中国人民大学法学院
数字法学教研月报

2025 年第 9 期（总第 21 期） 2025 年 9 月 24 日

本期看点

【数字法治大事件】国家网信办密集出台政策文件，包括发布《人工智能安全治理框架》2.0 版、《国家网络安全事件报告管理办法》，并就未成年人网络平台认定、电子单证应用、大型平台个人信息保护监督委员会设立等 3 项办法公开征求意见；行业与地方实践亮点纷呈，首批可信数据空间创新试点公布，国家发改委与能源局推“人工智能+”能源发展意见，北京以千亿条数据建“一区三中心”，西安“五位一体”打造“丝路数港”，湖北聚焦 AI 产业新高地建设。

【研究动态】本期研究覆盖数字法学核心领域。基础理论探讨数据爬取合法性、数字法律关系等；个人信息保护聚焦合规审计、生成式 AI 下权益保障等；数据确权与流通研究数据财产权定位、算力财产权等；人工智能涉及侵权责任、立法框架等；平台治理、数字行政与司法、虚拟财产等领域亦有深度研究，夯实数字法治理论基础。

【教研活动】中国人民大学法学院预告建院 75 周年系列活动，含世界百所法学院院长论坛及 14 个平行国际论坛；中国科学技术法学会举办“人工智能法律前沿问题”研讨会；第八届中国网络法治高端论坛在喀什召开，聚焦 AI 法治治理，促进学术与实践融合。

【数字法评】

《论“通知”规则在生成式人工智能作品侵权中的类推适用》，《比较法研究》2025 年第 4 期，作者：王利明、包丁裕睿。

《数智司法鉴定的关键要素——以特征比对型鉴定的核心环节为视角》，《数字法治》2024 年第 6 期，作者：李学军、宋华秋。

本期目录

数字法治大事件 3

关于公开征求《未成年人用户数量巨大和对未成年人群体具有显著影响的网络平台服务提供者认定办法（征求意见稿）》意见的通知 3

《人工智能安全治理框架》2.0 版发布 5

国家互联网信息办公室发布《国家网络安全事件报告管理办法》 5

《国家网络安全事件报告管理办法》答记者问 5

国家互联网信息办公室关于《促进和规范电子单证应用规定（征求意见稿）》公开征求意见的通知 7

国家互联网信息办公室关于《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）》公开征求意见的通知 10

专家解读丨落实个人信息保护法规定 设立大型网络平台个人信息保护监督机构 13

人民日报 | 首批可信数据空间创新发展试点名单发布 数据规模化流通有了“高速公路” 15

国家发展改革委 国家能源局关于推进“人工智能+”能源高质量发展的实施意见 16

地方动态 | 解锁公共数据密码 千亿条数据支持北京“一区三中心”数据发展 21

地方动态丨西安市“五位一体”协同发力 打造“丝路数港”西部数据流通新枢纽 22

地方动态 | 牢牢把握数据驱动人工智能发展重点任务 加快打造全国人工智能产业发展新高地 22

研究动态 24

基本理论 24

个人信息保护 29

数据确权与流通 31

人工智能 34

平台治理 38

数字行政与司法 39

虚拟财产 40

教研活动 41

中国人民大学法学院建院 75 周年系列活动预告丨世界百所法学院院长论坛 +14 个平行主题国际论坛 41

要闻 | 中国科学技术法学会“人工智能法律前沿问题”研讨会顺利举行 41

活动综述 | 第八届中国网络法治高端论坛暨“人工智能健康有序发展的机遇、挑战及其法律治理”学术研讨会顺利举行 42

数字法评 44

论“通知”规则在生成式人工智能作品侵权中的类推适用 44

数智司法鉴定的关键要素——以特征比对型鉴定的核心环节为视角 53

学术顾问：王利明

编 委 会：张新宝 丁晓东 王 莹 张吉豫

编 辑 部：阮神裕 卞 龙 艾 薇 邓语鑫 何 芮 梁因格 李佳丽 林诗敏 麻卓妍 乔彩霞 王 昊 朱恬馨

联系方式：RUCdigitallaw@163.com

本期编辑：梁因格

数字法治大事件

导言：当前数字技术深度融入经济社会各领域，数字治理体系建设成为推动高质量发展的关键支撑。近期，我国多部门密集出台政策文件、启动试点实践，从国家制度完善到地方创新探索，构建起覆盖网络安全、数据流通、人工智能治理、未成年人保护等领域的全方位数字治理框架，为数字经济健康发展筑牢制度根基。国家层面制度建设持续发力，国家互联网信息办公室先后发布《人工智能安全治理框架》2.0 版与《国家网络安全事件报告管理办法》，并通过答记者问解读政策细节，强化人工智能安全与网络安全事件处置的刚性约束；同时就未成年人网络平台认定、电子单证应用规范、大型网络平台个人信息保护监督委员会设立等 3 项办法公开征求意见，靶向回应未成年人网络权益、个人信息安全、产业数字化规范等核心关切，推动数字治理精准化、法治化。行业创新与地方实践同步推进，首批可信数据空间创新发展试点名单公布，为数据规模化流通搭建“高速公路”；国家发展改革委、国家能源局联合出台“人工智能+”能源实施意见，促进数字技术与能源产业深度融合。地方层面同样亮点纷呈，北京以千亿条公共数据支撑“一区三中心”建设，西安通过“五位一体”机制打造“丝路数港”，多地聚焦数据驱动人工智能发展，加快建设全国 AI 产业新高地，形成上下联动、区域协同的数字治理新格局，为培育新质生产力、抢占数字发展主动权提供坚实保障。

关于公开征求《未成年人用户数量巨大和对未成年人群体具有显著影响的网络平台服务提供者认定办法（征求意见稿）》意见的通知

原载：“网信中国”微信公众号

落实《未成年人网络保护条例》要求，为进一步强化未成年人网络保护，保护未成年人合法权益，国家网信办会同国家新闻出版、电影部门和国务院教育、电信、公安、文化和旅游、市场监管、广播电视等有关部门起草了《未成年人用户数量巨大和对未成年人群体具有显著影响的网络平台服务提供者认定办法（征求意见稿）》（以下简称《办法》），现向社会公开征求意见。

《未成年人网络保护条例》（以下简称《条例》）明确了网络平台对未成年人的普遍性保护义务，并在第 20 条对未成年人用户数量巨大和对未成年人群体具有显著影响的网络平台提出了特殊义务要求。《办法》落实《条例》要求，细化了具体认定标准、认定流程和相关工作要求，压紧压实网络平台未成年人网络保护主体责任，更好守护未成年人健康成长。

公众可通过以下途径和方式提出反馈意见：

1. 通过电子邮件方式发送至：ptrdbf@cac.gov.cn。

2. 通过信函方式将意见寄至：北京市西城区车公庄大街 11 号国家互联网信息办公室网络综合治理局，邮编：100044，并请在信封上注明“未成年人用户数量巨大和对未成年人群体具有显著影响的网络平台服务提供者认定办法”。

意见反馈截止日期为 2025 年 10 月 15 日。

国家互联网信息办公室

2025 年 9 月 16 日

未成年人用户数量巨大和对未成年人群体具有显著影响的网络平台服务提供者认定办法

（征求意见稿）

第一章 总则

第一条 为科学认定未成年人用户数量巨大和对未成年人群体具有显著影响的网络平台服务提供者范围，根据《中华人民共和国网络安全法》《中华人民共和国未成年人保护法》《未成年人网络保护条例》等法律法规规定，制定本办法。

第二条 认定工作坚持依法依规、公平公正、实事求是的原则，充分保障未成年人合法权益，综合平衡相关网络平台和相关方合法权益，发挥各方力量强化未成年人网络保护。

第三条　认定工作由国家网信部门负责统筹协调，国家新闻出版、电影部门和国务院教育、电信、公安、文化和旅游、市场监督管理、广播电视等有关部门依据各自职责共同参与，并指导设立认定咨询委员会承担具体工作。

第四条　认定工作应避免影响网络平台服务提供者的正常生产经营活动。网络平台服务提供者应当配合认定机构的认定工作。

第五条　认定工作原则上应当公开进行。认定工作涉及的国家秘密、商业秘密、个人隐私等应当依法予以保密。

第二章 认定标准

第六条　符合以下情形之一的，应当认定为未成年人用户数量巨大的网络平台服务提供者：

（一）该网络平台提供的产品或者服务专门以未成年人为服务对象，注册用户在 1000 万以上或者月活跃用户在 100 万以上。

（二）该网络平台提供的产品或者服务的对象不局限于未成年人的，未成年人注册用户数量在 1000 万以上或者月活跃未成年人用户在 100 万以上。

第七条　认定对未成年人群体具有显著影响的网络平台服务提供者，应当综合考虑以下因素：

（一）该网络平台下载量、注册用户数量、月活跃用户数量规模较大，或网络产品的销售额、交易量等较大；

（二）该网络平台未成年人登录频次、使用时长、喜爱程度、消费金额等指标较高；

（三）该网络平台涵盖大量涉及或面向未成年人的信息内容；

（四）该网络平台在 3 年内存在较多涉未成年人突出情况，违法违规问题较为突出，受到社会广泛关注；

（五）该网络平台在相关垂直领域排名靠前；

（六）其他对未成年人群体具有显著影响的因素。

第三章 程序启动

第八条　国家网信部门会同有关部门按照认定流程，研究启动认定工作。

认定工作原则上每 3 年开展一次，也可在网络平台出现用户数量激增、对未成年人影响显著提升、社会广泛关注等情形时视情启动。

第九条　认定咨询委员会根据认定标准与实际情况，提出纳入认定工作的网络平台服务提供者建议名单，经国家网信部门会同有关部门审定后，通知相关网络平台服务提供者开展自评估工作。

第十条　网络平台服务提供者应当按照认定标准，全面准确评估对未成年人的影响，并在收到通知后 20 个工作日内提交自评估报告。

第十一条　网络平台服务提供者对所提交的自评估报告及材料完整性、真实性负责，不得具有误导性，并根据要求提供必要解释说明等补充材料。

第四章 论证与决定

第十二条　认定工作应当通过座谈会、听证会、实地走访等多种形式听取各方意见建议。

认定名单征求意见稿向社会公开征求意见。公开征求意见的期限一般为 30 日。

第十三条　认定咨询委员会根据意见征求情况，拟定认定名单建议稿。

第十四条　国家网信部门会同有关部门根据认定标准，综合研究确定最终认定名单并向社会公布。

第十五条　网络平台服务提供者对认定结果存在异议的，可在 15 个工作日内，向认定咨询委员会提交书面异议申请及相关证明材料，详细说明异议理由。

第五章 认定调整

第十六条　国家网信部门会同有关部门对认定结论的实施效果进行跟踪监测。

已认定的网络平台服务提供者认为自身已持续 6 个月不符合认定标准的，可以提交变更认定结论申请以及证明材料。

国家网信部门会同有关部门按照本办法前述规定的有关程序，做出启动认定或者驳回决定。

第十七条　国家网信部门会同有关部门可根

据认定工作开展情况，按程序适时优化调整认定标准，并提前进行公示。

第六章 附则

第十八条 本办法所称网络平台服务提供者涵盖各类网络产品和服务提供者、智能终端产品制造者和销售者以及互联网新技术新应用新产品提供者等。

第十九条 本办法自公布之日起施行。

《人工智能安全治理框架》2.0 版发布

原载：“网信中国”微信公众号

9 月 15 日，在 2025 年国家网络安全宣传周主论坛上，《人工智能安全治理框架》2.0 版（以下简称《框架》2.0 版）正式发布。

落实《全球人工智能治理倡议》，《人工智能安全治理框架》1.0 版（以下简称《框架》）于 2024 年 9 月发布，并受到国内外广泛关注。一年来，人工智能技术和应用发展迅速，为应对新机遇新挑战，在国家网信办指导下，由国家互联网应急中心牵头组织人工智能专业机构、科研院所、行业企业联合制定了《框架》2.0 版。作为全国网安标委技术文件，《框架》2.0 版在 2024 年《框架》基础上，结合人工智能技术发展和应用实践，持续跟踪风险变化，完善优化风险分类，研究探索风险分级，动态调整更新防范治理措施。

国家互联网应急中心负责同志表示，《框架》2.0 版的发布，顺应全球人工智能发展潮流，统筹技术创新与治理实践，在人工智能安全、伦理、治理等方面不断深化共识，促进形成安全、可信、可控的人工智能发展生态，构建跨国界、跨领域、跨行业的协同治理格局。同时，有助于推进多边机制下人工智能安全治理合作，推动世界范围内技术成果的普惠共享，确保人类社会共享人工智能发展的红利。

国家互联网信息办公室发布《国家网络安全事件报告管理办法》

原载：“网信中国”微信公众号

近日，国家互联网信息办公室发布《国家网络安全事件报告管理办法》（以下简称《办法》），自 2025 年 11 月 1 日起施行。

《办法》共十四条，主要对网络安全事件报告适用范围、监管职责、报告主体、报告流程、报告时限、报告内容等提出规范要求。

国家互联网信息办公室有关负责人指出，为规范网络安全事件报告管理，及时控制网络安全事件造成的损失和危害，落实《网络安全法》《关键信息基础设施安全保护条例》等法律法规，国家互联网信息办公室制定《国家网络安全事件报告管理办法》，进一步规范和明确网络安全事件报告流程和要求。

目前，网信部门已开通 12387 网络安全事件报告热线、官网、微信公众号、微信小程序、邮件、传真等六类网络安全事件报告渠道，网络运营者、社会组织和个人可通过上述渠道向网信部门报告网络安全事件。

《国家网络安全事件报告管理办法》答记者问

原载：“网信中国”微信公众号

近日，国家互联网信息办公室公开发布《国家网络安全事件报告管理办法》（以下简称《办法》），自 2025 年 11 月 1 日起施行。日前，国家互联网信息办公室有关负责人就《办法》有关问题回答了记者提问。

一、问：请介绍一下《办法》的出台背景？

一是控制和减少网络安全事件造成的损失和危害。近年来，各类网络安全事件频发，影响范围和危害程度不断升级。从网络安全事件应急处置工作实践来看，发生网络安全事件后，及时向有关部

门报告，有利于及时处置网络安全事件，防止危害扩大或产生不良社会影响。

二是细化完善《网络安全法》等法律法规中有关规定的客观需要。《网络安全法》第二十五条明确，网络运营者应当在发生危害网络安全的事件时，按照规定向有关部门报告。《办法》作为专门规定，为网络运营者明确了网络安全事件报告的具体要求。

三是借鉴国际通行做法。网络安全事件报告是国际惯例，近年来，美国、欧盟、澳大利亚、印度等均通过立法或指令建立强制性的网络安全事件报告义务，明确网络运营者事件报告时限等要求。

二、问：什么是网络安全事件？

《办法》所指网络安全事件是指由于人为原因、网络遭受攻击、网络存在漏洞隐患、软硬件缺陷或故障、不可抗力等因素，对网络和信息系统或其中的数据和业务应用造成危害，对国家、社会、经济造成负面影响的事件。

三、问：《办法》的适用范围和事件报告主体是什么？

《办法》的适用范围和事件报告主体为在中华人民共和国境内建设、运营网络或者通过网络提供服务的网络运营者。

四、问：《办法》的主要内容有哪些？

一是明确了网络运营者的报告义务。《办法》规定，网络运营者在发生网络安全事件时，应当按照本办法的规定进行报告。

二是明确了网络安全事件报告的监管职责。《办法》明确，国家网信部门负责统筹协调全国网络安全事件报告管理工作，省级网信部门负责统筹协调本行政区域内网络安全事件报告管理工作。

三是明确了网络安全事件报告的流程和时限要求。《办法》针对关键信息基础设施、中央和国家机关及直属单位，以及其他网络运营者，分别明确了网络安全事件报告的流程和时限要求。

四是明确了网络安全事件报告的渠道。《办法》明确，网信部门建设 12387 网络安全事件报告热线电话、网站、邮箱、传真等方式，统一接收网络安全事件报告。

此外，《办法》还明确，对迟报、漏报、谎报或者瞒报网络安全事件造成重大危害后果的运营者依法从重处罚；对采取合理必要的防护措施，有效降低网络安全事件影响和危害，并按照规定及时报告的运营者，可视情从轻或不予追究责任。

五、问：网络安全事件报告的流程和时限要求是什么？

涉及关键信息基础设施的，网络运营者应当第一时间向保护工作部门、公安机关报告，最迟不得超过 1 小时。属于重大、特别重大网络安全事件的，保护工作部门在收到报告后，应当第一时间向国家网信部门、国务院公安部门报告，最迟不得超过半小时。

网络运营者属于中央和国家机关各部门及其直属单位的，应当及时向本部门网信工作机构报告，最迟不得超过 2 小时。属于重大、特别重大网络安全事件的，各部门网信工作机构在收到报告后，应当第一时间向国家网信部门报告，最迟不得超过 1 小时。国家网信部门收到报告后及时向有关部门通报。

其他网络运营者应当及时向属地省级网信部门报告，最迟不得超过 4 小时。属于重大、特别重大网络安全事件的，省级网信部门在收到报告后，应当第一时间向国家网信部门报告，最迟不得超过 1 小时，并同时向同级有关部门通报。

本行业领域有专门规定的，网络运营者还应当按照行业主管监管部门要求报告。

涉嫌违法犯罪的，网络运营者应当及时向公安机关报案。

六、问：网络安全事件报告的渠道有哪些？

为便于网络运营者、社会组织和个人快速、规范报告网络安全事件，网信部门已开通了六类网络安全事件报告渠道。一是可拨打 12387 网络安全事件报告热线按语音提示进行报告；二是可访问网络安全事件报告官网 12387.cert.org.cn 进行报告；三是可微信搜索“12387”小程序，进入首页后点击“事件报告”；四是可关注“国家互联网应急中

心 CNCERT”微信公众号，点击“事件报告”；五是可发送邮件至邮箱 12387@cert.org.cn 报告；六是可发送传真至 010-82992387 报告。

七、问：网络安全事件如何分级？

《办法》中明确了《网络安全事件分级指南》，作为《办法》附件。《网络安全事件分级指南》参照国家标准《信息安全技术 网络安全事件分类分级指南》（GB/T 20986-2023）制定，以有限枚举的方式给出特别重大、重大、较大、一般等四个级别网络安全事件的分级定量指标。

国家互联网信息办公室关于《促进和规范电子单证应用规定（征求意见稿）》公开征求意见的通知

原载：“网信中国”微信公众号

为了促进和规范电子单证推广应用，提高货物贸易和运输数字化水平，降低全社会物流成本，保障电子单证活动当事人合法权益，维护国家安全和社会公共利益，根据有关法律法规，我办会同有关部门起草了《促进和规范电子单证应用规定（征求意见稿）》，现向社会公开征求意见。公众可通过以下途径和方式提出反馈意见：

1. 通过电子邮件方式发送至：dzdz@cac.gov.cn。

2.通过信函方式将意见寄至：北京市海淀区阜成路 15 号国家互联网信息办公室信息化发展局，邮编 100048，并在信封上注明“促进和规范电子单证应用规定征求意见”。

意见反馈截止时间为 2025 年 10 月 13 日。

附件：促进和规范电子单证应用规定（征求意见稿）

国家互联网信息办公室

2025 年 9 月 13 日

促进和规范电子单证应用规定

（征求意见稿）

第一章 总则

第一条 为了促进和规范电子单证推广应用，提高货物贸易和运输数字化水平，降低全社会物流成本，保障电子单证活动当事人合法权益，维护国家安全和社会公共利益，根据《中华人民共和国电子签名法》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国海商法》等法律、行政法规，制定本规定。

