。本次发布的5起案例，覆盖直播电商、平台依法经营，市场竞争秩序维护，虚拟资产交易等多个场景，集中体现了人民法院依法规范平台经营、保护消费者合法权益的鲜明态度，

为各类市场主体明确行为规则、稳定经营预期提供清晰指引。

一、厘清多方主体责任边界，破解网络消费维权痛点，夯实平台信用基础

网络消费是平台经济的核心场景。实践中，部分电商平台保证金制度流于形式，入驻商户掏空账户后消费者退款求偿无门，是网络消费领域消费者维权面临的突出痛点，也透支平台企业的市场公信力；直播带货链条长、参与主体多，出现纠纷后销售方、直播推广方、平台常常相互推诿，消费者维权路径不清。人民法院通过界定各方主体法律地位与责任范围，压实平台实质监管责任，筑牢消费者权益保障防线，助力优化网络消费环境。在万某某、房某某诉北京某电子公司、某商贸公司信息网络买卖合同纠纷案中，法院明确电商平台对入驻商户保证金负有必要的监管义务。平台掌握入驻商户经营规模、资金流水、投诉记录等全部数据，知道或应当知道商户长期全额提现掏空账户、刻意逃避退赔责任，却未按规则动态调增保证金、未采取资金管控措施的，属于未采取《中华人民共和国电子商务法》规定的“必要措施”，应当与商户承担连带清偿责任。本案提供了与平台数据优势相匹配的注意义务认定标准，推动保证金制度从“准入门槛”回归“履约担保”本位，切实保障消费者求偿权益的实现。在周某诉某商贸公司、某购物公司、某网络科技有限公司信息网络买卖合同纠纷案中，人民法院对直播带货方明确责任：销售方是商品质量与违约赔偿的第一责任人，入驻平台的直播带货方作出的售后兜底、假一罚四承诺有效，应当依照承担连带责任。

二、划定平台经营合规红线，规范商业营销行为，引导企业诚信依法经营

直播带货、平台代运营是中小市场主体切入数字经济的重要业态，营销与运营行为依法合规是企业可持续发展的必要前提。实践中，部分直播经营者对商品作出片面化、误导性评价，引发商业诋毁纠纷；部分代运营服务商通过虚假交易、刷单炒信为商户“数据注水”，破坏平台信用评价体系，既

扰乱公平竞争的市场秩序，也让各经营主体面临较高的合规风险。人民法院通过明确商业言论边界、判令承担违约责任，为各类经营主体划定清晰的合规经营底线，引导行业诚信规范发展。在重庆某酒业公司诉某优选（北京）公司商业诋毁纠纷案中，人民法院明确直播带货属于经营行为，入驻平台的直播带货方的商业评论可以对同类商品进行评价，但相较于普通公众其负有更高标准的审慎注意义务，即时互动场景下主播的“临场发挥”不构成免责事由；即便主播言论含有部分真实因素，但通过片面陈述、不当关联等误导公众对同类商品产生错误认识的，仍构成商业诋毁。本案厘清了直播营销中正常商业评论与商业诋毁的边界，为直播类企业营销行为提供了明确的行为规范。在某代运营商诉某平台服务合同纠纷案中，人民法院认定平台禁止刷单炒信、扣除违规服务商保证金的格式条款，已通过加粗方式尽到合理提示义务，且内容符合法律规定与公平原则，合法有效。代运营商组织虚假团购、帮助商户虚构交易，属于严重违约行为，平台依约扣除全部保证金并无不当。本案明确了平台内代运营活动的依法合规底线，确认了平台自治规则的法律效力，实现行政监管与司法裁判对平台自治的有效衔接，引导代运营类企业诚实守信经营。

三、规范虚拟财产交易秩序，破解交易信息不对称难题，保障市场主体财产权益

随着流量经济的蓬勃发展，平台账号等网络虚拟财产的商业价值日益凸显。但虚拟财产交易中，出卖人掌握账号全部运营数据与瑕疵信息，买受人往往处于信息弱势地位，出卖人隐瞒账号处罚、功能受限等问题引发的纠纷频发，买受人难以追究出卖人违约责任成为常见问题。人民法院通过明确出卖人的瑕疵担保义务和如实告知义务，规范虚拟财产交易秩序，保障市场主体合法财产权益。在汪某诉武汉某公司买卖合同纠纷案中，法院明确平台账号转让交易中，出卖人负有如实告知影响账号使用效能与商业价值的重要信息的法定义务；出卖人隐瞒账号无法搜索、无法使用推广功能等重大瑕疵，导致买受人商业运营的合同目的落空的，构成根本

违约，买受人有权解除合同并要求返还全部价款。本案有效破解了线上虚拟财产交易中买受人维权难的困境，实现交易双方利益平衡，助力形成与数字经济相适应的法治化交易秩序。

习近平总书记深刻指出，“一个案例胜过一打文件”。本次发布的5起典型案例，贯穿平台经济交易、运营、竞争、资产处置全链条，既依法保护消费者合法权益，也平等保护平台企业、直播经营者、代运营商等各类市场主体的合法权益，通过明晰规则、划清边界、压实责任，向全社会释放规范平台经营、助力数字经济健康发展的明确信号。下一步，人民法院将继续发挥审判职能作用，持续完善平台经济裁判规则，优化数字领域稳定、公平、透明、可预期的法治化营商环境，助力平台经济创新 and 健康发展。

依法规范平台经营 保护消费者合法权益

典型案例

目 录

案例一：正确界定主播的正当商业评论与商业诋毁边界，提升直播带货企业依法经营意识——重庆某酒业公司诉某优选（北京）公司商业诋毁纠纷案

案例二：明确电商平台对入驻商户的保证金充实监管义务，优化网络消费环境——王某某、房某某诉北京某电子公司、某商贸公司信息网络买卖合同纠纷案

案例三：平台代运营商组织虚假交易构成严重违约，保证金可依约扣除——某代运营商诉某平台服务合同纠纷案

案例四：依法认定平台账号转让合同的违约责任，维护虚拟财产交易秩序——汪某诉武汉某公司买卖合同纠纷案

案例五：判定主播承诺的赔偿责任，促进直播带货行业健康发展——周某诉某商贸公司、某购物公司、某网络科技有限公司信息网络买卖合同纠纷案

案例一

正确界定主播的正当商业评论与商业诋毁边界，提升直播带货企业依法经营意识——重庆某酒业公司诉某优选（北京）公司商业诋毁纠纷案

【案例摘要】

某优选（北京）公司在直播带货过程中，其主播对重庆某酒业公司旗下某白酒产品发表片面对比、不当关联的评论。重庆某酒业公司认为上述言论误导消费者，损害其商业信誉，遂提起诉讼。人民法院认定直播带货行为属经营行为，主播虽然可以进行正当的商业评论，但应对同类产品的评论负有审慎注意义务，损害竞争对手的商业信誉和商品声誉的言论构成商业诋毁。本案厘清了直播带货中正当商业评价与商业诋毁的边界，明确了误导性信息的认定标准，有助于规范直播带货行为。

【具体内容】

重庆某酒业公司系某白酒注册商标专用权人。某优选（北京）公司运营的“某选”直播间有近3000万粉丝，是知名直播带货品牌。

2024年7月，“某选”直播推销其他品牌白酒时，其主播发表了涉及某白酒产品的言论，包括“现在国家的白酒标准要求必须是酿造的……加入食用酒精的酒在咱们国家已经不能被叫做白酒了，他们被称为调味酒，你现在去看某白酒的包装，上面没有‘白酒’这两个字，因为不允许……配料表里只要出现食用酒精，是不允许叫白酒的……小金标代表的是纯粮固态，买某小曲就没有这个标（小金标），因为它不是固态蒸馏的，所以不能算固态酒……”等内容。重庆某酒业公司认为，上述言论误导消费者认为某白酒产品非纯粮酿造，损害其商业信誉和商品声誉，构成商业诋毁，遂提起诉讼，请求判令赔偿损失。某优选（北京）公司辩称，某白酒品牌主营产品不是白酒而是果味酒，相关言论系基于果味酒不是国家标准确定的白酒这一客观事实作出，且属于主播临场发挥，不构成侵权。

重庆市第一中级人民法院经审理认为，首先，直播带货属于经营行为，平台内经营者及其主播在直播推销中对同类竞品作出的评价虽然属于商业评论范畴，可以进行一定的主观评价，但此种评价

并非毫无边界，应以不损害他人合法权益和公平竞争为前提。相较于普通消费者的日常交流，经营者及其主播应对评论内容负有更高标准的审慎注意义务，确保评论真实、客观、全面，即时互动场景下的“临场发挥”不构成免责事由。商业诋毁不仅包括虚构事实，也包括传播误导性信息。误导性信息即使含有部分真实因素，但通过片面陈述、不当关联、模糊指向等方式呈现，整体上足以使相关公众对竞争对手商品质量产生错误认识，仍应受到法律规制。本案主播将“白酒标准要求酿造”和“某白酒包装上无‘白酒’字样”不当关联，未区分某白酒旗下白酒与果味酒，也未呈现该白酒品牌多款白酒已获纯粮固态发酵认证的事实，经选择性呈现和不当关联后，整体上足以引导消费者得出该白酒品牌的白酒不符合白酒标准、非纯粮酿造的误解，超越了正当商业言论的边界，构成法律规制的误导性信息。最终法院认定某优选（北京）公司构成商业诋毁，并判令其赔偿重庆某酒业公司经济损失及合理开支共计30万元。一审宣判后，双方当事人均未上诉。

【典型意义】

本案是人民法院依法规制直播带货中商业诋毁行为的典型案例。首先，明确了直播带货主播在商业评论中的审慎注意义务的边界，强调网络主播在对比评论中应确保信息真实、全面，防止误导公众，为平台内的直播带货方营销行为提供了明确的行为规范。其次，厘清了误导性信息的认定标准，即评论内容即使部分真实也存在违法可能，若表达方式整体上导致公众误解，仍可构成不正当竞争，为类案纠纷的处理提供了裁判规则参考。最后，本案裁判有助于引导平台内经营者及平台企业提升依法经营意识，促进公平有序的市场竞争环境，推动数字经济时代直播营销行业在法治轨道上行稳致远，为平台经济健康发展提供有力司法保障。

一审案号：（2024）渝01民初606号

案例二

明确电商平台对入驻商户的保证金充实监管义务，优化网络消费环境——万某某、房某某诉北

京某电子公司、某商贸公司信息网络买卖合同纠纷案

【案例摘要】

万某某、房某某在电商平台入驻某商贸公司店铺购置洗衣柜，退货后商家签收退货却长期不予退款。经查入驻商户经营收入规模巨大，但平台仅设置最低基础保证金，未根据商户成交规模、投诉记录动态调增保证金，放任商户全额提现掏空店铺资金，保证金账户无资金可供赔付，导致消费者债权无法实现。一、二审法院均认定电商平台未履行必要的监管义务，判决商户退还货款并支付逾期利息，电商平台对全部债务承担连带清偿责任。

【具体内容】

万某某、房某某二人系夫妻关系。2025年1月12日，房某某在北京某电子公司运营的某商城平台，入驻的商户某商贸公司经营的店铺下单购买洗衣柜一件，商品价款1566元。2025年2月13日，房某某向商家提交退货申请，商家当日同意退货，商品退回，但商家始终拖延退款。二人多次催讨无果后，诉至法院，请求判令某商贸公司退还货款并支付逾期利息，北京某电子公司承担连带退款责任。

另查明，某商贸公司自2024年12月28日起，平台累计营业收入超34万元，但北京某电子公司仅为其设置1000元基础保证金，未按照平台阶梯保证金规则根据成交规模相应调增保证金；该商户已多次产生消费者投诉、赔付记录，平台亦未向其收取风险保证金、临时保证金。商户资金流水显示，每次经平台扣划赔付消费者后，商户均将店铺钱包余额全额提现转出，店铺长期无可用资金；平台后续核查确认该商贸公司存在售假行为。因商户保证金不足、店铺账户无余额，两名消费者的退款诉求无法通过平台保证金渠道实现。

人民法院审理认为，网络交易平台保证金是平台内经营者未履行消费者权益保障义务时用于向消费者赔付的资金，保证金账户是否充足对消费者权益保障尤为重要。《中华人民共和国电子商务法》第三十八条第一款规定：“电子商务平台经营者知道或者应当知道平台内经营者销售的商品或者提

供的服务不符合保障人身、财产安全的要求，或者有其他侵害消费者合法权益行为，未采取必要措施的，依法与该平台内经营者承担连带责任。”本案中北京某电子公司掌握商户经营规模、资金流水、投诉记录全部数据，具备远超普通消费者的管控能力；平台知道或应当知道商户长期提现掏空账户、刻意逃避退赔责任，却未动态调整保证金、未收取风险保证金，亦未对商户异常资金流动采取管控措施，直接造成消费者求偿无门，应当与商户承担连带责任。

浙江省德清县人民法院一审判决：某商贸公司向万某某、房某某退还货款1566元及利息；北京某电子公司对前述全部债务承担连带清偿责任，平台承担连带责任后有权向商贸公司追偿。北京某电子公司不服一审判决提起上诉。浙江省湖州市中级人民法院二审判决驳回上诉，维持原判。

【典型意义】

一、丰富了《中华人民共和国电子商务法》第三十八条第一款“必要措施”的内涵，明确平台管理义务的必要性持续性。平台保证金是平台内经营者不履行赔付义务时保障消费者求偿的兜底资金，是否充实、有效直接关系求偿权能否实现。本案认定厘清了平台管理义务的内容边界，为同类案件提供了可操作的裁判指引。

二、确立了与平台数据优势相匹配的“应当知道”认定标准。同类纠纷中，平台多以“不知情”“保证金不足非平台行为”“平台已尽到信息披露义务”等为由抗辩。本案明确，“应当知道”的认定应与这一优势地位相适应，平台不得以系经营者单方行为、客观状态为由免责。据此，本案将归责的知道要件从平台的被动知情提升为基于数据优势的主动注意，为破解此类案件中平台抗辩的认定难题确立了可循的规则尺度。

三、服务平台经济规范健康发展，助力优化消费环境。网络交易平台是数字经济的信用枢纽，保证金制度是平台履行“守门人”职责、保障交易安全的重要担保措施。本案通过司法裁判压实平台对资金担保的实质监管责任，推动保证金由“准入门

槛”回归“履约担保”的本位，对优化网络消费环境、提振消费信心、引导平台企业从源头规范平台内经营者经营行为，具有积极的规则示范和价值引领意义。

一审案号：（2025）浙 0521 民初 4818 号

二审案号：（2025）浙 05 民终 2945 号

案例三

平台代运营商组织虚假交易构成严重违约，保证金可依约扣除——某代运营商诉某平台服务合同纠纷案

【案例摘要】

某代运营商与某平台签订合作协议，为入驻商户提供店铺托管、营销策划等服务，并缴纳保证金 5 万元。合作期间，某代运营商通过组织虚假团购等方式帮助商户虚构交易、提升排名，被市场监管部门认定虚假商业宣传，责令其停止并改正违法行为，并处罚款 10 万元。某平台依据协议及服务商行为规范扣除全部保证金。现某代运营商提起诉讼要求某平台返还保证金及支付利息、律师费。上海市杨浦区人民法院经审理认定，相关诚信规则和保证金扣除条款虽属格式条款，但某平台已作显著提示，且条款内容公平合理；某代运营商实施刷单炒信构成违约，扣除保证金符合约定，且金额并未明显高于平台实际损失，遂驳回其全部诉讼请求。

【具体内容】

2021 年 2 月 9 日，某代运营商与某平台签订《服务商合作协议》，约定由某代运营商在指定区域为入驻商户提供门店托管运营、营销策划、数据分析等服务，并遵守协议附件及平台规则。同月 16 日，某代运营商缴纳保证金 5 万元。某平台《服务商行为规范》明确禁止协助商户炒作评价、炒作流量、刷单等违规提升星级排名的行为，并约定平台可视违规情形扣除保证金、收回后台权限及清退服务商；有关诚信经营和违约责任条款均以加粗方式列示。

合作期间，某代运营商为帮助商户提升榜单排名，安排账号购买并核销并无真实销售内容的低价团购项目。市场监管部门认定其通过组织虚假交易帮助其他经营者进行虚假商业宣传，责令停止违法

行为并处罚款 10 万元。某平台据此扣除诚信分、取消相关权益、扣除保证金并收回后台权限。某代运营商认为有关条款未经充分提示说明，遂诉请某平台返还保证金 5 万元并支付利息、律师费。

上海市杨浦区人民法院经审理认为，涉案协议及行为规范系某平台预先拟定并重复使用，其中关于诚信规则及保证金扣除的内容属于格式条款。但某平台已以加粗方式作出合理提示，且虚假交易、刷单炒信本为法律明令禁止的行为，某代运营商作为专业商事主体对此应有充分认知，相关条款未不合理免除平台责任、加重服务商责任或者排除服务商主要权利，应认定合法有效。某代运营商的行为直接落入协议约定的严重违规情形，损害平台信用评价体系、消费者知情权和诚信商户的公平竞争机会。结合违约性质、过错程度及平台商誉受损程度，扣除 5 万元保证金并无明显过高或显失公平。人民法院于 2025 年 9 月 5 日判决驳回某代运营商的全部诉讼请求，判决已发生法律效力。

【典型意义】

本案明确了真实交易、真实评价和真实流量是平台代运营活动的基本合规边界。一是划定代运营活动的合规底线。平台交易量、用户评价和榜单排名，是消费者决策、商户揽客及平台配置流量的重要依据。代运营商通过虚假团购、刷单炒信制造虚假数据，会误导消费者、损害平台信用体系并挤压诚信商户的竞争空间。本案明确将此类“数据注水”行为认定为违约，不受法律保护。二是厘清平台格式条款的效力标准。平台规则具有格式条款属性，并不当然无效。平台已对重大责任条款履行合理提示义务，且不存在不合理免除或者加重责任情形的，人民法院可以依法确认其效力，也支持平台依约清退违规服务商、扣除履约保证金，为平台建立透明、合理、可预期的治理规则提供了指引。三是实现行政监管与司法裁判对平台自治的有效衔接。数字经济越是依赖算法、流量和评价体系，越是需要坚守诚实信用这一民商事活动的根本原则，本案裁判为新业态的健康发展提供了规则支撑和价值引领。

一审案号：（2025）沪 0110 民初 8092 号

案例四

依法认定平台账号转让合同的违约责任，维护虚拟财产交易秩序——汪某诉武汉某公司买卖合同纠纷案

【案例摘要】

汪某与武汉某公司签订合同，以11万元受让某视频账号使用权。账号交付后，汪某通过咨询平台客服得知该账号因被平台处罚而存在不能被搜索、不能使用DOU+推广功能（某视频平台的视频推广工具，用于提升曝光率和互动量）等限制，武汉某公司并未提前告知，汪某据此诉请解除合同。人民法院认定出卖人负有告知买受人标的物状况的义务，其未披露某视频账号核心功能受限，构成根本违约，判令解除合同并由武汉某公司返还全部转让款。

【具体内容】

2023年9月，汪某与武汉某公司通过某电子合同平台，以电子签名方式签订《新媒体合作运营协议》，约定：武汉某公司将某视频账号使用权以11万元转让给汪某；账号已关注用户数284万，总获赞数4100万，有无违规情况为“评级恢复”；武汉某公司保证已完全披露账号的全部实际情况。合同签订后，双方按照某视频平台规则，在微信群内完成账号换绑交接，汪某向武汉某公司支付转让款11万元。后汪某咨询平台客服得知该账号曾因发布内容违规被平台处罚，导致无法被搜索及无法使用DOU+功能。汪某遂诉至法院请求判令解除合同并返还转让款。

湖北省武汉市洪山区人民法院经审理认为，出卖人依法应向买受人承担质量瑕疵担保责任，应当按照约定的质量要求交付标的物，如若标的物不符合质量要求，致使不能实现合同目的，买受人可以解除合同。汪某与武汉某公司系买卖合同关系，汪某已依约履行了支付转让款的义务，武汉某公司应按约定交付具备正常使用功能的某视频账号。武汉某公司未如实告知该账号不能被搜索且无法使用能提升曝光率、互动量及定向推广的DOU+功能。汪某花费11万元受让某视频账号使用权的目的系用

于商业运营，但账号受限直接弱化了账号的流量获取和商业变现能力，不具备完整的使用功能，不能实现汪某的合同目的，故汪某有权要求解除合同。因汪某于2023年11月6日送达解除通知，故法院判令案涉合同于当日解除，武汉某公司返还转让款11万元。武汉某公司提起上诉后自愿撤回上诉，湖北省武汉市中级人民法院裁定予以准许。

【典型意义】

随着流量经济和平台经济的蓬勃发展，网络平台账号的经济价值愈加凸显，属于法律保护的网络虚拟财产，但同时高收益低成本的运营模式也催生了以买卖平台账号营利的产业链，相关纠纷层出不穷。本案认定，出卖人对合同标的物负有质量瑕疵担保义务，应当主动告知买受人影响平台账号使用效能和商业价值的重要信息；若账号无法被搜索或无法使用推广功能，将直接削弱其流量获取与商业变现能力，致使买受人商业运营的合同目的落空，出卖人的隐瞒行为构成根本违约。本案为虚拟财产交易纠纷中根本违约的认定提供了可操作的分析框架，有助于形成同数字经济相适应的法治化交易秩序。

一审案号：（2024）鄂0111民初5421号

二审案号：（2024）鄂01民终16247号

案例五

判定主播承诺的赔偿责任，促进直播带货行业健康发展——周某诉某商贸公司、某购物公司、某网络科技公司信息网络买卖合同纠纷案

【案例摘要】

周某经某购物公司直播间推荐，在某商贸公司店铺购买面霜，某购物公司主播在直播间作出售后兜底、假一罚四承诺。周某收货后发现商品存在差异，委托机构鉴定为非正品。某商贸公司虽协商确认赔偿，但事后并未履行，周某据此提起诉讼。人民法院明确相关方责任：销售方是商品质量与违约赔偿的第一责任人，入驻平台的直播带货方作出的售后兜底、假一罚四承诺有效，应当依照承担连带责任，依法保障消费者合法权益。

【具体内容】

某商贸公司在某平台开设“某美妆专营店”，系案涉商品销售主体；某购物公司在某视频平台运营“某购物官方魅力号”，系直播推广方。2025年4月，周某经某购物公司直播间推荐，在某商贸公司店铺购买面霜一瓶，支付货款1859元。直播过程中，某购物公司主播公开承诺：“有任何问题我们赔付到底，假一罚四倍现金，给大家做售后的兜底”，并宣称商品为专柜正品、资质齐全、可溯源。

周某收货后经比对发现商品存在差异，委托专业机构鉴定为非正品，支出鉴定费500元。经市场监管部门协调未果，某商贸公司虽同意按四倍货款及鉴定费赔付周某，但未实际履行。周某遂诉至法院，要求某商贸公司、某购物公司承担赔偿责任，要求运营某平台的某网络科技有限公司对上述款项承担连带责任。

浙江省丽水市莲都区人民法院经审理认为，买卖合同出卖方为某商贸公司，其应承担出卖人法律责任。某购物公司系某视频平台直播推广方，但其主播在直播推广过程中，明确作出赔付到底、售后兜底等承诺，该承诺系其真实意思表示，且不违反法律、行政法规强制性规定，合法有效。周某基于对上述承诺的信赖，通过直播间链接购买案涉商品，双方就此形成合意，成立合法有效的合同关系，某购物公司应当依约履行售后兜底义务。平台方未参与交易、未作出承诺，且已经尽到了法律规定的网络交易平台提供者的资质审核、信息披露以及如实告知等义务，根据《中华人民共和国消费者权益保护法》第四十四条规定，只有网络交易平台提供者不能提供商家的相关信息，消费者才可以向平台提供者要求赔偿。最终判令某商贸公司赔付周某7936元，某购物公司对上述款项承担连带责任，并驳回周某的其他诉请。一审宣判后，双方当事人均未上诉。

【典型意义】

实践中，直播推广方带货时经常承诺对产品进行兜底赔偿，但消费者维权时却推诿扯皮，这一现象屡见不鲜。本案明确：销售方系商品质量和违约赔偿的第一责任人；直播推广方作出的售后兜底、

赔付承诺具有法律约束力，应当依法承担相应连带责任。案例引导直播带货行业诚信规范经营，促使直播推广方切实履行直播承诺，维护消费者合法权益，具有良好示范效应。

一审案号：（2025）浙1102民初5285号

来源：最高人民法院新闻局

《网络数据安全风险评估办法》 实施有关事项答记者问

原载：“网信中国”微信公众号

《网络数据安全风险评估办法》于2026年8月20日起施行，国家互联网信息办公室有关负责人就其实施有关事项回答了记者提问。

问1：如何申请网络数据安全风险评估服务认证？

答：《网络数据安全风险评估办法》第八条规定：“鼓励相关评估机构通过认证。评估机构的认证按照《中华人民共和国认证认可条例》的有关规定执行”。国家网信办数据与技术保障中心、公安部第三研究所、泰尔认证中心有限公司等认证机构，已向国家认证认可监督管理委员会备案《数据安全风险评估服务认证规则》，相关认证机构将依据认证规则和有关标准规范实施认证。评估机构可向上述认证机构申请服务认证。

问2：重要数据处理者如何报送网络数据安全风险评估报告？

答：《网络数据安全风险评估办法》第十六条规定：“重要数据处理者应当在年度风险评估完成后的20个工作日内按照有关主管部门要求向其报送风险评估报告。主管部门不明确的，向省级网信部门或者国家网信部门报送。”下表为国家和省级网信部门的联系电话，主管部门不明确的重要数据处理者可联系咨询报送风险评估报告事宜。

序号	单 位	联系电话
1	国家互联网信息办公室	(010) 55627565
2	北京市互联网信息办公室	(010) 55520121
3	天津市互联网信息办公室	(022) 88355280
4	河北省互联网信息办公室	(0311) 87808317
5	山西省互联网信息办公室	(0351) 3902026
6	内蒙古自治区互联网信息办公室	(0471) 4827210/18804712083
7	辽宁省互联网信息办公室	(024) 81680082
8	吉林省互联网信息办公室	(0431) 82761087
9	黑龙江省互联网信息办公室	(0451) 58685745
10	上海市互联网信息办公室	(021) 64271056
11	江苏省互联网信息办公室	(025) 86292870
12	浙江省互联网信息办公室	(0571) 81051900/81051292
13	安徽省互联网信息办公室	(0551) 62606014
14	福建省互联网信息办公室	(0591) 86300613
15	江西省互联网信息办公室	(0791) 88912737
16	山东省互联网信息办公室	(0531) 51773252
17	河南省互联网信息办公室	(0371) 65905939
18	湖北省互联网信息办公室	(027) 87231397
19	湖南省互联网信息办公室	(0731) 81121089
20	广东省互联网信息办公室	(020) 87100943
21	广西壮族自治区互联网信息办公室	(0771) 2093017
22	海南省互联网信息办公室	(0898) 65342106
23	重庆市互联网信息办公室	(023) 63151802/18723299060
24	四川省互联网信息办公室	(028) 86601862
25	贵州省互联网信息办公室	(0851) 85890278
26	云南省互联网信息办公室	(0871) 63902424
27	西藏自治区互联网信息办公室	(0891) 6591809
28	陕西省互联网信息办公室	(029) 63907138
29	甘肃省互联网信息办公室	(0931) 8928733
30	青海省互联网信息办公室	(0971) 8485117
31	宁夏回族自治区互联网信息办公室	(0951) 6668938
32	新疆维吾尔自治区互联网信息办公室	(0991) 2384855
33	新疆生产建设兵团互联网信息办公室	(0991) 2899091

专家解读 | 新形势下完善大型网络平台个人信息保护的重要举措

原载：“网信中国”微信公众号

日前，国家网信办、公安部联合起草的《大型网络平台个人信息保护规定（征求意见稿）》（以下简称《征求意见稿》）公开征求意见。《征求意见稿》立足新形势新挑战，围绕平台内部治理、数据处理规范、用户权益保障等方面进行精细化制度设计，提出了一系列具有针对性和前瞻性的举措，对于规范大型网络平台数据处理活动、推动平台经济创新 and 健康发展、完善公民个人信息保护制度体系具有重要意义。

一、新形势下完善大型网络平台个人信息保护的重要意义

（一）落实党的二十届四中全会精神的重要举措

中国共产党第二十届中央委员会第四次全体会议通过的《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》中明确提出，完善监管，推动平台经济创新 and 健康发展；深化网络空间安全综合治理，加强个人信息保护。大型网络平台是平台经济的核心载体，也是个人信息保护的重点领域。在此背景下，《征求意见稿》正是贯彻落实党中央决策部署、回应新阶段发展需求的重要举措，为实现规范与发展并重、安全与创新协同提供了关键的制度保障，意义重大而深远。

（二）配套实施个人信息相关立法的必要举措

《个人信息保护法》《网络数据安全管理条例》确立了大型网络平台个人信息保护制度框架。大型网络平台具有用户规模巨大、业务模式复杂、数据处理海量和社会影响力强等显著特征。在实践中，如何将个人信息相关立法的一般性规定精准应用于大型网络平台的复杂场景，亟需更具针对性和可操作性的实施细则。《征求意见稿》对《个人信息保护法》与《网络数据安全管理条例》相关制度进行了深化、细化和补充，填补了个人信息保护领域一般性法律与平台实践之间的操作空白，特别是对个人信息可携带权等内容作出了具体的操作指引，是确保个人信息相关立法在大型平台这一关键领域得到全面、深入贯彻执行的重要举措。

（三）推动平台经济健康发展与个人数据规范流动的有力支撑

数据要素是平台经济的核心引擎，大型网络平台是海量数据处理的关键枢纽，个人信息在平台间的规范、高效流动，是激发数据要素价值、发展新质生产力的重要基础。《征求意见稿》有利于打击部分大型网络平台对个人信息的违规处理，保障用户权益。通过划定清晰的合规底线和行为规范，消除不确定性，引导大型网络平台规范开展数据处理活动，有利于构建安全可信的数据处理与流动环境、赋能平台经济高质量发展。