第二条 本规定所称电子单证，是指采用数据电文形式，能够证明当事人之间存在货物运输、仓储、货物保险等法律关系的单证，包括电子提单、电子多式联运单证、电子海运单、电子铁路货运单、电子航空货运单、电子仓单、电子货物保险单等。电子单证包括可转让电子单证和不可转让电子单证。

本规定所称电子单证系统，是指基于网络信息技术，为接收、存储和发送电子单证信息提供技术服务的信息系统。

本规定所称电子单证系统运营者，是指负责建设、运营电子单证系统，向公众提供电子单证签发、存储、变更、转换、转让、质押、流转等服务的机构、组织。

本规定所称电子单证系统相关服务支持方，是指为电子单证系统有效运转提供支持或服务的机构、组织。

本规定所称电子单证系统用户，是指使用电子单证系统的机构、组织、个人。

第三条 坚持发展和安全并重、促进创新和依法治理相结合的原则，鼓励电子单证的推广应用，分类分级管理电子单证系统，提升货物贸易和运输的数字化、便利化水平。

第四条 国家网信部门和国务院工信、公安、交通运输、商务、海关、税务、市场监管、金融等部门，加强政策协同，依据各自职责促进和规范电子单证应用。

第五条 相关行业组织应当加强行业自律，建

立健全行业自律制度和行业准则，促进电子单证的规范应用和生态繁荣发展。

第六条　国家有关部门推动电子单证领域的国际交流与合作，参与相关国际规则制定和推广适用，推动相关国际互认。

鼓励相关企业、科研机构深化与国际组织、联盟机构的互动交流，广泛开展电子单证领域的国际业务合作，积极参与国际标准化工作。

第二章 电子单证应用的促进

第七条　鼓励货物贸易、物流、金融等领域机构和企业在开展业务时认可、使用电子单证，提升业务应用数字化水平，促进行业提质增效。鼓励金融机构在依法合规、风险可控前提下，根据电子单证特点，探索使用数字人民币等新型支付方式开展跨境支付，积极稳妥开展金融产品和服务模式创新。

第八条　鼓励相关企业、科研机构、行业组织和公共服务机构在电子单证技术创新、科技成果转化、风险防范等方面开展协作，分享实践经验，促进电子单证技术发展与应用。

第九条　国家有关部门依据各自职责，加强电子单证领域标准制定工作，及时组织制定国家标准、行业标准，鼓励行业协会、产业技术联盟等社会团体和相关企业参与电子单证相关标准制定，有序推进现有行业标准向国家标准转化，积极推动成熟国内标准向国际标准转化。

第十条　电子单证系统运营者、电子单证系统相关服务支持方从事电子单证业务活动，应当遵守相关法律、行政法规、强制性国家标准以及其他规范性要求。

鼓励电子单证系统运营者、电子单证系统相关服务支持方采用与电子单证有关的推荐性国家标准、行业标准，及时对标国际标准和国外先进标准，加强对电子单证信息的互认共享。

第十一条　鼓励电子单证系统运营者、电子单证系统相关服务支持方、电子单证系统用户开展电子单证标准实施效果评价，向国家标准、行业标准的制定机构反馈标准实施信息，提出标准修订建议，以促进标准持续优化，适应行业发展需求。

第十二条　电子单证系统运营者应当制定业务规则，依法核验用户的身份信息，并与用户签订服务协议，明确双方权利义务，要求其承诺遵守法律规定、业务规则。

电子单证系统相关服务支持方应当与电子单证系统运营者签订服务协议，明确双方权利义务。

第十三条　鼓励我国电子单证系统运营者在国家数据跨境安全管理制度框架下，依法依规向境内外用户提供跨境业务服务，促进国际贸易、运输领域的电子单证应用。

第三章 电子单证系统的可靠性、安全性

第十四条　鼓励相关机构、组织和个人通过可靠的电子单证系统从事电子单证的签发、存储、变更、转换、转让、质押、流转等活动。

可靠的电子单证系统应实现以下功能：

（一）确保电子单证信息全程可追溯，不可篡改；

（二）能够识别电子单证的签发人；

（三）若支持电子单证和纸质单证相互转换，应确保转换前后的信息一致，并在单证中体现相关转换信息。

为可转让电子单证提供服务的可靠的电子单证系统，还应当实现以下功能：

（一）能够识别电子单证并确保其具有唯一性；

（二）确保电子单证自生成至不再具有效力期间均处于排他控制状态，且能够识别其控制人；

（三）确保电子单证在转让时对其控制随之转移。

第十五条　电子单证系统的可靠性，是指系统在为电子单证签发、存储、变更、转换、转让、质押、流转等活动提供服务时，能稳定、持续运行并实现本规定第十四条所规定功能的能力。

评价电子单证系统可靠性的因素包括：

（一）适用于该系统的运行规则；

（二）对系统所存储数据完整性的保障；

（三）系统对电子签名可靠性的要求；

（四）防止未经授权访问或使用该系统的能力；

（五）该系统所使用的硬件和软件的安全性；

（六）该系统运行的稳定性；

（七）该系统的灾难恢复能力；

（八）该系统是否定期接受独立机构的审计及其频次和范围；

（九）本规定第十七条第一款所称认证机构就该系统可靠性作出的认证；

（十）相关技术标准；

（十一）其他相关因素。

第十六条　鼓励电子单证系统运营者和用户使用符合国家标准，具备企业用户身份核验认证、授权操作、自我管理、按需提供、安全可靠等功能，能有效支撑电子单证系统安全可靠运行的电子身份验证服务系统，和具备自然人身份核验功能的国家网络身份认证公共服务等权威匿名身份认证系统，保障货物贸易、运输的安全便利。

第十七条　鼓励电子单证系统运营者向依法设立的认证机构申请系统可靠性认证，规范开展电子单证系统建设与运维服务工作。

电子单证签发人使用的电子签名的可靠性认证，依照《中华人民共和国电子签名法》等有关法律、行政法规的要求实施。

第十八条　电子单证系统运营者应当加强风险管理，完善业务流程，支持相关方在签发时确认电子单证信息，防范电子单证记载货物信息与实际货物信息不符的风险。

第十九条　电子单证系统运营者应当遵守《中华人民共和国网络安全法》等有关法律、行政法规和国家有关规定，使用符合国家有关安全标准的技术和设备，落实网络安全等级保护制度，确保电子单证系统和电子单证的网络安全。

电子单证系统运营者应当建立健全网络安全技术措施，持续监测系统的运行状况，及时处置异常情形。应当制定网络安全事件应急预案，在发生网络安全事件时，立即启动应急预案，采取相应补救措施，并按照有关规定向有关主管部门报告。

电子单证系统属于关键信息基础设施的，电子单证系统运营者还应当履行关键信息基础设施运营者应当承担的网络安全义务。

第二十条　电子单证系统运营者和用户在处理电子单证数据时应当遵守《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律、行政法规和国家有关规定，加强电子单证数据分类分级保护，保障电子单证系统的数据安全，维护电子单证系统用户及相关主体的个人信息权益。

电子单证数据的存储，应当依其所属行业和类型，符合相关主管部门制定的关于数据存储和数据安全的规定。

第二十一条　向境外提供与电子单证有关的数据，应当符合国家关于数据出境的相关规定。国际贸易、跨境运输过程中收集和产生的与电子单证相关的数据向境外提供，如果不包含个人信息或重要数据，或者所涉个人信息仅为签发、转让、质押电子单证或行使电子单证权利所必需的，免予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。

第四章 监督检查和法律责任

第二十二条　国家网信部门会同国家有关主管部门针对电子单证的类型、技术特点、行业特点，依照有关法律、行政法规的规定，制定相应的分类分级管理规则或者指南，完善管理方式，鼓励电子单证的应用与创新发展。

第二十三条　国家有关主管部门依据各自职责，对电子单证系统建设运营和电子单证业务进行监督检查，电子单证系统运营者、电子单证系统相关服务支持方和相关当事人应当依法予以配合。有关部门实施监督检查，不得妨碍被检查对象正常的生产经营活动。

参与监督检查的相关机构和人员，对在履行职责中知悉的国家秘密、商业秘密、个人隐私和个人信息应当依法予以保密，不得泄露或者非法向他人提供。

第二十四条　电子单证系统运营者、电子单证

系统相关服务支持方和相关当事人违反本规定条款的，由有关主管部门依照《中华人民共和国电子签名法》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律、行政法规的规定予以处罚；法律、行政法规没有规定的，由有关主管部门依据职责予以警告、责令限期改正；拒不改正或者情节严重的，责令暂停提供相关服务；构成犯罪的，依法追究刑事责任。

第五章 附则

第二十五条 本规定自 年 月 日起施行。

国家互联网信息办公室关于《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）》公开征求意见的通知

原载：“网信中国”微信公众号

为指导规范大型网络平台设立、运行个人信息保护监督委员会，对个人信息保护情况进行监督，保护个人信息权益，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，国家互联网信息办公室起草了《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）》，现向社会公开征求意见。公众可以通过以下途径和方式提出反馈意见：

1.登录中国网信网（www.cac.gov.cn），进入首页“网信要闻”查看文稿。

2.通过电子邮件方式将意见发送至：shujuju@cac.gov.cn。

3.通过信函方式将意见寄至：北京市海淀区阜成路 15 号国家互联网信息办公室网络数据管理局，邮编 100048，并在信封上注明“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”。

意见反馈截止时间为 2025 年 10 月 12 日。

附件：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）

国家互联网信息办公室

2025 年 9 月 12 日

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）

第一条 为指导规范大型网络平台设立、运行个人信息保护监督委员会，对个人信息保护情况进行监督，促进大型网络平台个人信息保护合规水平提升，保护个人信息权益，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、行政法规和国家有关规定，制定本规定。

第二条 中华人民共和国境内提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者（以下称为大型网络平台服务提供者）设立、运行个人信息保护监督委员会，适用本规定。

本规定所称个人信息保护监督委员会，是指由大型网络平台服务提供者成立的，主要由外部成员组成的，对大型网络平台个人信息保护情况进行监督的独立机构。

本规定所称个人信息保护监督委员会外部成员（以下称为外部成员），是指具备个人信息保护专业知识和技能，不在受聘大型网络平台担任除监督委员会成员外的其他职务的人员。

国家网信部门会同国务院公安部门等有关部门依照有关法律法规规定，制定发布大型网络平台清单。

第三条 个人信息保护监督委员会（以下称为监督委员会）成员人数应与大型网络平台业务规模、用户数量等相匹配，一般不得少于 7 人，外部成员占比不低于三分之二。

第四条 外部成员应当保持身份和履行职责的独立性，受聘期间不得具有下列情形：

（一）本人或者其直系亲属在受聘大型网络平台服务提供者或者其子公司、分公司、控制企业任职；

（二）直接或间接持有受聘大型网络平台服务

提供者已发行股份百分之一以上，或者是受聘大型网络平台服务提供者前十名股东中的自然人股东及其直系亲属；

（三）本人或者其直系亲属在直接或间接持有受聘大型网络平台服务提供者已发行股份百分之五以上的股东单位或者在受聘大型网络平台服务提供者前五名股东单位任职；

（四）为受聘大型网络平台服务提供者或者其子公司、分公司、控股企业提供财务、法律、咨询、审计等专业服务的人员；

（五）其他可能影响外部成员独立性的情形。

第五条　担任监督委员会外部成员应当符合下列条件：

（一）符合本规定第四条规定的独立性要求；

（二）具备履行职责的专业素质，熟悉个人信息保护、数据安全相关法律法规、国家标准等，从事个人信息保护相关工作不少于 3 年；

（三）具备良好的声誉，能够客观公正、独立廉洁地履行职责；

（四）具有正常履行职责的身体条件、工作时间等；

（五）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；

（六）法律、行政法规规定的其他条件。

第六条　大型网络平台服务提供者组织提名外部成员时，应当充分了解被提名人职业、学历、职称、工作经历、兼职情况、有无违法犯罪和重大失信记录等，并对其符合独立性和担任外部成员的其他条件提出意见。被提名人应当就其符合独立性和担任外部成员的其他条件作出说明。被提名人同时受聘的大型网络平台不得超过三家。

外部成员聘任决定应当由大型网络平台服务提供者董事会等决策机构或其授权的董事长、执行董事等高级管理人员作出。

第七条　大型网络平台服务提供者可以按照国家规定，结合专兼职的工作内容和工作时长、工作量等情况给予外部成员与其承担职责相适应的报酬。报酬的标准由董事会等决策机构批准，并在大型网络平台服务提供者个人信息保护社会责任报告中披露。个人信息保护社会责任报告应当每年公开发布，并且便于查阅和保存。

除上述报酬外，外部成员不得从大型网络平台服务提供者及其持股百分之五以上股东、控股股东、实际控制人或者有利害关系的单位和人员取得其他利益。

第八条　监督委员会内部成员（以下称为内部成员）由大型网络平台服务提供者董事会等决策机构或其授权的董事长、执行董事等高级管理人员决定。

第九条　监督委员会设主任一名，由外部成员担任，经监督委员会全体成员选举产生，负责监督委员会工作。

监督委员会设秘书一名，可由内部成员担任，负责处理监督委员会的会议筹备、文件管理、组织联络等综合性事务。

第十条　监督委员会成员在同一大型网络平台任期为三年，任期届满，可以连任，连任不得超过两届。

监督委员会成员在任期届满前可以提出辞任。监督委员会成员辞任应当提前 30 个工作日向大型网络平台服务提供者董事会等决策机构或其授权的董事长、执行董事等高级管理人员提交书面辞任报告。

第十一条　监督委员会成员应当勤勉尽责，有下列情形之一的，由董事会等决策机构或其授权的董事长、执行董事等高级管理人员作出解聘决定：

（一）外部成员不再符合本规定第五条规定的条件；

（二）连续三次未出席监督委员会会议或者连续两次未出席监督委员会定期会议；

（三）不适合担任监督委员会成员的其他情况。

大型网络平台服务提供者解聘监督委员会成员的，应当允许被解聘监督委员会成员提出异议说明，并将解聘原因、异议说明及异议说明答复等情况及时报送所在地省级网信部门。

监督委员会成员在任职期内辞任或被解聘等，导致监督委员会成员少于 7 人或外部成员占比低于三分之二的，大型网络平台应当在 30 个工作日内补任相关人员；若辞任或被解聘成员为监督委员会主任，应当及时选举产生新的主任；若辞任或被解聘成员为监督委员会秘书，应当及时任命新的秘书；在补任完成前，个人信息保护监督委员会应当继续履行相应职责。

第十二条　大型网络平台服务提供者应当根据本规定，制定监督委员会规则，面向社会公开征求意见不少于 15 日，根据公开征求意见情况修改完善后，报经董事会等决策机构批准。监督委员会规则一般应当载明下列事项：

（一）监督委员会的组成、成员任期和任免程序；

（二）监督委员会职责及监督事项；

（三）监督委员会成员职责；

（四）监督委员会主任的选举和职责；

（五）监督委员会秘书的产生和职责；

（六）监督委员会会议的召开、通知、表决、监督意见形成和记录；

（七）监督委员会运行机制、经费保障；

（八）需要明确的其他事项。

第十三条　监督委员会重点对大型网络平台下列事项进行监督：

（一）个人信息保护合规制度体系建设情况；

（二）平台或产品个人信息保护规则制修订情况；

（三）敏感个人信息保护情况；

（四）个人信息保护影响评估开展情况；

（五）个人信息保护合规审计开展情况；

（六）落实监管机构提出的整改要求情况；

（七）个人信息安全事件处理情况；

（八）个人行使个人信息权益保障情况；

（九）向境外提供个人信息合规情况；

（十）个人信息保护社会责任履行及报告发布情况；

（十一）个人信息保护负责人履行职责情况；

（十二）利用个人信息进行自动化决策等情况；

（十三）与个人信息保护相关的其他重大事项；

（十四）法律、行政法规规定的其他监督事项。

监督委员会应当建立与大型网络平台用户常态化沟通机制，听取用户意见建议，回应用户关切。

第十四条　监督委员会成员履行下列职责：

（一）出席监督委员会会议，对审议监督事项发表意见，对需表决事项进行表决；

（二）了解大型网络平台个人信息保护情况，可就有关问题进行询问，并要求答复；

（三）可列席大型网络平台个人信息保护工作有关会议；

（四）听取大型网络平台用户的个人信息保护意见；

（五）向监督委员会报告大型网络平台个人信息处理活动相关风险和问题；

（六）法律、行政法规规定的其他职责。

第十五条　监督委员会应当至少每三个月召开一次定期会议，就大型网络平台个人信息保护监督事项进行审议，并作出监督意见。

主任或者三分之一以上成员提议，可召开临时会议，审议大型网络平台个人信息保护相关事项。

第十六条　监督委员会会议有过半数成员出席方可举行。秘书应当于会议召开 15 日前将会议的时间、地点、议题等事项通知全体成员，同时提供完备的会议资料。

主任或者三分之一以上成员认为会议筹备不充分的，可要求延期召开会议或者延期审议事项，秘书应当对会议延期情况进行记录。

第十七条　监督委员会成员应当按时出席监督委员会会议。确有原因不能出席的，应当对会议事项提出明确的书面意见。

第十八条　监督委员会应当就会议审议事项进行充分讨论，监督委员会成员应当客观地发表独立意见，监督委员会秘书应当完整准确记录会议情况，形成会议记录和决议记录，出席会议的成员应

当核实记录内容并签署意见。

监督意见应当取得全体成员三分之二以上同意。监督委员会应当及时将监督意见通知大型网络平台服务提供者。

第十九条　大型网络平台服务提供者应当自收到监督意见之日起 10 个工作日内处理监督委员会作出的监督意见，确有理由不予处理的，应当答复监督委员会。监督委员会认为答复理由不成立的，可以向所在地省级网信部门报告。

第二十条　监督委员会成员在履行职责过程中发现大型网络平台个人信息处理活动存在风险或违法违规收集处理个人信息等问题的，应当向监督委员会和大型网络平台服务提供者提出书面建议。监督委员会和大型网络平台服务提供者未处理的，或成员对处理结果有异议的，成员应当向所在地省级网信部门报告。

第二十一条　监督委员会及其成员在履行职责过程中，不得干预大型网络平台正常运营，对在履行职责过程中知悉的个人信息、商业秘密、保密商务信息等应当依法予以保密，不得泄露或者非法向他人提供。

第二十二条　监督委员会及其成员履行职责过程中，大型网络平台服务提供者有关组织、人员应当积极配合，不得恶意拒绝、阻碍或者隐瞒，不得干预其独立履行职责。

第二十三条　大型网络平台服务提供者应当为监督委员会及其成员提供履行职责所需的工作条件和协助，做好相关对接工作。个人信息保护负责人应当每三个月向监督委员会报告大型网络平台个人信息保护有关情况。

第二十四条　大型网络平台服务提供者应当及时向社会公开监督委员会规则、成员信息等。

已设立监督委员会的大型网络平台，不再满足本规定第二条相关条件，向所在地省级网信部门报告有关情况后，可以撤销监督委员会。

第二十五条　大型网络平台服务提供者应当在监督委员会成立、变更之日起 30 个工作日内，向所在地省级网信部门报送监督委员会规则、成员名单等信息。

监督委员会应当每年向所在地省级网信部门报送履行职责情况报告。

省级网信部门每年向国家网信部门报送大型网络平台个人信息保护监督委员会相关工作情况。

第二十六条　国家网信部门会同国务院有关部门建立健全信息共享和通报工作机制，对全国大型网络平台落实本规定要求的情况进行监督检查。

省级网信部门负责统筹协调本行政区域内大型网络平台落实本规定要求的监督管理工作。

第二十七条　监督委员会履行职责不到位，导致大型网络平台出现重大个人信息安全事件的，或严重违反个人信息保护相关法律法规的，省级以上网信部门应当要求大型网络平台服务提供者解散监督委员会，重新成立监督委员会。

第二十八条　任何组织和个人有权对大型网络平台服务提供者、监督委员会及其成员的违法违规活动向省级以上履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当在 15 个工作日内依法处理，并将处理结果告知投诉、举报人。

第二十九条　大型网络平台服务提供者违反本规定的，依照《中华人民共和国个人信息保护法》、《网络数据安全管理条例》等法律法规的规定处理；构成犯罪的，依法追究刑事责任。

第三十条　本规定由国家网信部门负责解释。

第三十一条　本规定自　年　月　日起施行。

专家解读丨落实个人信息保护法规定 设立大型网络平台个人信息保护监督机构

原载：“网信中国”微信公众号

作者：张新宝　中国人民大学法学院吴玉章高级讲席教授

国家互联网信息办公室发布《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）》

（以下简称《规定》），为大型网络平台设立、运行个人信息保护监督委员会提供了明确的规范指引，本文将从依据与目的、主要内容、配套国标等三方面进行解读。

一、依据与目的

2021 年 8 月 20 日第十三届全国人民代表大会常务委员会第三十次会议通过的《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）已自 2021 年 11 月 1 日起施行。《个人信息保护法》作为我国网络信息领域的三大支柱性法律之一，是保护公民个人信息权益、规范个人信息处理活动和促进个人信息合理利用的基本法律。《个人信息保护法》有诸多制度创新，其中第 58 条关于大型网络平台个人信息保护特别义务的规定就是一项全新的个人信息保护法律规范，在世界主要国家已有的个人信息保护立法中没有类似的先例。第 58 条规定：“提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行下列义务：（一）按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督；.....”由于《个人信息保护法》的许多规定属于没有先例可循的创新性规定，而且法律条文相对抽象和简略，因此施行这些规定需要相应的配套细则，方能落地实施并取得实效。《个人信息保护法》对国家网信部门的相关职责和权限做出了规定：“国家网信部门统筹协调有关部门依据本法推进下列个人信息保护工作：（一）制定个人信息保护具体规则、标准”（第 62 条第 1 款）。国家网信部门依据《个人信息保护法》和《网络数据安全管理条例》等法律法规制定了一系列实施《个人信息保护法》的规定和规章。此次发布征求意见的《规定》是其中之一。

二、主要内容

《规定》共计 31 条，分别明确了制定该文件的目的依据、大型网络平台与监督委员会及其成员的概念、监督委员会的设立要求、外部成员的独立性要求与履职条件、外部成员的提名与聘任及报酬、内部成员的任职、成员的任期与辞任及解聘、监督委员会规则和职责、成员职责、监督委员会的定期会议与临时会议、会议举行和延期、会议出席要求、监督意见的作出和记录、监督意见的处理、提出建议、保密要求、（大型网络平台服务提供者）配合履职要求、履职条件保障、委员会信息公开及撤销、信息报送、委员会履职监督、投诉举报、罚则和解释权等内容。

《规定》旨在指导规范大型网络平台设立、运行个人信息保护监督委员会，对个人信息保护情况进行监督，促进大型网络平台个人信息保护合规水平的提升，强化个人信息保护。“大型网络平台”是指在中华人民共和国境内提供重要互联网平台服务、用户数量巨大、业务类型复杂的网络平台，此等平台的清单将由国家网信办会同国家有关部门发布。个人信息保护监督委员会由大型网络平台服务提供者设立，成员一般不少于 7 人。监督委员会主要由外部成员组成，外部成员不低于三分之二。

《规定》明确，外部成员需要具备个人信息保护专门知识和技能，同时具备相应的独立性要求，具备良好的声誉和个人品德，能够客观、公正、正常（时间上和精力上）履职。外部成员由大型网络平台服务提供者提名，其聘任决定由大型网络平台的董事会或者其授权的董事长、执行董事等高级管理人员作出，外部成员可以获得与其履职工资相适应的报酬，报酬情况应当在相关文件中记载和披露。

《规定》明确了内部成员的任职要求、监督委员会主任、秘书的职责以及成员的任期、辞任与解聘的具体规则。《规定》规定了监督委员会的工作规则和重点监督事项，以及成员的具体职责、定期会议与临时会议规则与成员出席要求；明确了监督意见的作出、记录及其处理；成员有权提出建议，需要遵守保密要求，不得泄露或者非法向他人提供履职过程中知悉的个人信息、商业秘密等。

《规定》明确了大型网络平台服务提供者配合履职要求、提供履职保障的义务；明确了委员会信息公开及撤销制度和信息报送机制，明确了国家网

信部门等的监管职责和公众监督举报机制；还明确了依据《个人信息保护法》和《网络数据安全管理条例》的罚则和国家网信部门的解释权。

三、配套国标

今年稍早时候，国家市场监督管理总局、国家标准化管理委员会发布国家标准《数据安全技术 大型互联网企业内设个人信息保护监督机构要求》（GB/T 45404-2025）（以下简称国标），将自今年 10 月 1 日起实施。这一国标的编制与发布也旨在落实《个人信息保护法》第 58 条第 1 款关于大型互联网平台内设个人信息保护监督机构的要求。中国人民大学等高校和研究机构以及蚂蚁、京东等著名企业参与该国标的编制工作。国标侧重于从技术指标角度对大型互联网平台内部设置个人信息保护监督机构提出要求。本《规定》经过征求意见等环节后得到正式发布，将与配套的国标一起实施，二者相得益彰，共同为设立大型网络平台个人信息保护监督机构提供有力的制度保障和技术规范。

人民日报 | 首批可信数据空间创新发展试点名单发布 数据规模化流通有了“高速公路”

原载：“国家数据局”微信公众号

国家数据局公布首批可信数据空间创新发展试点名单，63 个试点项目入选，包括 13 个城市、22 个行业和 28 个企业可信数据空间，标志着我国可信数据空间发展正从概念验证快速迈向规模化推广的新阶段。

如何理解可信数据空间？“好比高速公路，有收费站、摄像头和管理机制等在确保汽车安全上路的同时还能跑得快，可信数据空间就相当于能让数据规模化流通的‘高速公路’。”清华大学社会科学学院经济所教授汤珂介绍，可信数据空间本质在于为数据的生成、流通、共享和使用提供一个“可控”“可管”“可计量”的安全可信环境。

数字经济已成为全球竞争新高地，但数据自由流通还存在不少壁垒。应用新技术，构建可确保数据安全可信流通的基础设施——可信数据空间，正成为破解“数据孤岛”问题的一条重要路径。

仅用 4 个月便锁定最优成分体系，较传统 2 年选材周期显著缩短；6 个月内就完成可焊接高强度抗氢钢开发，比原来提前一年……中国钢研北京新材道总经理赵旭介绍，公司打通了 50 多家产业链企业数据，上下游 26 万种材料产品信息实现一键筛选比对，帮助中国石化与中国钢研联合团队成功攻克石化氢能储运核心材料“卡脖子”难题，研发效率较以往提升一倍以上。

一条产业链涵盖了原材料生产、零部件加工、装备制造等数百家企业，产线、工艺、研发等数据都是各家企业的“宝贝”资产，企业凭什么愿意共享？

赵旭说，通过区块链、隐私计算等技术，公司打造了新材料产业链可信数据空间，确保“数据不出域，可用不可见”，“数据实质上并没有被集中收集起来，还在各家企业域内，但通过可信数据空间，企业可以实现数据资源供需高效对接，达到价值共创的效果。”

“对于新材料来说，企业传统的研发路径是由一个经验丰富的工程师，按照经验不断人工调整成分，每个成分比例烧炼一批样品，然后分析、调优，往复循环，直到找到最合适的成分比例。但这个过程速度慢、成本高，且解决方案不一定是最佳的。”赵旭说，打通产业链上下游数据后，可以直接通过数据和仿真计算工具筛选出一批接近要求的成分比例，再烧炼出来，研发时间大幅缩短，成本也更低。

应用可信数据空间赋能新材料研发，只是试点项目中的一例。“其他试点项目在应用场景创新、产业生态培育、规则机制构建等方面也都开展了积极探索，为推进数据规模化流通利用积累了宝贵经验。”可信数据空间发展联盟总体组组长、中国信息通信研究院信息化与工业化融合研究所副所长田洪川说。

国家数据局局长刘烈宏表示，各地要紧密服务企业、产业、城市发展的需求，将可信数据空间作为促进数据开发利用、培育数据产业、构建数据要素市场体系的关键抓手，制定培育方案，加大支持力度。承担试点任务的地方要边试点边探索边总结，为更大范围的可信数据空间实践提供经验。

国家发展改革委 国家能源局关于推进“人工智能+”能源高质量发展的实施意见

原载：“国家数据局”微信公众号

国家发展改革委 国家能源局关于推进“人工智能+”能源高质量发展的实施意见

国能发科技〔2025〕73 号

各省、自治区、直辖市及计划单列市、新疆生产建设兵团发展改革委、能源局，有关中央企业，有关行业协会：

为深入贯彻党中央、国务院关于发展人工智能的决策部署，落实《国务院关于深入实施“人工智能+”行动的意见》（国发〔2025〕11 号）有关工作要求，抢抓人工智能发展重大战略机遇，突出应用导向，加快推动人工智能与能源产业深度融合，支撑能源高质量发展和高水平安全，现提出如下意见。

一、总体要求

坚持以习近平新时代中国特色社会主义思想为指导，深入贯彻党的二十大和二十届二中、三中全会精神，全面贯彻习近平总书记关于推动人工智能与实体经济深度融合、培育壮大智能产业的重要指示精神，以拓展人工智能与能源领域深度融合应用场景为重要依托，以提升能源领域人工智能创新应用技术水平为主攻方向，以推进智能算力与电力协同发展为必要支撑，以健全能源智能化发展的创新体系为关键保障，着力提升能源系统安全可靠与灵活高效运行能力，保障能源安全稳定供应和绿色低碳转型，加快培育新质生产力，为新型能源体系建设提供有力支撑。

到 2027 年，能源与人工智能融合创新体系初步构建，算力与电力协同发展根基不断夯实，人工智能赋能能源核心技术取得显著突破，应用更加广泛深入。推动五个以上专业大模型在电网、发电、煤炭、油气等行业深度应用，挖掘十个以上可复制、易推广、有竞争力的重点示范项目，探索百个典型应用场景赋能路径，培育一批能源行业人工智能技术应用研发创新平台，制定完善百项技术标准，培养一批能源与人工智能复合型人才，探索建立能源领域人工智能技术研发应用金融支撑体系，形成符合我国国情的能源领域人工智能技术创新发展模式，能源领域智能化成效初显。

到 2030 年，能源领域人工智能专用技术与应用总体达到世界领先水平。算力电力协同机制进一步完善，建立绿色、经济、安全、高效的算力用能模式。能源与人工智能融合的理论与技术创新取得明显成效，能源领域人工智能技术实现跨领域、跨行业、跨业务场景赋能，在电力智能调控、能源资源智能勘探、新能源智能预测等方向取得突破，具身智能、科学智能等在关键场景实现落地应用。形成一批全球领先的“人工智能+”能源相关研发创新平台和复合人才培养基地，建成更加完善的政策体系，持续引导“人工智能+”能源高效、健康、有序创新，为能源高质量发展奠定坚实基础。

二、加快能源应用场景赋能

（一）人工智能+电网。围绕新型电力系统下的电网安全、新能源消纳、运行效率等要求，开展电力供需预测、电网智能诊断分析、规划方案智能生成等电网规划设计应用，加强电网工程智慧建设管理；推进电网多尺度智能仿真分析，探索人工智能模型在电网智能辅助决策和调度控制方面的应用，提升电力系统源网荷储全要素安全可靠低碳运行水平；稳步提高输变电等关键装备研制智能化水平；推动电力设备故障预测性维护，打造具备自主感知、决策、执行能力的电力设备健康管理智能体，提升设备精益化管理水平；推动营配调智能一体化应用，构建电网运营服务智能支撑体系，提升电力

客户全过程智能服务水平；促进人工智能技术融入电力应急体系和能力建设，提升电力系统防灾减灾救灾智能化水平。

专栏 1　人工智能+电网典型应用场景

电网智能规划设计与生产建设。构建电力供需智能预测、电网运行智能诊断分析、电网规划智能辅助决策、输变电设施智能设计等应用，应用人工智能技术开展规划设计和技术经济分析，推动电网规划设计作业模式向智能化转变。聚焦建设阶段的作业感知与业务监测，构建电网建设的人工智能违章识别、进度仿真、在线监测、管控指标实时分析、作业流程智能管理等应用，促进电网工程建造智能升级。

电网调度运行。在全国统一电力市场建设背景下，构建新能源功率预测、负荷预测、离线仿真分析、在线安全分析、极端应急处置、调度辅助决策、市场出清运筹优化、电力市场智慧决策等方面的智能化应用，持续完善新一代智能调控技术支持体系，支撑新型电力系统安全稳定运行。

电力设备状态评价与智能运维。构建设备状态智能感知与预警、设备故障智能定位与诊断、设备状态检修智能决策、设备灾害风险智能预测、检修工作票智能生成等应用，提升设备精益化管理水平。

配电网智能运行管理。构建配电网实时感知、风险分析、智能决策等技术应用，全面提升配电网智慧控制能力和供电可靠性，加强配电网层面源网荷储协同调控。

电力应急抢修。构建电力系统灾害风险智能预警、损毁情况智能分析、应急方案智能决策等辅助决策系统，推进电力应急抢修技术装备智能化应用，提升电力系统防灾减灾救灾能力。

（二）人工智能+能源新业态。围绕能源保供和绿色低碳转型需求，推进人工智能技术在虚拟电厂（含负荷聚合商）、分布式储能、电动汽车车网互动等灵活性调节资源中的应用，提升负荷侧群控优化和动态响应能力；加强人工智能技术在新型储能与电力系统协同优化调度以及全生命周期安全中的应用，推动可再生能源制氢生产工艺智能寻优。强化人工智能技术赋能能源生产过程中的节能和碳排放管理，提升多能互补综合能源系统电、热、冷、气联供的综合能效和降碳水平。推动人工智能在零碳园区、智能微电网、算电协同中的应用，提升源网荷储一体化智能运行水平，促进新能源就地消纳。

专栏 2　人工智能+能源新业态典型应用场景

虚拟电厂精准控制与智能运营。虚拟电厂运营商平台根据电网调节指令、市场信息，结合资源特性的动态变化，进行控制策略的智能优化和控制指令的智能生成，实现大规模灵活性资源聚合优化调控、实现虚拟电厂参与电力市场的智慧交易决策。

绿氢生产工艺智能寻优。融合风光功率波动预测、储氢罐容量、电解槽温度、催化剂状态等多维数据，基于人工智能算法，智能驱动电解槽电流密度动态寻优，构建电解制氢-储氢-用氢全链条智能调控系统，实现可再生能源功率波动与电解装置柔性负荷的毫秒级匹配。

园区智能降碳。基于光伏、储能等设备运行数据，园区智能降碳协同控制系统实时动态优化能源调度策略，结合电价与碳排放因子自动调节空调温度、充电桩功率及设备启停时序，通过增强现实可视化界面和语音助手向用户推送个性化节能建议，形成“碳-能-费”智能协同模式。

新型储能智能化运行。针对新型储能动态适配电力系统调度、广域协同互动、弱电网支撑、电池装备安全监测、设备本体评估与运维，通过人工智能技术，提升面向弱电网的多类型储能协调控制能力，构建新能源与配建新型储能广域协同优化控制、储能电站智能评估、智慧运维决策支持、全生命周期安全等应用体系，提升系统友好型新能源电站的电力供应保障能力。

智能营销服务。针对油、气、电等直接面向客户服务场景，构建座席业务受理智能辅助、智能客户服务、供电方案智能生成、综合用能方案智能生成、运维工单智能派发、用户用能异常诊断等智能化应用，打造交互式、伴随式的客服新模式，提升

客户全过程智能化服务水平。

（三）人工智能+新能源。针对新能源出力波动性与间歇性的问题，加快在高精度功率预测、电力市场、场站智慧运营、新能源规划、项目后评价等方向的人工智能应用，持续推动新能源关键材料及产品不断迭代和创新，推动复杂场景及转折性天气下功率预测大模型在更小尺度、更高精准度方向发展，支撑广域新能源资源协同优化，促进偏远地区新能源场站智能运维发展，打造“气象预测+功率预测+智慧交易+智能运维”一体化新能源智能生产模式，全力支撑新能源稳定供给。

专栏 3　人工智能+新能源典型应用场景

气象预报与新能源功率精准预测。构建以多时空尺度气象预报为核心的气象服务体系，建立气象-功率非线性关系精准挖掘与解析的多场景多周期算法大模型，实现新能源功率精准预测。

偏远地区场站智能运维。利用大模型、声纹检测、遥感、机器人、智能穿戴设备等技术装备，实时监测周边环境及设备运行状态，实现无人机、无人车、无人船、智能控制等多系统智能联动，提升设备巡检效率，提高场站的综合运营效率。

新能源规划设计。综合考虑发电效率、投资回报率等因素，构建智能化推荐引擎，提供最优机型匹配方案。融合大模型与设计软件，快速生成多版本设计方案并评估关键参数，提升设计效率与质量。

智慧工地建设。推动人工智能技术深度融入工程建设方案选择、人员管理、风险预警、工期管控等电力建设工程管理全流程，研发无人机巡检系统、风险自动研判预警系统等，实时捕捉施工人员违章行为，构建贯穿施工全过程的“智慧工地”管理平台，助力提升电力建设工程安全质量总体水平。

（四）人工智能+水电。聚焦高海拔高寒地区水电工程智能化建设与流域水电站群智慧调度运营，推进人工智能技术在水电工程建设中的应用，提升水电工程智能化设计施工管理水平；推进人工智能技术与传统水文模型、气象模型、大规模水库调度技术融合，提升气象、水文双向耦合预测精度，开展调度决策优化智能应用建设；推动知识图谱、大模型、智能体等技术融入新一代水电智慧运营大脑，在水电站智慧运维与精益检修、智能大坝态势感知与智慧管理等重点领域形成智能化解决方案。

专栏 4　人工智能+水电典型应用场景

智能水电工程建设。基于多源遥感数据融合和智能机器人等人工智能技术，建立水电工程地质智能化勘测设计体系，实现机组设备数字化智能化安装调试，提升水电工程智能化施工管理水平。

气象水文联合预测。基于流域气象水文双向耦合预测大模型，构建洪旱极端事件风险量化工具，充分融合气象知识、水文知识和流域地理信息，提升气象水文预报精度和预见期。

流域综合调度。基于流域站群联合智慧优化调度、风险控制和模拟仿真等关键技术，建设精准调度决策优化智能应用，实现对水资源调度方案执行情况的实时监测、分析和评估，在时间和空间上对水资源分配进行优化，提高水能利用率，增加发电效益。

设备智能运检。基于物理场、声学、视觉、智能传感器等多源数据以及知识图谱、大模型等技术，推动水电关键设备实现状态全息监测、全生命周期健康管理、智能运维和状态检修等业务领域全流程智能化升级，实现运维知识结构化管理与基于大模型-智能体的智能辅助决策系统。