二、大型网络平台个人信息保护制度的重要创新

（一）创新大型网络平台目录管理机制

《征求意见稿》在细化大型网络平台范畴的基础上，通过制定目录清单，增强对境内建设、运营的大型网络平台管理的透明度和可预期性。《征求意见稿》细化了《网络数据安全条例》中对于大型网络平台的定义，明确“业务类型复杂”是指经营重要网络服务或经营范围涵盖多个类型业务，同时要求其掌握的数据一旦被泄露、篡改、毁损将对国家安全、经济运行、国计民生造成重大影响。此外，《征求意见稿》也包括了由国家网信部门和公安机关规定的其他情形，确保监管覆盖的全面性。《征求意见稿》拟建立的目录管理机制，可以让监管机关和监管对象更清晰地识别规定的适用对象，最大程度地解决了大型网络平台界定上的确定性，同时也可以通过目录动态更新，及时回应平台经济发展中的新情况。

（二）健全大型网络平台内部治理架构

《征求意见稿》的核心举措之一，是明确要求大型网络平台建立并落实个人信息保护负责人制度，着力完善大型网络平台的内部治理架构。

一是严格限定了负责人的资质和权威性。《征求意见稿》要求负责人必须由管理层成员担任，且必须是中国国籍，无境外永久居留权或长期居留许可，并具备五年以上相关经验。为降低企业合规成本，允许数据安全负责人兼任。

二是赋予负责人实质性的决策权与监督权。

《征求意见稿》明确个人信息保护负责人有权参与个人信息处理相关决策并享有否决权，同时承担指导合规、配合检查，以及发现违法犯罪行为时向监管部门和公安机关报告的法定职责。

三是强调体系化保障。《征求意见稿》要求平台配备专门团队，协助负责人开展规则制定、权限管理、监测审计、应急演练和未成年人保护等工作。负责人的相关信息须统一报国家网信部门，再由国家网信部门向公安机关等部门共享，形成高效协同的监管闭环。

（三）完善大型网络平台治理与审计机制

《征求意见稿》着眼于数据流转的全链条安全，建立了一套严格的闭环治理机制。

一是强化数据存储的属地管理与“延伸监管”。

《征求意见稿》明确，境内收集和产生的数据原则上应在境内存储。对大型网络平台的监管延伸至数据中心，明确其负责人必须是中国国籍，无境外永久居留权或长期居留许可。数据中心的安全性要符合国家有关标准。数据确需出境的，必须严守国家规定。

二是健全风险处置与第三方协同机制。《征求意见稿》要求平台发现数据中心存在相关风险须立即补救并报告监管部门及个人信息保护负责人。若使用第三方数据中心，必须签订合同明确其职责，并要求其接受个人信息保护负责人的监督。

三是细化了强制合规审计的触发条件。《征求意见稿》明确，在发生严重风险、多次违规、导致100万以上个人信息或10万人以上敏感个人信息泄露的重大安全事件时，必须强制引入第三方审计，同时平台必须为第三方审计提供必要的访问权限和便利。

（四）细化个人信息可携带操作方案

《征求意见稿》对《个人信息保护法》中的个人信息可携带进行了操作层面的细化，为用户实现个人信息可携带提供了清晰路径。

一是明确了响应时限与流程。《征求意见稿》要求大型平台在收到用户转移请求后，原则上应在30个工作日内，以通用的机器可读格式完成信息转移，并通知个人结果。若因请求量大或操作复杂确需延期，在必要合理的前提下可再延长30个工作日，但必须向用户说明原因。

二是规范了技术实现与安全要求。《征求意见稿》支持通过应用程序接口或标准化方式进行转移，并要求平台在过程中采取身份验证和加密传输措施，确保数据转移全过程的安全可控。

三是平衡了权利与成本。对于不符合法定条件而无法转移的请求，《征求意见稿》要求平台必须向用户说明理由；同时，允许平台收取基于实际成

本的必要费用，确保了该机制的可持续运行。

《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》对有效市场和有为政府的结合提出更高要求，体现了从“管得住”到“管得好”的升维调整。相信经充分讨论和修改完善后，《征求意见稿》相关制度设计的科学性、可行性与可操作性必将得到进一步提升，有效实现大型网络平台个人信息保护“管得好”的目标，为平台经济的创新和健康发展提供更加坚实的制度保障。

作者：周辉 中国社会科学院法学研究所网络与信息法研究室副主任

专家解读 | 夯实能力、强化责任、构建托底机制——《大型网络平台个人信息保护规定》的监管逻辑与国际比较

原载：“网信中国”微信公众号

2025年11月22日，国家互联网信息办公室、公安部发布了《大型网络平台个人信息保护规定（征求意见稿）》（以下简称《征求意见稿》），旨在帮助具有海量用户和对全局有系统性影响的大型网络平台，进一步提升个人信息保护能力。该规定以强化平台能力建设为主线，从平台识别、专职负责人和组织保障、数据中心能力要求、数据跨境流动与数据可携权，以及必要时引入第三方数据中心托管等方面，构建了可问责、可验证、可托底的个人信息保护框架。

这一监管路径的逻辑在于：通过明确制定发布大型网络平台目录、确保平台内部建立完善的合规体系并接受外部监督、强化技术和基础设施保障、赋予用户对数据迁移和流动的权利，同时预设当平台自身能力不足或出现重大风险时的外部介入机制，从而全面提升个人信息保护水平。本文对《征求意见稿》所规定的五个关键制度设计，分析其科学性和必要性，并结合欧盟、美国等相关制度进行比较论证。

一、大型平台认定：细化明确系统性外部性平台义务标准

《征求意见稿》通过“双重标准”，即明确的用户数量阈值（如注册用户5000万以上、月活跃用户1000万以上）和服务性质（涉及重要网络服务、可能影响公共利益或国家安全），精准识别具有系统性影响和高风险的平台（第三条）。这一方式兼顾了可操作性和风险精准度，避免了监管的泛化与资源浪费。国际经验表明，欧盟《数字服务法》亦采用类似标准，将月活跃用户超过4500万的平台认定为超大型在线平台，实施更严格的风险评估、外部审计和数据共享义务。欧盟强调，此举正因大型平台对社会治理和公共利益的系统性外部性风险显著，必须通过高透明度和严监管加以控制。此外，美国学界也提出对具有重大社会影响的科技平台采用类似公共事业监管理念，强化其社会责任和外部监督。《征求意见稿》所设定的精准识别机制与国际监管实践高度一致，不仅提高了监管透明度与可预测性，也确保了监管资源的有效配置，实现了公共利益保护和风险精准管理的有机统一。

二、个人信息保护负责人制度及专门机构：责任落实与组织保障

《征求意见稿》明确规定大型平台须设立高层级个人信息保护负责人，负责参与重大决策、统筹制度建设与风险评估、监督投诉处理并组织制定专门的未成年人个人信息处理规则（第五条）。同时，要求配备专门的个人信息保护工作机构，并为其提供必要的经费、人员与技术工具等组织保障（第六条、第七条）。此外，针对负责人与机构信息的变更，要求平台在20个工作日内向监管部门进行报备（第八条）。这一制度设计体现了“责任到人”与“组织保障”相结合的监管思路，确保个人信息保护义务在企业内部真正落地执行。

从国际经验看，欧盟《通用数据保护条例》早已明确要求在处理高风险个人数据场景下设立数据保护官，并强调其职能独立性及直接向企业最高管理层汇报，以保证其合规监督的有效性。欧盟《数字服务法》则要求超大型平台建立专门的独立合规

部门,定期接受外部独立审计,通过内部责任落实与外部审计形成持续有效的问责链条。欧盟的思路在于,由于数字平台生态的复杂性,仅靠企业自律已难以保障合规,必须通过内嵌于企业组织结构的合规制度以及外部透明审计,形成可信的治理机制。

由此可见,《征求意见稿》所提出的个人信息保护负责人与专门机构制度,符合国际监管趋势,将抽象的合规要求转化为平台企业内部的明确职责与具体执行能力,形成了内外双重约束与治理闭环,极大提升了个人信息保护制度的可操作性和执行力。

三、数据中心能力建设与平台主动报告义务: 夯实基础设施合规与可监管性

大型平台由于处理海量个人信息,必须在技术和基础设施上具备足够的安全管理能力。《征求意见稿》将大型平台数据中心能力建设与主动报告义务结合设计,落实《个人信息保护法》要求,强调平台必须将在境内收集和产生的个人信息存储在境内(第九条),并建立完善的数据管理和技术安全规范体系,同时要求对重大风险或系统变更及时处置并向监管部门报告(第十条、第十三条)。这种“基础设施合规”与“可监管性”相结合的设计,突出了对平台数据安全能力的事前建设与事中事后的透明监督,确保合规能力真正可验证、可考核,而非流于形式。

从国际实践来看,欧盟《数字服务法》要求超大型平台每年必须进行独立外部审计,并向监管机构与独立研究者开放数据,以确保平台合规措施的持续可见性。此外,欧盟《网络和信息系统指令2》更是明确要求成员国对数据中心、云服务等关键数字基础设施实施严格的安全风险管理、通报机制和现场审计检查,以确保其安全性与可靠性。因此,欧盟的路径是《数字市场法》与《数字服务法》的监管侧重于平台“无形”层面,而对数据中心这类“有形”基础设施的监管,则由《网络和信息系统指令2》及各成员国法规起到重要的补充作用。

《征求意见稿》将数据中心的安全能力建设与主动报告紧密结合,与欧盟“审计+报告+现场检查”

的监管逻辑高度一致,不仅显著提升了监管的可操作性,也顺应了全球对数字基础设施监管日益强化的趋势。这种制度设计,有效强化了对个人信息安全的整体保障能力。

四、数据可携:用户赋权、平台互通与风险管控

《征求意见稿》第十四条明确规定,大型网络平台应保障用户可便捷地转移个人信息,并对转移请求设定了明确的受理时限和服务标准,如要求“30个工作日内答复与处理”,确保用户权利的落实具备明确的可操作性和可核查性。这种安排不仅从抽象权利宣示转化为可执行的服务承诺,更通过服务时限、流程和标准的明确规范,增强了用户对个人信息的自主控制力,降低了用户对特定平台的依赖程度。

从国际监管经验来看,欧盟《通用数据保护条例》第二十条也确立了类似的个人数据可携权,明确要求数据控制者需以结构化、机器可读的方式向用户提供其个人信息,以方便用户自由迁移到其他平台。此外,欧盟《数字市场法》第6(9)条更进一步强化对“守门人”平台的数据可携要求,要求其提供高质量、持续且实时的数据迁移服务,并积极鼓励第三方直接接入,目的是减少平台的锁定效应,促进数字市场竞争与用户的自由选择权。

欧盟的实践表明,数据可携权与平台互操作性已成为现代“公共事业式”监管的关键工具,能够有效改善市场的进入条件,打破数据孤岛局面,增强用户对个人信息的控制力和选择权。因此,《征求意见稿》强调数据迁移的便利性和时效性,充分体现了“用户赋权”与“市场竞争”的监管逻辑,与国际先进的监管理念高度一致。

五、托底机制:第三方数据中心存储的外部保障

《征求意见稿》第十七条明确规定,当大型网络平台出现重大安全风险、严重数据事故或执法发现系统性缺陷等极端情形,且平台自身能力不足以保障个人信息安全时,监管机关有权要求平台将个人信息转移至符合条件的第三方数据中心进行存

储和管理。这一安排旨在建立一种“托底机制”，提供关键时刻的结构性矫正与应急接管能力，有效防范因平台技术或管理能力不足而引发的个人信息安全风险扩散和失控。

这种机制在国际监管实践中具有显著的理论 and 制度基础。尽管欧盟《数字服务法》和《数字市场法》未明确规定“强制第三方托管”，但其制度设计包括限制令、暂停数据处理、外部独立审计与数据开放共享等多种外部矫正措施，实质上与第三方可信托管的理念相似。此外，欧美学界近年来将大型网络平台视为“新公共事业”的重要信息基础设施，强调其对社会稳定、连续性和公共利益的重要意义，提出在必要情形下应采取结构性手段介入，以确保平台生态稳定运行并防范系统性风险。

因此，《征求意见稿》所引入的第三方数据中心托底机制，是针对高风险场景的一种必要的工程化风险管控与应急保障措施。这种机制强调了个人信息保护的连续性与韧性，将抽象的制度要求转化为具体的应对能力，确保在关键时刻平台个人信息的安全性、合规性。这种制度设计不仅与国际主流的监管思路保持一致，更为高风险平台提供了明确、可验证且可实际操作的保障方案，体现出高度的监管科学性和制度正当性。

综上，《大型网络平台个人信息保护规定（征求意见稿）》通过上述五方面的制度设计，勾勒出我国个人信息保护监管的新思路：强调平台主体责任和能力提升，同时借鉴国际经验强化透明度和外部监督，并设置极端情况下保护用户权益的安全网。这一套框架既具有务实的制度逻辑，又体现了前瞻性的监管理念。对于监管部门而言，该规定提供了操作性强的工具箱，使对大型平台的监管“有据可依、有力可使”。对于企业而言，新要求倒逼其加强合规投入，提升数据治理水平，在国内国际双重标准下赢得用户信任。对于学界和公共政策制定者而言，这一探索也提供了可资借鉴的“中国方案”，印证了在数字时代如何通过综合治理来有效平衡个人信息保护与数字经济创新发展的命题。

作者：洪延青 北京理工大学法学院教授

个人信息保护政策法规问答 (2026年8月)

原载：“网信中国”微信公众号

国家互联网信息办公室持续加强个人信息保护相关政策法规宣贯，指导帮助个人信息处理者规范开展个人信息处理活动，保护个人信息权益。现将一些具有代表性的问题和答复公布如下。

1. 处理已公开的个人信息有哪些要求？

《个人信息保护法》第二十七条规定，“个人信息处理者可以在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；个人明确拒绝的除外。个人信息处理者处理已公开的个人信息，对个人权益有重大影响的，应当依照本法规定取得个人同意。”

《个人信息保护合规审计管理办法》附件《个人信息保护合规审计指引》第十二条对违法违规处理已公开个人信息情形作了细化：（一）向已公开个人信息中的电子邮箱、手机号等发送与其公开目的无关的商业信息；（二）利用已公开的个人信息从事网络暴力、传播网络谣言和虚假信息等活动；（三）处理个人明确拒绝处理的已公开个人信息；（四）对个人权益有重大影响，未取得个人同意；（五）收集、留存或处理已公开个人信息的规模、时间或使用目的超出合理范围。

2. 导致个人信息泄露的常见原因有哪些？

一是个人信息明文存储和传输，未采取适当的加密、去标识化等安全技术措施；二是存储个人信息的信息系统、数据库等未采取有效安全措施，如使用弱口令、无登录验证措施；三是可通过互联网访问的数据接口未采取有效的身份验证措施；四是互联网网站页面上包含网站关联的信息系统、数据库的登录账号与口令等。

《个人信息保护法》第五十一条规定，“个人信息处理者应当根据个人信息处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失：（一）

制定内部管理制度和操作规程；（二）对个人信息实行分类管理；（三）采取相应的加密、去标识化等安全技术措施；（四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；（五）制定并组织实施个人信息安全事件应急预案；（六）法律、行政法规规定的其他措施。”

2026年个人信息保护系列专项行动取得阶段性成效

原载：“网信中国”微信公众号

2026年个人信息保护系列专项行动开展以来，中央网信办、工业和信息化部、公安部会同相关部门，加强系统谋划部署，强化协调联动，持续开展巡查检测，加强典型问题公开通报和督促整改，各项任务取得阶段性成效。

一是累计对2万余款App、SDK个人信息收集使用情况开展核查检测，督促4000余款完成合规整改，公开通报1100余款存在违法违规问题的App、SDK，对400余款采取下架等处置处罚措施。

二是针对个人信息处理规则未明确收集个人信息用于广告、用户画像，未提供个性化广告关闭选项等问题，对1000余家企业和机构的相关产品开展核查检测并督促整改。

三是开展教育、交通、卫生健康、金融等领域个人信息风险排查，累计摸排9万余家企业和机构，发现并督促整改各类隐患问题1.2万余个。

四是加大个人信息违法犯罪打击力度，加强线索监测发现，严打涉信息泄露、信息倒卖等违法犯罪行为，严惩行业“内鬼”。

下一步，中央网信办、工业和信息化部、公安部将深入推进个人信息保护系列专项行动，加强典型违法违规问题治理，加快推进国家网络身份认证公共服务推广应用，深化个人信息保护宣传教育，不断夯实个人信息保护工作基础，有效维护公民合法权益。

国家互联网信息办公室关于《大型个人信息处理者个人信息保护规定（征求意见稿）》公开征求意见

原载：“网信中国”微信公众号

为规范大型个人信息处理者个人信息处理活动，保护个人信息合法权益，促进个人信息依法合理利用，根据《中华人民共和国个人信息保护法》、《网络数据安全管理条例》等法律、行政法规，国家网信部门将前期已公开征求意见的《大型网络平台设立个人信息保护监督委员会规定（征求意见稿）》、《大型网络平台个人信息保护规定（征求意见稿）》作了整合完善，形成《大型个人信息处理者个人信息保护规定（征求意见稿）》，现向社会公开征求意见。

大型个人信息处理者个人信息保护规定 （征求意见稿）

第一章 总 则

第一条 为了规范大型个人信息处理者个人信息处理活动，保护个人信息合法权益，促进个人信息依法合理利用，根据《中华人民共和国个人信息保护法》、《网络数据安全管理条例》等法律、行政法规，制定本规定。

第二条 大型个人信息处理者的个人信息保护及其监督管理，适用本规定。

对大型个人信息处理者的认定，应当综合考虑下列条件：

- （一）处理1000万人以上自然人个人信息；
- （二）提供涉及个人信息处理的重要网络服务，或者经营范围涵盖多种业务且涉及个人信息处理；
- （三）个人信息处理活动对国家安全、经济运行、社会稳定、公共健康和安全等具有重要影响。

第三条 处理1000万人以上自然人个人信息和自评估认为符合本规定第二条第二款第二项、第三项条件的个人信息处理者，应当通过所在地省级网信部门向国家网信部门申报大型个人信息处理者认定，并按照有关要求提交材料。

省级网信部门应当自收到申报材料之日起15个工作日内完成完备性查验,申报材料齐全的,将申报材料和初步认定意见报送国家网信部门;申报材料不齐全的,应当退回个人信息处理者并一次性告知需要补充的材料。

省级以上网信部门、电信主管部门、公安机关等履行个人信息保护职责的部门研究认为个人信息处理者符合认定条件但未主动申报认定的,应当督促其申报认定。

国家网信部门会同国务院电信主管部门、公安部门等履行个人信息保护职责的部门依据认定条件,研究确定大型个人信息处理者清单,并向社会公告。

被认定的大型个人信息处理者认为其已连续6个月不再符合认定条件,可以通过所在地省级网信部门向国家网信部门提出变更认定申请。

第四条 国家网信部门负责统筹协调大型个人信息处理者的个人信息保护工作和相关监督管理工作。国务院电信主管部门、公安部门等履行个人信息保护职责的部门,依照本规定和有关法律、行政法规的规定,在各自职责范围内负责大型个人信息处理者的个人信息保护和监督管理工作。

地方网信部门负责统筹协调本行政区域内的大型个人信息处理者的个人信息保护工作和相关监督管理工作。地方电信主管部门、公安机关等有关部门依据各自职责负责本行政区域内的大型个人信息处理者的个人信息保护和监督管理工作。

网信部门、电信主管部门、公安机关等履行个人信息保护职责的部门应当加强大型个人信息处理者有关信息的共享和工作协同。

第五条 大型个人信息处理者应当采取加密、去标识化、访问控制、匿名化等措施保障所处理个人信息安全,可以应用国家网络身份认证公共服务,鼓励使用数据标签标识技术、通过个人信息保护认证等,提高个人信息保护水平。

第六条 鼓励大型个人信息处理者开展个人信息保护相关技术、产品、服务创新,积极参与个人信息保护相关国际标准和规则制定,推动与其他

国家、地区之间的个人信息保护规则、标准协调互认。

第七条 境外的组织、个人从事侵害中华人民共和国公民的个人信息权益,或者危害中华人民共和国国家安全、公共利益的个人信息处理活动的,国家网信部门可以将其列入限制或者禁止个人信息提供清单,予以公告,并采取限制或者禁止向其提供个人信息等措施。

第二章 个人信息处理规则

第八条 大型个人信息处理者处理个人信息,应当遵循合法、正当、必要和诚信原则,遵守法律、行政法规,尊重社会公德和伦理。

第九条 大型个人信息处理者收集个人信息,应当坚持最小必要原则,限于提供产品或者服务所必需,不得过度收集个人信息。

第十条 大型个人信息处理者制定公开个人信息处理规则,应当通过清晰易懂的语言,真实、准确、完整、逐项列明下列事项:

(一)大型个人信息处理者名称、个人信息保护负责人姓名和有效的联系方式;

(二)以结构化清单形式列明每项功能服务收集使用个人信息的目的、方式、种类,调用权限名称、频度,收集使用敏感个人信息的必要性以及对个人权益的影响;

(三)嵌入软件开发工具包的,应当以结构化清单形式列明嵌入的软件开发工具包名称(包名)、版本、主要功能、运营者名称或者姓名、收集使用个人信息的种类和完整的软件开发工具包个人信息处理规则访问途径;

(四)向其他个人信息处理者提供个人信息的,应当列明接收方的名称、联系方式、处理目的、处理方式和个人信息的种类;

(五)个人信息保存期限和到期后的处理方式,保存期限难以确定的,应当明确保存期限的确定方法;

(六)个人查阅、复制、转移、更正、补充、删除、限制、拒绝处理个人信息以及注销账号、撤回同意的方式和途径等;

(七)法律、行政法规、部门规章规定应当告知的其他事项。前款规定事项发生变更的,应当将变更部分告知个人。

第十一条 大型个人信息处理者基于个人同意处理个人信息,应当采取对个人权益影响最小的方式,有下列情形之一的,应当取得个人的单独同意:

(一)向其他个人信息处理者提供所处理的个人信息;

(二)向中华人民共和国境外提供个人信息;

(三)公开所处理的个人信息;

(四)处理敏感个人信息;

(五)法律、行政法规规定的其他情形。大型个人信息处理者处理不满十四周岁未成年人个人信息的,应当取得未成年人的父母或者其他监护人的同意;大型个人信息处理者应当为监护人同意和撤回同意处理不满十四周岁未成年人个人信息提供便捷渠道。

第十二条 大型个人信息处理者基于个人同意处理个人信息的,个人信息的处理目的、处理方式和处理的个人信息种类发生变更的,应当重新取得个人同意。大型个人信息处理者基于个人同意处理个人信息的,应当提供便捷的撤回同意的方式,以结构化清单形式列明个人已同意大型个人信息处理者处理的个人信息种类,以及个人信息的处理目的、处理方式,便于个人选择。

第十三条 大型个人信息处理者应当将在中华人民共和国境内运营中收集和产生的个人信息存储在境内。

第十四条 大型个人信息处理者应当选择符合下列条件的数据中心,存储在中华人民共和国境内运营中收集和产生的个人信息:

(一)设立在中华人民共和国境内;

(二)数据中心管理机构的法定代表人或者实际控制人具有中华人民共和国国籍;

(三)符合国家有关政策标准要求。

第十五条 大型个人信息处理者的数据中心管理机构应当建立健全内部管理制度和操作规程,

协助大型个人信息处理者履行个人信息保护义务,具体职责包括但不限于:

(一)制定个人信息安全事件应急预案;

(二)发现系统、网络产品和服务等存在影响大型个人信息处理者履行个人信息保护义务的安全缺陷、漏洞等风险的,应当立即采取补救措施,通报大型个人信息处理者,并按照规定向有关履行个人信息保护职责的部门报告;

(三)发生个人信息安全事件时,应当立即通报大型个人信息处理者,及时启动应急预案,采取措施防止危害扩大,消除安全隐患,并按照规定向国家网信部门、国务院电信主管部门、公安部门等履行个人信息保护职责的部门报告;

(四)及时执行国家网信部门和国务院电信主管部门、公安部门等履行个人信息保护职责的部门的有关要求。

第十六条 大型个人信息处理者委托第三方数据中心管理机构等处理个人信息的,应当与其签订书面合同,约定委托处理个人信息的目的、期限、处理方式、存储地点、规模、种类、保护措施以及双方的权利和义务等,要求遵守本规定第十四条、第十五条规定。受托方应当协助大型个人信息处理者对个人信息处理活动进行安全管理。

第十七条 大型个人信息处理者通过自动化决策方式向个人进行信息推送、商业营销的,应当采取下列措施保护个人权益:

(一)设置易于理解、便于访问和操作的个性化推荐关闭选项;

(二)用户选择关闭个性化推荐的,大型个人信息处理者应当停止将相关个人信息用于个性化推荐目的;

(三)为用户提供删除针对其个人特征的用户标签等功能;

(四)法律、行政法规、国家有关部门规定的其他措施。

第十八条 大型个人信息处理者对个人信息进行汇聚或者融合等处理的,若处理后的个人信息符合《中华人民共和国个人信息保护法》第二十八

条规定,应当按照敏感个人信息进行识别与保护。

第十九条 对符合《网络数据安全管理条例》第二十五条规定条件的个人信息转移请求,大型个人信息处理者应当自完成个人身份验证和请求验证后30个工作日内采取通用或者机器可读的格式转移个人信息,并以邮件、电话、短信等方式告知个人处理结果;不能提供转移途径的,应当向个人说明理由。因请求数量、操作复杂等原因需要延长处理期限的,应当向个人说明延期理由,可以在合理、必要的情况下延长30个工作日。法律、行政法规、部门规章另有规定的,从其规定。

大型个人信息处理者应当采取身份验证、加密传输等安全措施保障个人信息转移安全。支持大型个人信息处理者通过应用程序接口或者其他标准化技术方式提供转移途径。

请求转移个人信息次数明显超出合理范围的,大型个人信息处理者可以根据转移个人信息的成本收取必要费用,收费标准应当公开透明。

第二十条 大型个人信息处理者因业务等需要,确需向中华人民共和国境外提供个人信息的,应当按照国家有关规定申报数据出境安全评估、订立个人信息出境标准合同或者通过个人信息保护认证等,健全个人信息出境安全相关技术和管理措施,及时防范、处置个人信息违法出境安全风险和威胁。大型个人信息处理者应当对境外接收方的管理和技术措施进行评估,发现境外接收方无法履行法律、行政法规、部门规章或者相关合同约定的个人信息保护义务和责任的,应当暂停向其提供个人信息。法律、行政法规和国家有关规定对于免于申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证另有规定的,从其规定。

第二十一条 大型个人信息处理者因业务等需要向其他个人信息处理者提供个人信息的,应当优先采取去标识化、聚合统计等措施,向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类,并按照《中华人民共和国网络安全法》第二十三条规定要求,采取监测、记录个人信息对外传输情况的技术措施,留存相关

日志不少于六个月。接收方应当在前款所述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的,应当重新取得个人同意。

第二十二条 大型个人信息处理者不得公开其处理的个人信息,取得个人单独同意的除外;公开个人信息,应当限于实现处理目的最小范围,采取去标识化等技术措施防范侵害个人权益风险;公开个人信息前,应当开展个人信息保护影响评估。大型个人信息处理者可以在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息;个人明确拒绝的除外。大型个人信息处理者处理已公开的个人信息,对个人权益有重大影响的,应当依照法律、行政法规规定取得个人同意。大型个人信息处理者应当为个人拒绝处理其已公开个人信息提供便捷途径。

第二十三条 大型个人信息处理者处理个人信息的保存期限应当限于提供产品或者服务所必需的最短时限。有下列情形之一的,大型个人信息处理者应当主动删除个人信息:

(一)处理目的已实现、无法实现或者为实现处理目的不再必要;

(二)大型个人信息处理者停止提供产品或者服务,或者保存期限已届满;

(三)个人撤回同意或者个人拒绝处理;

(四)大型个人信息处理者违反法律、行政法规或者违反约定处理个人信息;

(五)法律、行政法规规定的其他情形。

个人请求删除个人信息的,大型个人信息处理者应当及时删除;确有理由不能删除的,应当在15个工作日内答复。

法律、行政法规规定的保存期限未届满,或者删除个人信息从技术上难以实现的,大型个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。

第三章 大型个人信息处理者的义务

第二十四条 大型个人信息处理者应当围绕个人信息处理活动、个人行使权利响应、安全义务

履行等环节,建立健全内部管理制度和操作规程,加强个人信息安全监测预警,及时发现处置个人信息安全问题和事件,防范安全风险。管理制度至少包括以下内容:

(一)个人信息分类管理制度;

(二)个人信息处理涉及的安全存储、授权访问、可控传输、对外提供、行为审计等制度;

(三)个人信息安全风险监测、应急演练、应急响应等制度;

(四)个人信息保护影响评估、合规审计制度;

(五)未成年人个人信息保护制度;

(六)个人信息投诉举报受理处置制度;

(七)个人信息保护宣传教育培训制度。

第二十五条 大型个人信息处理者应当按照法律、行政法规的规定指定一名管理层成员担任个人信息保护负责人,并公开个人信息保护负责人的联系方式。鼓励个人信息保护负责人具备个人信息保护合规审计能力。

第二十六条 个人信息保护负责人应当履行下列职责:

(一)组织制定内部个人信息保护管理制度、操作规程以及个人信息安全事件应急预案,指导开展个人信息安全风险监测、风险评估、合规审计、影响评估、应急演练、教育培训等活动。

(二)指导业务部门相关人员合规开展个人信息处理活动,落实履行个人信息保护职责部门的要求,配合开展个人信息保护监督检查。

(三)参与大型个人信息处理者个人信息处理事项相关决策,对存在安全风险的决策及时提出意见。大型个人信息处理者对合规性意见无正当理由不予处理,或者处理结果违反法律、行政法规和国家有关规定的,个人信息保护负责人可以直接向所在地省级网信部门报告。

(四)负责对大型个人信息处理者个人信息处理活动以及采取的保护措施等进行监督,发生或者可能发生个人信息泄露、篡改、丢失等安全事件,或者存在其他可能导致大规模个人信息权益受损的重大违法情形的,应当立即组织采取补救措施,

并向所在地省级网信部门和电信主管部门、公安机关等履行个人信息保护职责的部门报告;涉嫌犯罪的,应当向公安机关报案;发现可能危害国家安全的,应当向国家安全机关报告。

(五)组织针对不满十四周岁未成年人制定专门的个人信息处理规则,对已满十四周岁不满十八周岁未成年人采取针对性个人信息保护措施。

(六)定期向个人信息保护监督委员会报告大型个人信息处理者个人信息保护有关工作。大型个人信息处理者应当为个人信息保护负责人履行职责提供必要支持。

第二十七条 大型个人信息处理者应当明确业务部门具备个人信息保护合规审计能力的人员负责个人信息保护工作,人员数量应当与业务部门的业务规模、履行的个人信息保护义务相适应,在个人信息保护负责人指导下,负责所在部门个人信息处理活动安全管理,明确所在部门个人信息处理规范,确保履行个人信息保护义务。

第二十八条 大型个人信息处理者应当以实现业务功能所需的最小授权为原则,为工作人员配置个人信息处理的操作权限。个人信息处理操作记录、权限审批记录等至少保存六个月;涉及个人信息保护影响评估报告和处理情况记录的,应当至少保存三年。

第二十九条 提供网络平台服务的大型个人信息处理者应当明确平台内产品或者服务提供者处理个人信息的规范、权限和保护个人信息的义务,督促其建立健全个人信息保护内部管理制度和操作规程,依法开展个人信息处理活动,履行个人信息保护义务。大型个人信息处理者发现平台内产品或者服务提供者严重违法违反法律、行政法规处理个人信息的,应当立即采取停止提供服务等处置措施,并向省级以上网信部门等履行个人信息保护职责的部门报告。

第三十条 大型个人信息处理者应当每年编制并于上半年发布上一年度个人信息保护社会责任报告。个人信息保护社会责任报告包括但不限于以下内容:

- (一)个人信息保护组织架构和内部管理情况;
- (二)个人信息保护能力建设情况;
- (三)个人信息保护措施和成效;
- (四)未成年人个人信息保护情况;(五)个人行使权利的的申请受理情况;
- (六)个人信息保护监督委员会履职情况、外部成员津贴标准;
- (七)重大个人信息安全事件处理情况;
- (八)个人信息保护宣传教育、公益活动情况;
- (九)法律、行政法规规定的其他事项。

第三十一条 大型个人信息处理者上线涉及自动化决策、敏感个人信息处理等可能对个人权益有重大影响的产品、服务或者功能,应当事前开展个人信息保护影响评估,并在评估完成后的15个工作日内通过所在地省级网信部门将影响评估报告报国家网信部门备案。个人信息保护影响评估应当包括以下内容:

- (一)处理个人信息的目的、处理方式是否合法、正当、必要,相关权限的调用频率、数据精度等是否限于实现业务功能的最低频度、最小范围;
- (二)个人信息处理活动对个人权益的影响及安全风险;
- (三)自动化决策机制避免精确定位到特定个人的措施及其有效性;
- (四)所采取的保护措施是否合法、有效并与风险程度相适应;
- (五)法律、行政法规、部门规章规定的其他事项。

第三十二条 大型个人信息处理者应当严格保护未成年人个人信息,通过网络身份认证公共服务等方式识别未成年人,并依照《未成年人网络保护条例》规定,每年开展未成年人个人信息保护合规审计。大型个人信息处理者应当指定专人负责未成年人个人信息保护工作。专人应当经过专门培训,熟悉未成年人特点和健康成长保护需要。

第三十三条 大型个人信息处理者应当每两年至少开展一次个人信息保护合规审计,每年对其个人信息处理活动开展风险评估,并对发现的问题

进行整改。鼓励大型个人信息处理者在显著位置公开展示合规审计、风险评估等结果。

第三十四条 大型个人信息处理者委托第三方专业机构开展个人信息保护合规审计、风险评估等活动的,应当配合第三方专业机构履行职责,为第三方专业机构开展工作提供必要保障,包括为第三方专业机构指定人员提供必要的访问大型个人信息处理者网络数据设施、系统及操作日志记录权限等。受大型个人信息处理者委托开展个人信息保护合规审计、风险评估等活动的第三方专业机构,应当注册在中华人民共和国境内。发现大型个人信息处理者的个人信息处理活动存在较大安全风险的,应当及时通报大型个人信息处理者并提出整改建议。

第三十五条 大型个人信息处理者应当建立便捷的个人信息投诉、举报渠道,在个人信息处理规则中提供有效的、易于访问的投诉举报渠道,健全投诉举报的受理、处置、反馈机制,在承诺时限内(承诺时限不得超过15个工作日,无承诺时限的,以15个工作日为限)受理并处置个人信息相关投诉举报。第三十六条 大型个人信息处理者应当自被认定之日起30个工作日内向所在地设区的市级网信部门报送下列信息:

- (一)个人信息保护负责人基本信息;
- (二)保障个人信息保护负责人履职的措施;
- (三)存储个人信息的数据中心基本信息,包括数据中心管理机构、内部管理制度、安全措施等信息,委托第三方数据中心管理机构处理个人信息的,还应当提交双方签署的合同文本。

个人信息保护负责人、数据中心等基本信息发生变化的,大型个人信息处理者应当自变化之日起30个工作日内报送变更信息。

大型个人信息处理者与第三方数据中心管理机构通过合同约定报送主体的,可以由合同约定的报送主体报送数据中心基本信息。

第四章 个人信息保护监督委员会

第三十七条 大型个人信息处理者应当自被认定之日起6个月内成立主要由外部成员组成的个

人信息保护监督委员会（以下简称监督委员会）对个人信息保护情况进行监督，按照本规定附件要求制定监督委员会工作规则，并通过所在地省级网信部门向国家网信部门报送监督委员会成立情况、工作规则、成员名单等基本信息。

监督委员会成员应当为单数，与大型个人信息处理者业务规模、用户数量等相匹配，不少于7名，外部成员占比不低于三分之二。监督委员会设负责人和秘书，负责人由外部成员担任，应当具备高级个人信息保护合规审计人员能力。大型个人信息处理者应当为监督委员会履行职责提供必要支持。

第三十八条 外部成员应当符合下列条件：

（一）符合本规定第三十九条规定的独立性要求；

（二）同时受聘的大型个人信息处理者不超过3家；

（三）具备个人信息保护合规审计能力，熟悉个人信息保护相关法律法规、国家标准等，从事个人信息保护相关工作不少于3年；

（四）具备良好的声誉，能够客观、公正、独立、廉洁地履行职责；

（五）具备履行职责所需的身体条件和工作时间等；

（六）具有良好的个人品德，不存在违法犯罪、重大失信等不良记录；

（七）法律、行政法规、部门规章规定的其他条件。大型个人信息处理者聘用外部成员的，应当对外部成员进行安全背景审查。审查时，可以申请公安机关协助。

第三十九条 外部成员应当保持身份和履行职责的独立性。最近一年内存在下列情形的人员，不得担任外部成员：

（一）在受聘大型个人信息处理者任职的人员及其近亲属；

（二）直接或间接持有受聘大型个人信息处理者已发行股份百分之一以上，或者是受聘大型个人信息处理者前十名股东中的自然人股东及其近亲属；

（三）在直接或间接持有受聘大型个人信息处理者已发行股份百分之五以上的股东单位或者在受聘大型个人信息处理者前五名股东单位任职的人员及其近亲属；

（四）法律、行政法规、部门规章和监督委员会工作规则规定的不具备独立性的其他人员。

外部成员应当每年对独立性情况进行自查，并将自查情况提交受聘大型个人信息处理者董事会等决策机构或者其授权机构。大型个人信息处理者董事会等决策机构或者其授权机构应当每年对在任外部成员独立性情况进行评估并出具专项意见，在个人信息保护社会责任报告中予以披露。

第四十条 大型个人信息处理者应当通过监督委员会工作规则明确外部成员津贴，津贴标准由大型个人信息处理者董事会等决策机构或者其授权机构批准。支持社会组织建设发布监督委员会外部成员推荐信息库，为大型个人信息处理者选聘外部成员提供参考。

第四十一条 监督委员会重点对大型个人信息处理者下列事项进行监督：

（一）个人信息保护合规制度体系建设情况；

（二）平台规则、个人信息处理规则等制定及重大修订情况；

（三）敏感个人信息、未成年人个人信息等保护情况；

（四）个人信息保护影响评估、合规审计、风险评估组织实施、报告编制、问题整改等情况；

（五）个人信息安全事件预防和处置情况；

（六）个人信息出境合规情况；

（七）利用个人信息进行自动化决策情况；

（八）个人行使个人信息权利申请受理、个人投诉举报处置等情况；

（九）个人信息保护负责人和其他个人信息保护相关人员履职情况；

（十）个人信息保护社会责任报告发布情况；

（十一）法律、行政法规、部门规章规定的其他监督事项。

第四十二条 国家网信部门等履行个人信息

保护职责的部门依法对大型个人信息处理者设立、运行监督委员会的活动进行监督管理,可以要求大型个人信息处理者对设立、运行监督委员会有关事项作出解释说明或者提供相关资料,大型个人信息处理者应当予以配合。被认定的大型个人信息处理者向国家网信部门提出变更认定申请并获通过的,可以撤销监督委员会。

第五章 监督管理和法律责任

第四十三条 大型个人信息处理者应当于每年第一季度通过所在地省级网信部门向国家网信部门报送监督委员会上一年度履职情况;至少每两年通过所在地省级网信部门向国家网信部门报送个人信息保护合规审计报告。国家网信部门将相关情况通报国务院电信主管部门、公安部门。

第四十四条 网信部门、电信主管部门、公安机关等履行个人信息保护职责的部门发现大型个人信息处理者个人信息处理活动违反有关法律、行政法规,报送的监督委员会履职情况、个人信息保护合规审计情况和个人信息保护影响评估情况存在违反法律、行政法规、部门规章和本规定情形的,可以依法开展现场检查、约谈、要求整改、督促解散监督委员会等处置措施。大型个人信息处理者未按要求整改或者未达到整改要求的,国家网信部门和国务院电信主管部门、公安、安全等部门,可以要求大型个人信息处理者采取向第三方数据中心托管个人信息等措施保障个人信息安全。

第四十五条 任何组织和个人有权对大型个人信息处理者、监督委员会及其成员违反本规定的活动,向履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理,并将处理结果告知投诉、举报人。

第四十六条 网信部门、电信主管部门、公安机关等履行个人信息保护职责的部门以及监督委员会、第三方专业机构、第三方数据中心管理机构的工作人员应当对工作中知悉的个人隐私、个人信

息、商业秘密、保密商务信息等依法予以保密,不得泄露或者非法向他人提供。

第四十七条 大型个人信息处理者、个人信息保护负责人、第三方专业机构或者数据中心管理机构违法处理个人信息,或者处理个人信息未履行个人信息保护义务的,由网信部门、电信主管部门、公安机关等履行个人信息保护职责的部门依照《中华人民共和国个人信息保护法》、《中华人民共和国治安管理处罚法》、《网络数据安全管理条例》等法律、行政法规处理;构成犯罪的,依法追究刑事责任。监督委员会成员违反本规定对大型个人信息处理者造成损害,依照与大型个人信息处理者签订的聘任合同承担相应民事责任;导致发生个人信息安全事件、违法处理个人信息等情形的,依照《中华人民共和国个人信息保护法》等法律、行政法规处理;构成犯罪的,依法追究刑事责任。

第六章 附 则

第四十八条 开展涉及国家秘密、工作秘密的个人信息处理活动,适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。大型个人信息处理者应当落实数据分类分级保护、网络安全等级保护、商用密码保护有关要求。属于关键信息基础设施的大型个人信息处理者,还应当遵守国家关于关键信息基础设施安全的有关规定。

第四十九条 本规定下列用语的含义:

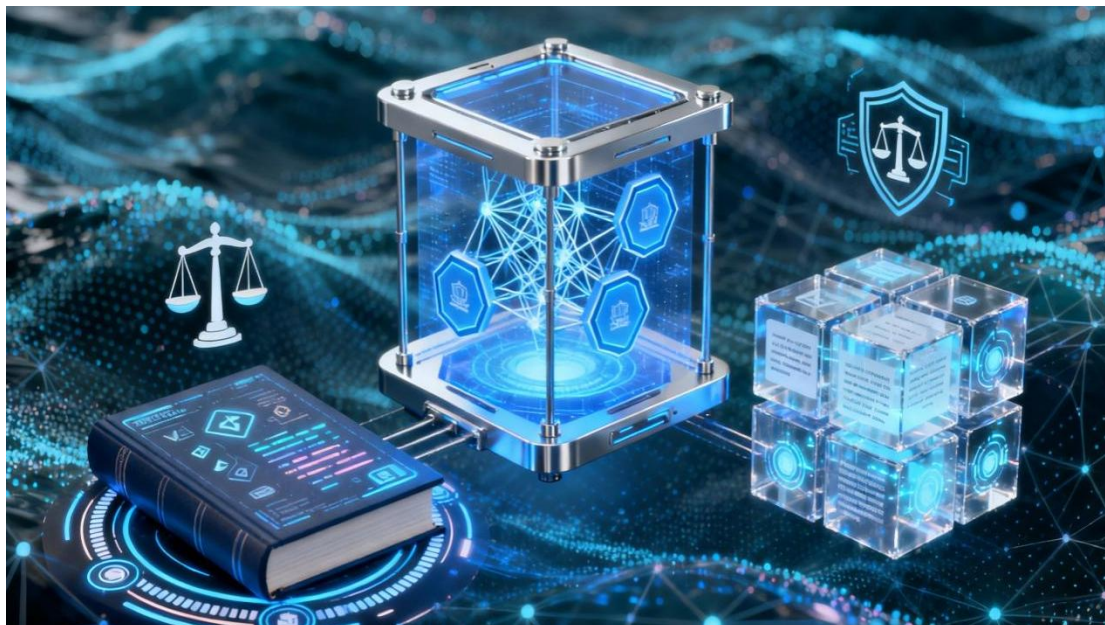
(一)数据中心管理机构,是指负责大型个人信息处理者个人信息处理活动全生命周期安全管理工作的组织机构,可以是大型个人信息处理者的内部机构,也可以是外部的第三方机构。

(二)业务部门,是指大型个人信息处理者内部负责产品、服务研发、运营等的相关部门。

第五十条 本规定自 年 月 日起施行。

(技术编辑:来唯希)

研究动态



数字法学基础理论研究

1、系统论法学的数字人权观（陆宇峰）

来源：《华东政法大学学报》2026年第4期

数字人权作为基本权利，在“复杂性自我增殖”的数字社会维系着“功能分化”，呈现主体多元化、内涵数字化和对象复合化三重特征。其中，“数字生存权”保障数字社会对个人的充分涵括，为诸功能系统的数字沟通提供基本前提，包括数字接入权和数字安全权；“数字发展权”维护从数字赋能到数字分配的平等，防止功能系统内部的过度再分化和数字社会的再阶层化，包括数字受教育权、数字劳动权和数字收益权；“数字自主权”抵御数字科技、数字经济等社会系统对心理系统的操纵，防止数字社会丧失环境中的人类创造性支持，包括个人数据权、算法推荐拒绝权和离线权（或断连权）；“数字参与权”推动直接民主和实质民主，抑制诸功能系统自主运转的负外部性，提升数字社会的自我反思能力，包括公共性数据获取权、公共治理算法知情权和数字共治权。

2、商谈法哲学中的数字人权（鲁楠）

来源：《华东政法大学学报》2026年第4期

哈贝马斯的商谈法哲学为系统审视数字人权的理论建构问题提供了独特视角。基于交往理性与“权利互赋”学说，可彰显数字人权的道义基础，明确人权扎根于平等主体的自由联合、生活世界的交往实践及人的尊严。信息社会赋予了哈贝马斯五种基本权利类型，即平等个人自由权、成员资格权、受法律保护权、政治参与权和生存条件权以新的内容。从权力循环视角出发，应阐明民主法治作为数字人权制度内核的不可替代性。如今，商谈法哲学在信息社会遭遇四重危机，即理想言谈情境的偏离、生活世界的数字化殖民、公共领域的结构扭曲与人的自主性危机，但商谈理论并非失效而是需要升级，以重新构想数字时代的规范制度条件。

3、数字人权中国家义务的体系化阐释（郑智航）

来源：《华东政法大学学报》2026年第4期

数字人权是人在数字化生存环境中应当享有的基本权利，是人权在数字时代的延伸、丰富和发展。人们在感受到数字技术赋能社会生产生活带来便利的同时，也切身体会到了数字技术可能给人权带来的挑战。这种人权风险主要体现为数字鸿沟的

纵深演进、数字歧视的普遍存在、数字监控的过度运用和数字霸权的根基深厚。尊严理论、数字权力理论和全球数字正义理论是国家应积极履行数字人权保障义务的法理基础。国家在数字人权保障方面主要履行尊重、保护和逐步实现三种基本义务，并为这些义务赋予了新的内涵。在具体实践中，数字人权中国国家义务主要围绕构建数字人权保障的法律制度体系、强化国家积极行动体系、建立有效的司法救济体系和推动构建全球数字人权治理体系四个方面展开。

4、从权利到身份：数字时代权利保护范式更新（郑泽星）

来源：《法学论坛》2026年第4期

人工智能技术的发展在展现巨大潜能的同时，也蕴含着前所未有的现实风险。数字时代的权利形态、风险外观以及保护方式均面临深刻变革。传统具体权利保护路径因其分散化、事后性和场景割裂等特征，难以全面应对数字时代权利的结构风险。数字时代权利保护亟须实现从具体权利救济向身份结构保护的范式更新。“数字人权”方案虽试图提供整体性回应，但在理论独立性、规范确定性及制度可操作性方面均存在不足。数字身份是自然人以基础身份信息为起点，在数字技术与社会互动的共同作用下，通过个人信息、行为数据、推断画像以及虚拟化身等要素生成的、能够指向并表征特定个体的数字化身份结构，具体可以区分为信息维度、交互维度和构建维度。将数字身份权能的分散保护与整体保护相结合，是数字时代对抗技术逻辑侵蚀、塑造公平可持续数字秩序、系统保护个人权利的有益路径。

数字时代的部门法研究

1、数智经济下的竞争损害标准：面向竞争过程标准的转型及限度（李子硕）

来源：《环球法律评论》2026年第4期

数智经济改变了市场竞争的运行结构，传统以价格、产量和消费者福利为中心的竞争损害标准面临适用困境。消费者福利标准以经济效率评估竞争结果，在数智平台场景中容易受因果链条过长、损害显现滞后和非价格竞争难以测度等因素制约，难以及时回应创新、分配公平和消费者选择权等多元竞争损害维度。为更契合数智经济实践，竞争损害标准亟需在“法学—经济学”的新平衡中合理配置法规范分析和经济效率分析的功能定位，兼顾竞争损害判断中的过程维度与结果维度，建构竞争损害标准的体系性框架。在引入法规范分析时，竞争过程标准的适用应当保持明确限度，避免竞争损害评估的泛化。我国“良性竞争”的市场秩序要求，应被转译为兼顾竞争结果与竞争过程的多元价值分析框架，以此促进数智经济健康、规范发展。

2、技术异化与刑法的分级保护——以深度伪造技术为例（阮晨欣）

来源：《华东政法大学学报》2026年第4期

科技进步带来的技术异化可能引发特定领域的潜在风险。以深度伪造技术为例，其异化导致了新技术治理的刑事应对乏力，这一问题源于缺乏法益侵害危险的衡量标准。因此，应当以危险的现实化说为法益区分的前提，以潜在的法益侵害危险为预防性衡量基准，并基于潜在风险等级的技术治理保护思路，对技术异化的相关类型进行分类，以此构建不同技术的分级保护模式，推动实现一体化的刑法保护。在刑事治罪层面，应区分恶意深度伪造技术的不法类型，从国家安全法益、社会秩序法益、公民个人合法权益三个层次，对法益侵害程度进行危险衡量。在刑事治理层面，应围绕标识责任义务原则和公民知情同意的核心要素，构建以前置义务分级保护体系为主要内容的刑法保护体系。

3、数据窝赃行为的刑法规制（江海洋）

来源：《法商研究》2026年第4期

我国刑法目前对非个人数据的保护主要限于前端非法获取环节；对于非法获取后的非个人数据

窝赃行为，则主要尝试以掩饰、隐瞒犯罪所得罪进行暂时性规制。数据窝赃行为侵害的法益并非权利人控制数据访问的形式数据秘密，而是数据所蕴含信息内容的实质数据秘密。掩饰、隐瞒犯罪所得罪的保护法益与数据窝赃行为的不法本质并不契合，数据窝赃行为也不满足前者的构成要件。有必要采取立法论路径，增设数据窝赃罪以系统规制此类行为。增设数据窝赃罪不仅具有目的正当性，也能够通过比例原则之适当性、必要性与均衡性的检验。该罪构成要件的设置需要注意：本罪对象为非公开非个人数据，且应对“物之同一性”作实质解释，只要求窝赃数据蕴含的信息内容直接来源于前端非法获取行为所获非个人数据即可；行为方式包括“为自己或他人获取”“提供给他人”“传播”三类；在对数据分类分级的基础上，应设置多维度的罪量要素。本罪法益非绝对不可克减，如基于国家安全、公共利益等正当事由，可对行为予以出罪。

4、数字时代票据法理论更新与制度变革（韩亮）

来源：《法学论坛》2026年第4期

数字票据发展过程中存在双轨制法制运行的弊端，导致司法实践中的法律适用难题。数字票据对传统票据法理论和制度都形成了挑战。数字票据不属于传统意义上的权券结合证券，数字票据的无因性基础与纸质票据不同。数字票据的行为性质也不能用传统的单方行为说来解释，而应该归类为契约说。数字票据时代，票据法的理论体系需要进行更新。在对数字票据理论更新的基础上，才能对票据制度进行重构。数字票据的立法模式可以选择修改《票据法》的模式，这种模式不会割裂与传统的关系，是最理想的数字票据制度变革模式。

5、人工智能时代淫秽物品犯罪的刑法处罚界限——以“AI聊黄案”的行为性质分析为切入点（陈晨）

来源：《法学》2026年第8期

对提供涉黄聊天功能的人工智能（AI）开发者、经营者能否以制作淫秽物品牟利罪定罪，核心是明确淫秽物品在公私领域的制作、传播规则。将“社

会善良风俗”这一集体法益还原为“性的非公开性”的观点，既不能对未成年人进行特殊保护，也难以依赖道德观念证立禁止公开传播淫秽物品的正当性。然将社会善良风俗法益具体化为“禁止身体物化与商品化的性道德”法益，可以解决上述问题。由此，除非以未成年人为对象创作淫秽内容，否则单纯制作、传播AI淫秽物品的行为没有刑罚处罚必要性。AI聊黄行为本质上属于制作淫秽物品以自用的行为，使用行为本身没有违法性，开发者、经营者和其他AI角色设计者即便以牟利为目的帮助制作淫秽物品，也不构成制作淫秽物品牟利罪。提供AI聊黄行为的服务可以区分为本地化部署和云服务部署两种模式，后者提供AI聊黄服务的行为可以被评价为传播淫秽物品行为，相关主体涉嫌构成传播淫秽物品牟利罪。

6、数字暴力的类型演进及其法治因应（蔡艺生）

来源：《政治与法律》2026年第8期

数字暴力是数字权力的异化与极端形态，是缺乏正当程序约束、导致系统性不公正的负面面向。其本质上是行为主体依托数字技术架构实施的系统性支配行为，其形态演进呈现清晰的类型谱系：从基于主观恶意、表现为离散侵害事件的“个体交互型暴力”，演化为嵌于算法系统、批量生产不公的“系统操纵型暴力”，并最终沉降为平台基于垄断地位行使“准公权力”的“基础控制型暴力”。这三类暴力叠加共生，对以明确行为主体、主观过错及直接因果关系为核心的传统归责与救济范式构成结构性挑战，暴露了私主体“社会权力”扩张引发的宪制性危机。为此，法律必须实现从“规制行为”到“驯化权力”的范式转型，并采取分层分类的因应路径：针对“个体交互型暴力”，应优化传统工具并强化执行效能；针对“系统操纵型暴力”，须构建算法问责制与新型权利体系；针对“基础控制型暴力”，需以公法原则约束私主体的“基础设施”权力，施加透明度、正当程序及互操作性等特殊义务；针对这三类暴力叠加而形成的复合危害，则应构建协同治理与穿透式监管机制。

7、“数字人大”视域中基层立法联系点意见征集智能化——理论逻辑、制度进阶与风险规制(程龙)

来源:《政治与法律》2026年第8期

基层立法联系点作为全过程人民民主的立法民意“直通车”,在完成初步信息化后,仍面临民意吸纳压力大、反馈链条不顺畅、参与样本覆盖失衡等现实困境。在数字人大视域中推动意见征集从信息化转向智能化有助于这些问题的破解。数字人大是数字民主理论在人大制度中的具体展开,其对基层立法联系点意见征集智能化的赋能,主要体现在吸纳、回应、覆盖三个方面。智能化建设需要打造公众参与端、联系点业务端和立法机关决策端的“一体三端”平台,通过画像推送、自然语言处理技术转译、虚实融合录入和可视化反馈,形成吸纳、回应、覆盖相衔接的治理闭环。智能化也可能引发个人信息过度处理、算法偏见、技术黑箱和履职空心化等风险。对此,应以负责任人工智能理念为指导,落实最小必要、去标识化、算法透明、人工兜底和合规问责机制,推动意见征集走向人机协同。

人工智能治理

1、人工智能代理的权力分配逻辑与刑事责任归属(姚万勤)

来源:《政法论坛》2026年第4期

人工智能刑事责任归属事关人工智能技术的风险分配与开发应用。归属得当则利于社会发展,归属不当则妨碍技术进步。既有关于人工智能刑事责任归属问题的理论研究,主要遵循能力分配逻辑:人工智能具有某种能力则应当成为刑事责任主体,反之则不能。该类研究视角隐含了能力具备即等同责任承担的逻辑预设,忽视了事实判断与价值判断的休谟鸿沟。对人工智能刑事责任归属的分析应当从既有的能力分配逻辑转向权力分配逻辑,因为权力分配可以直接影响刑事责任的归属。在价值论层面,人工智能不能拥有与人类平等的主体资格,因而人类与人工智能之间的权力分配,应当采取人工智能不能直接独立进行行动,只能代理人类之后进行

行动的人工智能代理模式。人工智能代理刑事责任的归属对象是人工智能所代理的被代理人,因而人工智能体本身不能成为刑事责任主体。以自动驾驶汽车交通肇事为例,因人类驾驶员拥有主动接管权的基础,原则上应被视为所有等级自动驾驶汽车的被代理人,在此前提下才可能构成交通肇事罪,而生产者则在此基础上才需考虑承担刑事责任的可能性。

2、人工智能时代的规范延迟:问题与应对 基于法哲学视角的考察(舒国滢)

来源:《中外法学》2026年第4期

人工智能技术狂飙背后潜藏着多重结构性挑战,它使人类现有的法律、伦理等规范跟进速度迟缓,难以穿透人工智能设计、生产和应用的全链条进行监管,由此产生调整滞后的规范治理时间差,甚或治理真空,此即所谓“规范延迟”现象。这需要我们审视有关“人工智能作为对象的治理”和“借助人工智能的治理”这两种治理类型,考察它们在人类现实生活中展现的相互交错关系,设计既尊重人类基本价值、又能发挥人工智能治理潜在效能的“人主机辅”“人一机规范协同”的秩序与规范世界图景。如果未来强人工智能(通用人工智能及超人工智能)在模拟人类的“意识”上真正实现了实质性的技术突破,则如何让人工智能变得更加安全便应当成为人类社会在发展和使用人工智能技术时的首要考量因素。我们应建立一种“安全防御”的新型治理范式,有必要将“人类主导权原则”和人类“不可让渡领域”以代码形式直接强制写入所有强人工智能系统的底层架构,确保最终撤销权与解释权属于人类本体。

3、人工智能刑事责任主体制度的重构(赵东)

来源:《现代法学》2026年第3期

人工智能刑事责任主体地位的确立,应当摒弃“自由意志+刑事责任能力”的拟人化认定标准,基于人工智能的技术属性,以“可评价和检验的自主行为能力”为核心,构建“自主决策能力+行为支配能

力+风险识别能力”的规范认定结构。在立法层面,应综合考量当前人工智能的技术能量、技术特征、应用实效与发展阶段,从控制必要性、控制强度和控制时机出发,采取刑事立法适度先行的规制策略,以回应人工智能技术福利与智能化风险之间的“科林格里奇困境”。在刑事归责模式上,伴随着“自然人→人工智能体”,刑事责任主体实现了人权主体性向社会工具性的角色转换,基于社会防卫论立场,对于人工智能犯罪,可采取客观事实归责模式下的严格责任论,以“过错推定(实体法的层面)+举证责任倒置(程序法的层面)”为严格责任认定模型,并配套设置以科技风险防范为核心内容的技术保安处分措施。

4、人工智能算法可专利性的判定逻辑与规则优化 (余力烱)

来源:《现代法学》2026年第3期

传统的专利客体严格构建在对技术方案的认知逻辑上。以专利来保护人工智能算法存在根本性的问题,即人工智能算法是否具有可专利性及如何判断其可专利性。由于抽象思想不是技术方案,而人工智能算法是技术属性与思想属性相互融合的整体,故其难以被界定为传统的专利客体。因此,人工智能算法可专利性的深入讨论将面临客体适格性与算法特征之间的冲突,这使人工智能算法在新颖性、创造性和实用性等专利授权要件上与传统技术方案相比存在特殊性。分析人工智能算法可专利性的判定逻辑,有利于厘清算法专利的认知体系,突破专利保护的规则局限。只有结合人工智能算法特性对可专利性判定的拟制主体及规则进行适应性调整及重构,才能合理维持算法专利的创造性高度,实现人工智能算法技术创新与权利保障的协同发展。

5、论人工智能模型开源的双层治理结构——以版权许可与平台规则为建构(辜凌云)