大坝高质量运行。构建大坝典型病害特征数据库与知识图谱，结合大坝智能感知-融合-诊断-防控理论方法，实现多元驱动的大坝安全状态早期识别-自诊断-自适应预警-智能馈控，确保水电站大坝运行安全，支撑水库大坝高质量运行管理。

（五）人工智能+火电。围绕火电清洁降碳、安全可靠、高效调节、智能运行的发展方向，在燃料管控、生产运行优化与智能控制、设备全生命周期管理等业务场景，协同开展人工智能赋能及技术创新。加快火电数字化设计建造和智能化升级，推动火电运行控制系统智能化发展和应用，提升火电关键装备全生命周期智能监测及健康管理能力，助

力火电支撑保障能力进一步提升。

专栏 5　人工智能+火电典型应用场景

燃料智能管控。基于燃料市场价格波动、库存量、耗煤量以及煤堆三维结构、煤质分析等多维度多类型数据，采用先进传感、图像识别、规则理解以及智能体等技术，实现燃料数量、质量等智能检测和智能管控。

生产运行优化。基于大模型和生产运营相关系统数据，实现生产运营过程中燃料掺配、运行优化、智能灵活调峰、安全智能管控等核心业务场景智能化升级，提升生产运营的智能化水平和效率。

设备全生命周期管理。基于大模型和机器人等人工智能技术，通过对汽轮机（含燃气轮机）、发电机、锅炉受热面等关键设备多类型数据进行实时状态监测，实现设备状态全景监测、健康量化评估、隐患识别与故障预警、剩余寿命预测、运行方案调整、异常分析判断和隐患闭环管理。

智能技术监督及评价。依托锅炉、汽轮机（含燃气轮机）、发电机等关键设备的海量运行数据与火电技术监督工作相关资料，基于火电大模型多模态分析能力，深度融合火电特色场景，提升技术监督的智能化和人员专业能力。

（六）人工智能+核电。围绕核电安全发展，构建核电安全预警、电站运行事件智能溯源分析、应急响应的智能辅助支持系统，开展核工业特种运维机器人技术攻关，持续推动核电系统的自动启停等技术升级演进，探索人工智能技术助力离子体预测控制、可控核聚变等技术路径，推动核电行业向数据驱动、模型牵引、智能管控的新模式稳步转型。

专栏 6　人工智能+核电典型应用场景

核电智能安全管控。借助数据治理及人工智能技术，聚焦运行事件溯源、技术规格书及运行参数边界条件，智能识别人员、设备、环境的不安全状态，推进安全预警、智能应急响应等场景技术攻关与应用。

核电智能运维。利用各阶段的构筑物、系统及设备/部件的数据，建立数据驱动的核电厂模型，推动核电人工智能小模型及专业大模型研发，推进人工智能技术在核电系统智能监测、预警、诊断和预测中的应用，提升机组性能智能诊断和优化能力，提升关键设备、系统及机组的一键启停等能力，拓展高放射性、水下及密闭空间等高危场景机器人作业的范围与深度。

可控核聚变智能控制。结合可控核聚变装置多物理场耦合特征，基于人工智能技术开展可控核聚变智能控制系统研究，研发等离子体位形实时预测-磁约束参数自适应调控智能模型，实现托卡马克等离子体稳态运行的智能化控制。

（七）人工智能+煤炭。聚焦地质勘探、煤矿采掘（剥）、煤炭洗选、生产调度、安全管控、设备管理等典型场景，稳定获取复杂地质、多工况以及多时空协同条件下的各种工况数据，融合应用智能模型，实现生产过程智能控制与自主决策，助力少人无人化作业常态化运行，稳步推进减人、增安、提效，进一步夯实煤炭在能源安全中的兜底保障作用。

专栏 7　人工智能+煤炭典型应用场景

煤矿地质勘探数智赋能。基于煤矿专业大模型，融合地面高精度勘探与井下动态智能探测的新技术，构建复杂地质条件下的煤矿地质数据库，实现矿井地质信息的全过程动态协同管理和预警，保障矿井高效、快速、绿色、智能生产。

（八）人工智能+油气。聚焦跨专业协同研究、现场作业操控、生产运行管控等方向，推动勘探地质目标智能评价、开发方案智能优化、钻井压裂等作业参数智能调整、炼化装置智能运行、管网运行实时仿真，加快智能钻机、机器人、无人机、智能感知系统等智能生产技术装备的研发与应用，推动生产现场等全过程智能联动与自动优化，推动油气产业链智能化升级建设。

专栏 8　人工智能+油气典型应用场景

油气勘探智能赋能。提升面向地震、测井、岩心露头等勘探专业领域的软件智能化水平，构建面向地震测井处理解释的专业大模型，打造面向有利地质目标综合评价的智能应用系统，实现可控震源智能辅助驾驶、地震检波器埋置等机器人示范应

用。

油气藏开发与生产智能管控。研发油气开发数据与知识智能化技术、智能开发优化软件和专业大模型，打造大模型驱动的协同研究与生产管理决策平台，构建面向智慧油气田开发生产管控的新模式。

海洋油气生产环境预测维护。聚焦海洋油气生产过程环境保护和重大风险防范、治理等需求，通过生产环境智能监测与异常预警、固废处理智能管控、溢油智能识别与应急预测等手段，形成覆盖油气田全域生态环境状况的风险预知、态势感知、事故早知和认知决策一体化能力。

工程技术智能优化。推进地面工程智能设计、钻井参数智能优化、录井实时智能判层、储层改造及智能故障诊断与风险评估，实现井控机器人示范应用，保障复杂地质环境下施工安全高效。

管网仿真及智能调控。推进市场洞察预测、管网实时仿真及动态优化、高效智能站库运行、空天地一体线路管理及关键设备监测预警，实现“黑屏”智能调控，提升油气管网安全生产、油气保供与公平服务能力。

炼厂生产营运一体化优化。面向全流程计划优化、安全生产智能识别、设备预防性维修等环节，攻关新材料研发科学计算大模型，通过大小模型协同、混合建模等技术手段，减少工艺波动，降低安全事故发生概率，提升生产运营智能化水平。

三、加大关键技术供给

聚焦能源领域数据孤岛化、算力碎片化、算法黑盒化、算力高耗能等技术瓶颈，推动开展适用能源领域的数据、算力、算法等共性关键技术攻关。

（一）夯实数据基础。针对能源领域高质量数据集构建和数据安全需求，推动数据智能标注、智能增强、数据合成等技术应用，推进能源数据分类分级技术、隐私计算技术以及智能数据动态加密和跨域可信溯源等技术研发，优化数据分享机制，加快形成能源领域高质量数据集，确保能源数据全流程安全可靠。

（二）强化算力支撑。针对能源领域租建结合模式下的多元异构算力融合利用需求，开展多元异构算力统一调度、任务智能编排、存算网一体化融合、算力池化等关键技术攻关，提升智算服务水平。持续开展能源算力需求监测，统筹规划算力、电力和通信网络资源，构建算力、电力深度融合的算电协同发展机制，不断提高算力中心绿电比例。

（三）提升模型基础能力。针对能源领域对于模型安全性和可解释性的需求，推动模型算法、应用系统等安全能力建设，加大多智能体协同、可解释性、模型轻量化推理等技术的研究，持续深化机器视觉、多模态、时序预测等人工智能关键技术在能源领域的应用研究，推动人工智能与能源领域软件深度融合。针对人工智能计算耗能问题，加快突破人工智能绿色低碳技术瓶颈，研究柔性直流供电、模块化小型堆等能源供给技术，鼓励数据中心液冷技术、废热回收、备电集约化等高效能源综合利用技术的应用。

四、保障措施

（一）强化组织实施。各地方能源主管部门和相关中央企业要根据意见要求，建立健全工作机制，统筹衔接好相关规划，结合实际加快推动本地区、本单位“人工智能+”能源的发展，做好各项要素保障，探索构建安全治理体系，形成上下联动、层层落实、安全发展的工作格局，加快推进人工智能在能源领域融合应用的技术研发、示范试验、推广应用等工作。

（二）推动协同创新。围绕能源领域人工智能融合创新应用关键共性技术和配套专用技术，推动建设一批行业研发创新平台。鼓励企业牵头联合科研机构、高校、社会服务机构等单位，建设以技术创新融合应用为目标的跨领域、跨学科的“人工智能+”能源创新联盟，深化产学研用合作，构建开放协同、共创共享的能源智能化创新生态体系。

（三）加强标准规范建设。在深入总结应用示范实践的基础上，加快编制能源数据治理、多元异构算力融合、典型场景设计等一批技术标准规范，推动能源领域人工智能标准体系建设，探索建立人工智能应用评估指标体系和行业级人工智能应用

标准测试平台，提升能源领域人工智能技术安全应用水平。鼓励能源企业主导制定国际标准，以技术标准“走出去”带动人工智能技术和产品在海外能源市场推广应用。

（四）开展试点示范。组织开展能源领域人工智能应用试点示范，遴选一批可复制、易推广的场景和企业标杆应用。鼓励开展能源和交通融合、油气和新能源融合等跨领域、跨行业典型场景示范。能源领域人工智能应用相关技术装备优先纳入能源领域首台（套）重大技术装备支持范围。支持具备条件的地区和企业，因地制宜开展能源领域各类人工智能应用试点示范，在技术创新、商业模式、发展业态、体制机制等方面深入探索、先行先试。

（五）加大支持力度。充分发挥中央财政资金带动作用，依托能源领域、人工智能领域国家科技重大专项和重点研发计划等科技专项，有序推动能源领域人工智能技术应用创新。发挥多层次资本市场支持科技创新关键枢纽作用，引导社会资本参与人工智能科技项目实施和成果转化应用。

（六）完善人才培育生态。鼓励能源企业与高等院校、科研院所共建“人工智能+”能源人才培养基地，以行业需求为导向设计跨学科课程体系，重点培养具备能源系统知识、人工智能算法应用能力的复合型人才，通过产教协同增加复合型人才供给。

国家发展改革委　国家能源局

2025 年 9 月 4 日

地方动态 | 解锁公共数据密码 千亿条数据支持北京“一区三中心”数据发展

原载：“国家数据局”微信公众号

北京市深入贯彻落实中办、国办印发的《关于加快公共数据资源开发利用的意见》，以公共数据驱动数据要素市场化配置改革综合试验区建设，持续推进公共数据高质量供给、高效率流通、高水平应用，充分释放公共数据要素潜能。

一、完善数据开发利用制度体系

2022 年，北京市陆续出台数字经济促进条例、北京数据二十条、专区建设指导意见、授权运营管理办法，为开发利用提供法律和政策保障环境。2025 年，先后印发了《关于建设数据要素综合试验区 深化数据要素市场化配置改革的实施意见》《关于加快公共数据资源开发利用的实施意见》，一体化设计共享、开放、授权运营等配套制度，全面构建数据资源开发利用制度体系。

二、创新开展公共数据授权运营

2019 年，北京市在全国首创政企数据融合共用的“数据专区”机制，创新建设金融公共数据专区。按照今年国家出台的公共数据资源登记、授权运营、价格等开发利用配套制度要求，进一步规范我市授权运营管理模式。一是拓展授权运营范围。加快推进金融、气象、时空以及整体授权的建设运营，编制专区授权运营实施方案，明确授权运营管理要求。二是规范开展运营机构遴选。针对拟建设气象、时空等专区，按照市政府审议通过的实施方案，以公平竞争方式遴选专区运营机构，并签订授权运营协议。三是高效开展资源登记。组织数据提供部门在公共数据资源登记平台完成 38 类公共数据资源登记，指导运营机构完成 20 类公共数据产品和服务登记。四是完善专区安全管理体系，依托目录区块链系统开展数据共享授权，实现数据共享申请和数据调用的全流程管控；不断完善数据使用备案、质量反馈和成果反哺机制，提升数据的质量和应用成效。

三、金融公共数据专区建设运营情况

历经五年建设，金融公共数据专区在数据赋能金融“五篇大文章”上发挥了积极作用。截至 2025 年 6 月，金融公共数据专区累计可触达数据量 67 亿条，聚焦金融机构的营销、准入审查、额度测算、授信审批、风险洞察等需求，形成了涵盖数据接口、企业画像、信息查询、竞争力分析、征信报告等业务的产品体系，为银行、保险、担保等 60 余家金融机构以及 70 万家市场主体提供服务超过 4 亿次，

有效破解中小微企业融资难融资贵等问题，支撑金融机构推动线上普惠贷款“量增、价降、面扩”，实现融资服务周期从按月到最快 5 分钟的转变。

下一步，北京市将健全公共数据开发利用配套制度体系，研究设计授权运营评估指标体系，规范运营行为，面向市场公平提供服务，积极争取国家部委数据授权使用，形成权责清晰的部市协同授权运营格局。

地方动态丨西安市“五位一体”协同发力 打造“丝路数港”西部数据流通新枢纽

原载：“国家数据局”微信公众号

西安市作为全国数据基础设施建设的首批试点城市，融合可信数据空间、数据元件和隐私保护计算三条技术路线，探索“标准引领、平台创新、政策配套、生态筑基、园区聚势”五位一体推进数据基础设施建设。

一是建强基础设施，打造枢纽能力新支撑。遵循国家数据基础设施相关标准和技术文件，建成数据接入、加工、流通、应用全链条服务能力。建设城市普惠性可信数据空间，具备智能合规检测、数据安全防护、链上可信存证、跨区域协同开发等核心能力；开发基础型、标准型、拓展型三类接入连接器，降低企业数据接入与交付门槛；推出数据元件源端加工一体机，硬件部署要求降为 6 台服务器；研发基于专用加速芯片的隐私保护计算平台，计算效率较传统 CPU 架构提升 1-2 个数量级。实现与丝路数据交易平台对接互通，并通过互联互通测试和四城联合复杂跨域加工场景验证，初步形成多业务协同、跨区域联动的枢纽能力。

二是创新制度政策，构建优良发展新环境。将试点工作充分融入西安市经济产业发展，通过《西安市加强网云算数安新型基础设施体系建设实施方案（2025-2026 年）》《西安市建设软硬一体技术适配和产品开发中心促进信息产业高质量发展行动方案（2025-2027 年）》等文件支持本地 3500 余家软信服企业转型数据服务商，对开展数据交易、建设可信数据空间、建设行业高质量数据集、数据标注、打造典型示范用数场景等情形进行奖补，支持数据技术攻关，以应用场景驱动科技创新与产业发展。

三是培育生态体系，拓展场景应用新空间。以试点为契机，建设“丝路数港”省级数据产业集聚区，深入走访调研 25 家重点企业，面向社会发布“入港”倡议书，召开 3 场企业推介会并常态化组织企业沙龙活动，建立“一对一”数商服务机制，按照“全域可见、跨域可用、价值释放”三步走，已接入 244 家市场主体，登记数据资源 176 项，上架 1080 个数据产品，重点支撑打造智游三秦、个人背调、企业评分、智能制造产业链分析等 10 余个应用场景。

下一步，西安将持续攻关隐私保护计算等关键技术，深化制度创新，强化市场需求牵引，推动数据产品从“量”到“质”提升，打造更多特色示范场景，为构建全国一体化数据市场贡献西安智慧和方案。

地方动态 | 牢牢把握数据驱动人工智能发展重点任务 加快打造全国人工智能产业发展新高地

原载：“国家数据局”微信公众号

王忠林在湖北省市厅级主要领导干部专题培训班上强调牢牢把握数据驱动人工智能发展重点任务加快打造全国人工智能产业发展新高地

李殿勋孙伟诸葛宇杰出席 刘烈宏作辅导报告

9 月 16 日上午，湖北省市厅级主要领导干部专题培训班暨省委理论学习中心组集体（扩大）学习举行。湖北省委书记、省人大常委会主任王忠林主持会议并讲话。他强调，要深入贯彻习近平总书记关于数据发展和安全的重要论述和考察湖北重要讲话精神，抢抓数据驱动人工智能产业发展的战略机遇，着力打造全国人工智能产业发展新高地，

为加快建成中部地区崛起的重要战略支点提供有力支撑。

省委副书记、省长李殿勋，省政协党组书记、主席孙伟，省委副书记诸葛宇杰，省人大常委会党组书记、常务副主任王艳玲出席会议。

会上，国家发展改革委党组成员、国家数据局局长刘烈宏以“扎实做好数据工作、助力人工智能高质量发展”为题作辅导报告，系统梳理了习近平总书记关于数据发展和安全的重要论述，全面阐述了高质量数据对人工智能高质量发展的重要性，详细介绍了数据要素市场化配置改革的推进情况和国家层面推动人工智能发展的有关重点工作；同时，立足湖北实际，从释放数据要素价值、加强高质量数据供给、加快建设数据强省等方面，提出了市场空间巨大的基础优势，抢抓大数据、人工智能等新经济发展机遇，按照“芯片引领、模型驱动、企业强基、场景示范”的思路，坚持技术创新、产业培育、基础支撑、融合应用“四位一体”统筹推进，加快构建“以科技创新为牵引、产业能级为基础、数字底座为支撑、场景应用为导向、人才引育为保障”的人工智能发展体系。要牢牢把握数据驱动人工智能发展的重点任务，着力实施创新驱动引领工程，推进深度学习通用芯片、存算一体 AI 芯片、车规级智能座舱芯片、三维闪存等优势领域集聚攻坚，突破 6G 网络、大模型基础架构创新、多模态数据处理等关键共性技术，推动人工智能创新实现从“跟跑”到“领跑”的跃升；着力实施基础支撑提能工程，强化算力、算法、数据支撑，加快推进国家（武汉）新型互联网交换中心等国家级节点项目建设，构建生态开放、应用引领的人工智能产业公共服务体系，努力打造中部数据要素流通枢纽，建设数据强省；着力实施产业集聚培育工程，充分发挥人工智能驱动产业变革的强大作用，赋能传统产业“智改数转”、新兴产业发展壮大、未来产业前瞻布局，推动实数融合走深走实，为发展新质生产力、塑造发展新动能新优势提供有力支撑；着力实施“人工智能+”应用场景示范工程，推动高端光芯片、元宇宙、自动驾驶、低空飞行等制造领域高质量发展，提升政务服务、城市治理等社会领域治理效能，创新教育、医疗、养老、托育等民生领域新场景、新模式、新业态，不断满足人民群众对美好生活的向往。

王忠林指出，数据是赋能人工智能发展的重要引擎、是发展新质生产力的关键要素、是塑造发展优势的战略资源，已经成为推动经济社会高质量发展的重要驱动力。要深刻认识数据资源的战略性、基础性作用，切实增强做好数据工作的责任感紧迫感，把数据发展置于重要位置，顺应新质生产力发展规律，更大力度、更深层次采集数据、开发数据、应用数据，充分发挥数据要素放大、叠加、倍增效应，优化数据资源配置，释放市场发展活力，促进产业高端化、智能化、绿色化发展。

王忠林强调，要充分发挥湖北省数据资源丰富、产业体系完备、枢纽地位突出、应用场景广阔、意见建议。

王忠林强调，以数据驱动人工智能发展，是一项跨领域、跨部门、跨层级的系统工程。各级各部门要拧紧责任链条，加强统筹协调，强化科技创新、要素支撑、场景打造、融合应用等政策供给，凝聚齐抓共管的强大合力。各级领导干部要加强前沿知识学习，提高驾驭、引导、运用以数据驱动人工智能发展的本领。要及时总结宣传湖北省人工智能发展的新进展、新成效，引导全社会主动拥抱人工智能、学习人工智能、用好人工智能，形成全社会共同支持数字经济和人工智能产业发展的良好氛围。

省委常委，省人大常委会、省政府、省政协领导同志，省法院院长、省检察院检察长等参加学习。培训采取线上线下相结合的方式举行，各市（州）设分课堂。

（技术编辑：何芮）

研究动态

基本理论

1. 网络数据爬取合法性判定的三阶层认定标准（刘云）

来源：《东方法学》2025 年第 4 期

网络数据爬取是一项价值中立的数据采集工具，对于海量数据索引建档、保护互联网开放性、促进社会智能化转型具有不可或缺的作用。《网络数据安全管理条例》第 18 条为网络数据爬取行为的合法性判定提供了一个三阶层的判定依据。一是对数据的公开性进行判定，认定公开数据均具有“可爬性”，该限制属于对公开数据的合理使用。二是对爬取技术的正当性进行判定，对技术行业的整体发展水平和被爬取方的技术防护成本进行平衡考虑，区分破坏性技术和规避性技术。三是对数据用途的差异性进行判定，根据数据爬取方的用途评估对被爬取方是否产生实质性替代的影响，判断应否支持对他人公开发布的数据的转化性使用。

2. 从财产到合同：论数据爬虫法律规制的范式转型（孙济民）

来源：《东方法学》2025 年第 4 期

当前针对数据爬虫行为的司法实践与理论发展已逐步形成权利保护与自我规制这两种基本范式。其中，权利保护范式旨在为多元主体赋予标准化法定权利，并通过持续完善权利体系以应对不足；自我规制范式则通过信赖行为主体的自我判断能力和市场调节机制，借助法律规范推动谈判的积极作用，形成开放式规制框架以提升效率，并平衡私人权利与公共利益的冲突。由于权利保护范式在实践中存在技术适配性差、忽视公共利益和多方协作受挫等问题，加之作为公共商品的数据具有非排他性与异质性价值，“搭便车”的批评难以成立，有必要采纳自我规制范式，并对合同法规范予以重构。为此，需要超越传统合意框架，转而以公共利益具体阐释为目标，依据数据互联互通原则，充分评估被爬取数据带来的技术创新能否形成互惠机制，从而形成多元主体参与的规制框架。

3. 大模型运行损害的归因范式与责任机制（汪青松）

来源：《东方法学》2025 年第 4 期

大模型具有自主演化性、数据依赖性与算法黑箱性三大核心技术特征，由此引发输出内容安全性隐忧、数据使用正当性质疑、因果关系认定难题等风险挑战。大模型运行引发的损害不仅样态繁多，且具有独特的法律特征，传统归责体系面临前所未有的挑战，主要法域相关立法变革也存在缺陷。为此，需要借助风险分配与矫正正义的耦合来重构大模型运行损害责任分担的理论基础，创建兼容技术、控制和收益的三维归因模型。在此基础上构建多元主体的分层义务，遵循相应归责原则，利用原因力分析来合理划分比例责任，并结合动态风险协议制度来形成适应大模型技术特征与发展需求的动态、灵活且公正的责任分担机制。

4. 医用脑机接口技术所涉权利再造与法律规制（杜仪方）

来源：《东方法学》2025 年第 4 期

随着脑机接口技术在医疗领域的广泛应用，传统权利体系面临巨大挑战。在现有权利框架下对脑机接口技术所涉权利的分析，忽视了该技术对个体意志造成的影响及对权利基础的动摇。医用脑机接口所涉权利的内容应包括认知自由、精神隐私、精神完整性和心理连续性等。为实现权利保障，应从宏观、中观和微观层面进行法律规制：宏观上以保护人类自主权为前提，中观上遵循自主性、非恶意、公正性和透明度四项准则，微观上通过决策前伦理审查、决策中增强透明度、决策后长期优化等策略，旨在构建以“人”为核心的技术治理体系，实现技术发展与权利保障的平衡。

5. 脑机信息隐私属性泛化之反思与规制（闫冬）

来源：《东方法学》2025 年第 4 期

脑机接口技术在采集与解码脑电信号过程中，已展现出识别个体内在认知与意图的能力，进而引发了对“脑隐私”及其法律保护边界的讨论。以脑机技术在医疗领域的应用为样本，依据当前脑机设备的解析能力可将采集的电子数据划分为无法解码与可以解码数据两种类型。在此基础上，根据信息内容可将可以解码的数据进一步细分为个人信息与个人隐私，由此提炼出脑机信息在法律范畴下的三种形态——无法解码的数据、个人信息、个人隐私。脑机信息不应仅因来自大脑意识就被泛化定性为隐私而升级规制或厚此薄彼，须以三种形态的实际特点为准分别调整，力求在推动医疗技术发展与防范病患信息泄露风险之间达成平衡。同时，对脑机信息的保护还须实时关注脑机解码技术的动态变化，及时调整三类脑机信息形态之间的边界与范畴，并开展有针对性的制度调适。

6. 新技术新应用风险规制的结构性反思与法律理念的重塑（汪庆华）

来源：《法律科学(西北政法大学学报)》2025 年第 3 期

新技术新应用是数字经济发展的主要动力。对于人工智能等新技术新应用，我国没有采取统一立法的模式，而是针对特定技术和行业应用，出台专门的规则。我国对新技术新应用的规制经历了从最初的规制不足，到目前的及时跟进、动态均衡。在风险规制的视野下，我国的新技术新应用立法呈现出即时性、行为规制以及法律效力的溢出性等特征，具有作为预防手段、非对称监管、动态监管等结构性要素。就风险规制合宪性的一般分析框架而言，新技术新应用的立法需要满足法律保留原则、比例原则和明确性原则。

7. 可信数字身份的法律保障（李晓楠）

来源：《法律科学(西北政法大学学报)》2025 年第 3 期

数字身份是现实世界中自然人身份在数字空间的映射，其可信性构成了数字空间安全的重要保障、数字经济的信任基础、数字治理的有效工具。当前法律规制未能有效满足数字身份的可信性需求，包括安全、互操作和个人控制等，制度碎片化有余而体系化不足、纵向规范有余而横向标准支撑不足、风险防控有余而个人控制不足。随着数字身份法律内涵的不断扩张，通过法律规制实现可信数

字身份构建应当注重规范与标准的融合、个人控制与数字身份处理的协调、安全性与效率性的平衡。在具体制度层面上，应在基于全流程的数字身份安全监管制度、基于认证效力互认的数字身份互操作制度、基于权益保障的数字身份个人控制制度等方面进行适应性的制度体系革新。

8. 央地互动视角下我国数字经济立法之优化（宋保振）

来源：《法商研究》2025 年第 4 期

高水平立法是推动数字经济高质量发展的制度保障。中央立法与地方立法的有效互动作为数字经济立法的内在逻辑，具有充分的理论基础和规范依据，是优化我国数字经济立法的突破口和着力点。当下我国数字经济立法中的央地互动既面临传统央地立法难题所呈现出的“新样态”，又面临数字经济领域立法特有的“新难题”。固守技术主义下央地关系分析的“集权-分权”逻辑，忽视治理主义下地方立法的实践性权威，是影响数字经济立法央地有效互动的重要原因。为全面优化我国数字经济立法，应在革新央地互动理念的基础上，着重完善央地互动关系：一是通过“事权区分化”界分央地立法权属；二是借助“政策法律化”畅通央地互动渠道；三是经由“立法协同化”拓展央地互动形式。

9. 网络交易中电子代理人的法律性质与财产犯罪归责（涂龙科）

来源：《法学》2025 年第 7 期

电子代理人的广泛运用改变了人与物之间的控制形态和人与人之间的交易模式。基于对电子代理人法律性质的不同认识，衍生出涉电子代理人行为的刑法定性的重大争议。国内司法实践中一般持代理意志说的立场，将针对电子代理人的非法取财行为认定为诈骗罪。该结论在论证逻辑和方法运用上皆有不当，难言合理。理论上，关于电子代理人的法律性质还包括预设意志说、法律主体说两种观点。预设意志说对于判断权利人是否同意转移占有，从而推断是否构成盗窃罪具有较强解释力，但是其解释范围不能及于诈骗罪。法律主体说缺少必要的理论与事实依据，可靠性存疑。诈骗罪与盗窃罪并非“非此即彼”的关系，电子代理人的出现凸显了处于上述两个罪名之间的处罚空白的行为，即由于电子代理人的介入而无法证明权利人陷入错误认识的，不违背权利人预设意志，但事实上侵害了权利人财产权益的行为。对于这类行为，无论认为是构成盗窃罪还是信用卡诈骗罪，均具有明显的解释局限。为完善涉电子代理人的刑事归责，上述处置空白可通过法律拟制的立法方式，以诈骗罪的特别条款予以处罚。

10. 数字营销中默认选择的运用及其法律规制（应飞虎）

来源：《法学》2025 年第 7 期

数字营销中默认选择的运用成本低廉且效果显著，被经营者广泛运用。默认选择之所以产生有利于经营者的结果，主要缘于其对消费者认知偏差（如现状偏差、损失厌恶）及有限注意力等心理特质的利用。有限注意力导致部分消费者未能察觉勾选选项；即使察觉，现状偏差和损失厌恶等认知偏差仍会促使部分消费者维持默认状态。这种维持现状的决策驱动力，并非源于意识层面的主动选择，而是源于消费者潜意识层面的心理机制。我国现行法律体系对默认选择的规制相对滞后。一些制度采取问题导向的应对模式，制度整体略显碎片化、具体化；一些制度在内容设计上有失精准。数字营销中的默认选择构成与传统营销不同的全新规制领域，在构建相关规制体系时，必须深入把握行为背后的心理机制，突破传统基于理性人假设的规制理念，采用与问题本质相匹配的规制路径，进而构建系统精准的数字营销默认选择规制制度。

11. 数字法律关系的法理学阐释（郑智航）

来源：《法学论坛》2025 年第 4 期

数字技术的迅猛发展深刻地改变着人类相互连接的方式，扩展着人类社会交往的空间，塑造着

社会的组织结构，重构着社会的运行逻辑，并最终推动了法律关系基本形态的发展与变革。人工智能能否成为数字法律关系的主体，并享有一定的权利或者承担和履行一定的义务在学术界产生了广泛讨论。数字法律关系的客体除了包括传统的物、具体人格利益、智慧成果以外，还包括数据、信息、虚拟货币、数字资产和算法等。数字技术的发展进一步扩展权利的分析范式、丰富权利的主要权能、模糊权利的基本属性。数字技术在催生权利发展的同时，推动了义务的发展，并产生了一些新兴的义务。数字权力是一种基于数字技术和算法而产生的具有支配和控制他人行为作用的权力形态。数字社会需要强化对数字权力的控制，引导数字向善发展。

12. 数字法治理论的理念转型及其与法律方法的智能化融合（魏治勋）

来源：《法学论坛》2025 年第 4 期

伴随着信息科学新技术革命对法学领域的影响，“数字法治”研究成为法学研究的热门话题。作为一个新兴研究领域，“数字法治”研究正在逐渐形成自身的研究基本框架。它以当代信息科学领域的新技术革命给法律系统带来的冲击和挑战为基本问题线索，以法治经典理论在新技术革命时代的理念转型和方向调整为逻辑基调，在方法论上关注法律方法与智能技术的融合。当代“数字法治”研究已经形成了自身初步的逻辑脉络，但由于当前尚欠缺自身独立的概念体系，因而还不能成为一种独立的法学理论体系。要推动“数字法治”研究的进一步成熟，则必须注重概念的建构和体系思维的运用，并构造起相对完善的“数字法治”概念群，才有可能将新技术革命中出现的新生事物真正带入到法学理论体系的内部结构中去。

13. 个人数字权利实现的立体均衡逻辑（徐明）

来源：《法学评论》2025 年第 4 期

均衡是具有针对性、有效性、可行性的个人数字权利实现态势。个人数字权利的实现设定在三个内外纵横的立体均衡层面上：一是横向层面上个人数字权利相互之间的均衡，二是纵向层面上个人数字权利和数字义务之间的均衡，三是纵向层面上个人数字权利和数字权力之间的均衡。这三个纵横层面构成立体均衡的个人数字权利实现系统，根据系统论方法和数字权利动态发展机理，三个纵横层面的个人数字权利均衡包括整体性均衡、有序性均衡、结构优化性均衡和动态均衡，分别从“权利共处”出发确定各种个人数字权利在“量”上的合理分配比例、从“权利本位”出发确定个人数字权利和数字义务在“量”上的合理分配比例、从“权利保障”出发确定个人数字权利和数字权力在“量”上的合理分配比例，最终达到个人数字权利的主体维度均衡、内容维度均衡、空间维度均衡和时间维度均衡，在均衡中实现数字权利。

14. 数据安全法治的法理检视及治理之道（梅傲）

来源：《法学杂志》2025 年第 4 期

数据安全法治的实现是国家安全法治的重要环节，总体国家安全观的提出赋予数据安全更具时代性的内涵。在信息技术迭代加速的背景下，将数据安全的治理纳入法治轨道，实现数据安全治理的制度化、规范化，是实现国家治理体系和治理能力现代化的必然要求。数据安全法治以数据正义为根基，以维护国家数据主权与数据主体的数据权利为价值追求。为实现上述价值目标，一方面需要在立法层面进行审慎的法律选择，另一方面还要在执法层面实现数据安全的全流程妥善监管，方可在总体国家安全观框架内达到数据安全治理法治化的目标。

15. 算法个性化定价侵权责任的规则构建（刘迎霜）

来源：《法学杂志》2025 年第 4 期

算法个性化定价是平台经济中的普遍现象，对其规制的首要前提是明晰其法律性质。在当前法律语境下，算法个性化定价既不是《反垄断法》和《价格法》中的价格歧视行为，也不是《消费者权益保护法》《价格法》《明码标价和禁止价格欺诈规定》

等法律法规中的价格欺诈行为，其本质是一种大数据时代的自动化决策行为。秉持价格自由基本原则，是否需要以及如何对其进行法律规制和救济需要审慎分析行为产生的诸多损害，以获得正当性基础和恰当救济途径。算法个性化定价行为产生了降低市场效率、掠夺消费者剩余、侵犯消费者个人信息自决权、损害社会公平和数字社会信任等多法域的损害。算法个性化定价行为应属于侵权行为而不仅是合同违约行为。算法个性化定价侵权责任应采过错责任为归责原则，并应实行举证倒置和过错推定。行业惯例、动态定价、提供比价服务等应是算法个性化定价侵权责任的抗辩事由；私人诉讼、代表人诉讼与公益诉讼都是算法个性化定价侵权责任的诉讼形式；填补损害、停止侵害、惩罚性赔偿是算法个性化定价侵权责任之承担方式。

16. 何谓“数字法治”？（张文显）

来源：《法制与社会发展》2025 年第 4 期

近几年，“数字法治”成为越来越流行的法学概念和公共话语，已经被载入法学期刊论文、法学教科书、数字法学著作、传媒作品之中。那么，如何理解“数字法治”？或者说，如何给“数字法治”下一个定义或作出一个定义式表述呢？

17. 包容性和代表性同意框架的理念：将数据主体带入数据保护话语（Paarth Naithani, Indranath Gupta）

来源：International Data Privacy Law, Vol.15, Issue 1 (2025)

同意是为交易和个人数据处理提供有效性、可靠性和真实性的必要催化剂。知情同意是高级阶段的同意，可防止活动和事件对同意者造成无例外和意想不到的隐私后果。至关重要的是提供者对特定数据交易的理解（“可理解性”）。否则，如果没有理解，同意就会变得毫无意义。否则，它就变成了一种纯粹的交易活动，在那里没有独立的思想，并且个人对自由意志的行使是值得怀疑的。本文旨在带回同意中的理解元素。具体来说，它将捕捉不同数据主体在流行的隐私行为理论背景下所经历的决策过程的重要性，进而提出如何考虑多种因素的多样性来设计同意（包括在 cookie 的背景下）。法律规定了一种同意结构，从技术上讲允许数据主体从事隐私保护行为，以清晰简单的语言提供的信息有助于该人从事此类行为，关于同意和信息的规定允许数据主体对信息的处理进行控制。该法律假设人们根据隐私微积分理论做出决定，其中指出，人们会权衡隐私成本和收益来做出同意决定。它使用户能够在开始数据共享过程之前权衡成本和收益。

18. 智慧城市数据保护方法比较：新加坡的数字同意和问责框架（Wenxi Zhang et al.）

来源：International Data Privacy Law, Vol.15, Issue 1 (2025)

智慧城市代表了数字技术与城市基础设施的集成，从根本上改变了城市收集、处理和使用有关其公民和运营的数据的方式。这种转变有三个关键维度。首先，城市环境的“智能”改造涉及在整个城市嵌入传感器和数据收集设备。采用传感器和电子方法收集数据，用于多种目的，使包括个人数据在内的数据收集和使用量空前增加。其次，这些数据的实时处理和分析用于为城市运营提供信息。第三，旨在加强公共和私人服务的提供，通常是通过利用这些数据和分析的数字平台。新加坡的智慧国家计划就是这一转变的例证。自 2014 年推出以来，这个城邦一直致力于跨越广泛的政府和私人服务的数字化转型，此后被描述为世界上“最智能的城市”之一。例如，在新加坡，使用互联网进行网上银行的人数比例从 2017 年的 56%增加到 2021 年的 71%。从自动化交通管理和环境监测到综合支付系统和市政服务，数字技术已经并将继续融入城市日常生活的结构中。这种整合为改善城市服务和生活质量创造了前所未有的机遇。然而，它也给数据保护带来了独特的挑战，超出了数字环境中传统的隐私问题。因此，智慧城市背景提供了一个有用的背景，可以探索现有数据治理框架的局限性及其传统

理由和组织概念的充分性。

19. 重新审视数据可移植性：迈向未来以人为本、人工智能驱动的数据生态系统（Fenwick Mark et al.）

来源：Vanderbilt Journal of Entertainment and Technology Law, Vol.27, Issue 3 (2025)

本文批判性地审视了美国围绕数据可移植性的当代监管框架和话语。本文以欧盟最近的监管发展为例，表明尽管数据访问和可移植性在多个政策工具中被确定为重要问题，但至少在当前的迭代中，可移植性的法律概念继续加强服务提供商和数据控制者企业的利益，而不是个人最终用户的利益。本文认为，必须发生范式转变，转向更加以人为本的数据治理数据方法，在这种方法下，数据将被视为数字时代个人身份的基础。因此，应该交到个人手中，而不是服务商或数据控制企业手中。本文考虑了欧盟的技术和市场趋势，这些趋势揭示了并促进了这种变化。它建议监管框架应更好地与这些技术和市场发展保持一致，以鼓励市场参与者之间产生引发变革的趋势。简而言之，本文确定了一种变革性的数据可移植性方法，使个人能够自由和能力将其数据聚合到其控制或控制下的安全个人空间中。这种以人为本的数据可移植性视角对于为个人消费者构建人工智能（AI）驱动的应用程序至关重要，这可以为未来以人为本、人工智能驱动的数据生态系统铺平道路。

20. 危险的数字立足点：运用 Spokeo 和 TransUnion 案例解析网络隐私侵害（Ten Eyck Michael E.）

来源：Vanderbilt Journal of Entertainment and Technology Law, Vol.27, Issue 3 (2025)