来源:《清华法学》2026年第4期

人工智能模型开源正在改变技术演进与产业创新的底层逻辑,其创新开放的客体已从传统的软

件源代码扩展至模型代码架构、参数权重、应用工具包及数据集等多元内容,并形成了传统开源许可证与 Llama、RAIL 等为典型的新类型开源许可证共存的局面。现有对开源行为及许可证的治理思路仍停留于传统代码开源时代形成的静态的版权侵权判定与责任分配模式,而忽视了新类型许可证条款中对版权权利的设计与分配,特别是版权的行使由原本的单次授权重新配置为附条件解除并受持续约束的授权模式。在模型权重等可版权性存在争议的客体上,平台规则通过技术与合同手段填补了版权权利未能控制的部分,由此形成“版权许可+平台规则”双层治理结构。基于行动者网络理论,这一结构揭示了许可证与平台规则作为非人行动者在权利设计、分发与许可中的关键作用,通过网络效应驱动、成本结构重置与分层竞争三大逻辑,使得版权权利的让渡能够被转化为显著的市场竞争优势,形成闭环的利益转换体系。针对数据与代码贡献激励减弱的现状,可构建与权利分配相适应的收益反哺机制,通过优化许可证与平台规则价值链体系,建立起涵盖企业、社区、贡献者多主体参与的开放版权协同治理机制,以实现人工智能模型开源生态中知识共享与商业利益的动态平衡。

6、人工智能一人公司的公司法规制(陈洪磊)

来源:《东方法学》2026年第4期

“单人+AI”的人工智能一人公司作为一种新型创业范式,正在重塑我国的企业组织形态,其镌刻着股东有限责任的制度基因与促进民营经济发展的社会经济需求,在数字技术赋能的基础上,具有效率高、成本低等优势,已在我国各地广泛兴起。人工智能一人公司以一人公司为法律载体,具有明显的劳动雇佣资本、经营管理高度智能化以及企业家中心主义突出等特点。既有的公司法规制体系仍以传统商事主体为规制原型,未能供给充足且适配的激励性机制与约束性机制,难以实现人工智能一人公司的健康可持续发展。为此,在激励机制端,于准入方面,应当缓和公司住所的登记限制,允许人力资本作价出资;于运营方面,应当为人工智能参与公司治理

预留制度通道,搭建适配人工智能一人公司的多元融资渠道;于退出方面,应当调试公司简易注销制度,激活歇业制度,创设人工智能一人公司极简注销机制。在约束机制端,应当强化人工智能一人公司内部的监督力量,要求创业者承担促进企业社会责任实现的义务和监督“数字员工”的义务,落实内部主体的个人责任。

7、人工智能贸易的 RTA 区域治理范式:挑战与应对 (谢迪扬)

来源:《东方法学》2026年第4期

人工智能贸易是以人工智能本身为标的的贸易活动,现已发展出人工智能技术贸易、服务贸易、货物贸易和综合贸易四种类型。人工智能贸易的 RTA 区域治理范式可归纳为“要素化治理”,即通过知识产权、数据、硬件产品等条款,规制人工智能“三驾马车”(算法、数据和算力)的跨境移转。在贸易治理重心从多边向区域转移的大背景下,这一范式具有突出的重要性。对主要 RTA 人工智能贸易相关规则深度的评估表明,RTA 治理范式面临“俱乐部式”“不完全”和“碎片化”三重挑战,不仅影响中国人工智能产业与贸易的发展以及国际规则制定权竞争,更会使国际社会陷入“智能鸿沟”加速扩大的被动局面。我国可以以制度型开放为引领,深化数字包容性的双多边规则构建,健全人工智能贸易中算法、算力等新议题的治理机制,构建具有中国特色的 RTA 人工智能专门性条款或章节,以完善的法治助力全球人工智能贸易行稳致远。

8、人工智能版权训练数据来源合法性的规范构造 (徐小奔)

来源:《法学论坛》2026年第4期

人工智能模型开发者在使用他人作品作为训练数据进行模型训练时,应基于尊重在先权益原则,承担通过合法来源获取版权训练数据的注意义务。在鼓励 AI 开发者与版权人达成合作以激励更多训练数据高质量供给的规范目标下,版权训练数据来源合法性具有重要的实践意义,是版权合理使用

“三步检验法”中“不得不合理地损害著作权人的合法权益”要件的重要判断因素。因此, AI 开发者应在合理的技术成本范围内,积极承担版权训练数据获取的手段披露义务、模型训练目的的说明义务和数据溯源的辅助标识义务等三项基本义务,由此更好地提升版权训练数据的来源合法性。

9、生成式人工智能对法律职业的解构与重塑 (王迎龙)

来源:《法学论坛》2026年第4期

以生成式人工智能技术为代表的新科技革命的迅猛发展,促进了科学技术与法律场域的深度融合,推动了法律职业的结构性质重塑。生成式人工智能的技术特征与加速迭代,正在解构传统法律知识生成范式,打破了法律职业赖以存在的知识垄断,实现了从以“人”为中心向以“算力”为支撑的法律知识生成范式的转型。在法律知识范式进化与革命的影响下,法律服务模式由信息辅助向算法决策发展,使得市场主体间的差异格局被重新界定,法律服务市场“割据化”现象进一步加剧。基于上述变革,生成式人工智能的强势介入一方面对法律职业化及其理论提出挑战,消解了以劳动分工与专业技能为基础的法律职业化,一定程度上降低了法律职业自主性,影响了不同职业主体间的职业地位;另一方面也为高质量法律服务的发展提供了契机。在恪守法律职业者价值判断主导地位的前提下,构建与完善人机交互的法律服务模式,是新科技革命时代法律职业得以高质量发展的未来路径。

10、智能体时代授权的逻辑限度与法律建构 (李汶龙)

来源:《法学论坛》2026年第4期

以大模型为基础的智能体正在重塑人机协作与任务执行方式,其在开放环境中自主拆解目标、调用工具并跨系统执行操作,使传统基于单一行为、单次授权的逻辑面临挑战。我国《智能体规范应用与创新实施意见》已将用户授权范围、决策边界、行为追溯以及用户最终决策权置于智能体

治理的核心,但现有规范有待从原则层面进行细化,对复杂授权关系中的行为归属与责任分配进行系统回应。本文提出应超越以自然语言为中心的授权表达,转向以机器可执行的权限边界与能力约束为核心的结构化治理机制。在分析智能体场景下授权载体不充分、授权表达不清晰、授权主体不显明以及授权后果不可控等困境基础上,提出以授权辅助、权限控制、外观管理、公平交互与责任承担为核心的智能体授权治理框架。责任配置亦需从用户授权转向服务提供者的结构性责任,通过可追溯性、可中断性、偏离控制与授权链条管理等制度工具,实现从授权证明到责任映射的转型。只有在授权表达机制与责任体系同时重构的前提下,智能体经济方可成为可控可持续的制度基础设施。

11、论人工智能立法中的国家安全原则及其制度跟进(张先贵)

来源:《政治与法律》2026年第8期

在人工智能相关立法中,国家安全不仅是科技安全与技术发展的平衡点,而且是实现技术自主与战略部署所必需。因为其维护传统价值观和意识形态的功能,人工智能立法应明确国家安全作为基本原则的地位,这不仅是由其承载的独特功能所决定的,而且是其体系上的应然定位。此外,在国家安全原则之体系表达上,应确保规范内容与国家安全理念一致,遵循“总-分”结构,并协调其与发展价值、效率价值、自由价值之间的关系。从目前来看,设立基于行业伦理和底线伦理的综合伦理审查制度,在不同应用领域推行以参数为标准的用途管理制度,明确责任主体和责任类型的场景化类型,以及“政策+市场”双轨制保险制度,是人工智能立法中国家安全原则得以有效实现的重要制度支撑。

网络平台治理

1、平台数字权力对公共领域的技术解构与法律规制(梁西圣)

来源:《华东政法大学学报》2026年第4期

人工智能技术与平台资本耦合,孕育出兼具技术垄断与治理权能的平台数字权力主体。这类主体凭借对数据、算法与架构的排他控制,以格式协议、算法黑箱与流量治理取代公开的立法、行政与司法程序,导致公共领域私有化、公民权利商品化,民主协商所依赖的“主体间性”被系统性削弱。在将公共领域私有化和解构的过程中,平台数字权力不断打破传统治理框架下的权力平衡,动摇公权力通过民主协商机制获得合法性的基础。由此,权力完成了从授权到掠夺的嬗变,实现了从公共性向隐蔽公共性的转变,进而对公共领域既有权力(权利)结构造成破坏。对此,应强化公权力的监督和缓冲作用,建立对平台数字权力的人格化、可视化问责机制,限制平台数字权力在进入公共领域时的非公共性,促使其回归权力行使时的公共属性。同时,应以公权力方式实现对平台数字权力自我赋权的限制和约束,以算法“权利束”实现公民私权利与平台数字权力的平衡,恢复公共领域的应有属性,重构多元主体的理性对话机制。

2、数智时代版权侵权平台责任判定的权责匹配逻辑(管育鹰)

来源:《中外法学》2026年第4期

版权法是维系多方利益平衡的法律框架,“先授权再使用”规则一直支撑着内容产业的健康发展。信息技术的快速更迭改变了传统的内容产业链,互联网发展初期对仅提供技术服务、不介入版权内容经营的平台中立性之假定,已不适用于数智时代越来越多以技术控制内容生产和传播、以流量分成作为营收的多功能综合平台。基于“避风港”规则适用在我国遭遇多重困境和平台“注意义务”标准设定无法形成共识的现实,结合数智技术掌控者已深度介入和实质性控制内容产业运行的实际,应更新平台版权侵权责任判定的理念,依权责匹配逻辑按“技术—市场”控制力高低,分层判定不同类型平台的侵权责任,尤其是基于用户协议直接控制用户内容传播并以此获利的平台之替代责任。

3、数字平台权力行使的正当程序研究（罗英）

来源：《中外法学》2026年第4期

如何规范平台经济健康有序发展是重要的时代命题。面对数字平台巨大的事实权力,仅为其设置实体义务不足以保护平台用户的基本权利,正当程序原则于此具有适用空间。平台的事实权力在规范层面或归入行政法上的第三方义务,或归入私法上的用户协议和安保义务。在前一种情形下,平台履行第三方义务是行政机关进行利害调整的环节之一,受到基本权利的直接拘束。利害调整的不同环节均需适用完整的正当程序原则,不同利害调整环节下的具体程序规则存在差异。在后一种情形下,程序规则根据利益分布状态进行个案调适。在平台为一方当事人的双边关系中,程序设置需要对称衡量平台与用户的基本权利,通过特定程序化解基本权利冲突;在平台居中处理用户纠纷的三边关系中,程序设置以平等对待为核心。

4、人工智能时代网络平台的版权安全保障义务（杨依楠）

来源：《法商研究》2026年第4期

通过在推荐、搜索、创作辅助等环节部署人工智能,网络平台正经历数智时代的技术转型与服务升级。人工智能驱动的网络平台服务易产生为侵权内容分配更高流量权重、诱发用户浏览侵权内容意图等问题,传统的被动注意义务规范已无法满足版权侵权治理的需要。为网络平台设定版权安全保障义务更契合技术中立思想下的利益平衡原则,可以较好地兼顾人工智能技术创新与版权保护,且具备充分的规范依据。网络平台版权安全保障义务具有多重来源,可依据所部署人工智能的种类及潜在风险,为网络平台灵活配置情境识别与行为引导、算法评估与修正、版权过滤以及作品数据收集等具体义务。在义务边界认定方面,应在保留侵权事实明显性标准的同时,结合人机协同的治理模式变化灵活调整认定标准。应通过优化举证规则、厘清法律责任等途径,构建面向人工智能时代的网络平台版权注意义务体系。

智慧行政与智慧司法

1、数字政府中正当程序的底层逻辑与重塑路径（彭涛）

来源：《法商研究》2026年第4期

数字政府的运行依赖于人工智能技术,而人工智能在世界运行规律、认知模式和决策模式上都与传统政府存在根本差异。这些差异意味着,传统正当程序虽然能够约束政府权力,却难以约束数字政府中的算法权力。人工智能在三个层面影响传统正当程序。一是人工智能基于相关关系运行算法,传统正当程序以因果关系审查权力正当性,这一冲突弱化了审查效果;二是人工智能对社会整体结构、人类价值判断和社会网络的认知出现化约错误,数字政府据此容易作出错误决策;三是人工智能的决策包含难以解释的“暗知识”,弱化政府决策的理性程度。重塑正当程序的路径包括:首先,要审查三种类型的相关关系,以减少相关规律对程序正当性的弱化;其次,在涉及社会事实的决策中排除自动化决策,以减少认知错误对决策正当性的弱化;最后,扩张正当程序的规制范围,设置数字政府的三种强制性算法解释义务,减少人工智能对公共权力行使及决策正当性的影响。

2、科技创新促进中政府行为的法治边界与制度优化（彭诗程）

来源：《东方法学》2026年第4期

在加快实现高水平科技自立自强、发展新质生产力的背景下,政府在科技创新促进中承担制度供给、资源配置、公共服务和风险监管等重要职责。科技创新的有效推进,既有赖于市场在资源配置中的决定性作用,也离不开政府在基础研究支持、创新环境营造和制度保障等方面的积极作为。政府在介入科技创新的过程中,其行为模式可以归类为管理型政府行为、调控型政府行为以及赋能型政府行为。政府促进科技创新的法治化路径,需以习近平法治思想为指引,遵循科技创新规律和市场运行规律,在法治轨道上合理界定政府权限边界,优化政府服务科技创新的职责配置,进而提升国家创新体系整

体效能,为科技强国建设提供坚实法治保障。

新技术的法律规制

1、物联网产品网络安全缺陷的产品责任与公法规制（李钊）

来源：《法商研究》2026年第4期

物联网产品因网络安全缺陷而造成人身或财产损害时,生产者责任恰落在《网络安全法》的行政监管义务与《产品质量法》的产品责任之间,受害人难以索赔。这一问题源于传统产品责任制度所暗含的“完成性”预设,即产品在交付时属性固定,生产者责任以交付为限。物联网产品的“生成性”瓦解了这种预设。生产者在交付产品后,仍能通过网络连接持续塑造产品的功能与安全状态,对产品的控制力并未随其交付而消失。因此,对物联网产品的产品安全规制应在时间上延及全生命周期,在内容上自物理结构延及网络领域。网络安全是产品应当具备的安全品质,包含信息机密、系统完整与功能可用三项规范要求,可据此认定产品缺陷、设定公法义务。其中,网络安全缺陷致人身损害或缺陷产品以外的其他财产损害的,依产品责任制度追究损害赔偿,以功能主义标准界定产品范围,并限缩免责事由。持续维护产品网络安全能力的供给性责任则不以损害为前提,而应由公法经全生命周期义务与基于风险分级的合规机制予以确立。

2、适老化具身智能“监护”与生活安宁权的冲突及调适（杨睿）

来源：《东方法学》2026年第4期

具身智能与养老服务的深度融合旨在应对人口老龄化背景下的护理资源供需失衡,但具身智能的全时段物理在场与拟人化凝视对老年人的物理空间、精神安宁及行为自由构成实质性干预,形成了生存安全刚需与生活安宁保护的深层张力。在涉及生命救助的紧急监护场域下,知情同意规则因生存依赖而面临适用局限,相关主体基于避责动机实施过度监管,侵权责任认定亦面临定性、损害后果量化与因

果证明等多重难题。化解此种冲突需通过精细化的法益衡量,构建基于法益位阶的动态平衡机制。应确立人格尊严的基础性规范边界,以最小伤害原则界定技术干预的合理限度,并构建场景分级治理机制:在紧急救助场景确立生命法益绝对优先,在常态化监护场景回归安宁法益优位。同时,通过配置物理阻断功能以强化技术正当程序,并建立责任豁免机制以缓解产业界的风险压力,最终实现老年人权益保障与数字技术发展的协同演进。

3、论对区块链的法律介入——以作为修辞的去中心化作为研究起点（李志颖）

来源：《东方法学》2026年第4期

法律如何介入区块链是法律与区块链法理研究的基本议题。该议题以“作为修辞的去中心化”为研究起点,可以导向法律如何评价区块链引发的权力科层结构改变这一研究思路,并为法律如何介入区块链提供融贯的理论框架。若法律对权力科层结构的改变持消极评价,则会抑制这一结构的改变,从而形成对区块链的监管逻辑;若法律对权力科层结构改变持积极评价,则会接受这一结构的改变并协同区块链演进为新的法律秩序,进而形成对区块链的协同逻辑。此外,该理论框架还能与法规范的性质相匹配。在法律表达上,监管逻辑侧重对风险的处理,而协同逻辑则侧重对新权力科层结构的安置。由此,该理论框架既能融贯地解释当下区块链法律实践,亦能指导未来区块链法治的发展。

4、语言游戏视角下元宇宙的个性化法律是否可能?（翁壮壮）

来源：《东方法学》2026年第4期

元宇宙由概念叙事转入沉浸式平台并对权利义务进行差异化配置,使个性化法律看似具备可能性。但问题的核心不在于技术能否实现,而在于法律作为语言游戏所依赖的语用前提是否仍得到满足。法律并非命令集合,而是在共同体中被使用的规则体系,其具备公共性、可追随性与语境依赖性,并通过规则使用者的理由交换构建语用共同体。元宇宙中,个性

化法律加剧了规则个性化与规则共同性之间的悖论,规则的差异化生成机制导致规则意义不可通约。此时,既有规范的“行为—后果”链条被模型的“输入—输出”逻辑改写,法律交往结构也因此趋于静默。通过克服元宇宙法律制定与实施的沟通障碍,划定个性化法律的容纳边界,并借助程序性机制重构与法治化安排,可使个性化法律回溯于公共规则与公共理由。否则,所谓个性化法律将徒具法律之名,而在实质上沦为针对个体的情境化指令,缺乏法律应有的品格。

5、人机共驾交通事故侵权的归责难题与破解（徐振华）

来源：《法学论坛》2026年第4期

随着自动驾驶技术的快速发展,人机共驾模式下的交通事故侵权归责问题日益凸显。在责任主体层面,自动驾驶系统的技术局限性决定了驾驶员作为“操作者”的法律地位,但其与系统开发者的权责划分仍存在争议;在过错认定层面,过错认定的复杂性源于智能驾驶技术链条的多元参与主体及其交互影响。为了应对该新型归责难题,需要通过法律定位、技术缺陷分析及风险分配,构建驾驶员为“操作者”、开发者与制造商承担产品缺陷责任的归责体系。同时,须按自动化等级梯度配置差异化的归责原则。

6、自动驾驶的业态发展与风险管理：基于实质刑法观的展开（赵龙）

来源：《政治与法律》2026年第8期

自动驾驶技术的发展促进了自动驾驶业态的形成,自动驾驶技术正处于从实验测试阶段走向规模化商业应用的关键过渡期,需要基于鼓励科技创新、促进产业发展和保障公共安全三方平衡的目标,构建自动驾驶多主体注意义务体系、归责体系和出罪体系。基于实质刑法观理论,应以“技术-解释-立法”的渐进模式作为自动驾驶业态发展中刑法治理的基本逻辑。对涉L3、L4等级及以上自动驾驶过失犯罪构成要件要素及主体的注意义务应进行实质

化认定,现阶段应以一般过失犯罪的实质解释实现涉自动驾驶风险行为入罪的合法性。在出罪体系层面,依托实质可罚性理论,以前置程序出罪、因果关系中断出罪以及紧急避险的实质化解释,构建阶梯化的合理出罪体系。通过技术理性嵌入规范理性的范式,在风险预防与技术发展之间确立刑法的介入程度,为技术创新留出必要的容错空间。

数据法学

1、数据跨境治理的充分性认定制度——基于欧盟范式的批判性审视与中国因应（汤净）

来源：《法商研究》2026年第4期

数据跨境治理中的充分性认定制度,已从《欧盟通用数据保护条例》所确立的技术性数据保护工具演变为全球数字治理领域的重要制度范式和权力博弈载体。该制度虽然以保障数据出境安全、促进数据跨境自由流动为初衷,但是其充分性标准的模糊性及评估程序的非公开性,导致该制度在实践中被高度政治化,沦为制度输出国延伸数字主权、塑造他国数据规则的单边政策工具。这种政治化操作不仅可能导致新型数字贸易壁垒,与有关国际经贸规则产生冲突,而且可能对发展中国家的制度自主权构成挑战,固化南北国家间的数据鸿沟进而侵蚀发展中国家的发展权,并通过其“俱乐部效应”加剧全球数据治理体系的碎片化。面对这一格局,中国不宜简单模仿或寻求加入欧盟主导的制度体系,而应在深刻把握自身数据跨境治理底层逻辑的基础上,通过制度竞合与替代路径实现规则对接,最终推动建立更加公平、包容的全球数据跨境治理秩序。

2、个人信息单独同意的法理基础及其权利适配（龙松熊）

来源：《政治与法律》2026年第8期

单独同意是一种增强的同意方式,单独同意的增强并不体现在形式上的增强,而是体现在知情权的保障。个人单独同意中的充分知情是实然的充分知

情。单独同意中，个人信息处理者应当采取必要措施保障个人完全知晓个人信息处理规则。单独同意不需要采用书面形式，甚至不需要采用明示同意的方式。单独同意后，个人查阅复制个人信息应当免费，个人信息处理者应当提供便捷的查阅方式且在最短时间内提供个人信息。在同意撤回中，撤回单独同意与撤回概括同意所导致的损害赔偿规则应

当区分对待。基于个人信息处理者取得同意的成本和进行同意时知情权保障的不同，个人对撤回单独同意所产生的损失应当承担赔偿责任，但只限于信赖利益损失。个人撤回概括同意后不需要承担损害赔偿，但应返还基于概括同意所获得的利益。

（技术编辑：毕坤阳）

教研活动

Andreas Sattler 教授：欧盟《数据法》及其对商业秘密保护与竞争法的影响

2026年7月10日，由中国人民大学法学院、未来法治研究院、知识产权学院、世界知识产权组织(WIPO)中国联合主办的学术讲座在明德法学院楼502教室线上线下同步成功举办。本次讲座由卡尔斯鲁厄理工学院(KIT)信息与经济法研究所 Andreas Sattler 教授担任主讲人，中国人民大学法学院助理教授孙靖洲主持，法学院博士生田雨阳参与与谈。



卡尔斯鲁厄理工学院(KIT)信息与经济法研究所教授 Andreas Sattler

在主题演讲中，Andreas Sattler 教授开展题为“欧盟《数据法》及其对商业秘密保护与竞争法的影响”的专题讲座，讲座围绕中欧数据治理模式差异、数据访问权与商业秘密保护之间的冲突等问题展开深入讨论，系统地从数据的结构、句法、语义三个层面，以及数据非竞争性、无损耗性等经济特征出发，分析了数据治理中的关键问题。他指出，语义层数据与个人信息、商业秘密密切相关，是数据监管与创新利用的核心领域。同时，教授结合数据孤岛等现实问题，介绍了欧盟《数据法》的立法背景，并对比了中欧数据治理路径的差异。他指出，欧盟《数据法》并未创设新的数据财产权，而是以物联网使用者的数据访问权和使用权为核心，建立了“设计即访问”、第三方数据共享以及云服务商切换等制度，并通过标准化合同条款促进数据流

通。例如，在 B2B 场景中，德国汽车协会(ADAC)代表会员向汽车制造商请求车辆数据，就是数据访问权实践应用的典型案例。与欧盟路径不同，中国依托数据产权束理论，探索构建数据资源持有权、数据加工使用权和数据产品经营权相分离的“三权分置”制度，以协调数据来源者、处理者和经营者之间的权益关系。随后，Andreas Sattler 教授重点讨论了欧盟《数据法》实施中的主要矛盾，即数据访问义务与《通用数据保护条例》(GDPR)个人信息保护、企业商业秘密保护之间的协调问题。他指出，物联网数据往往难以明确区分普通个人数据与敏感个人数据，相关数据集可能受到更严格的隐私保护。企业可以通过保密协议(NDA)、技术保护措施等方式支持数据共享，但当数据开放可能导致重大经济损失时，企业仍可拒绝披露相关商业秘密。此外，教授还结合全球云服务市场的发展情况，介绍了欧盟关于云服务商切换的相关规则，包括转换期限、费用限制、迁移标准以及失败处理机制等。他认为，中欧均面临语义层数据流通与保护之间的平衡难题，未来需要借助数据分类识别工具、智能合约等技术手段，实现数据利用、隐私保护与商业秘密保护之间的协调。

在互动环节，博士生田雨阳提问：欧盟《数据法》确立的数据访问权在实践中主要由哪些主体行使？普通用户是否会主动利用该权利？Andreas Sattler 教授回应，普通消费者可能由于数据价值认知不足、行使成本较高等原因，并不会频繁主动使用数据访问权。但在 B2B 场景下，数据访问权具有更明显的实践价值。例如，德国汽车协会(ADAC)曾代表会员向汽车制造商请求获取车辆相关数据，体现了消费者组织代为行使数据访问权的典型模式。未来，随着数据价值不断提升，数据访问权可能更多通过行业组织、专业服务机构等方式实现。

本场讲座系统厘清了中欧数据治理制度层面法律适用难题，讲座在热烈的学术讨论氛围中圆满落幕。

John F. Duffy 教授：人工智能时代姓名与肖像的财产化

2026年7月14日，由中国人民大学法学院、未来法治研究院、知识产权学院、世界知识产权组织（WIPO）中国联合主办的“人工智能时代姓名与肖像的财产化”学术讲座在明德法学楼402教室成功举办。本次讲座特邀美国弗吉尼亚大学法学院塞缪尔·H·麦考伊二世（Samuel H. McCoy II）法学教授 John F. Duffy 担任主讲人，中国人民大学法学院副院长丁晓东教授主持，中国人民大学法学院金海军教授、中国人民大学未来法治研究院执行院长张吉豫教授担任与谈人。

Duffy 教授在演讲中围绕姓名、形象与肖像（Name, Image and Likeness, 简称 NIL）权利的财产化趋势，从产权理论出发，系统考察了这一新兴权利形态在全球多个法域的生成与发展。他指出，当前美国、中国、欧洲等多国正尝试赋予个人对自己的形象、姓名、声音乃至数字画像以财产性权利，这是一场正在发生的制度变迁。Duffy 教授以丹麦一度拟议并原定于2026年7月生效的版权法修订为例，说明该国试图将“逼真的数字模仿”纳入版权保护，且保护范围不限于表演者，普遍适用于每一个自然人；尽管该法案因议会选举等突发政治变数尚未生效，但已清晰折射出财产权路径的立法意向。实践中，OpenAI 等商业机构已主动承诺移除未经许可使用他人肖像的内容，而美国大学体育协会（NCAA）运动员的 NIL 权利诉讼（如杜克大学运动员因转会引发的 NIL 权益纠纷），则进一步印证了财产权观念正在自下而上产生。



在理论层面，Duffy 教授援引哈罗德·德姆塞

茨（Harold Demsetz）的产权理论，认为当内部化外部性的收益超越成本时，新产权便应运而生。相较于德姆塞茨所依据的拉布拉多半岛原住民皮毛产权历史案例——该案例因缺乏文字记录、发展过程无从考证，且欧洲人同时带入文字和产权概念而产生“同时性”干扰——当下 NIL 权利的出现记录完整性、过程可观察性以及免受外部文化同时性干预等方面具有显著优势，为研究产权制度的涌现提供了更优质的样本。Duffy 教授还将 NIL 权利与商标权的历史演进进行类比，指出二者皆起源于政府强制要求（例如政府要求个人在护照、驾驶证等证件上提供姓名与肖像），早期均以侵权责任而非财产权形态存在，直至逐步被承认为独立的财产权；二者还面临着命名选择、多重品牌策略、名称冲突以及第一修正案（言论自由）限制等共同议题。他特别以 J.K. 罗琳（J.K. Rowling）使用笔名罗伯特·加尔布雷思（Robert Galbraith）创作成人侦探小说为例，说明个人如同企业，亦会采取多品牌策略来区隔不同受众群体。Duffy 教授强调，正是少数高度关注自身标识价值的个体与实体，推动了整个制度领域的转型。



Duffy 教授进一步对 NIL 财产权的未来发展作出了六项预判：立法与司法将逐步明确 NIL 的财产属性；许可与转让将日趋普遍；注册登记机制有望建立；以私人执行为主导的民事救济将更加活跃；人工智能技术降低了权利的界定与执行成本；以及，此类财产权有可能取代现行隐私法，为个人提供更有效率的保护架构。他以美国频谱财产权取代行政管制的历史为例，说明财产权范式能够以简驭繁，减少不必要的政府规制。



在与谈环节，**金海军**教授首先从中国民法典出发，指出中国现行法虽将姓名、肖像等定位于人格权而非财产权，但通过损害赔偿数额的差异化裁量，实际已承认了这些人格标识的财产价值。他进而就丹麦采用版权模式保护个人形象的做法提出商榷，认为商标路径或许更为顺畅。**Duffy**教授回应称，他起初亦倾向于商标进路，但后来意识到个人形象塑造过程中通常包含了最低限度的创造性，因此对丹麦的版权方案持开放态度，愿视其为一种差异化探索。



张吉豫教授则关注保护的层次性问题。她提问：针对人格标识的不同利用场景（如侮辱性使用、商业代言、仅供AI模型训练等），是否应赋予不同强度与范围的保护，以及此种区分能否被统合进**Duffy**教授所主张的财产权框架。**Duffy**教授回应指出，财产权制度的一个核心优势正在于其简化性——赋予权利人排他权，使其无需逐一证明自身利益类型，便可直接控制对自身标识的利用，从而避免复杂的个案权衡。他借自身物理学训练背景比喻道，正如科学偏爱从简单模型出发理解基本原理，法律规则亦当追求简明，以揭示制度的核心逻辑。

在随后的提问交流环节，现场同学分别就**NIL**权利边界模糊、美国**NIL**制度是否仅局限于**NCAA**运动员、以及个人数据多重法律规制下的界限等问题与**Duffy**教授展开互动。