近年来，《加州侵犯隐私法》（CIPA）已被用来起诉网站控股公司使用记录在线对话的聊天机器人。此类索赔已经引发了备受瞩目的集体诉讼和多地区诉讼，预计还会有更多诉讼。由于当网站保留其聊天框中的数据时，违反 CIPA 的行为通常会发生，并且该法规规定的损害赔偿相对较高，因此原告律师有动力寻求汇总索赔，从而产生耗时的诉讼。同时，提起诉讼的人所遭受的伤害属于无形隐私损害的范畴。美国第九巡回上诉法院关于地位的判例法显示，对潜在的名义伤害有更广泛的考虑。这与美国最高法院在 TransUnion LLC v.拉米雷斯强调伤病的具体性以赋予地位。虽然最近的判决表明 CIPA 在聊天室类型的集体诉讼中的有效性有限，但至少有一个法院认定 CIPA 原告没有任何看似具体的损害。本说明描述了在加州联邦法院引起大规模诉讼的潜在虚幻主张。然后，它分析了 TransUnion 的拟议解读下的常见伤害，该解读否认对大多数无形伤害的影响。它最终得出的结论是，上诉审查应迫使恢复第九巡回法院适用于无形数字损害的有限地位。然而，环联的决定可能基于不稳定的宪法基础。托马斯大法官提出了一种植根于历史的反对观点，强调了相关权利的性质。 这种观点可能会在更具原创性的司法机构中获得关注，并最终可能占上风。虽然托马斯法官的观点将允许看似无意义的法定损害赔偿诉讼，但本说明认为，它还可以告知立法机构在旨在保护数字隐私权时制定诉讼因由的最佳方式。

个人信息保护

1. 个人信息保护合规审计的基本框架与制度衔接（赵精武）

来源：《法律科学(西北政法大学学报)》2025 年第 3 期

我国近期公布的《个人信息保护合规审计管理办法》旨在落实《个人信息保护法》第 54 条和第 64 条规定的个人信息保护合规审计制度。然而，现有研究并未对该类合规审计机制的功能定位和具体内容进行系统性讨论，甚至存在将合规管理与合规审计等同看待的概念认知误区。个人信息保护合规审计机制不同于个人信息保护影响评估、数据安全风险评估等个人信息保护制度，而属于面向个人信息业务合规的专项合规审计活动，其“审计”属

性大于“合规”属性。个人信息保护合规审计机制是以传统的合规审计理论为起点，基于风险管理的传统理论建立的机制，其功能包括合规监督、合规鉴证和合规评估，规范包括审计基本原则、审计证据规则和审计报告规则等。个人信息保护合规审计制度中规定的前期证据调取、合规管理事实评定、审计报告出具和后期审计建议整改监督有助于促成个人信息保护合规审计与其他个人信息保护配套制度的相互支撑。

2. 信息信义关系的法律保护（刘亚菲）

来源：《法律科学(西北政法大学学报)》2025 年第 3 期

数据、信息、知识与智慧，共同构成数字时代的知识生产机制循环。在整个以信息流转为核心的闭环或开放系统中，应将属于自然人人格权益的个人信息权益作为最重要的权益加以保护。然而在智能化时代，信息处理者处理个人信息的方式更为隐蔽，对权益的侵害也更为隐蔽。现有告知同意规则与个人信息保护监管制度在保护个人信息权益方面虽然均发挥了重要作用，但其中却隐藏着一个需要在个人与信息处理者之间产生内生性信赖关系的地带。信息信义关系是弥合个人与信息处理者之间不对等地位以及建立信赖关系的重要纽带。信息信义关系既包括理念上的信任与信赖，也包括具象化的信息信义义务。这一义务构造以忠实义务为基础，以注意义务为拓展，进一步强化信息处理者积极履行保护个人信息合法使用的义务。信息信义义务之实现建立在明确信义关系的构造、明确目的限制原则、构建损害赔偿责任体系的基础上，进而作用于个人与信息处理者信任关系之建立。

3. 生成式人工智能背景下的个人信息保护：范式转换与规则完善（叶雄彪）

来源：《法学家》2025 年第 4 期

大数据刺激了生成式人工智能的智力涌现，也加剧了数字时代的隐私和个人信息保护难题。算法和大数据的叠加让生成式人工智能的数据处理过程迥异于传统网络服务，呈现出自动化、规模化和多样化特征。既有个人信息保护基础理论和相关规则难以在生成式人工智能领域有效适用，无法为用户信息权益和其他人身财产权益提供合理保护，更无法有效抑制违法数据处理导致的其他社会风险。面向人工智能时代的个人信息保护规则，需要以风险防控为核心，以国家强制力约束生成式人工智能设计者、研发者和提供者等主体的数据处理行为，并进一步完善个人信息获取规则、使用规则、存储和流通规则及救济规则。

4.《个人信息保护法》的私法功能及其式微（郭传凯）

来源：《法学论坛》2025 年第 4 期

《个人信息保护法》的私法功能在于授权信息主体以私人途径维护个人信息权益，其主要通过个体控制机制与私人诉讼制度予以实现。然而，个体控制机制的制度定位与私人诉讼制度的基本内容均有待明确。通过阐明私密个人信息保护与敏感个人信息保护的界线，以及《民法典》与《个人信息保护法》在非私密个人信息或非敏感个人信息保护上的分工，个体控制机制的制度定位得以确定，即保障信息主体通过私人途径应对算法决策问题，避免个人信息在算法决策的过程中遭到滥用。通过界分《个人信息保护法》的过错推定原则与《民法典》隐私权侵权的一般过错原则，阐明“权利束”保护之诉的可行性，私人诉讼制度的基本内容获得明确。个体控制机制难以限制算法决策技术的滥用，私人诉讼制度则面临过错推定原则的适用难题和信息主体的诉讼困境。因此，《个人信息保护法》的私法功能难以发挥重要作用。《个人信息保护法》私法功能的式微应通过公法途径予以回应。

5. 个人信息分类处理规则的解释适用——基于损害风险的视角（夏庆锋）

来源：《法学评论》2025 年第 4 期

我国《个人信息保护法》以个人信息是否具有敏感性区分为一般个人信息与敏感个人信息，对个

人信息各项权益进行分类保护。但是，由于非敏感的一般个人信息与敏感个人信息具有紧密关系，且伴随算法推测技术的不断发展，不同类型个人信息的边界范围愈发模糊。不当处理一般个人信息与敏感个人信息造成的损害后果也体现出同等水平，例如不当处理元信息、家庭/工作单位地址、性格类型、照片信息等一般个人信息造成的严重损害，以及一般个人信息能够作为敏感个人信息的“代理信息”共同造成损害等。因此应当以损害风险为依据对个人信息处理规则进行解释适用，尊重个人知情同意、顾及个人信息的处理目的与结合损害风险的动态性特征，从而发挥法律制度在保护个人信息权益与促进个人信息利用两方面的平衡功能。

6. 评估中国个人信息保护法的实施情况：两年回顾（Guosong Shao et al.）

来源：International Data Privacy Law, Vol.15, Issue 1 (2025)

《个人信息保护法》（PIPL）是中国第一部旨在保护个人信息的综合性法律。尽管《个人信息保护法》被称为中国的欧盟《通用数据保护条例》（GDPR），但它与《通用数据保护条例》有很大不同。本研究通过内容分析来评估 PIPL 在 2021 年 11 月 1 日至 2023 年 9 月 30 日期间在行政执法和法院裁决中的应用。研究表明，在《个人信息保护法》实施后的 2 年内，该法框架下共发布行政处罚公告 143 份，涉及 2993 件案件。此外，63 起一审法院判决书引用了 PIPL。对样本数据的详细分析表明，个人信息保护法在行政执法和司法应用中都处于次要甚至边缘的作用。换句话说，《个人信息保护法》尚未达到立法者预期的对个人信息保护的重大影响。建议中国在《个人信息保护法》框架内加强保护个人信息的国家义务。虽然行政执法可以作为主要的保护手段，但中国也应该放宽对公益诉讼的限制，允许个人民事诉讼作为这些救济的补充。

数据确权与流通

1. 论数据财产权的法律定位（于雯雯）

来源：《比较法研究》2025 年第 4 期

数据不宜在一般意义上赋予财产权，但基于特定目的而依法收集的数据集合可获得财产权。于财产权体系之中，数据财产权宜定位为一种新型财产权，具有财产权的排他支配性，同时于权利客体和权利限制等方面呈现特殊性。在财产的分类体系中，数据宜作为与智力创造成果相并列的无形财产。按照传统财产权的入法思路，宜单独立法，而与物权法、知识产权法并行。其在制度设计时需要重点关注权利的限制，可能涉及数据财产权并不赋予权利人对数据所载信息的权利，数据财产权的取得、行使受到所载信息的法律限制，数据集合的开放，数据集合的强制许可等方面，以实现权利与权利限制的平衡。

2. RCEP 数据跨境流动基本安全例外条款适用问题研究（郭德香）

来源：《当代法学》2025 年第 4 期

RCEP 数据跨境流动基本安全例外条款的设置回应了数字贸易领域非传统安全问题的扩张，旨在实现数字经济商业价值与监管规制的平衡。在规则设计方面，RCEP 数据跨境流动基本安全例外条款的文本设置过于灵活，以至于关键概念表述模糊、对缔约方自裁决权的约束有限、争端解决机制的不足等问题影响了条款的适用。对此，可以采取善意解释的解释方法、注重对限制措施与基本安全利益间关联性的论证、增强对条款适用的约束等措施实现安全例外条款的合理适用。我国应当明确 RCEP 数据跨境流动基本安全例外条款适用的中国立场，确保中国数据跨境流动规制措施援引该条款的合法性。

3. 数据产权：从物权到互操作权的变革（周汉华）

来源：《东方法学》2025 年第 4 期

数据产权的界定关系数据基础制度建设和数据作用的发挥。目前的主流界定方案深受物权法观念的影响，以确立数据持有者的权利为中心，以数

据交易作为数据价值的实现形式，既不利于数据流通利用，还会滋生各种连锁问题。因此，应当发挥数据要素乘数效应，创新数据产权观念，以互操作权为基础推动我国法律制度系统性变革，在使用中实现数据价值。互操作权以确立网络用户使用数据的权利为中心，以互操作作为数据价值的实现形式，在推动数据开放与共享的同时确保法治底线。此外，需要以权利束方式解释数据产权与三权分置，构建具有中国特色的数据产权制度体系。

4. 数据产权需要期限制度吗？（赵陶钧）

来源：《东方法学》2025 年第 4 期

域外数据库立法历程表明，不恰当的期限制度可能动摇产权建构的信心并减损其实施效益，期限问题应当得到重视。现有讨论受物权式思维和知识产权式思维惯性的影响，无法给出是否设置数据产权保护期限的圆满答案。期限制度的本意并非一味扩充公有领域，而是着眼于恢复被市场独占权损害的公平竞争秩序，以免去追踪成本和许可成本的方式便利客体的市场化利用。数据价值的强时效性致使数据产权的垄断效应有限，进而期限制度在数据市场中所能发挥的作用有限，同时也无力保障公众对数据的非市场化利用。期限制度还须设置易于辨认的保护期计算起点以及清楚、明确的期间，以便他人预测产权到期时间。但数据条目的事前认知成本过高，致使可供识别的起点极难选定、妥适的期间长度极难确定。综上，数据产权期限制度的代价与效益不成比例。为促进数据的流通，存在限缩初始权能、构建例外、反向设权、鼓励数据共享等期限制度的替代方案。

5. 算力财产权理论图景（温昱）

来源：《东方法学》2025 年第 4 期

作为数字时代基础设施以及人工智能发展的战略支点，算力财产权亟需确立。法学方法的理论储备与法体系空间为算力财产权的设立供给了制度支撑。从现实的算力保障需求上升为一项权利，需要阐明算力财产权内在理由蕴含的人格尊严和平等价值。算力财产权作为数字社会的“元权利”以及“普遍权利”的正当性应予规范承认。算力财产权外在理由强调算力在数据要素化和数字经济发展中的关键作用，凸显加强法律保护的必要性。算力财产权在规范层面应构建为一种具有普遍性、可及性与制度正当性的权利。举凡具有法律人格者均享有作为算力财产权主体的资格，范围涵盖从算力供给侧到终端使用的各类主体。算力具备财产权客体要求的可支配性、排他性、可转让性和价值性。算力财产权在数字环境下能够实现排他占有、竞争使用、双重收益和代码化处分。

6. 医疗数据共享之私权激励与行为规制（吴桂德）

来源：《东方法学》2025 年第 4 期

当前，医疗数据囤积的“数据孤岛”现象与不当利用行为频频发生，容易引发抑制竞争与创新、隐私权与知识产权侵权、互操作性受阻等挑战，因而需要制度层面合理的界权保护及其运行机制调整。一方面医疗数据可携权滥觞于民法上的健康权与人格权保护，另一方面医疗数据使用权源起自私法上对财产性利益的权利保护，其中的知识产权特征凸显。同时，法律制度的核心激励在于私法上的确权保护，并在技术支持背景下辅之以其他制度的协同共治，特别是公共利益维度，比如宪法层面的价值指引和反垄断法层面的行政监管与干预。故此，有必要构建医疗数据可携权与使用权形成合力的“二元权利架构”激励机制，即以私法赋权激励为主、公法行为规制为辅，并以数据信托为理论基点、医疗数据池打造为具体操作，实现医疗数据共享的公私法协同适用与社会福祉的提升。

7. 数据产权登记制度的体系构建（包晓丽）

来源：《法学家》2025 年第 4 期

数据产权登记是权利人将数据权利状况予以记载，并通过登记系统对外公示的行为，是数据要素市场建设中的关键环节。尽管数据内容具有实时变动性，但数据权利状况具有特定性，数据财产权具有登记能力。当前的数据登记多以信息发布和交

易匹配为主要目的，难以发挥降低权利识别成本和辅助流通监管等功能。数据登记制度的建设应当转而聚焦对数据权利状况进行实质性审查的数据产权登记，并根据登记阶段的差异区分为首次登记和流转登记。首次登记发挥权利推定效力，流转登记发挥对抗效力。登记并非数据财产权取得与变动的生效要件，宜以登记对抗为原则，这有助于节省排他性交易中当事人的权利公示成本和第三人的权利核验成本。

8. 数据权益损害赔偿规范体系构造论（朱晓峰）

来源：《法学论坛》2025 年第 4 期

数据权益是大数据时代产生的一种独立的新型权益，内部呈现出个人数据权益和非个人数据权益的二元构造，后者包括企业数据权益和公共数据权益。侵害个人数据权益导致的损害赔偿既包括对财产损失的赔偿，也包括对精神损害的赔偿。由于《民法典》第 1183 条第 1 款、第 998 条结合《精神损害赔偿解释》第 5 条确立的精神损害赔偿规则，与《民法典》第 1182 条、《个人信息保护法》第 69 条第 2 款结合《民法典》第 998 条所确立的财产损失赔偿规则中关于赔偿认定方法及考量因素的耦合，使个人数据权益侵害场合的财产损失与精神损害赔偿二者之间原本显著的区别被消弭了。非个人数据权益的侵权损害赔偿，应在特别法规定与一般法规定所分别确立的财产损失赔偿规范体系内明确各自的适用领域和界限，防止特别法规定的计算方法向《民法典》第 1184 条规定的“其他合理方式”这一一般条款逃逸，避免立法者通过特别规定对特定行为予以特殊调整的立法目的落空。

9. 论公共数据类型化及其收益分配标准（唐安然）

来源：《法制与社会发展》2025 年第 4 期

公共数据内涵及其收益分配无法脱离公共性语境与公共性目标。规范主义和功能主义的立场导致公共数据的内涵缺乏一致性和流于泛化，这亟需在公共性语境下基于数据来源将公共数据划分为“不源于任何个体的公共数据”“政府数据与个体数据混合的公共数据”和“个体数据归集而成的公共数据”。公共数据收益分配应基于不同的行政法基础，按公共数据类型重新选择“国家所有与全民共享”的所有者标准、“谁提供、谁获益”的来源者标准和“谁投入、谁获益”的贡献者标准。由此，“不源于任何个体的公共数据”适用所有者标准，“政府数据与个体数据混合的公共数据”适用贡献者标准，“个体数据归集而成的公共数据”组合适用来源者标准和贡献者标准，从而赋能公共数据的价值实现。

10. 数据秘密：数据法的新商业秘密框架（Ella De Noyette, Leander Stähler & Thomas Margoni）

来源：IIC-International Review of Intellectual Property and Competition Law, Vol.56, Issue 5 (2025)

新近通过的《数据法案》（DA）在欧盟范围内建立了规范特定数据访问、再利用及可移植性的全新监管框架。该框架的核心在于商业秘密（TS）的作用定位，这体现了数据共享义务与商业机密保护需求之间微妙的平衡关系。本文批判性地探讨了《数据法》对同时构成商业秘密的数据（我们称之为“数据秘密”这一新类别）的管理方法，重点阐述两大要素：行政主管机构与技术保护措施（TPMs）。《数据法》在商业秘密生命周期中新增设立的国家主管机构，实质上对商业秘密主张实施事前评估，从而改变了传统的私权救济机制。与此同时，TPMs 通过技术监管手段为商业秘密增添保护层，可能延伸其类似财产的效力。通过分析物联网（IoT）和企业对政府（B2G）场景中的这些发展，本研究指出《数据法》实质上创设了独特的商业秘密类别，或将在重塑欧盟数据经济中发挥重要作用。然而，这种演变引发了关键的解释性与实践性问题，尤其涉及行政一致性、技术实施成本，以及对市场竞争力和创新激励的影响。归根结底，数据保密制度代表着重要的立法创新，需要进行严格评估以确保数据透明度与保密性之间的平衡。

人工智能

1. 论“通知”规则在生成式人工智能作品侵权中的类推适用（王利明、包丁裕睿）

来源：《比较法研究》2025 年第 4 期

生成式人工智能作品侵权的责任承担，既关系到受害人权益保护，也关涉技术利用与创新、产业发展以及信息自由等重要价值。在坚持过错责任原则的前提下，唯有合理设定生成式人工智能服务提供者的注意义务、审慎判断其是否构成过错，方能实现多元利益之间的有效平衡、促进社会整体福祉。我国民法典第 1195 条规定的“通知”规则，为判断网络服务提供者是否具有过错提供了一种具体化、可操作的路径。尽管生成式人工智能作品侵权与传统网络侵权在结构上有所不同，但在主体、价值、情境等本质特征上具有高度相似性，从而具备了类推适用“通知”规则的正当性基础。在具体适用上，“通知”规则所要求的“合格通知”与“必要措施”，应结合生成式人工智能服务的运行机制和技术特点加以解释。与之配合，我国民法典第 1197 条规定的“知道或应知”规则的类推适用构建了生成式人工智能服务提供者在未接到通知情况下的注意义务。两者共同构成了一个动态的注意义务体系，注意义务的标准随“现有技术水平”的发展而不断更新。

2. 通过技术标准规制人工智能：基于合作规制的法理（张涛）

来源：《比较法研究》2025 年第 4 期

如何对人工智能进行有效治理是当前学界重点关注但又尚未形成广泛共识的问题。从国家治理的角度看，技术标准的规制效能逐渐获得理论与实践的肯认，成为一种重要的人工智能规制工具。在理论上，将技术标准嵌入人工智能治理体系中，契合嵌入式伦理、治理生态、知识共创、分层治理等治理逻辑。然而，在实践中，人工智能标准化治理也面临正当性、科学性、协调性和有效性方面的困境，难以最大限度地发挥治理效能，需要选择一个合适的规制模式进行重新构造。相比纯粹的行政规制和自我规制模式，合作规制模式不仅契合人工智能标准本身的内在规律，而且可以有效解决人工智能标准面临的现实困境。基于此，可以通过对人工智能标准的功能地位、内容设计、制定程序和实施监督进行制度设计，实现基于合作规制的人工智能标准化治理。

3. 人工智能供应链市场的反垄断规制革新（徐则林）

来源：《东方法学》2025 年第 4 期

在风险社会中，人工智能的垄断风险治理不容忽视。沿着人工智能的供应链，从模型上游基础层的数据、算法、算力，到下游的主机层、应用层，几乎在每个环节都存在已出现或即将形成的垄断结构。这一供应链中的垄断结构不仅源于经营者对各要素资源的控制，还源于其构建的独特生态系统。在这一垄断结构之上，经营者的垄断行为同时表现为以人为主导和以算法为主导两种形态。从市场特殊性来看，人工智能供应链中的动态竞争是市场常态，竞争与垄断并非相互对立，垄断者随时可能由于动态性竞争和颠覆性创新而失去垄断地位。显然，人工智能垄断风险治理必须在动态竞争观下革新传统的反垄断法规制范式。反垄断旨在制止人工智能供应链市场中排除、限制竞争的行为，但并不意味着追求原子型的市场结构，应避免政府对市场的过度干预，建立更符合动态竞争特点的违法性认定规则、补足有利于恢复市场竞争的救济措施，并以智慧化方式提升反垄断监管的精准度。

4. 人工智能立法的动态演化框架与制度设计（李学尧）

来源：《法律科学（西北政法大学学报）》2025 年第 3 期

如何构建兼具稳定性与灵活性的人工智能立法框架是一个全球性议题。针对规范方法论主导下的人工智能立法思路可能引发的制度适用问题，应采取“适应型法”的立法思路。为了实现法律规则

与技术演进的动态适配，还应结合本土实践探索人工智能立法的“适应性法治”路径：审慎对待体系化、部门法化的立法目标，尽量在传统部门法的实体法框架中采用立改废释的方式实现人工智能的立法目标；动态适应性原则应是人工智能立法的核心原则；条款拟制应从“义务本位”转向“行为激励”；学理阐述需把重点放在如何建立“法治化”“中央底线规则+地方差异化试点+司法判例引导”的多层治理体系，进一步优化“软硬法协同”在内的中国式法治实践。这样既可以延续中国改革开放以来“试验—推广”的制度创新传统，也可尝试为全球技术治理贡献具有普适价值的制度分析工具。

5. 深度伪造技术滥用行为的刑法回应（郑高键）

来源：《法律科学(西北政法大学学报)》2025 年第 3 期

深度伪造技术的滥用已然超越了纯粹的人工智能技术边界，迈入违法犯罪的灰色地带。深度伪造技术在社会生活中的不当和非理性适用，带来了一系列刑事治理层面的疑难问题。为回应这一问题，在学理层面，应当阐明深度伪造技术滥用的不法形式和危害样态，揭示技术发展与刑法之间的治理鸿沟，形塑全新的刑法理念和解释规则，理顺刑法规制深度伪造技术滥用行为的制度逻辑；在治理路径方面，应当将技术原理作为法益界定的重要基础，构建符合涉罪特质的法益保护体系，依托刑法体系进行合理解释，并坚持刑法文本的规范指引作用，明确不法行为的认定标准，为相关行为的刑法治理提供坚实的理论支撑和有效的实践框架，以实现对深度伪造技术滥用行为的有效规制。

6. 版权法上生成式人工智能输出的定性及其责任规则（梁志文）

来源：《法学》2025 年第 6 期

在生成式人工智能生成物与版权材料构成实质性相似时，在法律定性上必须从技术本质出发。生成式人工智能的基础是大模型，它将训练数据样本分解成令牌以确定内容特征上的统计相关性，输出过程是具有统计相关性特征的随机性重组。大模型通过应用程序编程接口与用户交互而形成人类能理解的作品，但在特定情形下可能照搬训练数据中的版权材料。大模型并非作品的复制工具，不属于“索尼案”实质性非侵权用途标准的适用范围，但属于具有双重用途的技术。大模型既未主动输出、也未存储生成物，用户输入提示词、参数等并选择最终的成品；其大多数应用场景与搜索引擎类似，属于信息社会的新型服务，应适用“通知移除”制度等“避风港”规则，并不负有公法上网络治理规则施加的义务。服务提供者在大模型开发、部署时采取了技术可行且考虑合理使用情形的必要措施，不承担赔偿责任。大模型输出生成物类似于用户通过使用搜索引擎获得相应结果，故“避风港”规则不能延伸适用于生成物的传播和商业利用行为，后者将构成直接侵犯版权的行为。

7.“四法并置”:迈向适应性治理范式的人工智能立法（陈坤）

来源：《法学论坛》2025 年第 4 期

基于人工智能领域的特点、人工智能善治的目标以及平衡安全与发展的现实需求，人工智能治理需要迈向适应性治理范式。在人工智能治理问题上，适应性治理范式从敏捷性治理、协作式治理与自适应治理三个面向提出了若干具体要求。为满足这些要求，也为最大程度地实现人工智能治理的全面性、有效性与及时性，我国人工智能立法宜采取由总纲性的“人工智能基本法”、规制风险的“人工智能规制法”、鼓励创新的“人工智能促进法”与规范人工智能在法律领域应用的“人工智能控权法”构成的“四法并置”立法路径。为实现或接近“维护基本价值”“增进社会福祉”“推动个人发展”的善治状态，人工智能立法还应充分考虑“四法并置”专门法体系与其他法律规范、技术标准、伦理规范以及国际治理体系的外部耦合问题。

8. 人工智能生成内容可版权性的认定方法研究（张

究）

来源：《法学评论》2025 年第 4 期

人工智能技术的快速发展对著作权制度提出了新的挑战。人工智能的自主决策性及生成过程的黑箱性使得著作权法“创作-作者-作品”之间的逻辑关系发生了断层，在人工智能生成内容可版权性认定中，确认作者身份成为了核心争议。拨开技术迷雾，解决人工智能生成内容的“作者身份”问题无需突破著作权法理论框架，应以“智力贡献论”为理论基础确立合理的认定方法。该认定方法的适用价值体现于，在关注内容生成过程中人类行为活动的创造性时，充分考虑人工智能的技术特殊性，厘清创作者行为与作品呈现内容之间的因果关系。基于人工智能生成内容与实用艺术品同处于著作权保护范围边缘的客体共性，实用艺术品可版权性认定中的“分离原则”及“概念性分离测试”能够为确立认定方法提供启示。将人工智能生成内容视为若干创作决策叠加作用产生的结果，确认“作者身份”的关键在于将其中的人类创作决策分离出来，重新整合为一个独立于人工智能决策的虚拟创作计划，判断人类创作决策所指向的具体的创造性表达是否为最终呈现内容中的实质性部分。

9. 构思决定论视野下生成式人工智能生成物的版权保护（张金平）

来源：《法学研究》2025 年第 4 期

我国法院通过类比摄影作品，初步构建了生成式人工智能（GenAI）生成物的版权司法保护模式，但可能引发三重转向：独创性的判断和实质性相似的比对都从最终表达转向构思，而版权直接侵权责任从执行者转向构思者。然而，GenAI 与照相机在执行人类构思上存在根本差异，并非机械固定而是“自主”转化，故类推适用摄影作品构思决定论之“可视化构思+机械固定”二元要件难以支撑三重转向。为此，建议将构思决定论修正为三元要件：一是“‘可视化’构思”延续传统理论；二是“受控固定”要求作者通过合理控制保障其独创性构思是 GenAI 生成最终表达的有效原因，维系思想与表达二分法；三是“创作记录”作为作者证明独创性贡献的必要证据，既划定权利边界又防范滥用 GenAI。

10. 生成式人工智能、模型内部的复制品以及向公众开放（Tim W. Dornis）

来源：IIC-International Review of Intellectual Property and Competition Law, Vol.56, Issue 5 (2025)

生成式人工智能（AI）模型的训练需要收集和分析数量惊人的数据，其中大部分由受版权保护的作品组成。迄今为止，这些作品的复制品是否在模型训练期间在模型内部创建的问题很少被讨论。这是争论中的一个严重盲点，因为此类复制品（例如，在 ChatGPT 或 Stable Diffusion 的模型中）可以提供给最终用户，因此，当在线提供人工智能服务时，也可以向公众开放。根据 InfoSoc 指令，这可能是侵犯版权的。届时，欧盟成员国的国家版权法将适用，其国家法院将拥有国际管辖权。从这个角度来看，广泛传播的非欧盟人工智能开发者不受欧盟版权法约束的说法是一种错觉。

11. 人工智能、刑事侵权和意图——所有作品的保护真的平等吗？（LauraTammenlehto, Heikki Kallio）

来源：IIC-International Review of Intellectual Property and Competition Law, Vol.56, Issue 5 (2025)

本文研究了芬兰人工智能辅助著作权犯罪中犯罪意图的实现问题。随着技术持续发展，新型行为已纳入著作权法广泛的刑事保护范畴，并挑战了传统刑事责任归责理论。就生成式人工智能而言，最终产物的生产者实为整合多源信息的 AI 系统，而非编程者——后者仅设定生成特定类型的输出指令。这种结构在犯罪意图认定上存在法律困境：传统法学要求犯罪意图须涵盖非法行为的所有要素，但 AI 的介入导致意图评估存在不确定性，尤其体现在认知层面，此点可通过案例分析加以阐释。除阐释犯罪意图的构成要件外，本文还从刑法与著作权法双重视角，审视终极手段原则的分析结

果，评估该体系在所述情境下的适用性。研究表明，当前人工智能语境下对犯罪意图学说的解释倾向于保护知名作品。我们得出结论：用刑事手段解决技术发展及其应用所引发的问题缺乏正当性。权利人的法律地位应当通过其他途径予以保障。

12. 为什么田纳西州的《猫王法案》是人工智能保护之王（Fowler Sarah Luppen, Fowler John D.）

来源：Vanderbilt Journal of Entertainment and Technology Law, Vol.27, Issue 2 (2025)

人工智能（AI）正在快速发展和进步。随着人工智能的进步，它给个人和行业带来了新的法律问题。例如，人工智能现在可以很好地模仿著名音乐家的声音，以至于听众几乎不可能辨别人声是来自这些音乐家还是用人工智能生成的。然而，在现行的法律框架下，模仿著名艺术家声音的新作品可以由任何人创作和发行，无需音乐家同意，也不会产生任何法律后果。幸运的是，立法者正在提议立法，以防止在面对人工智能时未经授权使用他人的声音、图像或肖像。第一部以人工智能为重点的州法律，田纳西州的《确保肖像、语音和图像安全法案》（ELVIS 法案）于 2024 年 3 月 21 日通过，并于 2024 年 7 月 1 日生效。此后，多个州和联邦立法者提出了类似的法律。本文认为，《猫王法案》是一般人工智能保护，特别是录音艺术家的黄金标准，它提供的保护应纳入联邦公开权法。事实上，《猫王法案》的许多关键条款都包含在与人工智能保护语音、图像和肖像相关的联邦立法中。包括《猫王法案》中许多主题的联邦立法将保护艺术家的声音免于被新兴人工智能技术不公平地挪用，并以他们未经授权的方式使用。它将提供统一的保护，从而防止目前拼凑而成的宣传法体系进一步分开。随着人工智能的发展速度比美国社会中任何其他部门（包括法律）都要快，立法者现在可以通过快速通过国家立法来弥补差距。

13. OpenAI 的专利承诺：后 Moderna 分析（Gabriela Lenarczyk, Mateo Aboy）

来源：Journal of Intellectual Property Law & Practice, Vol.20, Issue 6 (2025)

专利质押越来越多地被用作私人订购机制，以促进创新和协作，同时平衡专利持有人的专有利益。英国高等法院的 Moderna 诉辉瑞/BioNTech 案的判决标志着对此类质押的可执行性和解释的首次司法分析。OpenAI 的专利承诺承诺在特定行为条件下进行防御性专利使用，这引发了新的解释问题。他们的承诺与传统承诺不同，侧重于防御性使用，以特定的行为触发因素为条件，例如避免针对 OpenAI 的伤害或采取法律行动。本文通过 Moderna 框架的视角审视该承诺，分析其范围、可撤销性和作限制。该承诺依赖于广泛的行为条件并且缺乏明确的时间标记，带来了值得注意的法律和实践复杂性。这些因素影响其可执行性，并为第三方依赖带来挑战。我们的分析强调了专利持有人的战略灵活性与明确性以促进实施者之间信任的必要性之间的平衡。研究结果强调了促进创新和保护专有利益之间的平衡。

14. 我即将被人工智能取代吗？（Beverley Potts）

来源：Journal of Intellectual Property Law & Practice, Vol.20, Issue 7 (2025)

自 OpenAI 的 ChatGPT 在 2022 年末席卷全球以来，众多律所纷纷试用各类人工智能系统，并制定其 AI 应用策略。这确实令人振奋——我们都有希望机器接管的琐碎事务。然而想到科幻灾难场景可能近在眼前，机器随时准备自动化我们的一切工作并最终取代人类岗位，这种念头又令人心生恐惧。我们尚未走到那一步，尤其考虑到当前 AI 系统普遍存在的问题。我曾亲历 AI 工具对法院判决进行摘要后，竟自信满满地给出完全错误的结论。那些冗长繁琐的生成式 AI 回复也令人失望——字数堆砌却毫无实质内容。此外，偏见问题、隐私保护及潜在版权侵权等诸多争议仍悬而未决。

15. 人工智能版权诉讼中的诉状问题：Getty v Stability（英国）和 Doe v GitHub（美国）的经验

教训（Brendan Guildea）

来源：Journal of Intellectual Property Law & Practice, Vol.20, Issue 7 (2025)

本文考虑了声称其受版权保护的作品被人工智能（AI）提供商侵权的作者所面临的困难。特别是，它着眼于当地启动诉状的实务规则所要求的事实细节程度与生成式人工智能工具的“黑匣子”性质之间固有的紧张关系——尽管有强制性报告要求，例如欧盟《人工智能法》（法规（EU）2024/1689）第 53（1）（d）条规定的报告要求）。借鉴英国 Getty 诉 Stability 案和美国 Doe 诉 GitHub 案的临时裁决，它将考虑通常要求详细描述被告涉嫌犯下的错误的法院规则是否对索赔人构成障碍。有人会争辩说，中间证据开示申请（在某些法域称为“披露”）目前没有为潜在索赔人提供适当的途径来获得书面证据，而书面证据对其预期案件具有证明作用。因此，需要一种新型的诉讼前程序来重新平衡作者与新兴技术经营者的权利。

16. 人工智能时代的发明：审查美国专利商标局人工智能辅助发明指南（Mateo Aboy et al.）

来源：Journal of Intellectual Property Law & Practice, Vol.20, Issue 7 (2025)

人工智能（AI）在创新领域的迅速崛起在专利法和人工智能（包括发明人身份）的交叉领域带来了具有挑战性的问题。对此，美国专利商标局（USPTO）发布了 2024 年《人工智能辅助发明发明指南》，强调发明人身份以人为本。人工智能系统不能被命名为发明人，但如果自然人对发明的构思做出重大贡献，它可能会协助可申请专利的发明过程。这一立场基于法定语言、司法先例以及专利旨在承认和奖励人类聪明才智的观点。本文研究了美国专利商标局的发明指南，分析了其人工智能辅助创新的指导原则和示例。关键要素包括“人类重大贡献”标准，该标准要求一个人的角色不仅仅是简单地作或解释人工智能系统的输出。我们还讨论了 Pannu 因素的作用——共同发明人的长期标准，在指南中重新用于评估当人工智能协助发明开发时人类是否达到发明人的门槛。对于从业者来说，该指南更加明确了人工智能辅助发明的发明人要求，强化了人类大量参与其构思的要求。重要的实践经验教训出现了。此外，各种更深层次的问题仍有待进一步研究。

平台治理

1. 超级平台国家安全自治及其监管（杨永红）

来源：《法商研究》2025 年第 4 期

随着超级平台渗透人类社会活动的方方面面，超级平台自治的私权力已扩张到传统国家公权垄断的国家安全领域。超级平台的崛起正在以新的方式塑造国家安全的治理。由于超级平台具有私人中介实体的法律地位，禁止一般监管与中介责任豁免原则成为超级平台自治的一般性原则，权力主体的错位使国家缺乏法律手段对超级平台公权私用进行监管。尽管欧盟对超级平台的监管已向强监管模式转向，但并未改变超级平台自治的一般性原则。因私主体进入公权领域而产生的结构性矛盾使美国能够借助非正式监管有效地影响超级平台国家安全自治，同时逃避公权所应受到的国内法与国际法的限制，在缺乏法律与领土限制的情况下隐蔽地实现了美国的长臂管辖。在私人第三方争端解决机构尚未构成对超级平台的有效限制、科技外交未能促成国际监督机制的情况下，美国超级平台的国家安全自治放大了美国的数字霸权。中国一方面，应积极支持我国大型平台的全球发展，并建设有中国特色的超级平台国家安全自治监管模式，以平衡美国数字霸权；另一方面，应在联合国框架下大力构建多利益攸关方参与的国家与私主体合治的国际监督机制，为构建网络空间命运共同体提供治理经验与发展基础。

2. 我国预防性平台纠纷治理的实践逻辑与优化路径（李朝）

来源：《法商研究》2025 年第 4 期

作为平台纠纷治理的主要方式，我国预防性平台纠纷治理发轫于平台在线纠纷解决经验的全球化推广，延展于数智赋能的技术驱动，并契合新时代“枫桥经验”的价值导向。预防性平台纠纷治理围绕“社会效果优先”的治理目标、“平台客服+大众评审”的人员配置、“准司法式”的评审程序以及“内部绩效与外部动员并列”的分类激励展开，但是在实践中存在治理目标为企业利益所俘获、不同纠纷治理方式的关系错置、人员构成不合理且激励杠杆难以维持，以及外部衔接受阻而致孤岛作业等问题。针对这些问题，既要向内强化“目标—执行”的链式监管、理顺不同纠纷治理方式的适用标准、提升解纷主体的纠纷治理能力，也要向外整合衔接协作口径，推进多元化平台纠纷治理的联合作业，拓展预防性平台纠纷治理的适用空间，实现治理效益最优化。

数字行政与司法

1. 完美的效率还是负责任的正义？——大语言模型时代数字司法的价值反思（雷磊）

来源：《东方法学》2025 年第 4 期

大语言模型时代的数字司法在价值上最显著的优势是实现了几近完美的效率，但因为无法进行价值判断而很难满足实质正义的要求，更无法实现司法裁判所要求的“负责任的正义”。负责任的正义是一种基于论证和代表的程序正义，要求司法裁判同时提起“真实性宣称”与“正确性宣称”。基于大语言模型的技术限制，数字司法既因为幻觉问题和完美训练集问题而存在真实性缺陷，又由于只能掌握“语词”（标识）而非真正的“语言”（意义），以及存在用数字技术消解司法程序空间的倾向而遭遇正确性或可证成性缺失的问题。基于大语言模型的伦理限制，人工智能系统不应为司法裁判负责，人类法官也不应放弃自己的道德自主，将司法裁判的责任推给机器。在根本上，大语言模型只是裁判辅助技术，既不能、也不应为司法裁判的正义负责。