Duffy教授逐一回应：其一，任何财产权均存在一定程度的不确定性，无论是专利权还是土地权利（他以自己购置房产后才发现边界标识有误的经历为例），模糊性并非**NIL**权利所独有；其二，**NIL**早已超出大学体育范畴，广泛应用于职业运动员和网络影响力者，实为全球性现象；其三，财产权范式有望以统一、简洁的规则统合当前庞杂的数据保护法律，正如美国历史上无线电频谱财产权替代了诸多繁复的行政管制。



丁晓东教授在总结中对**Duffy**教授富于理论与现实洞察的演讲表示感谢，指出讲座为思考人工智能时代人格标识财产化问题提供了重要比较法视角，并期待**Duffy**教授日后再度来访，深化相关研究议题的对话。

讲座在师生合影中圆满结束。

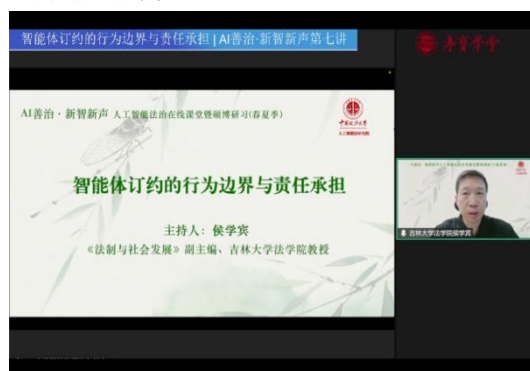


“AI 善治·新智新声”人工智能法治在线课堂暨硕博研习(春夏季)第七场

7月30日,“AI 善治·新智新声”人工智能法治在线课堂暨硕博研习(春夏季)第七场在线课堂顺利举办。本场活动由中国政法大学人工智能法研究院牵头,联合多所知名政法院校与科研机构共同打造,聚焦“智能体订约法律规制与治理路径”,通过线上研学形式,为全国硕博学子呈现了一场兼具前沿视野、现实关切与学理深度的学术盛宴。



本场在线课堂由《法制与社会发展》副主编、吉林大学法学院侯学宾教授主持。侯教授指出,随着智能体在交易场景中自主性的不断增强,其在订约环节引发的法律边界与责任归属问题日益受到关注。本场讲座围绕“智能体订约法律规制与治理路径”展开,从多重视角探讨技术演进与法律治理之间的协调路径。



《法制与社会发展》副主编、
吉林大学法学院侯学宾教授

主讲环节,华中科技大学法学院讲师李雅男以“智能体订约的行为边界与责任承担”为主题开讲。李雅男老师围绕智能体在订约场景中的角色定位与行为边界,梳理了当前实践中的若干核心议

题,并就责任承担的思路分享了自己的观察,为后续的深入研讨奠定了讨论基础。



华中科技大学法学院讲师 李雅男

与谈环节,三位与谈嘉宾从不同视角展开深度对话,观点交汇、精彩纷呈。

武汉大学法学院黄志雄教授从技术中立原则的角度切入,谈到随着智能体从被动工具逐步转向具备一定能动性的参与者,对于技术中立的理解或许需要随之调整,并认为“有意义的人类控制”的理念在智能体风险预防层面具有一定的参考价值。



武汉大学法学院黄志雄教授

北京理工大学法学院洪延青教授从公法视角出发,对智能体订约所处的“前合同秩序”提出了自己的观察,认为技术通道并非完全中性,相关入口的准入与限制已形成具有一定基础设施性质的治理安排,值得从公法角度予以关注与规范。



北京理工大学法学院洪延青教授

北京新橙科技有限公司(iCourt)法律AI研究院院长**李小武**结合产业实践与比较法经验,就现有法律框架的适用空间谈了自己的看法,认为既有合同法、侵权法等规则仍具有一定弹性;同时他也提到,面对不同技术路线下复杂的调用链路,责任归因仍是值得进一步探讨的现实议题。



北京新橙科技有限公司(iCourt)法律AI研究院院长 李小武

三位专家观点碰撞、思想交融,全方位、多层次丰富课程内涵,让在线研习的硕博研究生拓宽视野、深受启发。

硕博研习环节,来自西南政法大学的博士生**杨长元**、中南财经政法大学的博士生**薛少雄**踊跃发言。杨长元同学就不同技术路线导致的风险与准入差异问题向嘉宾请教,李小武院长回应指出,法律规制可更多着眼于智能体的自主决策程度与风险等级,尝试建立更具针对性的治理思路。

薛少雄同学围绕智能体能动性增强后技术中立原则是否仍具适用空间问题与嘉宾交流,黄志雄教授认为技术中立原则仍有其参考价值,但宜从更为动态、有限的视角加以理解。就公法注意义务如何转化为私法责任的问题,侯学宾教授表示,现阶段可更多从公法层面设定外部规则,并在具体司法实践中探索二者的衔接方式。

本场在线课堂的顺利举办,延续了“AI善治·新智新声”系列活动的学术品质,聚焦智能体时代的前沿法治命题,全国各地的硕博学子齐聚线上,在主讲与对谈中展开了一场有深度、有交锋、有启发的学术对话。未来,“AI善治·新智新声”人工智能法治在线课堂暨硕博研习系列活动将持续推出高质量学术内容,为硕博学子搭建与顶尖学者交

流对话的稳定平台,为促进人工智能法治研究、服务国家数字化发展战略贡献学术力量。

“个人信息保护的新发展”研讨会

2026年7月21日下午,由上海政法学院数智法学院(知识产权学院)主办的“个人信息保护的新发展”研讨会在上海世博桐森酒店成功举办。本次研讨会聚焦智能体与社交场景中的个人信息保护前沿问题,邀请来自上海交通大学、中国社会科学院、中国人民大学、上海社会科学院、西南政法大学、华东政法大学等高校和科研机构的专家学者,围绕个人信息保护的实践发展及其理论回应展开深入交流。

上海政法学院数智法学院(知识产权学院)院长、教授**曹阳**致开幕辞。曹阳指出,以生成式人工智能、AI Agent大模型为代表的新一代数字技术正以前所未有的速度重塑社会生活,数据作为核心生产要素在释放巨大经济价值的同时,也带来了数据安全与个人信息保护的严峻挑战。他表示,数智法学院(知识产权学院)始终立足“数智+法学”前沿交叉领域,致力于探索兼顾权益保护与数据流通利用的平衡机制,期待本次论坛为我国个人信息保护法治体系完善提供前瞻性思路。

本次研讨会分为两个专题,即智能体场景中的个人信息保护和社交场景中的个人信息保护。

专题一 智能体场景中的个人信息保护

本专题由**曹阳**教授主持。

上海交通大学凯原法学院院长、特聘教授**彭诚信**以《“推定”同意:人工智能背景下个人信息的保护与利用》为题作主题发言。彭诚信指出,传统《个人信息保护法》采用的“同意—无需同意”两分法过于刚性,在人工智能背景下存在“虚假合法性”“有效同意的幻觉”等困境。他提出了“推定

同意”(Prima facie consent)制度构想,即在处理活动遵守基本原则、经过正当程序评价且不对人格权益造成不利影响的前提下,法律暂时推定信息主体已作出有限同意。该制度填补了明确同意与法定许可之间的中间地带,构成“明确同意—推定同意—无需同意”的三层合法性基础体系,尤其为人工智能训练场景中个人信息利用提供了制度通道。此外,彭诚信强调,无论是个人信息保护问题还是其他数字法学问题,都应在数字社会背景下讨论,不能将其与传统线下社会面临的问题混为一谈。



中国社会科学院法学研究所网络与信息法研究室副主任(主持工作)、副研究员周辉以《智能体场景下的个人信息保护》为题展开分析。周辉指出,智能体技术使个人信息保护的风险焦点从“信息收集”转向“代理行动”,自主规划、持续记忆与工具调用构成新的制度增量,单一任务即可触发多次、跨主体的数据处理。他建议从治理视角构建智能体场景下的个人信息保护框架,关注智能体全链条中各主体的角色认定与义务配置。



中国人民大学法学院助理教授阮神裕就《智能体个人信息处理链的关系认定与责任配置》展开发

言。阮神裕提出,智能体系统具有复合性,包含智能体模块、基础模型模块和工具模块,其自主性带来多方主体参与和责任认定的复杂性。他依据“谁决定处理目的和处理方式”的实质标准,对部署者、智能体提供者、模型提供者和工具提供者的法律身份进行了系统界定,并指出《个人信息保护法》第20条至第23条的多方处理规则与《民法典》第1168条至第1172条的多数人侵权规则具有足够灵活性,挑战主要是实践性的而非理论性的。



在圆桌与谈环节,与会专家就智能体场景中个人信息处理的技术原理、智能体跨平台获取数据的法律规则、个人信息保护在智能体场景中面临的新挑战等问题展开了热烈讨论。周辉认为,智能体场景中各方主体的义务和责任配置须根据具体的商业模式来分别判断。阮神裕认为,智能体是否是个人信息处理者,与指令内容相关。若指令包含个人信息(如预订机票),智能体在传递信息过程中构成“提供-接收”关系;若指令不包含个人信息,则难以评价为个人信息处理者。此外,若存在多个主体涉及个人信息泄露但无法查明责任归属,法院可能认定相关主体承担连带责任。徐伟认为,对智能体全链条中各方主体的义务和责任,不必囿于先对主体定性再定义义务和责任的思路,而是可以直接根据最小成本防范等理念来确定主体义务和责任。

专题二 社交场景中的个人信息保护

本专题由上海社会科学院法学所副研究员孙大伟主持。



西南政法大学高等研究院院长、教授**郑志峰**以《数智技术下的个人信息保护——智能体、社会网络》为题发言。郑志峰提出，技术重塑了个人信息的认定标准——从人类识别到算法识别再到机器识别，并拓展了设置信息、关系信息等新类型。他同时指出，“越便利越难必要”“技术越复杂越难公开透明”，且个人信息保护基本原则的适用面临张力，并建议关注行业惯例和“机器法则、习惯法”作为可合理利用的补充依据。



华东政法大学中国法治战略研究院特聘副研究员**向秦**探讨了《智能化社交中的个人信息保护》。向秦指出，人工智能不仅处理用户提供的信息，还处理行为数据、推断数据和生成数据，个人信息的范围从“已公开信息”扩展到“可计算、可推断信息”。她还建议将《个人信息保护法》中的“目的限制”原则解释为“目的兼容性”检测，借鉴欧盟基于科研目的处理个人数据的最新实践。



上海政法学院数智法学院（知识产权学院）副教授**商建刚**围绕《小程序用户隐私条款展示方式合规性分析》作主题发言。商建刚结合《个人信息保护法》《网络数据安全条例》等法律法规，提出了小程序隐私条款展示方式的六阶段合规审查体系，涵盖首次进入告知展示、亮照界面展示、内容完整性审查、同意有效性审查、展示内容与实际处理一致性审查、用户权利保障与后续管理。他指出，合规审查最终需结合内容完整性、同意有效性、第三方共享披露、敏感信息单独同意、用户权利行使路径及实际处理一致性综合判断。



在圆桌与谈环节，与会专家围绕朋友圈信息公开性认定、半自动化模板隐私政策的有效性、隐私政策展示方式、数字人致害的责任等议题展开热烈讨论。商建刚结合最高人民法院相关判决指出，朋友圈发布的信息不宜一律认定为公开信息；隐私政策展示方式的有效性不应拘泥于是由平台抑或平台内经营者提供隐私政策，而是应重点关注信息主体是否能够充分了解隐私政策；关于数字人致害的责任分配问题，可采“链式责任”的分级规制思路。向秦基于“基础设施化的合规”理论提出，由平台提供的半自动化模板隐私政策有助于提升对用户的个人信息保护程度，应认可此类隐私政策的效力。上海交通大学凯原法学院博士后再高苒认为，当前智能体实践尚未严重挑战现行法律框架下的数据流通规则，但现行法的解释适用有必要结合智能体场景进行必要的反思。此外，现行法关于个人信息合规的要求对初创企业可能构成较重的负担。

会议总结

在总结发言中，徐伟教授从价值和议题两个方面做了总结。在价值方面，徐伟教授指出，与会专

家呈现出明显的共识，即普遍在探索适当放宽个人信息处理规则。这并非追求降低对信息主体的保护，而是反思既有规则是否仍然合时宜。在议题方面，与会专家重点就“智能体/人工智能对个人信息保护的影响”“智能体全链条中的各方主体及其义务和责任的配置”“告知同意规则在实践中的认定”等议题展开了深入探讨。智能体对个人信息的影响不仅体现在主体更多元导致的法律关系复杂化，也对个人信息保护的诸多基本原则带来了挑战。智能体全链条中各方主体的义务须根据场景来判断，主体间的法律关系则要基于是否满足共同处理、委托处理、提供接收等构成要件来判断。在告知同意方面，不宜拘泥于告知和同意的具体形式，而是应以是否有助于提升对信息主体权益的保护和实现数据价值释放为根本遵循。例如，平台在充分尊重平台入驻者（例如小程序开发者）意愿情况下，协助平台入驻者配置的隐私政策，可避免因平台入驻者的设计差异和合规水平差异导致的用户理解成本增加及违规情形，应当被视为平台入驻者作为个人信息处理者的有效隐私政策，认可其法律效力。平台统一设置四步内跳转隐私政策链接的路径，有助于用户在统一位置查看相关个人信息处理规则，保障用户个人权益。

本次研讨会实现了学者间的智慧碰撞，为个人信息保护制度的完善提供了丰富的理论资源 and 实践参考，取得了圆满成功。

Anupam Chander 教授：TikTok、Anthropic 案与美欧国家安全互联网的兴起

2026年7月14日，由中国人民大学法学院、未来法治研究院、知识产权学院、世界知识产权组织（WIPO）中国联合主办的学术讲座在明德法学院402教室成功举办。本次讲座主题为“TikTok、Anthropic 案与美欧国家安全互联网的兴起”，特邀乔治城大学法学院斯科特·K·金斯伯格（Scott K. Ginsburg）法律与技术教授 Anupam Chander 担任主

讲人。讲座由中国人民大学法学院副院长丁晓东教授主持，中国人民大学法学院金海军教授、未来法治研究院执行院长张吉豫教授、法学院助理教授孙靖洲担任与谈人。

主题演讲



乔治城大学法学院斯科特·K·金斯伯格法律与技术教授 Anupam Chander

在主题演讲中，Chander 教授基于其新近发表于《乔治城国际法期刊》的论文“国家安全互联网”（The National Security Internet）及系列研究，系统阐述了美欧互联网治理逻辑从“促进商贸的自由流动”向“防范国家安全威胁”的根本转向。他首先回溯了 2013 年斯诺登事件对世界的影响，指出该事件使各国政府普遍将跨境数据流动本身视为对国家安全的潜在威胁，而不再只是将其作为全球化经济的基础设施。Chander 教授认为，目前正在形成一种“国家安全互联网”，其核心诉求已超越一般的数据本地化，不仅要求数据在本地存储，更要求数据必须由本地公司控制和运营，以寻求“对外国管辖的免疫”。

为印证上述判断，Chander 教授以美国近年密集的立法与行政措施为例展开分析。在基础设施领域，美国斥资数十亿美元实施“拆除与替换”计划；在消费市场，美国国会于 2024 年底通过《国防授权法案》，大大抬高了应急救援等领域的成本，甚至被一线救援人员指为“事关生死”的问题。美国商务部还发布了“联网汽车规则”禁止中国整车进口，福特汽车等产业主体也公开批评该规则将增加成本、干扰全球供应链。Chander 教授将 TikTok 案视为上述逻辑的集中体现。他梳理了案件的立法与

司法进程：2024年4月，美国国会迅速通过一项旨在禁止 TikTok 或强制其剥离的法律；2025年1月，美国最高法院以一致意见驳回 TikTok 及其用户的宪法诉请。

Chander 教授指出，最高法院在裁决中刻意采取了一种“假定国会仅凭数据监控这一国家安全理由即可通过该法”的论证策略，回避了对立法过程中包含的限制外国言论这一更棘手的宪法问题的审查，从而使该法律得以维持。特朗普政府随后通过行政决定暂缓执行禁令，并推动由美国及阿联酋投资者组成的财团收购 TikTok 美国业务 80% 的股份，但 TikTok 全球平台仍深度参与美国版的电商与广告运营，这一安排本身具有鲜明的政治与商业博弈色彩。

在论及欧洲时，Chander 教授提醒听众注意一个历史性的内在矛盾：欧盟 1995 年《数据保护指令》以及后续的《通用数据保护条例》（GDPR）的正式标题均将“确保个人数据的自由流动”作为核心立法目的之一，但如今的执法现实却因数据跨境传输本身就对 Meta、Uber 等公司处以数亿欧元的巨额罚款，欧盟委员会自身也因使用微软 365 软件而被其下属的数据保护监督机构（EDPS）认定为违规。这种只要数据“触碰他国土壤”即视为违法的极端逻辑，在 Chander 教授看来，如果推演至极致，将导致国际贸易的全面停滞。美国近期生效的“大宗数据交易规则”，更授权联邦政府直接阻断达到一定门槛的数据流动，进一步强化了这一趋势。

面对上述困局，Chander 教授分析了企业的应对策略。许多跨国公司试图将自己塑造为“数字瑞士”（Digital Switzerland），通过数据最小化、加密、设立数据受托人、本地化存储乃至对抗母国政府的数据请求等方式，证明自身的独立与中立。他还通过 Solar Winds 攻击案强调，位于美国本土的公司同样会遭到外部渗透，所谓“数据由本地公司控制即可杜绝安全风险”的威胁模型难以成立，它忽视了网络安全的普遍脆弱性。因此，当前诸多措施存在成本高昂、收益高度不确定的问题。

Chander 教授最后提出，更务实的出路在于各

国修改自身的对外监控法律，明确限制对非本国公民的无差别监视，同时推行由独立第三方实施的网络安全审计与持续监控机制，以技术化的方式验证数据流是否依规处理。他特别警示应避免陷入“零风险谬误”——互联时代的本质决定了风险无法彻底消除，真正的目标应是在控制风险的基础上重建全球数字信任。

嘉宾与谈

金海军教授认为，本讲主题已远不止私法问题，而是触及公法与宪法层面的核心命题。他聚焦于 TikTok 剥离案的后续进展，发问当前由美国财团控股 80%、字节跳动继续提供技术支持的“德克萨斯方案”式的混合模式，究竟是一种可持续的良性方案，还是仅为一时的政治权宜，尤其是在美国政权更迭后可能面临更为严峻的挑战。



张吉豫教授高度赞扬 Chander 教授一贯的学术品格，将其比作爱因斯坦所比喻的“在最厚的地方钻孔”的研究者。她坦言自己对全球数字市场走向孤立与供应链失稳的现状并不乐观，但正因为此，探寻问题根源并寻找操作化路径的努力更显珍贵。她向主讲人提问：在当下大国间激烈博弈的地缘环境下，达成某种全球性的数字文明新秩序或协议，到底存在哪些可能的进路？



孙靖洲助理教授则从两个实践维度发问。其一，联网汽车的禁售不仅影响物理价值链，更因物联网的普及涉及海量数据的控制权，未来中国汽车在欧洲市场可能面临怎样的数据访问权争端？其二，企业若想成为真正的“数字瑞士”，相较于微软等巨头，中国科技公司应具备何种核心能力与战略举措？



开放提问环节

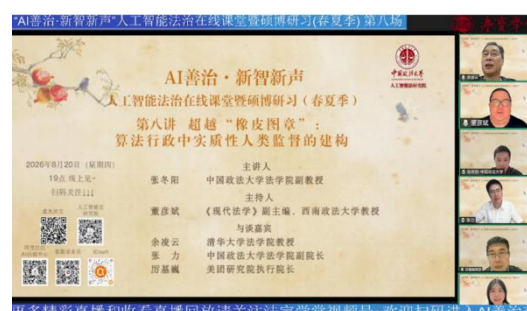
在开放提问环节，多名同学参与了讨论。有同学提出，美国联邦法院在 TikTok 案中以一个简略的“国家安全”理由便轻易绕过了对第一修正案的实质审查，其司法逻辑的专业性与中立性是否值得怀疑。有同学追问所谓外国平台操纵美国选举的担忧，在历史中是否有真实案例支撑。有同学以特斯拉在中国市场的成功为例，指出消费者对平台的选择似乎并未明显受安全风险的影响，安全考量与实际市场行为之间存在背离。还有同学就当科技公司实力足够强大时如何迫使其遵守当地法律等问题向教授请教。Chander 教授逐一进行了回应。他以巴西成功封禁并迫使 X 平台妥协为例，指出各国政府其实拥有充分的法律与市场权力，问题往往在于部分小国缺乏行使权力的技术认知或政治意愿。对于舆情操纵，他表示外国势力通过购买广告、控制信息流等方式干预选举是已知实践，但这并非必须依赖对平台所有权的控制才能实现。在“数字瑞士”的构建上，他指出最大的障碍之一恰恰来自母国——若美国政府直接持有 OpenAI、Anthropic 等企业股份，这些企业的独立性和全球可信度将大打折扣。面向未来，Chander 教授重申，建立由独立第三方执行的网络安全验证体系，是让跨国公司的产

品在全球范围被信任的关键路径，而这需要企业与政府超越“零风险”的幻想，共同致力于透明的、可审计的风险治理框架。

总结环节丁晓东教授在总结中感谢 Chander 教授以宏大的视野和深刻的洞察，为在座师生勾勒出国家安全互联网兴起的全景图及内在机理，并对各位与谈人的精彩点评和学生的踊跃提问表示赞赏。本次讲座在热烈的学术讨论氛围中圆满落幕。

“AI 善治·新智新声”人工智能法治在线课堂暨硕博研习(春夏季)第八场

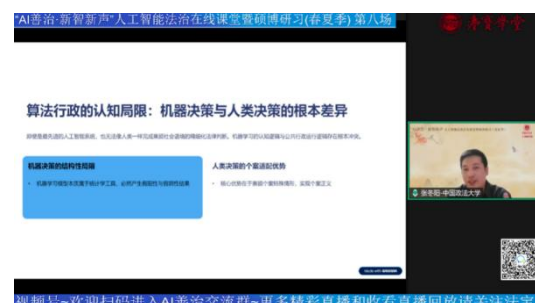
8月20日，“AI 善治·新智新声”人工智能法治在线课堂暨硕博研习(春夏季)第八场顺利举办。本场活动由中国政法大学人工智能法研究院牵头，联合西南政法大学科技法学研究院、华东政法大学数字法治研究院等高校科研机构，携手北京科技创新中心研究基地、AI 善治学术工作组，并获 iCourt 支持。在线课堂以“超越‘橡皮图章’：算法行政中实质性人类监督的建构”为主题，围绕算法介入行政决策后人类监督的正当性、失效风险与制度保障展开讨论，来自多所高校的专家学者、业界代表和硕博研究生在线参与研习。



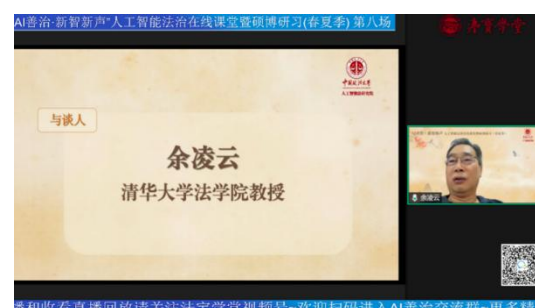
活动伊始，中国政法大学人工智能法研究院李筱璐老师介绍本场在线课堂的主题与议程，《现代法学》副主编、西南政法大学董彦斌教授担任主持。

主讲环节，中国政法大学法学院副教授、行政法研究所副所长张冬阳老师以“超越‘橡皮图章’：算法行政中实质性人类监督的建构”为主题开讲。张冬阳老师从欧盟《人工智能法案》、我国政务大

模型应用规范及相关裁判切入,说明人类监督已成为算法风险治理的重要制度要求。张冬阳老师指出,机器决策可能因模型偏差忽略个案特殊性,人类判断则能够运用行政裁量校正结果、维护个案正义;但自动化偏差、算法不透明、信息过载、监督能力不足和责任分散,也可能使人工复核停留在“盖章确认”。对此,应以“制度性不信任”为出发点,从制度、组织、程序和激励四个方面完善保障,包括开展人机协作评估、配置复合专业人员、合理设置监督介入节点、保障监督过程留痕,并建立行政机关与技术提供者之间的反馈和责任分配机制。

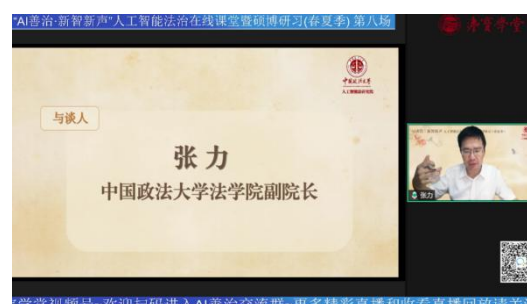


与谈环节,清华大学法学院余凌云教授指出,算法行政中强调人工监督,首先是为了确保行政决定体现行政机关的真实意思,并由行政机关承担相应责任。人工控制不应只停留在决策后端,还应延伸至技术引入前的审核与合法性评价;对于高度智能化、难以解释的系统,可通过当事人投诉、定期抽查和结果回溯,检验算法输出的稳定性与可靠性,并进一步追溯算法设计和数据训练环节。

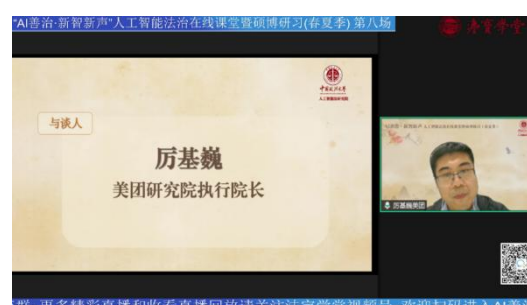


中国政法大学法学院副院长张力教授从功能主义、规范主义与组织法三个层面展开分析。他提出,人类监督不仅作用于缓解算法风险,也承担着重新连接民主问责与行政合法性链条的功能。同时

需要区分“人类监督”与“人类干扰”,防止人工介入反而削弱统一、严格的执法标准。从决策类型看,批量、非争议事项可以采用“机器决策加人类监督”的方式;涉及重要权利或纠纷处理的事项,则应坚持“人类决策加人工智能辅助”。



美团研究院执行院长厉基巍从产业和技术实践出发,梳理了规则算法、统计学习、深度学习到大模型的发展变化。他指出,算法越趋复杂,系统的不透明性、数据局限和责任模糊问题越突出,人类监督也面临能力不匹配、信息不对称、资源不足等现实困难。实质性监督应当分类分级展开:在高风险场景中保留人的最终决定权,事前开展算法备案和对抗测试,事中记录输入输出及人工干预过程,同时赋予监督人员真实的否决权、日志查验权和自主抽样权,并通过独立考核、分级复核和盲测机制提高监督有效性。



三位与谈嘉宾分别从行政法理论、组织法结构和算法治理实践切入,进一步揭示了实质性人类监督所涉及的权力配置、程序保障、技术条件与责任机制,为在线参与研习的硕博研究生提供了多维度的分析框架。

在硕博研习环节,中国政法大学博士研究生洪一凡围绕行政机关的实质性监督义务、相对人的程序权利,以及强制性义务与助推工具如何配合提出

问题。余凌云教授认为,应当同时保障相对人选择线上或线下办理的权利,并坚持将智能技术定位为行政机关的辅助工具。张力教授进一步提出“存在义务、回应义务和巡检义务”三项基础要求,并主张在此基础上通过适当的行为机制,推动执法人员主动审查算法输出,为相对人提供充分信息和真实选择。



浙江工商大学博士研究生**许颖**就如何通过人员权限和流程设计避免人工复核沦为形式,以及不同算法行政场景应如何确定人的介入程度提问。厉基巍院长提出,关键是让“认真审查”成为监督人员的理性选择,通过能力匹配、监督独立、问责对称、真实否决议、分级复核和盲测等机制,为纠偏提供制度条件。董彦斌教授指出,算法始终是行政活动的工具,人的角色本质上仍是执法者;对于涉及人身自由等重大权利义务处分的事项,执法人员必须实质在场并作出最终判断。

在线课堂尾声,**董彦斌**教授主持了“AI善治·新智新声”人工智能法治在线课堂暨硕博研习(春夏季)系列活动的闭幕环节。北京新星科技有限公司(iCourt)法律AI研究院院长李小武代表支持单位作总结致辞。他回顾了春夏季八场在线课堂围绕人工智能法治前沿问题形成的持续交流,向主办团队、主讲与谈嘉宾及参与研习的青年学子表示感谢,并期待系列活动在秋季继续汇聚学界与业界力量,推动技术实践与法治研究相互促进。

本场在线课堂的圆满举办,为算法行政中的人类监督从原则性要求走向可操作的制度安排提供了多层次思路,也为“AI善治·新智新声”人工智能法治在线课堂暨硕博研习(春夏季)画上圆满句号。自3月启动以来,八场在线课堂持续聚焦人工

智能法治前沿议题,通过主题分享、专家与谈和硕博互动,搭建起学界、业界与青年学子交流对话的平台。感谢各位专家学者、青年学子、广大参与者以及各合作单位的一路同行与持续关注。

未来,中国政法大学人工智能法研究院将继续聚焦人工智能法治前沿议题,推出更多高水平学术活动,深化跨学科、跨领域交流,为青年学子搭建与专家学者交流互动的平台,进一步拓展学术视野、强化问题意识,推动人工智能法治研究与人才培养不断深化。敬请持续关注!

“2026年人工智能法青年研习营”成功举办

2026年8月17日至21日,由中国社会科学院法学研究所、中国法学会网络与信息法学研究会联合主办的“2026年人工智能法青年研习营”(以下简称“研习营”)在北京成功举办。本届研习营由中国社会科学院法学研究所网络与信息法研究室承办,《网络与信息法学研究》编辑部协办,来自全国高校的36名优秀青年学子入选正式营员。8月17日,研习营开营仪式在中国社会科学院法学研究所举行。中国社会科学院法学研究所、国际法研究所联合党委书记、研究员**翟国强**,中国法学会网络与信息法学研究会副会长、学术委员会主任、中国人民大学法学院教授**张新宝**出席开营仪式并致辞。开营仪式由中国法学会网络与信息法学研究会常务副秘书长、中国社会科学院法学研究所网络与信息法研究室副主任(主持工作)**周辉**主持。开营仪式结束后,中央财经大学法学院副院长、《财经法学》副主编**刘权**教授作嘉宾演讲。



本次研习营为期五天，课程设置兼顾理论前沿与实践需求。在教学安排上，研习营围绕人工智能法前沿问题设置专题授课、案例研讨等环节，并组织营员赴科技企业开展实践调研与交流，引导营员在真实产业场景中深化对人工智能法律问题的认识，促进法学理论、制度研究与产业实践相互贯通。

在师资方面，研习营邀请了来自北京大学、清华大学、中国人民大学、中国社会科学院法学研究所、中国社会科学院国际法研究所、同济大学、中国医学科学院及科技企业等单位的专家学者和实务人士开展专题授课与交流。授课教师包括（按照授课顺序排列）：中国法学会网络与信息法学研究会常务副秘书长、中国人民大学法学院教授、未来法治研究院执行院长**张吉豫**，北京大学法学院长聘副教授、副院长、数字法治研究中心副主任**戴昕**，清华大学智库中心助理研究员**刘云**，清华大学公共管理学院长聘副教授、清华大学科技发展与治理研究中心主任助理、清华大学人工智能国际治理研究院专家**陈天昊**，中国社会科学院法学研究所助理研究员**刘灿华**、**徐玖玖**，中国社会科学院国际法研究所科研处副处长、国际经济法研究室副主任（主持工作）、副研究员**孙南翔**，同济大学法学院助理教授、上海市人工智能社会治理协同创新中心研究员**王伟**，中国医学科学院医学信息研究所医疗卫生法制研究室主任、研究员**曹艳林**，中国法学会网络与信息法学研究会常务副秘书长、中国社会科学院法学研究所网络与信息法研究室副主任（主持工作）

周辉，联想集团全球法务执行总监**吴凡**，清华大学法学院教授、副院长**刘晗**等。

研习营的顺利举办，离不开专家学者和工作人员的共同支持。中国社会科学院法学研究所副研究员**萧鑫**、**张浩然**先后担任课程主持人；中国社会科学院法学研究所副研究员**蔡睿**、中国社会科学院国际法研究所副编审**谭观福**、抖音集团法律研究总监**刘明**、腾讯研究院高级研究员**彭云**共同担任结业考核评审，为研习营各项活动有序开展提供了有力保障。

8月21日下午，“2026年人工智能法青年研习营”结业典礼举行。全体营员顺利完成研习课程及交流汇报。经综合评议，研习营共评选出10名优秀营员、3名优秀组长和2个优秀小组，表彰营员在课程学习、研讨交流和团队协作等方面的突出表现。

本次研习营的成功举办，为青年学子深入研究人工智能法律问题、开展学术交流、拓展实践视野搭建了重要平台。通过高校、科研机构与科技企业之间的交流互动，研习营进一步促进了人工智能法领域的青年人才培养与学术 research 交流，为推进人工智能治理法治化凝聚了青年力量。未来，研习营将继续聚焦人工智能法前沿问题，支持青年学子开展深入研究，为人工智能法治建设和数字法治发展持续贡献力量。

（技术编辑：吕昊然）

数字法评

数据不正当竞争行为认定逻辑的重塑与承继

此处删除了原文脚注，全文请参见《法律适用》2026年第6期，转载或引用请注明出处。

作者：孟雁北

内容提要：数据不正当竞争行为的认定对于解决数据权属争议、塑造数字经济领域的的数据获取和使用规则，具有重要的时代价值。我国司法实践已经初步形成了数据不正当竞争行为的认定逻辑且仍在动态发展中，2025年修订的反不正当竞争法通过新增数据不正当竞争专款重塑了数据不正当竞争行为的认定逻辑。一般条款不再是认定数据不正当竞争行为的主要法律依据，竞争关系的判断将不再具有必要性，“合法持有数据”取代“受法律保护的数据权益”的判断，扰乱市场竞争秩序成为核心后果要件，进而形成经营者是否合法持有数据、是否以不正当方式获取或者使用数据、是否扰乱市场竞争秩序的数据不正当竞争行为认定逻辑，实践中已经积累的裁判经验仍会在重构后的数据不正当竞争行为认定逻辑中得到承继并被优化。

数据是数字经济和智能经济时代最重要的资源与竞争要素之一。《中共中央关于加强新时代审判工作的意见》要求人民法院“依法审理数据产权归属认定、市场交易、权益分配、利益保护等纠纷，推动数据要素高效流通和交易”。2025年8月21日，国务院发布《关于深入实施“人工智能+”行动的意见》，强调要“加强数据供给创新。以应用为导向，持续加强人工智能高质量数据集建设。完善适配人工智能发展的数据产权和版权制度”。当数据的无体性、非消耗性、多栖性、多样性、价值动态性等特点给数据赋权制度带来诸多挑战时，关于数据产权的归属确定问题，学界存在多种数据赋权学说或方案，例如“数据产权说”“企业数据有限产权说”“用益权说”“知识产权说”“商业秘密说”“新型权利说”“权利束说”“场景化界定

说”等，目前仍很难达成关于数据赋权的理论共识，从而使得数据赋权具有不确定性。实践中，数据权益保护最初以著作权法为制度文本，以数据库为保护对象。尽管数据存在被认定为著作权并通过著作权法保护的可能性，例如，在“虚拟数字人案”中，审理法院将符合作品构成要件且本质为数据集合的“虚拟数字人”认定为美术作品、视听作品，但由于数据集合被认定为具有独创性的作品难度很大，著作权法保护范围重在表达而不当然延及作品中包含的数据信息，因此很难满足市场主体保护数据权益的实际需求。虽然数据也存在被认定为商业秘密的可能性，如在浙江淘某网络科技有限公司等诉某数有限公司等不正当竞争纠纷案中，审理法院认为，淘某平台的非公开经营数据因具备秘密性、价值性并采取了合理的保密措施而构成商业秘密，但是由于秘密性是构成商业秘密的核心要件，公开数据较难通过主张侵犯商业秘密来予以充分救济。因此，当大量涌现的数据权益争议较难通过数据权益的确权与侵权认定来予以纾解时，数据权属不明与数据流通需求之间的矛盾就更加凸显。如何维护数据市场公平竞争秩序，推动我国数字产业高质量发展，成为司法亟需回应的现实命题。反不正当竞争法的行为法特点及探究商业行为底线的功能契合了数字市场对数据要素市场化的规则需求，从而成为解决数据权属争议和保护数据合法权益的最主要法律路径。

数据不正当竞争行为的认定在解决数据权属争议、塑造数字经济领域数据获取规则和数据使用规则等方面，具有重要的时代价值。我国法院在司法实践中依据2025年修订前的反不正当竞争法持续探索并初步形成了数据不正当竞争行为的认定逻辑，当2025年修订的反不正当竞争法新增数据不正当竞争专款时，数据不正当竞争行为认定的法律依据发生了根本性变化，需要进一步关注以下问题：我国司法实践中已有的关于数据不正当竞争行为的认定逻辑是怎样的？该认定逻辑是否会因为2025年修订反不正当竞争法新增数据不正当竞争专款而被重塑？重塑后的认定逻辑与已有的认定

逻辑之间是否具有承继性？哪些数据不正当竞争行为的裁判经验能够被承继？这些被承继的裁判经验是否需要被进一步优化？

一、数据不正当竞争行为认定逻辑的形成与动态发展

数据在经济生活、市场竞争中的重要性以及数据权益纠纷解决对反不正当竞争法的依赖性使数据不正当竞争行为的案件逐年增多。例如，北京知识产权法院适用反不正当竞争法在2021年审结的涉数据知识产权案件为75件，2022年为90件，2023年为174件。全国法院审理的涉数据类案件数量也增长明显，2024年一审审结的案件数是2021年的两倍。面对数据不正当竞争案件，法院从较早的“微某诉脉某案”开始通过个案不断探索并初步形成了数据不正当竞争行为的认定逻辑，即判断数据持有者是否对数据享有可保护法益，被诉行为是否对数据持有者的法益造成了损害、是否损害了市场竞争秩序，进而判断被诉行为是否构成不正当竞争行为。浙江省高级人民法院也指出，在适用反不正当竞争法一般条款对数据权益进行保护时，认定获取和利用商业数据是否构成不正当竞争行为，需要综合分析数据类型、对数据持有方的损害程度、获取和使用方式是否违背商业道德以及个人信息保护等因素，来判断竞争秩序是否受到损害、被诉行为是否构成不正当竞争，并归纳总结出原告数据权益的合法性及受保护程度、被诉行为系竞争行为、被诉行为对原告造成了实质损害、被诉行为具有不正当性的数据不正当竞争行为认定逻辑。

根据2025年修订前反不正当竞争法的规定，纵观法院审理数据不正当竞争案件的实践做法，尽管认定数据不正当竞争行为本身具有个案性，认定标准仍在发展中，但可以认为数据不正当竞争行为目前的认定逻辑为：判断是否具有竞争关系、是否存在受法律保护的数据权益、是否存在数据获取或者使用行为的不正当性、是否存在数据获取或者使用行为的损害后果。

（一）竞争关系的判断

反不正当竞争法是维护市场竞争秩序的法律

制度，判断争议当事人之间是否具有竞争关系通常是认定不正当竞争行为的逻辑起点，法院在司法实践中也倾向于通过确定当事人之间是否存在竞争关系来判断争议行为是否应当受到反不正当竞争法的规制。如在北京微某公司诉上海复某公司不正当竞争纠纷案中，法院认为，结合双方当事人提供服务的实质、用户和经营范围的重叠程度、流量和数据对平台企业的价值等因素进行分析，可以认定原、被告双方存在竞争关系。不过，在不正当竞争案件中，法院从广义视角出发对竞争关系进行判断，认定标准越来越宽松。《最高人民法院关于适用〈中华人民共和国反不正当竞争法〉若干问题的解释》第2条关于“与经营者在生产经营活动中存在可能的争夺交易机会、损害竞争优势等关系的市场主体，人民法院可以认定为反不正当竞争法第二条规定的‘其他经营者’”的规定，也可以从侧面反映出不正当竞争行为认定中法院对竞争关系从宽认定的发展趋势。在认定数字市场不正当竞争行为时，竞争关系的认定已经不再局限于同一产业或领域范围内，在涉数据不正当竞争案件中也未出现法院最终认定数据权益争议当事人之间不具有竞争关系的案件。

（二）受法律保护的数据权益的判断

判断数据持有者是否享有受法律保护的数据权益是目前认定数据不正当竞争行为的前提条件。法院主要从数据持有者是否为涉案数据的合法运营主体、数据的形成是否合法、数据持有者对于数据形成是否有相应的贡献或者付出、数据持有者对数据是否提供了经营服务、数据持有者与用户之间是否签订有关于数据权属及使用条款的协议、数据的经济价值和交换价值是否能够给数据持有者带来竞争优势等方面来判断。如在某甲公司诉某乙公司等不正当竞争纠纷案中，法院认为，某甲公司的SMM价格数据系其采用独创的价格方法论进行深度分析整理、整合加工而形成的衍生数据，具有较高的经济价值和社会价值，该数据信息能够为某甲公司带来客观的商业利益和独特的竞争优势，该权益可以在反不正当竞争法领域获得保护。正是因为

认定数据不正当竞争行为的案件中需要判断数据持有者是否享有受法律保护的数据权益,才会引发关于反不正当竞争法是否可以给数据赋权以及如何恪守其行为法本质属性的讨论。

(三)数据获取或者使用行为不正当性的判断

判断数据获取或者使用行为的不正当性,首先需要确定是适用2025年修订前《反不正当竞争法》第12条第2款第4项还是适用第2条一般条款来认定数据不正当竞争行为。根据2025年修订前《反不正当竞争法》第12条第2款第4项的规定,经营者不得利用技术手段,通过影响用户选择或者其他方式,实施妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为。由于经营者不当获取或者使用数据的行为更多是为了实现商业利益,通常不以“妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行”为目的,因此实践中多数数据不正当竞争行为的认定不是依据《反不正当竞争法》第12条第2款第4项的规定,而是依据《反不正当竞争法》第2条一般条款即“经营者在生产经营活动中,应当遵循自愿、平等、公平、诚信的原则,遵守法律和商业道德。本法所称的不正当竞争行为,是指经营者在生产经营活动中,违反本法规定,扰乱市场竞争秩序,损害其他经营者或者消费者的合法权益的行为”来认定。

判断数据获取或者使用行为是否具有不正当性时,目前的司法实践从行为目的、方式以及后果等多角度出发,聚焦是否符合“合法、正当、必要”的标准,是否越过一定的合理界限,通过判断数据获取或者使用行为是否得到了许可,是否遵守了Robots协议,是否破坏或者绕开了技术管理措施,是否遵循了相关技术规范,是否侵犯了个人信息权益,是否影响了其他经营者的数据安全性,是否不合理地增加了其他经营者服务器的负担,是否不合理地提高了其他经营者的经营成本等来进行认定。如在深圳市腾某公司等诉北京字某公司等不正当竞争纠纷案中,法院在认可数据互联互通价值的前提下,重点审查了技术手段与商业道德的契合度,认为被告采用伪造浏览器标识、动态IP切换等技

术手段突破某公众平台设置的Robots协议,系统性抓取公众号文章,割裂用户与平台的交互纽带对原告构成实质性竞争损害,因而行为具有不正当性。

法院在审理数据不正当竞争案件中创设并经常适用“实质性替代标准”来判断数据持有者的数据合法权益是否受损,进而判断数据获取行为或者使用行为是否具有不正当性。如在某某公司4诉某某公司1等侵害著作权及不正当竞争纠纷案中,法院认为,某某公司1集约化提取数据并出售的行为,攫取了小某书平台流量,对小某书数据服务构成实质性替代,并导致用户对小某书的安全性评价降低,实质性损害了某某公司4的竞争利益。不过,在数据不正当竞争行为认定中是否以及如何适用“实质性替代标准”本身是存在争议的。《禁止网络不正当竞争行为规定(公开征求意见稿)》第20条中曾将“实质性替代标准”作为认定数据获取或者使用行为不正当性的后果要件之一予以规定,但在国家市场监督管理总局2024年正式颁布的《网络反不正当竞争暂行规定》中则没有关于通过“实质性替代标准”认定数据获取或者使用行为不正当性的内容。同样地,《最高人民法院关于适用〈中华人民共和国反不正当竞争法〉若干问题的解释(征求意见稿)》第26条中也曾有关于“实质性替代标准”的表述,但在2022年正式发布的司法解释中,也没有“实质性替代标准”的相关内容。在认定数据不正当竞争中如何准确适用“实质性替代标准”需要进一步思考。

(四)数据获取或者使用行为损害后果的判断

在认定数据不正当竞争行为的司法实践中,关于数据获取或者使用行为不正当性的判断常与损害后果的判断融合在一起。既可能是通过数据获取或者使用行为的目的、表现和方式进行判断,也可能是通过数据获取或者使用行为是否损害了其他经营者合法权益、消费者合法权益和市场竞争秩序进行判断。但无论如何,数据不正当竞争行为都需要具备损害经营者权益、消费者权益和市场竞争秩序的后果要件。如在北京百某网讯公司等诉北京互

动某网络技术公司不正当竞争纠纷案中，法院认为，被告未经原告许可，采用技术手段批量抓取来自百某百科中的涉案词条内容高达60余万条，同时伪造用户信息，以普通用户发布的形式，将抓取的词条内容上传至其运营的百科中，向其自身用户进行展示和提供服务，涉及范围广，足以对百某百科产生部分实质性替代的效果。被诉行为损害了百某网讯公司等的竞争利益及网络用户的合法权益，扰乱了市场竞争秩序，构成不正当竞争。

实务中除了适用“实质性替代标准”对数据获取或者使用行为是否损害经营者权益和市场竞争秩序进行判断外，还会适用“破坏性利用标准”进行判断。即结合数据可替代性等特点，通过考量数据使用本身的创新程度、对数据持有者利益的影响等因素，综合判断数据获取或者使用行为对数据持有者数据资源是否构成破坏性利用或者是否违反法律规定，从而判断是否扰乱了市场竞争秩序。目前如何判断构成数据不正当竞争行为的后果要件，仍在个案探索中。

总之，数据不正当竞争行为认定逻辑一直在动态发展中，数据不正当竞争行为的认定本身仍具有个案分析的特点。例如“实质性替代标准”目前有有时是认定行为不正当性的方法，有时是认定扰乱市场竞争秩序或者经营者合法数据权益受到损害的方法，甚至有时是认定数据不正当竞争行为是否成立的方法，其在认定数据不正当竞争行为中的作用并不明确且存在争议。

二、数据不正当竞争行为认定逻辑的重塑

为了更好地回应数字市场竞争给反不正当竞争法带来的挑战，2025年修订的《反不正当竞争法》新增了第13条第3款“经营者不得以欺诈、胁迫、避开或者破坏技术管理措施等不正当方式，获取、使用其他经营者合法持有的数据，损害其他经营者的合法权益，扰乱市场竞争秩序”的内容。虽然2025年修订的反不正当竞争法没有选择通过独立法条的形式规定数据不正当竞争行为，但该专款关于数据不正当竞争的规定，已经具有独立的违法行为构成要件。其中对数据获取行为、数据使用行为分别

予以规定的立法选择，以及对“合法持有的数据”的立法表述都极具智慧地避免了对数据进行赋权以及认定数据不正当竞争行为时对数据赋权的依赖，是对已经积累的司法裁判经验的总结，体现了反不正当竞争法行为法的特点，并将重塑数据不正当竞争行为的认定逻辑。

（一）一般条款的“原则退场”与判断竞争关系的非必要性

根据《最高人民法院关于适用〈中华人民共和国反不正当竞争法〉若干问题的解释》第1条“经营者扰乱市场竞争秩序，损害其他经营者或者消费者合法权益，且属于违反反不正当竞争法第二章及专利法、商标法、著作权法等规定之外情形的，人民法院可以适用反不正当竞争法第二条予以认定”的规定，2025年修订前的反不正当竞争法没有关于数据不正当竞争行为的专门规定，故存在适用《反不正当竞争法》第2条一般条款对数据不正当竞争行为予以认定的空间。也因此出现了在一系列数据不正当竞争案件中，法院根据经营者的数据获取或者使用行为是否违反了公平、诚实信用原则和公认的商业道德适用一般条款来予以认定的现象。不过，数字市场一些新兴领域关涉公平竞争的商业规则仍处于探索之中，市场竞争行为是否违反了商业道德还很难达成共识，公认的商业道德正在形成过程中，有时是法官通过认定数据不正当竞争行为来塑造数据获取或者使用的行为规则和数据领域公认的商业道德。由此，需要注意避免过度泛化适用反不正当竞争法一般条款认定数据不正当竞争行为。有学者提出，应当警惕过度强调商业惯例的趋势，尤其是将市场广泛实践直接等同为商业惯例，并据此肯定竞争行为正当性的现象。也要关注商业道德的扩大化解释导致的“泛道德性”解释问题，以及出现泛道德化倾向后导致难以清晰认定不正当竞争行为，进而可能会不当限制市场主体的经营自主权的问题。2025年修订的反不正当竞争法新增数据不正当竞争行为专款规定后，《反不正当竞争法》第2条一般条款原则上将不再是数据不正当竞争行为的认定依据，从而在一定程度上可以减少一

般条款难以输出稳定的规则指引、数据不正当竞争行为违法构成要件不确定等问题,有助于数据不正当竞争行为认定标准的统一,在一定程度上可以为市场主体的数据获取或者使用行为提供比较明晰的行为指引,促进数据流通使用和数据要素价值的释放。

另外,尽管判断竞争关系是法院审理不正当竞争行为的习惯做法,但是随着竞争关系认定的广义和宽泛解释,竞争关系并非认定不正当竞争行为的必要条件的观点已经逐渐被接受。有学者认为,互联网经济下竞争关系的相对性正在消解,竞争关系不再是认定不正当竞争行为发生的前提,在不正当竞争行为的认定中,可以放弃竞争关系的要件地位,而在反不正当竞争法中采用广义“竞争行为”的概念更具现实意义。由于数字市场平台竞争、数据竞争、跨界竞争等特点非常明显,从数据不正当竞争行为的理论、立法和实践来看,认定数据不正当竞争行为时,判断竞争关系将不再具有必要性。

(二) 合法持有数据的判断取代受法律保护的数据权益的判断

当事人在数据争议中所针对的常常不是数据本身,而是负载在数据之上所产生的数据权益。市场主体期待通过适用反不正当竞争法来保护数据权益,但反不正当竞争法作为行为法并不会也无法设定或者确认数据权益。或者说,反不正当竞争法介入数据权益保护时,既要有所侧重,也要有所克制,其规制的是数据的不当获取或者不当使用行为,是以行为保护模式实现对数据的保护,应避免在反不正当竞争法中设定数据权利条款,进行权属界定、权能配置等。正因如此,我国2025年修订反不正当竞争法时将经营者“合法持有数据”作为认定数据不正当竞争行为的基础要件,回避了对数据权益的属性作出判断,使数据不正当竞争行为的认定逻辑更为清晰。我国是否需要制定专门的“数据法”尚不明朗,目前对“合法持有数据”主要依据个人信息保护法、数据安全法、网络安全法、《关键信息基础设施安全保护条例》《网络数据安全管理条例》以及省级地方性数据法规、规章等来进行

判断。在具体认定数据是否属于“合法持有”时,仍需要对数据进行类型化细分,如数据是公开数据还是非公开数据,是公共数据还是商业数据,是原始数据还是衍生数据等。

2025年修订反不正当竞争法新增的数据不正当竞争专款已经彰显出反不正当竞争法是行为法而非权利法的底色,对于数据不正当竞争行为的认定可以起到正本清源的作用。当认定不再从是否“存在受到法律保护的数据权益”而是从是否“合法持有数据”的角度入手时,认定的重心将不是“权利或者权益是否受到侵害”而是“不正当行为是否存在”。当不正当竞争行为的认定并不以权利或者权益的存在作为前提时,就正在重塑数据不正当竞争行为的认定逻辑,并与反不正当竞争法的本质属性更加契合。

(三) 获取、使用数据方式的不正当性判断

2025年修订的反不正当竞争法新增的数据不正当竞争专款从数据获取、使用“两分法”出发分别判断数据获取、使用行为正当性边界,可以为数据行为提供更清晰的行为准则。准确而言,数据获取、使用的正当性评价并不相同,甚至有明显的差别性。关于数据获取,可以从数据获取手段是否合法正当,是否通过伪装成数据平台、用户或者会员等欺骗方式获取数据,是否破坏了技术保护措施,是否得到了许可,是否违反了Robots协议,是否违反了平台规则等方面予以判断。关于数据使用,可以从数据使用行为是否违反约定超范围使用获取的数据,是否超出数据合理使用的限度,是否产生实质性替代后果等方面予以判断。如在数某(北京)公司诉隐某(上海)公司不正当竞争纠纷案中,法院认为,数据需求方获取、使用开源数据应当遵守开源协议已成为行业共识,涉案众多数据服务平台采用知识共享协议的事实可以证明此点。当数据集持有者对数据集开源时,数据需求方的获取、使用行为是否遵循开源协议是衡量该行为是否违反数据服务领域商业道德的重要考量因素。

《反不正当竞争法》第13条规定,即数据不正当竞争专款对于行为方式不正当性的列举更多

是关于数据获取行为的不正当方式，尚需要在司法实践中探索更多的数据获取、使用的不正当方式，该专款中“等”的规定亟需被激活和丰富。

（四）数据获取或者使用行为的损害后果判断

反不正当竞争法是维护市场竞争秩序的法律，数据获取或者使用行为是否产生了扰乱市场竞争秩序的后果是数据不正当竞争行为的违法构成要件之一，这一点在以往的数据不正当竞争行为案件中也可以体现出来。如在某科技有限公司诉某文化传媒有限公司不正当竞争纠纷案中，法院认为，某文化传媒有限公司未经许可，抓取搬运案涉数据集中大量用户信息、短视频和用户评论在乙 App 使用，导致乙 App 与甲 App 内容高度同质化，网络用户不使用甲 App，通过乙 App 也可观看相同内容，实质性替代了某科技有限公司经营的甲 App 产品和服务。由此，某文化传媒有限公司抓取搬运案涉数据，并在乙 App 使用的行为，损害了某科技有限公司的经营性利益。某文化传媒有限公司的案涉行为扰乱市场竞争秩序，损害其他经营者、消费者合法权益，构成不正当竞争行为。又如在某网络信息技术有限公司诉某信息科技有限公司不正当竞争纠纷案中，法院认为，网络平台向用户提供关联账号服务，经用户授权后转移其在关联网络平台获取的数据，为用户在合理范围内处理该数据提供便利，未扰乱市场竞争秩序的，不构成不正当竞争行为。

尽管目前我国已经有越来越多的案件在认定行为不正当性时，将涉诉行为置于社会公共利益、经营者利益与消费者利益的“三元叠加”利益衡量格局下进行判断，但在一定程度上还存在着侵权判断范式的色彩，这主要体现在数据不正当竞争行为的认定中过分重视通过数据持有者具有受到法律保护的数据权益、涉诉行为对数据持有者的损害、数据获取或者数据使用主体的主观过错等来判断行为的正当性。在判断数据不正当竞争行为是否损害其他经营者的合法权益、扰乱市场竞争秩序时，需要根据不同市场参与者基于竞争享有的不同利益来判断，各种利益之间没有固定的价值位阶和权重。某种具体不正当竞争行为的认定，可能强调其

中一种利益，但三种利益评价往往相互交织。如果将反不正当竞争法所保护的对象确定为市场竞争秩序，那么反不正当竞争法在干预失衡失序的市场竞争时，就需要更加重视扰乱市场竞争秩序这一后果要件在认定数据不正当竞争行为中的重要性，而将对数据不正当竞争专款中“损害其他经营者的合法权益”和反不正当竞争法立法目的条款中“保护消费者的合法权益”的判断内化在“扰乱市场竞争秩序”的判断之中。

总之，基于 2025 年反不正当竞争法的修订，数据不正当竞争行为的认定将会以数据不正当竞争专款规定为依据，遵循经营者是否合法持有数据、是否以不正当方式获取或者使用数据、是否扰乱市场竞争秩序的认定逻辑进行判断，从而使执法者和法官有了更清晰的认定准则，并将在处理数据争议中发挥重要甚至不可或缺的作用。

三、数据不正当竞争行为认定逻辑的承继与优化

数据不正当竞争行为认定逻辑的变化主要是认定的法律依据因 2025 年修订的反不正当竞争法而发生了改变。由于反不正当竞争法的立法目标、基本原则和本质属性并没有发生变化，因此实践中积累的裁判经验仍会在重构后的数据不正当竞争行为的认定逻辑中得到承继并不断被优化。

（一）判断合法持有数据的非赋权性

反不正当竞争法所保护的利益有很大的模糊性，其并不要求一定构成权利，而是一种不很确定、不很稳定的法律上的利益，是否保护常常取决于个案的判断，此观点也同样适用于数据权益争议。在认定数据不正当竞争行为时，如果说 2025 年反不正当竞争法修订之前认定数据不正当竞争行为时需要判断的“数据持有者享有受法律保护的数据权益”要件还有关于数据赋权可能性争议的话，那么 2025 年修订之后的数据不正当竞争专款规定的“合法持有数据”要件则明确地表明数据不正当竞争行为认定的非赋权性。

2022 年 12 月发布的《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》明

确指出我国建立数据资源持有权、数据加工使用权、数据产品经营权等分置的数据产权运行机制。数据持有权是最为基础和重要的数据财产权，可从数据的复制、传播、演绎角度对其进行理解和构造。数据持有权的正当性基础在于数据的收集和管理行为，这体现了数据处理者的劳动。广东省高级人民法院对“某API案”的判决，被认为是在司法裁判中认可和保护了互联网平台企业等主体的“数据资源持有权”。但在认定数据不正当竞争行为时，判断“合法持有数据”存在与否并不需要经营者证明其拥有数据资源持有权，而只需要证明“合法持有数据”即可。

在证明“合法持有数据”的过程中，依据2025年修订前反不正当竞争法判断“数据持有者享有受法律保护的数据权益”的裁判经验可以被承继。如果可以证明“数据持有者享有受法律保护的数据权益”成立，在大多数情况下也能够证明“合法持有数据”的成立。如在G两公司诉万某有限公司不正当竞争纠纷案中，法院认为，涉案日级拥堵延时指数数据集是G两公司付出技术、资金、人力、物力等的实质性投入合法生成的衍生数据，可对城市拥堵状态及其趋势以精确、简练、直观、量化的方式呈现，在原始地图数据基础上添附了更多的商业价值，能够满足各方主体的数据需求，可为G两公司吸引流量、带来交易机会与竞争优势等商业利益。上述论证过程和裁判经验也可以用于证明“合法持有数据”的成立。甚至可以说，“合法持有数据”的证明相对“数据持有者享有受法律保护的数据权益”的证明而言会更简单直接，证明难度也会降低，证明的逻辑也更清晰。如在我国目前数据登记的形式有数据知识产权登记、数据资产登记、数据产品登记、数据要素综合登记等，尽管这些数据登记均无法证明数据权益的性质和内容，也并不具备数据权利创设或证明的效力，但在没有反证的情况下，可以初步证明经营者在数据收集、加工使用、经营以及删除等全生命周期的合法合规。因此，即使这些数据登记并不是设权登记，甚至也不一定能够证明“数据持有者享有受法律保护的数据权益”的内

容，但可以成为经营者“合法持有数据”的重要证据之一。这也可以从侧面表明，证明经营者“合法持有数据”的非赋权性特征使其比证明“数据持有者享有受法律保护的数据权益”相对更容易。

（二）判断数据获取或者使用行为方式不正当的开放性

认定数据不正当竞争行为需要判断数据获取或者使用行为的方式具有不正当性。尽管我国已有的大量数据不正当竞争案件是适用2025年修订前《反不正当竞争法》第2条一般条款，修订后的《反不正当竞争法》第2条一般条款原则上不再是认定数据不正当竞争行为成立的法律依据，但是根据一般条款认定行为具有不正当性的裁判经验仍可以被承继，用来证明数据获取或者使用行为方式的不正当性。根据2025年修订后数据不正当竞争专款的规定，在认定“经营者不得以欺诈、胁迫、避开或者破坏技术管理措施等不正当方式，获取、使用其他经营者合法持有的数据”时，由于欺诈、胁迫的情形较为少见，如何认定“避开或者破坏技术管理措施”以及“等”这一开放性表述，需要借鉴以往的裁判经验，如破解加密文件、持续性地使用会员账户名和密码登录以查看或获取他人信息的撞库方式、绕开平台滑块验证等登录机制、修改哈希值等都有可能被认定为行为方式具有不正当性。

在借鉴以往的裁判经验时，需要关注反不正当竞争法的根本属性是行为法，其并不是通过对经营者利益提供排他性保护来达到维护市场竞争秩序的目的。以往裁判实践中形成的“三重授权”规则、“非公益必要不干扰”规则本质是财产性权益的保护方式，经营者如果没有遵循上述规则尚不足以被直接认定为其数据获取或者使用行为的方式具有不正当性，还需要结合数据持有者为数据设定的保护方式，经营者获取或者使用数据的方式，数据获取或者使用行为是否与数据持有者的正常经营活动相冲突、是否遵守了相关法律规定、诚信原则和公认的商业道德等来综合判断和个案分析。不正当的行为方式是丰富且变化莫测的，对其认定也应当具有开放性。

（三）判断数据获取或者使用行为损害后果的聚焦性

数据不正当竞争行为的成立不仅仅需要认定数据获取或者使用行为方式具有不正当性，也需要认定该行为的后果具有违法性。反不正当竞争法的核心目标是维护市场竞争秩序，其对于经营者和消费者合法权益的维护是次要目标，我国1993年在制定反不正当竞争法时就有这样的认识。当时参与立法的专家认为，经营者的合法经营受到许多法律的调整，各个法律从不同角度保护合法的经营者，反不正当竞争法对合法经营者的保护，是建立在维护市场经济秩序的基础上，故反不正当竞争法亦被称为维护市场经济秩序的法律。市场竞争秩序事实上是经营者合法权益、消费者合法权益、社会公共利益、公平原则、诚实信用原则、公认的商业道德等要素共同组成的动态系统，认定数据不正当竞争行为需要具备的后果要件应当聚焦于是否扰乱了市场竞争秩序。无论是2025年修订前还是修订后的反不正当竞争法，认定不正当竞争行为成立需要具备“扰乱市场竞争秩序”这一后果要件都没有发生变化，竞争关系的认定、消费者与经营者合法权益的保护都应当内化在市场竞争秩序损害的认定之中，“扰乱市场竞争秩序”这一后果要件在认定数据不正当竞争行为中应当被进一步聚焦。

在目前认定数据不正当竞争的案件中，如何认定扰乱市场竞争秩序这一后果要件，以及如何处理这一后果要件与损害消费者、经营者合法权益的关系尚需要进一步优化。例如，认定数据不正当竞争行为中经常会适用“实质性替代标准”来进行后果要件的认定。在天某公司诉衡某公司等不正当竞争纠纷案中，法院认为，被告开发的侵权软件绕过天某公司对平台设置的技术防护措施，非法爬取并复制平台的商品数据，导致其他平台及商家对天某平台及商家形成实质性替代；同时，爬取行为增加了天某平台的不正常流量，妨碍了其流量监控与服务效能，被告的行为违背了诚实信用原则和公认的商业道德，破坏了市场竞争秩序，损害了消费者和平台商家权益，构成不正当竞争行为。

可进一步关注的是，“实质性替代标准”可以作为“损害其他经营者的合法权益和扰乱市场竞争秩序”的认定标准之一，但不能将其唯一化。数据获取或者使用行为即便没有产生实质性替代后果，也有可能产生扰乱市场竞争秩序的后果，并进而构成不正当竞争行为，而实质性替代后果是否扰乱了市场竞争秩序也需要进一步论证。或者说，认定数据不正当竞争行为需要具备的后果要件应当聚焦于扰乱市场竞争秩序本身就意味着“实质性替代标准”并不是也不能独立地成为数据不正当竞争行为的认定标准。以往数据不正当竞争案件中关于如何认定“扰乱市场竞争秩序”已有很多裁判经验可以被关注和借鉴。如在北京某科技公司诉某信息技术公司不正当竞争纠纷案中，法院认为，市场竞争秩序是否被扰乱取决于影响竞争如何产生、竞争如何进行的各要素之间的结构和运行机制是否被干扰。影响竞争的市场运行机制包括准入机制、供求机制、价格机制、信息机制、信用机制和创新机制。如果被诉行为直接影响到上述六种机制作用的正常发挥，则可认定其干扰了市场竞争秩序。在数据不正当竞争行为的认定中，如何聚焦“扰乱市场竞争秩序”这一后果要件进行判断，仍需要通过个案进一步探索。

结语

数智经济时代，技术在不断更新迭代，源于数据又由数据衍生的商业模式在不断变化，数据的重要性以及市场主体对数据权益保护的需求也在不断增强。在保护数据权益的路径中，既存在“权利保护路径”，也存在“行为规制保护路径”。尽管数据存在被认定为著作权或者商业秘密的情形，但由于是否以及如何对数据单独赋权在比较长的时间内仍会具有不确定性，通过“权利保护路径”来实现对数据权益的保护尚不普遍也无法满足市场主体的期待，而“行为规制保护路径”是通过对数据获取或者使用行为进行正当性判断来实现对数据权益的保护，可以淡化数据权利归属和法律属性的争议，满足市场主体保护数据权益的现实需求。因此，反不正当竞争法作为行为规制法对数据权益

的保护具有重要的时代价值。

我国反不正当竞争法的核心立法目标不是保护经营者、市场参与者和消费者，而是维护市场竞争秩序，通过维护市场竞争秩序来提升社会公共利益，并实现对经营者和消费者合法权益的保护。同样地，反不正当竞争法也不以确认数据权利或者数据权益为目的，而是通过制止数据不正当竞争行为维护市场竞争秩序来保护数据持有者或者数据处理者在市场竞争中的权益，并在一定程度上回应数字经济时代关于数据财产价值的实践需求。

依据2025年修订之前的反不正当竞争法，我国司法实践中已经初步形成了判断竞争关系、受法律保护的数据权益、数据获取或者使用行为的不正当性、数据获取或使用行为损害后果的数据不正当竞争行为认定逻辑，且该认定逻辑一直在不断探索和动态发展中。2025年修订的反不正当竞争法基于其作为行为法的特征，聚焦是否扰乱市场竞争秩序的后果要件，避免对数据赋权作出规定，通过新增数据不正当竞争专款重塑了数据不正当竞争行为

的认定逻辑。一般条款不再是认定数据不正当竞争行为的主要法律依据，竞争关系的判断将不再具有必要性，“合法持有数据”取代“受法律保护的数据权益”的判断，扰乱市场竞争秩序将成为核心后果要件，进而形成经营者是否合法持有数据、是否以不正当方式获取或者使用数据、是否扰乱市场竞争秩序的数据不正当竞争行为的认定逻辑。按照重塑后的数据不正当竞争行为的认定逻辑对数据不正当竞争行为进行判断时，司法实践中已经积累的裁判经验将会得到承继并被优化。

2025年修订反不正当竞争法新增数据不正当竞争专款的规定，使数据不正当竞争行为的认定逻辑日渐具体、清晰和完善，可以在一定程度上纾解对数据不正当竞争行为认定中“泛商业道德化”和过度适用“实质性替代标准”的问题，为执法与司法认定数据不正当竞争行为提供较为明确的指引，也有助于执法与司法在数据不正当竞争案件中更好地处理数据权益保护与数据流通的关系，促进我国数字经济健康有序地发展。

论数字司法价值对齐的实现路径

此处删除了原文脚注，全文请参见《中国法学》2026年第3期，转载或引用请注明出处。

作者：彭中礼

内容提要：数字司法中算法决策与司法价值的偏离容易引发伦理与法律风险。在数字司法场域中推进价值对齐，应当坚守司法本质以定其向，防控技术风险以固其基，筑牢司法信任以彰其效，融合司法文明以臻其境。数字司法价值对齐要求算法的价值追求与法律精神、社会伦理、人文关怀形成动态适配，其具体要求体现为维护一致性、确保可控性、保持鲁棒性以及避免恣意性。推进数字司法价值对齐，需凝聚全链条、全过程的协同合力，在源头校准层、运行管控层、迭代优化层与安全保障层系统构建层次化推进的过程机制。理论分析表明，数字司法中的价值对齐通过将人类多元价值转化为技术可理解、可执行的逻辑，让人机协同从效率适配的工具层面跃升为价值共生的生态层面，最终形成技术进步与人类发展深度契合的良性循环。

一、引言

近年来，人工智能等现代数字科技在司法领域的应用，已从单纯的司法辅助工具逐步向深度嵌入司法决策的方向演进。2024年12月，《人民法院第六个五年改革纲要（2024-2028年）》提出“完善数字法院建设体系”，以数字法院建设为代表的数字司法发展进入新阶段。在数字司法中，新科技的深度应用打破了传统司法对物理场所、专业中介机构、人类决策者的依赖，突破了既有流程的局限与固有目标的束缚，已然掀起司法转型的全新浪潮。

但是，数字科技在司法领域的深度应用，也带来了一系列亟待回应的伦理与法律难题。算法的纵深渗透与技术创新的加速迭代，进一步加剧了算法逻辑与法律体系之间的结构性紧张关系。其中尤为突出的是，算法歧视、黑箱决策等典型问题充分暴露出人工智能在理解法律原则、权衡司法价值等方面存在缺陷，容易导致“合法但不合理”的价值困境。因此，需要在算法设计与应用中积极稳妥推进

价值对齐，将法律原则、司法价值嵌入算法逻辑，实现算法运行与司法目标的协同一致。

当前，哲学、伦理学有关价值对齐的研究较为丰富，主要聚焦在三个方面：一是从伦理的角度对价值对齐进行研究；二是对价值对齐的概念、应有内涵以及实施路径进行讨论；三是对人工智能或者大模型是否需要价值对齐进行讨论。法学界也已经开始关注价值对齐：一是对生成式人工智能的价值对齐问题进行法理反思，探讨法律原则作为价值对齐的标准；二是对价值对齐的法治进路进行宏观讨论，试图构建法治化机制；三是基于具体的部门法探讨价值对齐的实现，关注自动驾驶过程中的个性化价值对齐和智慧税务中的价值对齐等问题。然而，现有关于价值对齐的研究尚未充分关注数字司法场景，对数字司法中价值对齐如何实现的问题更是缺少系统性分析，以至于当前的数字司法建设缺乏充分的智识支撑。为此，本文首先剖析数字司法中价值对齐实现的逻辑机理，并揭示其规范要求，继而系统分析实现价值对齐的过程机制，为数字司法有效推进价值对齐提供可能的路径指引。

二、数字司法价值对齐的逻辑机理

数字司法价值对齐，是指在司法数字化、智能化过程中，通过技术嵌入、制度校准、伦理约束，确保算法模型、数据治理与数字司法系统的运行目标、逻辑和结果，与司法核心价值以及人类社会主流价值观保持一致、协同适配的理念与机制。在数字司法中坚持价值对齐，既符合技术赋能的实践逻辑，也契合筑牢数字司法正当性根基的理论逻辑。为此，数字司法要通过价值对齐坚守司法本质以定其向，防控技术风险以固其基，筑牢司法信任以彰其效，融合司法文明以臻其境。

（一）坚守司法本质

价值对齐及其所凸显的人类价值共识问题，从根本上要求我们深刻把握并始终坚守全人类共同价值。这种共同价值“以共在为前提，以共感为基础，迈向主体间性，运用横向理性，构建公共理性”。当然，数字司法价值对齐并非单一维度的价值适配，而是既要锚定人类共同价值，又要紧扣司法价

值的本质要求，从而契合数字司法的特定价值导向。

第一，数字司法要通过价值对齐锁定司法价值，坚守司法的本质属性。司法价值如同深嵌司法制度的“基因”，既决定司法的本质属性，更引领司法制度的演进方向。传统司法向数字司法转型，是技术手段的升级，而非价值基础的重构。数字司法作为司法制度的数字化转型形态，需以司法正义为核心价值引领，才能避免技术工具理性凌驾于司法价值理性之上。所以，人们需要将司法价值确立为技术应用的根本准则。数字司法若放弃对司法价值的维护，就会沦为技术的附庸，导致其结果与社会公众的价值预期脱节。

第二，数字司法要通过价值对齐防止价值遮蔽，实现司法的价值引领。司法问题一旦转化为技术路径，就容易形成事实上的技术权力。这样，“算法超越其原本的工具属性，获得了实质调配资源的力量”。这种权力形态容易遮蔽司法原有的核心价值内容，造就“算法利维坦”，从而可能导致司法价值的偏离。数字司法价值对齐，是要推动司法数字化进程深度契合人民群众对司法的根本期待，因而需始终锚定并坚守人的核心价值本位。

第三，数字司法要通过价值对齐约束技术理性，明晰司法的价值边界。数字司法必须确立清晰的价值边界，这既是由司法的本质属性与数字科技的工具理性之间的内在张力所决定，也是确保数字司法不偏离其根本目标的逻辑必然。尽管技术迭代日新月异，数字社会下的纠纷样态也层出不穷，但司法公正、权利保障等核心价值始终是不可逾越的底线。唯有通过价值对齐锚定技术应用的方向，才能让数字科技始终扮演司法的赋能者而非主导者，确保数字司法在时代变革浪潮中守住司法初心。

（二）防控技术风险

贝克认为，“风险已经是工业时代的特征”。数字司法在运行过程中存在数据安全、隐私泄露等风险。价值对齐在技术维度的核心意义在于，通过技术架构的优化，将抽象的司法价值转化为可量化、可执行的技术规则，从而为防控技术风险带来

新的思路。

第一，数字司法要通过价值对齐防控技术异化带来风险。数字技术天然带有工具理性取向，对司法的伦理维度与价值属性缺乏内在敏感。若缺乏制度对核心价值的维护，技术极易依循自身发展逻辑而走向异化。技术异化不仅危害物质文明，亦会侵蚀精神文明，其原因在于人类对现代技术难以实现完全的支配与规训。当技术异化传导至司法领域，便容易导致数字司法对司法核心价值的偏离，因此必须通过科学合理的制度设计加以规范与约束。

第二，数字司法要通过价值对齐实现风险防控整体协调。数字司法虽然是人工智能、大数据等技术在司法领域应用的结果，但要建好数字司法，绝非依赖单纯的“技术叠加”，也需要多主体形成整体协同的发展合力。尤其是在数字司法运行体系中，算法设计者、算法监督者、司法办案人员等核心主体，必须锚定司法公正等核心价值实现价值对齐。进而言之，应统筹协调各类司法参与主体，凝聚统一的司法价值共识，再通过价值对齐机制将共识内嵌于数字司法全流程，以统一价值理念引领、规范和指引数字时代的司法实践，筑牢数字司法风险防控的价值根基。

第三，数字司法要通过价值对齐防止风险防控无差别对待。在人工智能、大数据等技术的发展大潮中，不同性质的算法可能带来不同程度的风险。如对其采取同质化防控，易在数字司法中牺牲司法的核心价值。如，算法常被用于案件分流、证据分析、量刑辅助等环节，其中既存在算法歧视这类偏离法律面前人人平等原则的共性风险，又存在因应用环节不同而风险强度与表现也不同的个性风险。这要求价值对齐必须精准化，依托价值对齐识别数字司法各阶段的具体风险，实现风险有效防控与司法价值坚守的有机统一。

（三）筑牢司法信任

信任是建立社会秩序的主要工具之一。在数字司法领域，价值对齐是构建社会信任，进而保障其可接受性的核心路径。数字司法可接受性的实现，并非单纯依赖国家强制力，更根植于社会公众的信

任与认同。若数字司法脱离价值对齐的导向,极易使其丧失公众信任,最终侵蚀司法权威根基。

第一,价值对齐要契合社会大众对司法的价值期待,从而构建公众对数字司法本质的信任。公众对司法的信任,首先源于对司法本质属性的确认,即社会大众判断司法工作是否坚守司法公正、程序正当等核心价值,能否切实维护这些价值。通过司法实现公平正义,是社会正义理论体系探索的一个基本命题。数字司法若一味强调技术效率,忽视对司法价值的回应,极易引发公众对技术异化司法的担忧,进而否定其可接受性。价值对齐的核心作用,正是将抽象的司法核心价值,转化为数字司法中可计算、可呈现的具体形态,让公众清晰感知到,数字工具并未改变司法以人为本的本质,从而筑牢社会大众对数字司法的价值信任根基。

第二,价值对齐要契合社会大众对司法技术风险防范的期待,从而构建公众对数字司法安全的信任。技术的迅速发展,确实给人类带来很多便利,但是也存在很多风险。虽然工业社会由其自身系统制造的危险而突变为风险社会,但人民的安全仍至关重要。在数字化背景下,公众对数字科技介入司法领域抱有安全隐忧,隐私侵犯、数据泄露、算法偏见等问题极易引发信任危机和认同障碍。若无法以价值共识化解此类风险,即便数字司法大幅提升效率,也会因安全隐患失去社会认同。价值对齐以安全为重要导向,通过植入价值考量的风险防控机制,将安全要求深度嵌入数字司法的全流程,能有效消解公众焦虑,为数字司法筑牢安全层面的信任根基。

第三,价值对齐要契合社会大众对司法技术价值共识的期待,从而构建公众对数字司法认同的信任。司法的可接受性,既源于对法律规则的严格恪守,又依托于对社会普遍伦理共识的有效契合。在平等参与和协商交流的当代社会中,共识的缺位将使得司法过程缺乏基础的正当性。数字司法若脱离社会共识,即便严格依法裁判,也可能出现合法不合理的情形,进而引发公众质疑。价值对齐的重要功能正是将动态发展的社会共识融入数字司法的

运行逻辑,增强司法的社会认同与可接受性。没有价值对齐,数字司法可能沦为效率至上的“技术玩具”,即便技术再先进,也会因缺乏信任支撑而难以落地。而通过价值对齐构建的社会信任,能让数字司法真正突破技术桎梏,成为公众可接受、可认同的数字时代正义的新载体。

(四) 融合司法文明

司法文明是司法活动及其制度在历史演进中形成的进步形态与文明程度,是法治文明的核心组成部分。数字司法虽是技术与制度融合的产物,但也承载着社会道德共识与人文关怀,为其价值对齐提供了根本性精神指引。这一精神内核能够有效规约算法应用边界、锚定技术赋能方向,深度契合司法文明发展脉络,有助于构建现代化司法文明体系。

第一,数字司法要以价值对齐彰显司法温度,这是数字司法融入司法文明的核心方向。司法是承载价值判断的实践活动,绝非技术逻辑的简单叠加。如习近平总书记所说,“司法活动具有特殊的性质和规律,司法权是对案件事实和法律的判断权和裁决权”。数字技术在提升司法效率、优化流程管理的同时,其“冰冷”的理性特质易使司法过程趋于机械化、程式化,消解司法本应蕴含的人文关怀与温度。因此,数字司法建设必须强化对伦理维度的审视与把控。在算法设计、流程构建、规则制定等全环节,需将公平正义、人权保障、程序正当等核心司法价值作为根本遵循,实现技术逻辑与价值理性的深度融合。

第二,数字司法要以价值对齐维护隐私、保障尊严,这是数字司法融入司法文明的底线要求。在数据驱动的司法模式下,当事人的个人信息、生物特征及生活轨迹等数据被高频采集,若单纯追求技术效率而漠视隐私保护,极易背离司法尊重个体尊严的初衷。为此,数字司法的伦理建构必须通过价值对齐,严守“最小必要原则”,严格限定数据采集范围,禁止司法数据流入非司法场景,从源头防范技术对权利的侵蚀。通过价值对齐的制度化落地,确保数字技术在提升司法效能的同时,始终承

载人文关怀，筑牢司法伦理的坚固防线。

第三，数字司法要以价值对齐促进司法文明导向的技术动态迭代，这是数字司法融入司法文明的关键保障。有人可能会产生疑问，数字司法价值对齐究竟是通过技术优化实现“看得见的正义”，还是通过伦理嵌入重构司法与社会的互动、赋予司法文明新的时代内涵？笔者认为，数字化深刻重塑人类生活，必然推动司法文明演进。数字技术与司法文明的融合并非静态适配，而是随技术革新与文明发展持续调适的动态过程。价值对齐作为维系技术与司法文明同频共振的核心纽带，以司法文明的核心要义为根本遵循，将有效打通技术研发与司法实践之间的壁垒，最终助力实现司法文明的迭代升级与提质增效。

三、数字司法价值对齐的规范要求

一般意义上的价值对齐，强调人工智能应当秉持“与人类一致的价值观”。在此语境下，数字司法以人类共同价值为对标方向，精准契合价值一致性的核心要义。推进数字司法价值对齐，先要明确其规范基准，确立其底层标尺与正当性根基，再进一步细化推进价值对齐的具体要求，为数字司法价值对齐的落地实施提供清晰明确的行动指引。

（一）数字司法价值对齐的规范基准

在数字司法语境下，价值对齐需契合司法价值尤其是数字司法价值的特殊性。一方面，数字司法的价值导向需深度契合人类社会的普遍共识，与人类社会普遍的道德判断、核心伦理认知保持同频共振；另一方面，数字司法的运行全流程更需借助价值对齐机制，充分彰显司法本身的应然价值内核。因此，数字司法价值对齐的规范基准是数字司法中的司法价值。

1. 数字司法价值对齐要对齐司法价值

有学者认为：“司法的元价值主要有秩序、正义、法治与人权。”而秩序、正义、法治、人权等司法元价值，本质上就是法律价值。司法固然应当遵从这些传统价值，但数字司法所遵从的并非单纯的传统法律价值，而是在司法特定场景中经过改造的价值，可概括称之为司法价值。具体可从以下三

个维度进行解释：

第一，数字司法的核心场域是司法实践，价值对齐需适配司法权运行的特殊规律。数字司法是司法权在数字时代的运行形态，是技术进步在法律系统中引发的重大变革，其场域限定于立案、审理和裁判等司法活动。价值对齐的核心目标是解决技术逻辑与司法权运行逻辑的适配问题，而非对整体法律价值的全面映射。

第二，数字司法的核心功能是实现司法公正与效率的统筹推进，价值对齐需直接锚定司法的价值目标。法律价值的功能是为整个法律体系提供价值引领，其目标具有宏观性与间接性；而数字司法的核心功能是通过技术赋能优化司法过程、提升司法质量。数字司法价值对齐将防止技术工具偏离司法的目标，避免技术工具侵蚀司法公正。

第三，司法价值是法律价值在司法场域的具象化与实践化，价值对齐需具备可操作性。法律价值与司法价值是本源与派生、指导与践行的关系。一方面，法律价值是司法价值的本源与核心指引，它为司法价值划定了根本边界与价值基准；另一方面，司法价值是法律价值的实践转化与特殊呈现。司法价值是法律价值在司法场域的派生形态，聚焦司法活动的具体目标与准则。

2. 数字司法价值对齐要凝聚数字司法价值

数字司法价值对齐的司法价值是在数字司法中能够实现的数字司法价值。数字司法价值是司法价值在数字场景中的具象化体现，是新科技应用于司法领域时，所要实现的符合司法本质要求的价值追求。数字司法价值与传统司法价值之间存在承续与分野，进而彰显出自身特有的理论内核与实践品格。

第一，数字司法价值以传统司法价值为底色，叠加数字正义的新内涵。传统司法价值以公平正义、程序正当等为核心基准，该基准构成数字司法的价值底色。但数字司法的价值基准并非对传统司法价值基准的简单复刻与移植，而是深度融入包括数据资源合理分配、数字权利充分配置、算法决策公开透明和代码规制规范有效等在内的数字正义

特殊意涵,形成“传统基准-数字维度”的复合价值结构。

第二,数字司法价值以传统司法价值为根基,深度依赖数字化新载体。传统司法价值的实现,主要依赖“人力+制度”的双重载体。法官的专业素养、职业道德是实现司法公正的核心人力保障,诉讼法、证据规则等则是规范司法行为、保障价值实现的制度支撑。而数字司法价值的实现,形成了“技术+数据+制度”的多元复合载体。其中,智能系统成为司法价值实现的重要中介,司法数据则成为驱动司法价值优化的核心要素。

第三,数字司法价值以传统司法价值为遵循,呈现数字司法价值冲突新形态。传统司法价值冲突,多表现为形式正义与实质正义、效率与公平等经典维度的张力,其消解路径主要依靠法官行使司法裁量权、运用法律解释方法予以调适平衡。而数字司法领域的价值冲突既涵盖传统司法固有的冲突样态,更衍生出技术逻辑(效率优先等)与司法价值之间的特殊对立,其消解路径亦需深度嵌入技术规制理念与规则。

3. 数字司法价值对齐中司法价值的双层内涵

数字司法价值对齐的司法价值,既要涵盖传统司法核心价值,也要囊括数字技术赋能司法实践所衍生的独特价值,即数字司法价值。传统司法价值与数字司法价值,共同构成了数字司法发展中必须深度融合的价值共同体,是数字司法价值对齐必须遵循的规范基准。

一方面,传统司法价值相对固定,主要围绕公正、权利保障、程序正当等核心要素展开,这些要素均根植于司法权的权力属性与社会治理功能。其中,公正是司法的首要价值,是司法权运行的根本准则,确保纠纷解决的结果公平合理;权利保障是司法的核心使命,聚焦于维护公民合法权益,彰显司法的人文关怀;程序正当是司法公正的重要支撑,通过规范司法流程,保障诉讼参与人的各项权利。这些司法价值并非主观建构,而是依托司法权的公权力属性,结合司法的纠纷解决、社会治理等职能,在长期的司法实践中逐步沉淀而成,构成司

法活动必须恪守、不可逾越的价值底线。

另一方面,数字司法在承续传统司法价值的基础上,添加了技术安全、数据伦理、透明公开等新兴价值维度,这些维度成为数字司法价值体系的重要组成部分。技术安全价值主要体现为保障数字司法系统的稳定性、安全性与可靠性,避免因技术故障、网络攻击等导致司法程序中断、数据泄露或裁判错误。数据伦理价值聚焦于规范司法数据的采集、存储、使用与共享,避免数据滥用对当事人隐私权等合法权益造成侵害。特别是司法数据包含大量当事人的个人信息、案件敏感信息,若缺乏规范约束,可能出现数据泄露、过度采集等问题,违背司法保障权利的核心要求。透明公开价值是数字技术赋能下司法公开原则的升级与延伸,其核心是依托数字化手段,打破司法流程中的信息壁垒,实现司法活动全环节、全要素的可查询、可监督、可追溯,既坚守传统司法公开的核心要义,又结合数字技术特性形成独特的实践形态。

(二) 数字司法价值对齐的具体要求

价值对齐作为数字司法健康发展的核心逻辑,需以规范基准为出发点,推动数字司法中的算法价值追求与法律精神、社会伦理及人文关怀深度契合、同频共振,其具体要求集中体现为维护一致性、确保可控性、保持鲁棒性、避免恣意性四个方面。

1. 维护一致性

算法深度融入司法运行全过程,催生了以技术赋能司法、数据驱动正义为特征的数字司法新形态。在这一阶段,“技术深度赋能司法体现为最大化司法裁判的可计算空间”。但数字司法中的算法是天然的“技术派”,可能缺乏对司法价值的自主感知与主动承载,为此,需要通过价值对齐实现算法价值与司法价值的契合。

第一,通过价值对齐实现数字司法追求程序公正与实体公正的统一。关于程序公正和实体公正的关系,有学者认为二者可能有冲突,但更多学者主张二者是统一的。程序公正和实体公正的统一在数字司法中要得到充分体现,一方面,算法设计要能够将司法流程环节标准化,保证司法参与人均能够

获得相应的程序性权利；另一方面，算法设计也要坚持排除非理性干预，实现规则统一适用，减少人为裁量的随意性，为司法公正筑牢技术屏障。

第二，通过价值对齐实现数字司法追求司法效率与司法公正的统一。司法的效率与公正问题，在市场经济时代尤获关注。在市场经济活动日益频繁的现代社会，如何在确保司法公正的前提下更快提高司法效率，是世界各国司法程序所关注的焦点。在数字司法中，一方面，算法要能够促进资源优化以契合司法繁简分流、快速解纷的现实需求，并帮助司法文书快速生成；另一方面，运用算法提升司法效率不得偏离司法的本质，不能违背司法公正的要求。

第三，通过价值对齐实现数字司法追求司法普遍性与司法个性化的统一。在保障司法普遍性上，数字司法依托价值对齐中统一法律适用的核心要求，通过标准化技术架构消解差异。依托统一的智能办案平台，将法律条文、司法解释、类案裁判规则转化为算法模型，为不同地域、层级的司法主体提供一致的法条检索、类案推送服务。同时，在落实司法个性化上，数字司法以价值对齐精准推进权利保障为导向，通过技术精准赋能实现差异化裁量，使二者在公正、权利保障的核心价值引领下达成统一。

2. 确保可控性

数字司法所运用到的大模型，是人类智能技术赋能司法实践的结果。在数字科技深度融入司法领域的进程中，价值实现的可控性已成为防范数字司法技术异化的核心前提，而价值对齐通过将数字司法的技术逻辑与司法价值深度“捆绑”，正成为构建这一可控性框架的关键路径。

第一，通过价值对齐实现数字司法中算法价值取向的可控性。数字司法价值对齐并非对技术应用的绝对管控，而是关于数字司法价值的制度设计与技术校准之间的动态平衡。确保数字司法的运行逻辑始终围绕司法价值展开，避免因技术自主迭代、效率优先导向引发数字司法中的算法价值偏离，是价值对齐的首要任务。人应当始终是机器的尺度。

数字司法中的人工智能可依托数据与算法辅助司法流程和司法决策，但绝不能突破工具属性这一定位，更不能上升为司法价值观念的最终决定者。

第二，通过价值对齐实现数字司法中算法价值内容的可控性。价值对齐中所要对齐的价值内容，需要由人类来定义。主体价值的内容是主体的创造力，它是主体创造客体价值的能动力量。人作为主体，一切价值均由人生产且契合人的需求，因此数字司法中，价值必须由人类定义和评判。司法价值并非抽象规则，而是植根于社会伦理共识、法律精神与个案情理的有机整体，需法官结合个案裁量、回应当事人诉求、契合社会动态期待，而非让人工智能反向塑造司法的价值内核。

第三，通过价值对齐实现数字司法中算法价值基准的可控性。数字司法价值对齐要求算法运行始终契合人类司法固有的价值准则，这既是司法活动的本质要求，也是数字司法必须坚守的价值前提。司法固有的价值基准，既回答了司法为何存在的根本命题，也为司法运行划定了不可逾越的边界，更是数字科技深度融入司法、防范技术异化的根本遵循。因此，技术在司法中的赋能水平越高、影响力越大，对价值引领的依赖与紧迫性就越强。唯有坚持以公平、正义、人权、程序正当等核心价值引领技术应用，让科技服务司法而非主导司法，才能实现数字赋能与司法价值同频共振，使数字司法成为守护社会正义、保障人民权利的坚实支撑。

3. 保持鲁棒性

鲁棒性是一个跨学科词汇，指的是既保持稳定但又具有一定灵活性的状态。在不确定性和危机出现的情况下，鲁棒性已经成为系统能否生存的关键，因为鲁棒性证明系统有提供值得信赖的服务的能力，能够在特定条件下保持系统/制度稳健运行。在数字司法中，通过价值对齐实现算法价值的鲁棒性，是让算法在数据变化、场景迭代、社会价值共识微调的复杂条件下，始终保持对司法价值基准的稳定遵循。

第一，通过数字司法价值对齐保持司法价值的稳定性。数字司法实现价值对齐，乃是技术理性回

归司法本位的核心路径。这一目标要求技术应用必须深植于司法的价值谱系,以规范算法逻辑、构建统一裁量参考系为抓手,将形式正义与实质正义的内在要求内嵌于技术规则之中。此举既能通过数据闭环防止裁量权滥用,确保裁判尺度统一,又能以技术透明消解暗箱操作,维护司法权威以提升司法公信力。因此,即便司法形态随技术迭代不断演进,价值对齐始终是平衡司法变革之“变”与法理坚守之“不变”的关键,确保数字司法在效能提升与价值实现之间行稳致远、达致双赢。

第二,通过数字司法价值对齐实现司法价值的可塑性。王泽鉴认为,各国法律多以一定之人的形象为规范基准。此言揭示了法律与人的深层共生关系。不同的群体形象塑造了特色各异的法律制度,进而沉淀出独特的司法价值内核。司法价值并非无源之水,其生成既植根于社会结构与理论体系的交融,其形塑亦依托于特定时代的群体画像。因此,司法价值绝非亘古不变,而是随时代演进不断迭代的动态体系,呈现出鲜明的时代特征。鉴于此,数字司法的构建须秉持辩证思维:既要坚守司法价值的本质属性以维护制度根基,又要顺应技术变革赋予其在特定时空与主题下的弹性与可塑性,最终确保其精准契合数字时代的治理需求,实现基础理论与现代技术的有机统一。

第三,通过数字司法价值对齐实现司法价值的适应性。随着数字司法的发展,算法应用场景从裁判辅助拓展至合法性判断甚至智能裁判等领域,场景变化可能带来价值位阶的模糊,从而模糊司法价值的本来意义。这种场景化的价值对齐,需要算法在功能拓展时始终以司法程序确定为基准,避免因场景复杂而出现程序简化甚至程序剥夺的风险,实现算法对场景变化的动态适应。因此,数字司法价值对齐始终要按照司法价值的要求,适应当事人程序权利保护的需要,遵循司法程序的公开性、中立性、救济性,避免算法因追求场景适配效率而稀释程序价值及其相应的实体价值。

4. 避免恣意性

司法既是约束权力恣意的重要控制手段,也是

保障公民权利的关键制度安排。若司法权缺乏刚性法律约束,其裁判功能极易偏离权利保障与权力监督的初衷,甚至异化为司法擅断,滋生司法腐败。在数字司法场景中,恣意裁判的倾向更容易被放大,价值取向也可能偏离社会共识。因此,必须通过价值对齐,确保数字司法价值的统一性与共识性,防范选择性司法,守住司法公正底线。

第一,通过促进司法价值的共识性避免恣意性。数字司法运行中若缺乏有效约束,极易为追求技术目标而偏离司法本质。价值对齐需依托制度与技术双重路径,明确要求数字司法始终恪守司法核心价值,杜绝因地域差异、平台偏好、供应商选择等导致价值取向随意化。数字司法强调价值共识,并非否定价值多元性,而是坚守司法领域已形成普遍共识的核心价值,排除非司法价值的不当干扰。同时,排除外部干扰不等于司法封闭运行,而是防止非司法因素对裁判结果形成实质性影响。在此过程中,尤其要避免片面追求司法效率等功利目标,侵蚀算法设计的公正性与价值中立性。

第二,通过警惕数字司法价值的擅断性避免恣意性。数字司法价值对齐通过制度设计与技术优化,杜绝数字司法在该优先何种价值上自主选择,将其价值判断逻辑牢牢锁定在司法价值的框架内,最终实现不同场景、不同系统中数字司法价值标准的统一,避免因技术逻辑异化或地方差异导致司法价值碎片化。数字司法价值对齐防止数字司法权擅断的要求具体表现为如下两点:一是在数字司法场景中,无论是民事案件还是刑事案件,司法价值要能够得到无差别的体现;二是在数字司法系统中,无论是案件事实认定系统还是结果裁判系统,都应当始终贯彻司法价值。

第三,通过防范数字司法价值的选择性避免恣意性。确定性与秩序本身就是社会福利的一部分。司法价值的确定性也是人们一直讨论的话题,并一直在司法实践中努力推行。人类社会发展中,具体价值虽不断变迁,但对核心价值的追求始终未变。在算法实践中,若缺乏核心司法价值锚定,数据筛选偏好、技术依赖等问题易催生新型选择性司法,

加剧恣意风险。数字司法中,价值对齐的初衷是通过制度设计、技术赋能与伦理塑造,避免算法实践中因数据筛选偏好、技术依赖而滋生的司法恣意。

四、数字司法价值对齐的过程机制

数字司法作为司法领域与数字科技深度融合的产物,其价值对齐绝非单纯的技术适配或制度调整,而是关乎司法本质、社会秩序、国家治理乃至全球司法协作的重要议题。按照对齐数字司法价值规范基准、落实价值对齐具体要求的思路,数字司法价值对齐需要在源头校准层、运行管控层、迭代优化层与安全保障层系统构建层次化推进的过程机制,推动价值对齐与司法本质、技术应用、实践需求深度融合,确保数字司法始终坚守核心价值导向、彰显司法本质属性。

(一) 筑牢数字司法价值对齐的算法根基

在数字司法价值对齐的推进过程中,源头校准层需要将司法价值嵌入数字司法技术研发的初始环节,从源头规避算法偏见、数据失真等价值偏离风险,夯实数字司法运行的算法基础。

1. 将司法价值嵌入算法逻辑

在数字司法价值对齐的实践中,将司法价值转化为可执行的算法逻辑是技术嵌入的核心环节,也是筑牢数字司法价值对齐的前置基础。技术层面的价值嵌入突破了价值理念悬浮于技术之上的困境,将抽象司法价值拆解为量化指标、规则模块与约束条件,让算法在运行中主动遵循司法的价值导向。

第一,价值具象化是司法价值转化为算法逻辑的基本前提。法律价值在信息化时代,不仅需要体现人类的情感和道德需要,也需要可计算。甚至还有学者认为,可计算性标准的兴起与动态规则的演进,终将成为这个时代对法律表达范式的历史性贡献。因此,要实现价值对齐,就要将价值进行具象化表达,使司法价值成为可量化、可判断、可校验的具体指标,形成“价值-指标”映射的体系。从数字司法的全流程场景来看,司法价值的具象化表达应当按照不同的场景进行拆解,形成针对性的价值预设指标体系。如在司法审判中,可将正当程序价值依托指标识别转化为具象价值。具体核心指标

为:一是庭审参与完整度,要精准统计当事人发言时长占比、关键意见表达次数;二是异议响应时效与质量,要考核法官异议回应时长,评估回应的针对性与合法性;三是程序告知完备率,要对照法定告知清单,量化权利义务、庭审流程、法律后果告知的完整性与及时性;四是质证权利保障度,要围绕质证环节实质化,评判质证权实现成效,杜绝质证形式化;五是庭审流程合法率,要对标法定庭审规范,量化回避、举证、辩论、最后陈述等环节的合法性程度。依托上述量化可核验参数,可将抽象程序正义转化为算法要素,实现司法价值精准内嵌于算法设计。

第二,使具象化价值进行算法逻辑表达是司法价值转化的核心要义。具象化价值契合算法逻辑,强调司法价值的技术表达与算法能力的价值承接,是数字司法遵循司法规律的重要体现。具体而言,可以分为如下阶段执行:一是在理念构思层面,要预设能够被算法实现的价值具象化技术。这需要算法工程师从技术层面设计衡量指标或者校正指标以表明价值的具象化可行性。二是在具体落实层面,要让数据成为价值的承载体。“数据是一种资源……通过海量数据训练,人工智能迅速掌握技能,从而在很多领域辅助人类完成各项工作,实现人类生产力水平的提升。”所以,数据是一种绝佳的决策工具和价值传递载体。在数字司法全流程中,通过对数据的筛选、关联、计算、校验等使用行为,将抽象的司法价值转化为可落地的具体实践,让数据成为价值传递的介质。

第三,将法律价值特别是司法价值嵌入算法模型,实现价值导向与技术逻辑的有机融合。算法逻辑与法律规范的深度融合,核心是将算法运行的技术原理与法律的规范体系,通过系统性整合实现相互赋能。具体而言,可以从三个层面推进:一是对法律条文进行语义解构,从而将法律规则和基本法律原则嵌入算法模型。对于自然语言所表述的法律条文,算法语言无法直接识别,需推进“代码即法律”向“代码循法律”的转变。“人的指令先通过高级语言传达给某个应用层,再通过逐步翻译、解

释变成硬件能直接反应的机器语言。”把法律变成可供算法遵循的语言，核心是打破自然语言的模糊性、开放性与算法逻辑的精确性、封闭性之间的壁垒，通过语义解构实现法律规则的形式化、逻辑的编码化，让法律从纸面文本变为算法可识别、可运算、可追溯的规则。二是将法律逻辑转化为算法逻辑，实现法律规则向数字代码的形式化转化。语义解构后的法律要素需进一步转化为算法可运算的形式化语言，打破自然语言法律文本与机器可读代码逻辑的壁垒，将法律的规范要求、构成要件、裁量标准转化为可被算法执行的精准代码，既确保代码对法律规则的忠实还原，又实现法律适用的自动化与标准化。例如，可以针对法律规则的构成要件，按“法律规则=构成要件+法律后果+例外情形”的逻辑结构，对条文进行层级化拆解，形成意义明确的规则单元。三是将法律价值特别是司法价值运用算法规则表达出来。“基于模拟大脑运作的机制、深度学习理论以及计算机对人类心理状态的阅读，人工智能能够处理价值问题，并通过属性特征、属性值以及最终形成特征向量的过程使得价值数据化，形成价值数据集。”在数字司法中，价值、技术与规范应当深度耦合，才能够契合司法发展的时代要求。通过设定权重参数、约束条件和优先级规则，在算法中体现公平、正义、比例原则等。如在刑事案件中运用司法自由裁量权时，不能将“刑期”简化为“犯罪金额×情节系数”的机械计算，而应保留对社会危害性、悔罪表现等非量化因素的权重设置，确保算法输出的结果符合司法价值的要求。

2. 为数字司法价值对齐算法培育高质量数据

算法的有效运行离不开数据的支撑。高质量数据是数字司法价值实现的基础，其真实性、完整性、公正性直接决定算法运行的科学性，为公正、高效、便民等价值落地提供坚实的数据保障。然而，数据质量参差不齐的问题，在科技领域早已成为共识。脏数据、错误数据更是无处不在，容易产生消极影响。在数字司法中，数据污染不仅可能直接导致算法决策偏差、证据认定失误，而且可能使司法裁决结果与公平正义背道而驰，降低司法公信力。培育

高质量数据的相关制度包括以下方面：

第一，建立数据采集标准制度。要明确数字司法数据采集的范围、格式、编码规范与填写要求，统一案件信息、人员信息、证据材料等各类数据的采集标准，细化数据采集颗粒度，修订完善案件信息业务标准，适配审判执行各业务条线精细化分析需求，避免因标准不一导致的数据混乱、缺失问题，实现数据的规范性与统一性。

第二，建立数据质量保障制度。该制度应当由以下制度构成：一是司法数据标准统一制度，明确司法数据采集、加工和存储等的统一规范；二是全流程司法数据质量管控制度，覆盖数据采集、清洗、存储、应用的全生命周期；三是司法数据质量审核与核查制度，建立事前审核、事中监测、事后核查的系统性规则；四是司法数据分类分级与权益保障制度，依据数据来源（公共、企业、个人）与敏感程度分类分级管控，对涉案个人信息、涉密数据强化脱敏处理与隐私保护，明确数据各参与方权责，规范数据加工使用权限。

第三，建立数据清洗校准制度。该制度聚焦反向纠偏，通过驱除脏数据、修正错误数据，确保司法算法所依赖的数据始终保持纯正与可靠。一是从制度内容看，要以数字司法价值为标尺明确核心制度内容，优先划定歧视性数据清除标准，将年龄、性别、身份偏见等违背司法公正的数据列为必清项。同时，规范数据清洗全流程，明确清洗范围、操作步骤、结果校验要求，留存清洗过程完整记录。二是从清洗方法看，要整合多元清洗方法形成适配体系，分类规范各类方法的适用场景与操作准则。如基于完整性约束的方法用于排查数据缺失、格式异常问题；基于规则的方法适配歧视性数据精准筛查，通过预设司法公正规则定向清除偏见数据等。三是从责任主体看，明确多元主体责任边界，落实全链条追责。司法机关作为核心主体，统筹负责并牵头制定清洗标准，承担最终审核与责任兜底义务；技术服务提供商为操作主体，对操作合规性与结果准确性负责；数据提供方承担源头责任，确保原始数据无刻意偏见信息。

（二）强化数字司法价值对齐的流程约束

在数字司法价值对齐的推进过程中，运行管控层的核心旨趣在于，以常态化制度与动态审查为抓手，确保数字司法技术在应用全流程中能够及时识别并纠正价值偏差，从而筑牢价值对齐的持续性与稳定性防线。这一目标的实现，有赖于一系列制度、机制作为支撑。

第一，建立预设和校准数字司法价值模型的制度。计算机编程形成的模型预设了法律数据的“输入-输出”方式，为数字司法价值对齐算法模型提供基础预设模式。具体而言，该制度包括：一是从制度内容看，以数字司法价值为核心明确制度核心内容，划定模型预设校准的范围、标准与底线。聚焦数字司法价值，细化算法参数设定、逻辑框架、决策阈值的校准规范，严禁嵌入歧视性、倾向性预设。二是从校准方法看，采用分层校准、双重核验并融合动态迭代推进方法。分层校准即先完成核心参数价值适配校准，再开展场景化细节校准；双重核验结合算法自动校验与跨领域专家评审，邀请各领域专家联合核查校准结果。三是从校准类型看，在数字司法算法编码开发阶段，针对法律规范与法律原则两类核心司法要素，分别构建专项测试机制与动态校正制度，规避仅依赖法律规范“单刀直入”的机械适用局限，实现技术赋能与司法规律深度契合。四是从责任主体看，要遵循权责对等、全程追溯原则划分多元主体责任。司法机关作为主导主体，牵头制定校准标准，审核校准结果，承担最终责任兜底义务；技术研发主体负直接责任，严格按照标准开展预设校准，保障算法逻辑与参数设定合规；第三方伦理审查机构承担监督责任，独立核查校准过程的价值适配性。

第二，建立数字司法价值对齐算法的审查和备案制度。《最高人民法院关于规范和加强人工智能司法应用的意见》中就提到要“坚持技术研发、产品应用、服务运行的透明性，保障人工智能系统中的……各个环节能够以可解释、可测试、可验证的方式接受相关责任主体的审查、评估和备案。”数字司法在建设过程当中，不仅应当将价值对齐算法

作充分论证，也需要通过程序上的审查和备案制度保证价值对齐算法符合司法价值的要求。价值对齐算法开发者在应用该算法之前应当将算法模型方案（含校准标准、技术路径）报有权部门审查和备案，相关材料需包含价值偏差应急预案，并明确未来校准的触发条件。其具体流程包括四个步骤：第一步由算法研发主体提交备案材料，含算法逻辑、价值校准方案、测试报告等核心文件；第二步是司法机关收件后，在特定工作日内完成材料完整性审核；第三步开展实质审查，联合技术、法学和伦理学专家，核查算法价值适配性与合规性，通过模拟案例测试验证效果，出具审查意见；第四步是将审查通过的算法予以备案。

第三，建立数字司法价值对齐算法的透明与公开制度。在人类社会，透明是交往顺畅的前提。在数字司法中，“算法透明原则，既适用于政府的算法规制，也适用于私营机构的算法规制”。算法透明要求算法的可解释性与司法公开原则相结合，让技术决策过程成为司法透明的有机组成部分。算法的核心逻辑需向司法参与者公开，这是破解司法算法黑箱、保障司法透明与程序正义的关键举措。具体而言，可结合不同司法参与者的角色定位与实际需求，构建分层、精准、可理解的公开体系。其一，对司法参与者而言，要消除数字鸿沟，保障程序参与权、知情权。当事人、律师等是司法程序的直接参与者，其主体性的丧失往往源于自身的数字能力不足或被技术流程排斥。为此，需要通过确立技术适配、线下兜底等制度，确保所有参与者能平等享受数字司法的便利，而非因技术导致边缘化。其二，对司法监督者而言，要打破技术黑箱，保障知情权与监督权，确保司法监督者的主体性。公众对司法的信任源于看得见的正义，数字司法的技术复杂性若转化为“黑箱”，会削弱公众的监督能力。监督是数字司法获得更好发展的有效途径。确保数字司法系统透明和负责任，将有助于建立对这些系统的信任和信心，并确保它们得到合乎道德且有效的使用，推动数字司法工具与司法规律、公众需求深度适配。

第四,建立数字司法价值对齐算法的第三方评估制度。作为一种治理工具,第三方评估具有广泛的制度意义。在算法深度应用的行业领域,第三方评估制度亦逐步兴起。此类评估能够为算法使用者提供客观依据,进而推动开发者持续优化算法体系。第三方评估具备独立性、专业性、权威性等鲜明特征,评估结果相对公正、客观。通过建立第三方评估制度,客观验证算法价值主张与利益相关方诉求的一致性,可以防范算法偏差引发的伦理风险、权益损害及社会争议。其具体制度内容包括:一是从评估主体看,明确评估主体为独立第三方机构,需与司法机关、算法研发主体无利益关联,保障评估中立性。二是从评估资质看,设定严格资质准入标准,第三方机构需取得司法行政部门备案许可与数据安全等级保护认证,具备固定办公场所与专业团队。三是从评估能力看,强化评估能力建设,第三方机构需搭建适配数字司法场景的评估体系,具备算法逻辑解析、数据质量校验、价值偏差识别等能力。四是从评估效力看,明确评估结果的法定效力与应用场景,评估报告作为算法备案、迭代优化、责任认定的重要依据,司法机关需将其纳入算法监管档案。

(三) 推动数字司法价值对齐的迭代优化

在数字司法价值对齐的推进过程中,迭代优化层的核心目标是实现价值对齐的优化升级,通过全流程追溯、问题整改与经验转化和标准更新,推动制度与技术持续适配司法价值需求。

第一,建立数字司法价值对齐算法迭代的可追溯制度。算法在任何程序中的使用都并非无形无迹,而是会留下可追溯的操作痕迹。从数据输入、参数运算到结果输出,算法运行的每一个环节都会在系统中生成相应记录。这些记录既包括数据流转轨迹、运算逻辑节点,也涵盖结果生成的时间与条件,为后续的算法监管、问题排查和责任追溯提供了基础依据。算法溯源更多关注的是算法软件在程序实现过程中输出量值的准确可靠,因此,算法的可追溯性应贯穿算法全生命周期。一是从概念看,算法可追溯性是对算法设计、开发、运行等过程的

关键节点进行结构化记录、存储与关联,保持算法全生命周期的可记忆性,确保任何环节的算法操作、数据或决策都可被反向查询、验证与还原。二是从方法看,可追溯制度要构建技术留痕与合法性审查相结合的双重追溯体系。在技术层面,依托区块链存证等技术,对算法训练数据集、模型结构调整等关键信息进行哈希加密与链式存储,实现全流程不可篡改;在法律层面,建立“版本回溯-差异比对-价值校验”的审查方法,通过对比迭代前后算法在相似案件中的决策输出,校验其是否偏离预设的司法价值。

第二,建立数字司法价值对齐算法问题导向的持续改进制度。该制度聚焦数字司法实践中价值对齐的现实困境与显性问题,包括以下四个层面:一是在问题层面,构建多源联动的线索采集机制,确保数字司法价值偏差问题被全面、及时识别。既要打通算法运行的全场景数据接口,自动抓取案件裁判中的算法决策输出等结构化数据,标注价值冲突的异常节点,也要建立常态化的人工排查渠道,定期梳理典型案例,明确问题描述、提交主体,为后续研判提供清晰、可追溯的基础素材。二是在研判层面,需依托技术和法律融合的双维度分析框架,定位问题产生的核心诱因。在技术上,组织算法研发人员、数据工程师对模型架构、训练数据集、参数设置进行全链路复盘,排查是否存在数据样本偏差、算法逻辑漏洞等技术缺陷;在法律上,由法学专家、资深法官对照司法价值,分析算法设计是否违背法律、法规、司法解释等。三是在整改层面,需针对根源研判结论制定差异化的修复策略。针对数据样本偏差问题,扩充多样化、代表性的案件数据集,剔除带有偏见的样本,补充特殊类型案件的标注信息,优化训练数据的价值导向性。四是在优化层面,推动算法与司法价值的动态适配。在整改方案试点验证通过后,将优化后的算法模型纳入正式运行体系,建立版本迭代备案制度,明确新版本的价值锚点、优化内容与适用范围。

第三,建立数字司法价值对齐算法的经验转化与标准更新制度。数字司法实践中,算法可能出现

价值偏差、与司法需求脱节等问题，而经验转化与标准更新正是破解这一难题的重要支撑。推进算法价值对齐的有效经验、成熟做法要进行提炼、固化，同时要动态更新算法设计、数据应用、流程规范等相关标准，确保算法始终与司法本质、社会伦理、公众需求保持一致。该制度的核心框架为：一是在制度内容上，需以经验沉淀、标准迭代和价值锚定为核心框架，明确制度适用范围、主体权责与运行规范。二是在转化路径上，要融合实践、理论与技术三个维度，实现司法经验向算法标准的精准转化。从实践维度看，建立典型案例萃取机制，从算法价值对齐的成功判例中提炼裁判规则、价值导向与适用场景，形成可复制的实践经验库；从理论维度看，组织法学与算法专家对实践经验进行解构，将隐性的司法价值判断转化为显性的理论模型与量化指标；从技术维度看，推动理论指标向算法代码与参数的转化，嵌入算法训练与决策流程，确保经验转化的技术可行性与价值一致性。三是在联动机制上，需构建跨主体、跨环节与跨层级融合的协同体系，保障经验转化与标准更新的高效运转。在跨主体联动方面，建立司法实务部门、算法研发机构、标准化组织、第三方评估机构的联席会议制度，定期通报经验采集进展、转化难点与标准实施效果。在跨环节联动方面，设计“经验采集→理论转化→技术适配→标准制定→落地应用→效果反馈”的流程，明确各环节的衔接节点与反馈机制。在跨层级联动方面，打通上下级司法机关的经验共享通道，提升制度的系统性与适用性。

（四）构建数字司法价值对齐的保障机制

在数字科技深度嵌入数字司法的决策场景中，安全保障层的闭环监管已成为维护人类主体核心地位的关键防线。其核心目标是在 AI 等智能工具提供司法决策支持的同时，始终将人类置于目标定义者、逻辑审查者、最终决策者的核心位置，避免因技术依赖导致人类主体地位被弱化、边缘化甚至替代。

第一，要通过公众参与吸纳多元价值诉求。司法价值的内涵具有社会性，若仅由算法开发者或企

业定义价值，易导致企业利益优先而忽视公共利益。价值对齐需通过多元主体参与，形成符合社会共识的公平价值标准。“作为一套制度系统的公众参与，不论是在国家宏观的政治生活中，还是在微观的行政过程中，都被理解为健全国家民主制度、提升公共生活民主性和公共性的重要途径。”数字司法虽依托技术提升了效率，但其核心仍需锚定司法为民的本质。公众作为司法服务的直接受众与社会价值的承载者，其多元诉求是数字司法避免技术异化、专业封闭的重要校准器。唯有通过制度化的公众参与，将不同群体的价值期待嵌入数字司法的设计、应用与优化全流程，才能让数字工具真正对齐社会共识性正义。此外，公众参与机制的有效性还需破解认知鸿沟与代表性不足两大难题：一方面，需通过数字司法科普降低参与门槛，用典型案例说明公众诉求如何影响系统优化，避免因公众对技术或法律的认知不足导致诉求偏离实质；另一方面，需通过分层抽样确保公众参与的代表性，可通过基层自治组织协助收集诉求、组织线下会议等形式，避免参与权集中于数字素养较高的群体。

第二，要通过风险干预精准纠偏，防范人类主体地位丧失。无论是数字算法还是人类算法，每种算法都有自己的优缺点。因此，如何规避缺陷而放大优势，需要有必要的监管措施。价值对齐的核心风险在于 AI 自主决策可能偏离人类需求，算法黑箱引发决策失控、价值偏差持续放大侵蚀主导权，因此制度设计需聚焦关键决策环节，通过强制介入确保人类的主体地位不被架空。风险干预制度正是通过提前预警、实时阻断、事后修复的全链条设计，将这些隐性风险转化为可控变量，从源头守住人类在技术体系中的核心位置。一是从风险预警来看，需建立多维度风险监测指标，精准识别主体地位弱化的信号。在数字司法领域，针对智能量刑辅助系统，可设置法官对 AI 建议的采纳率阈值、个案人工修正率过低等指标，防止法官因过度依赖 AI 丧失独立研判能力。二是在风险阻断环节，需明确分级处置机制，避免风险扩散。对偶尔出现价值偏差的轻度风险进行人工干预，要求技术方在规定时限

内结合人类专家意见优化算法。三是事后修复环节需聚焦风险影响的挽回与制度漏洞的补位。一方面，对因AI风险受损的人类权益进行救济，建立AI失误补偿基金制度，提供兜底保障；另一方面，针对风险暴露的制度缺陷及时修订，不断补充完善指标体系，避免同类风险重复发生。

第三，要保留司法人员对算法结论的最终审核权，实现权利保障。在社会交往中，人类努力以主体身份出现，避免沦为他人支配或操纵的对象。因此，保留司法人员对算法结论的最终审核权，并非对技术的否定，而是对司法本质与价值对齐目标的坚守。这种不可或缺的最终审核权，其必要性根植于两个层面：一是从算法的固有局限看，司法人员的最终审核权是弥补技术缺陷、规避价值偏离的必然要求。算法的决策逻辑始终依赖训练数据与预设模型，其自身存在三重局限：训练数据偏差易导致决策结论失准；算法模型无法覆盖司法实践中诸多非量化的价值维度；法律原则的灵活适用、个案中的利益权衡，均超出了算法的机械运算能力。这些固有局限，迫切需要司法人员通过最终审核予以弥补和修正。二是从司法的本质属性看，最终审核权是维护司法权人类主导属性、保障价值对齐方向的核心锚点。数字司法价值对齐是让技术服务于司法为民的目标，而非让技术逻辑主导司法决策。若放弃司法人员的最终审核权，将算法结论直接作为裁判依据，实则是将司法权的核心价值判断与正义裁量让渡给技术，会导致司法异化为数据驱动的机械流程，偏离以人为本的价值初衷。此外，最终审核权还需通过制度细化实现从原则到操作的转化，避免沦为形式。一方面，需明确审核权的实质审查义务，要求司法人员不仅对算法结论的合法性进行审查，更要对合理性进行研判，且需在裁判文书中书

面说明采纳或修正算法结论的理由；另一方面，需配套算法可解释性支撑，要求算法提供结论生成依据。如此一来，在数字司法价值对齐的推进中，司法人员对算法结论的最终审核权将成为技术工具性与司法主体性的平衡支点、效率提升与价值坚守的结合纽带，最终让技术真正成为赋能司法、守护正义的工具，而非主导司法、偏离价值的力量。

五、结语

数字司法价值对齐并非技术功能与司法制度的简单耦合，而是以司法本质属性坚守为核心导向，通过多维度协同机制实现技术理性与司法价值理性动态均衡的系统性工程。本文探讨数字司法价值对齐的逻辑机理、规范要求与过程机制等核心议题，不仅回应了数字司法价值对齐如何落地的问题，更厘清了技术赋能与司法本真的辩证关系。价值对齐的革命性意义在于，它打破了传统人机关系中技术主导、人类被动的单向桎梏。从技术路径来看，价值对齐机制通过将人类多元价值转化为技术可理解、可执行的逻辑，为人类赋予了主导技术方向、优化技术路径的主动权，让人机协同从效率适配的工具层面，跃升为价值共生的生态层面，最终推动技术进步与人类发展形成深度嵌合的良性循环。

需说明的是，本文聚焦于宏观层面的理论建构与框架设计，后续研究还可从两方面深化拓展：一是开展特定司法场景的实证研究，细化不同场景下价值权重的动态配置标准与适配机制；二是对数字司法特殊价值的实现路径进行深入探究。唯有持续推进理论深化与实践探索，才能使价值对齐机制与数字司法的发展演进形成良性适配，为司法现代化进程提供更为坚实的理论支撑与实践指引。

（技术编辑：邓语鑫）