2. 数字体行政组织法地位的审查框架（白云锋）

来源：《东方法学》2025 年第 4 期

以数字技术为支撑的各类数字体的行政组织法地位问题是确定数字体行政法律责任的前提性问题。面对科技发展的不确定性，相较于追寻主体性问题的终极结论，提供一套通向结论的判断方法是更为科学与开放的方案。人工智能等数字体主体性的判断本质上非以自然人为标尺。无论自然人还是法人作为法律主体，均是基于法律系统的“自创生”。数字行政工具、数字行政系统、智能行政工具与智能行政系统四类行政数字体，从不同维度冲击着现有行政组织体系。数字体进入行政法主体体系，需要经过“事实可行性”与“规范必要性”的双要素考量，以及“行政工具→一般法私主体→行政法公主体”的三阶段审查，满足对应阶段的条件方具有对应的行政组织法地位。目前关于自动化行政的合法性控制实质上只是第一个阶段的审查。为合理分配行政法律责任并保有人类的主体性地位，只有通过三阶段审查并得到立法授权的数字主体才能成为独立承担行政职能、具有有限人格的行政法公主体。否则，数字体仅能作为行政工具或受委托的一般法律主体。

3. 刑事司法大数据一体化的实践问题与机制建构（漆晨航）

来源：《法学论坛》2025 年第 4 期

刑事司法机关的履职活动大量收集、产生、使用与储存数据，为充分挖掘大数据价值，各机关积极推动以数据汇聚与共享为表现形式的刑事司法大数据一体化实践。但自主性、行政性、有限性的实践特征，催生过度重视数据汇聚却忽视共享，数据主体扩容诱发数据安全与个人信息保护风险，因数据权限不明导致刑事司法机关职权混同竞合等关键问题。分析问题成因，直接成因是相关规则的系统性缺位，根本成因则是并未就刑事司法大数据一体化达成共识，故而应以法治方法推动机制建

构。首先，以刑事司法职权为依据厘清大数据处理细化刑事司法大数据一体化平台建构指南，明确平台运行维护主体、数据目录与安全规范等问题。最后，要求检察机关承担平台监管职责，制定大数据分析系统备案规则，并向辩护方与公民开放部分数据，以促进刑事司法大数据一体化的多元制约。

4. 犯罪追诉数字化背景下嫌疑判断的演化与程序法规制的因应（裴炜）

来源：《法学研究》2025 年第 4 期

数字技术的发展正在重塑犯罪嫌疑的生成与判断逻辑。传统的嫌疑判断，主要依赖执法人员对具体行为的直接观察以及以其为基础的经验推断。然而，大数据与人工智能等技术的深度应用，改变了嫌疑的信息基础结构，使嫌疑的信息基础从核心案件事实延展至更为广泛的外围信息。伴随这一变化，嫌疑的判断逐步呈现出由个体转向群体、由自然人转向数字人、由事实转向情报、由人类理性转向机器理性的变迁与融合。这一趋势在提升侦查效能与潜在犯罪发现能力的同时，也引发了“嫌疑稀释”的现象。该现象会削弱嫌疑作为刑事诉讼程序规制工具的核心功能，并对正当程序的实现及公民基本权利的保护构成严峻挑战。因此，现有刑事诉讼制度有必要作出相应调整，将“嫌疑信息密度”纳入嫌疑的评价维度，通过程序过滤机制确保嫌疑判断与具体诉讼措施和决策之间的匹配性，从而推动数字技术在嫌疑判断以及以其为基础的犯罪追诉中的合理应用，保障刑事诉讼在数字化转型中的制度稳定性。

虚拟财产

1. 数据资产出资适格性的检视与完善（李欢）

来源：《东方法学》2025 年第 4 期

进入数字经济时代，传统非货币出资“三要件”，即可转让性、可评估性、合法性，正面临数据资产的新挑战。核心争议聚焦于“可转让性”标准的法域冲突，民法强调权利的归属性，数据法侧重流通、控制，而公司法则关注资本真实性。这种规范错位导致数据资产权利结构面临“双重切割”风险：横向切割产生重复出资，纵向切割导致出资价值虚化。应建构单一数据财产权制度，并使其排他性受到双重限制：一是个人信息权益的人格权保留；二是数据来源者的法定使用权。数据出资适格性判定应建立“基础+特殊”复合标准体系：基础要件包括数据合法性、确定性及质量完整性；特殊要件要求业务关联性、价值稳定性及可独立转让性。数据出资还应做好配套制度建设，着重构建数据出资登记公示系统、动态评估机制及责任追偿体系，并通过穿透式监管防范资本虚化风险。

2. 数字遗产继承的理论构建与基本框架（谭佐财）

来源：《东方法学》2025 年第 4 期

将实物遗产继承规则直接适用于数字遗产面临理论障碍，有必要系统反思并构建相应的继承规则。数字遗产的可继承性是首要问题，关于侵犯死者或通信对象的隐私、破坏社会信任基础等担忧均可通过学理阐释或技术方式予以化解。若将继承法上的遗产性质界定为一项法律地位，即可将数字遗产纳入实证法调整范围。简单地以用户协议中的数字遗产条款来安排权利结构可能有悖于继承法原则，具体规则构建应当以尊重死者意愿为核心原则，依序通过遗嘱等书面指示、平台在线工具、平台规则等方式认定死者意愿。若前述方式缺位，则根据数字遗产的商业性程度和人格属性嵌入程度，设计类型化的死者意愿默示规则。为平衡网络服务提供者、死者、近亲属、通信对象及公共利益，应当以比例原则为分析框架合理限制数字遗产继承，包括以正当理由为继承条件，排除其他用户的数字资产，遵循最小必要原则确定继承方式等。

（技术编辑：李佳丽、麻卓妍）

教研活动

中国人民大学法学院建院 75 周年系列活动预告丨世界百所法学院院长论坛 + 14 个平行主题国际论坛

第四届 21 世纪世界百所著名大学法学院院长论坛暨人工智能时代全球法治大会将于 2025 年 10 月 3-4 日召开。会议嘉宾约 400 人，包括外籍嘉宾一百余人，汇聚五大洲 30 多个国家的知名法学院院长、专家学者及相关国际组织负责人。

会议将聚焦**“人工智能时代全球法治”**，深入探讨**数字法学与未来法治、民法与《民法典》、全球南方与“一带一路”法治、知识产权法、刑事法、刑事诉讼法、比较公法、国家法学、纠纷解决、数字经济竞争法、数字资产与数据法、人权与残障人权利保护、食品安全治理、气候变化与环境法**等主题。

2025 年 10 月 3 日上午将进行第四届 21 世纪世界百所著名大学法学院院长论坛暨人工智能时代全球法治大会开幕式，同日下午将进行第四届 21 世纪世界百所著名大学法学院院长论坛。

2025 年 10 月 3 日下午至 10 月 4 日全天将举行十四个平行主题论坛，包括第六届“未来法治与数字法学”国际论坛(The Sixth International Conference onthe Future Rule of Law and Digital Law)、数字资产的全球法治回应论坛(Global Legal Responses to the Digital Assets)、第二届人工智能与纠纷解决论坛暨 AI 时代的纠纷解决国际论坛(International Forum on Dispute Resolution in the Artifcial Intelligence Era)、全球南方与“一带一路”法治论坛(Forum on the Rule of Law for the Global South and the Belt and Road Initiative)、国际比较视野下公法的新发展论坛(The Changing Public Law: An International Perspective)、人工智能与刑事司法研讨会(Al and Criminal Justice Seminar)、比较法视野下的中国民法典论坛(Chinese Civil Code from a Comparative Perspective)、人工智能时代的知识产权新平衡论坛(International Forum on Emerging Ip Issues in the Age of AI)、国家法学:基础理论与时代挑战(The Study of State Law: Foundational Theory and Contemporary Challenges)、数字经济竞争法的理念转型和新维度论坛(The Conceptual Transformation and New Dimensions of Digital Economy Competition Law)、《<刑事诉讼法典>专家建议稿》新书发布会暨刑事诉讼法修改研讨会(Book Launch of“Expert Draft of the Criminal Procedure Code”& Symposium on the Amendment of the Criminal Procedure Law)、科技时代的人权保障与无障碍建设:全球视角与国家实践(Human Rights Protection and Accessibility in the Technological Age: Global Perspective and National Practice)、亚太食品安全治理国际论坛(International Forum on Asia-Pacific Food Safety Governance)、应对气候变化与绿色低碳发展论坛(Roundtable Forum on Climate Change and Green Low-Carbon Development)。

要闻 | 中国科学技术法学会“人工智能法律前沿问题”研讨会顺利举行

2025 年 9 月 20 日，中国科学技术法学会在河北省检察官学院成功举办了“人工智能法律前沿问题”的研讨活动，就人工智能发展对法律制度提出的挑战，人工智能主体性、伦理性的一般法理，人工智能法律制度建设方向等问题展开了热烈且充分的研讨。

中国科学技术法学会会长**董开军**出席会议并发表讲话。中国科学技术法学会副会长、北京大学人工智能研究院 AI 安全与治理中心主任**张平**教授，中国政法大学数据法治研究院**王立梅**教授等参加会议并围绕上述问题发表观点。来自河北省人民检察院、北京大学、中国政法大学、中国社会科学院

大学、中国科学院、中国人民公安大学等高校及科研院所的多位专家学者参与研讨。

活动综述 | 第八届中国网络法治高端论坛暨“人工智能健康有序发展的机遇、挑战及其法律治理”学术研讨会顺利举行

8 月 23 日，由武汉大学网络治理研究院、喀什大学法政学院联合举办的第八届中国网络法治高端论坛在新疆喀什召开。本次论坛以“人工智能健康有序发展的机遇、挑战及其法律治理”为主题，聚焦人工智能时代法治建设的核心议题。来自北京大学、清华大学、中国人民大学、武汉大学、中国社会科学院、复旦大学、北京航空航天大学、东南大学、西南政法大学、西南大学、郑州大学、中南财经政法大学、安徽大学、新疆大学等高校与科研机构的专家学者，以及新疆维吾尔自治区党委网信办等实务部门代表共四十余人齐聚喀什，围绕人工智能立法模式、侵权责任、权利保障、跨境治理等热点问题展开深入研讨。本次论坛积极响应党的二十届三中全会关于完善人工智能政策体系的号召，为推动人工智能与法治深度融合、构建中国自主的人工智能治理体系提供了重要交流平台。

本次会议开幕式由喀什大学法政学院党委书记迪力**夏提 • 阿木提**主持，喀什大学党委常委、副校长**罗浩波**，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**周辉**，武汉大学网络治理研究院院长**黄志雄**分别致辞。

喀什大学法政学院党委书记 迪力夏提 • 阿木提

罗浩波结合喀什作为“一带一路”核心区的战略地位，阐释了人工智能技术对提升对外开放水平和社会治理的特殊意义，并介绍了喀什大学在法学、计算机、经贸等学科交叉融合方面的成果。

喀什大学党委常委、副校长 罗浩波

周辉副秘书长从国家战略层面强调人工智能立法的紧迫性，指出中国需在安全与发展间取得平衡，并强调喀什作为数字丝绸之路节点的区位优势。提出应在安全与发展之间寻求平衡，并发挥喀什在数字丝绸之路建设中的桥梁作用，推动中国方案走向国际。

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 周辉

黄志雄院长介绍了武汉大学网络治理研究院在网络空间治理、数据产权、平台反垄断等领域的研究成果，提出人工智能治理的三大核心维度：权利保障再定义、责任边界重构和国际规则构建。喀什正崛起为数字丝绸之路核心节点，黄志雄院长呼吁以喀什为支点，推动中国从“网络大国”迈向“网络强国”。

武汉大学网络治理研究院院长 黄志雄

主旨发言环节由武汉大学网络治理研究院院长助理**周围**副教授主持，北京大学法学院**张平**教授、清华大学法学院**程啸**教授、中国社会科学院法学研究所网络与信息法室副主任**周辉**、武汉大学网络治理研究院副院长**袁康**教授分别就人工智能立法与治理的核心问题发表演讲。

本次论坛设三个平行分论坛，分别围绕“人工智能发展中的新型权利保障”“人工智能发展中的法律风险及其治理”“人工智能发展中的跨境治理与国际合作”三个主题展开深入研讨。

分论坛一围绕人工智能背景下新型权利的设置与保障问题展开，五位发言人分别以人工智能背景下个人信息分类规则的处理适用、人脸识别视角下个人信息保护影响评估的适用路径、AI 预训练中的个人信息保护、人工智能时代肖像可识别性的判断标准、基于功能主义的网络虚拟财产排他性判断标准设计为主题进行了深入探讨，结合理论研究与实践案例，提出了具有前瞻性和现实意义的观点。

第二分论坛就大语言模型训练数据治理、智能养老服务法律风险、人机共同驾驶中的主体性危机、数字“复生”场景化规制等前沿问题展开交流。

第三分论坛探讨了跨境人工智能服务安全监管、中美人工智能战略竞争与国际治理话语权博弈、人工智能赋能网络安全的国家责任法问题、《人工智能框架公约》中预防原则的适用等跨境治理议题。各分论坛的积极讨论充分体现了人工智能法治化建设的复杂性与紧迫性，凸显了立法、监管与国际协同并重的治理路径需求。

论坛闭幕式由喀什大学法政学院院长**杨陶**教授主持，新疆维吾尔自治区党委网信办副主任、一级巡视员**冯明亮**作嘉宾发言，武汉大学网络治理研究院副院长**袁康**教授致闭幕辞。

中国网络法治高端论坛目前已成功举办八届，在凝聚学界共识、推动网络法治建设、加强学术研究与实践探索等方面发挥了积极作用。本届论坛首次在新疆喀什举办，不仅体现了我国人工智能治理研究的多地域、多视角融合，也为“数字丝绸之路”建设与人工智能法治发展提供了重要的理论支撑和智力支持。

技术编辑：林诗敏

数字法评

论“通知”规则在生成式人工智能作品侵权中的类推适用

此处删除了原文脚注，全文请参见《比较法研究》2025 年第 4 期，转载或引用请注明出处。

作者：王利明，包丁裕睿

摘要：生成式人工智能作品侵权的责任承担，既关系到受害人权益保护，也关涉技术利用与创新、产业发展以及信息自由等重要价值。在坚持过错责任原则的前提下，唯有合理设定生成式人工智能服务提供者的注意义务、审慎判断其是否构成过错，方能实现多元利益之间的有效平衡、促进社会整体福祉。我国民法典第 1195 条规定的“通知”规则，为判断网络服务提供者是否具有过错提供了一种具体化、可操作的路径。尽管生成式人工智能作品侵权与传统网络侵权在结构上有所不同，但在主体、价值、情境等本质特征上具有高度相似性，从而具备了类推适用“通知”规则的正当性基础。在具体适用上，“通知”规则所要求的“合格通知”与“必要措施”，应结合生成式人工智能服务的运行机制和技术特点加以解释。与之配合，我国民法典第 1197 条规定的“知道或应知”规则的类推适用构建了生成式人工智能服务提供者在未接到通知情况下的注意义务。两者共同构成了一个动态的注意义务体系，注意义务的标准随“现有技术水平”的发展而不断更新。

一、引言

随着 Deepseek 等人工智能大模型的横空出世，我们已经进入人工智能时代。人工智能带来了前所未有的发展机遇，也带来了前所未遇的风险。从法律层面看，生成式人工智能所带来的风险主要是其输出作品侵害他人的人格权、知识产权等权益。[1]在人工智能生成的内容侵害他人民事权益时，如何准确认定相关主体的侵权责任，成为亟需解决的重大问题。[2]

在我国已有的司法实践中，针对生成式人工智能侵权，法院主要依据过错责任而非严格责任的归责原则认定侵权责任。例如，广州互联网法院在“上海新创华文化发展有限公司与广州年光公司网络侵权责任纠纷案”中指出，“赔偿损失责任的承担需要考虑被告的过错问题”。[3]杭州互联网法院则在“上海新创华文化发展有限公司与杭州某智能科技有限公司著作权侵权及不正当竞争纠纷案”中指出，“生成式人工智能服务提供者系提供生成式人工智能技术服务，对用户输入的提示词、训练图片等数据内容，以及生成物的传播等行为并不当然负有事先审查的义务，只有当其对具体侵权行为具有过错时，才可能构成帮助侵权”。[4]这种归责原则的选择符合对人工智能技术所应采取的审慎包容、鼓励发展的政策。同时，采用过错责任也有利于平衡权益保护与行为自由。国内外学界具有共识性的观点也认为，应当对人工智能侵权采过错责任原则，避免抑制人工智能技术的利用和发展。[5]然而，在过错责任原则之下，生成式人工智能服务提供者过错的认定是一大难题。

为了规范并鼓励互联网技术的运用和发展，《中华人民共和国民法典》（以下简称“《民法典》”）第 1195 条规定了“通知”规则。[6]根据该规定，只有在权利人通知网络服务提供者后，网络服务提供者才有义务采取必要措施制止侵权。“通知”规则为信息高度流通与扩散的数字生态中网络服务提供者过错的认定提供了明确的标准，也为其提供了侵权责任的“避风港”。然而，“通知”规则可否适用于生成式人工智能侵权并不明确。应当看到，生成式人工智能服务与传统网络平台存在本质区别：用户的信息交互对象是人工智能服务提供者本身，而非其他用户。这也决定了，生成式人工智能作品侵权不能完全适用针对网络服务提供者的“通知”规则。但从立法目的、价值考量等因素出发，在认定生成式人工智能服务提供者的侵权责任时，应当类推适用“通知”规则，避免生成式人工智能服务提供者被迫投入大量资源用于防控潜在风险，甚至因此限制或放弃对相关技术的开发与应用。本文拟对生成式人工智能侵权中“通知”规则的适用问题展开研究，以求教于大家。

二、“通知”规则在生成式人工智能作品侵权中的不可直接适用性

在生成式人工智能作品侵权场景下，“通知”规则是类推适用，还是直接适用，存在不同观点。[7]杭州互联网法院在判决中援引《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》（法释[2012]20 号）第 7 条第 3 款有关侵犯信息网络传播权的“通知”规则作为裁判依据，是在生成式人工智能作品侵权案件中直接适用了“通知”规则。[8]本案的判决思路和判决结果未必有误，但在未讨论“通知”规则的可适用性的情况下径行将其适用于生成式人工智能作品侵权，值得商榷。相比传统网络平台，生成式人工智能具有独特的内容生成、传播机制，生成式人工智能作品侵权的法律结构也不完全符合《民法典》第 1195 条预设的法律构造。[9]因此，生成式人工智能作品侵权不能直接适用“通知”规则。

第一，生成式人工智能侵权作品的产生原因具有复杂性。与传统网络侵权行为源于用户发布侵权信息不同，生成式人工智能输出的侵权内容既受用户输入内容的影响，也受到模型训练数据与算法机制的影响。侵权信息的产生可能源于用户输入的特定提示词诱导模型生成涉嫌侵权的内容，或者用户输入的语料本身具有侵权性质（如他人私密信息），也可能源于人工智能训练语料的瑕疵、算法机制设计不当、模型未进行适当微调等原因，还可能源于纯粹的小概率随机事件。

第二，生成式人工智能作品侵权的法律结构具有多样性。《民法典》第 1195 条所针对的侵权场景是，网络用户通过网络平台发布侵权内容，受害人通过网络平台发现侵权行为，并向网络服务提供者发出通知，要求其采取必要措施。这与生成式人工智能作品侵权的法律结构有所不同。在生成式人工智能作品侵权的场景中，可能存在两种侵权结构：一是用户与被侵权人是同一主体，用户在使用生成式人工智能服务过程中发现其输出内容侵犯了自己的权益；二是用户与被侵权人不同，用户在输入合法提示词、侵权提示词或诱导侵权的提示词后，生成式人工智能所输出的内容侵犯了他人权益。

第三，生成式人工智能作品侵权可能不存在实施侵权行为的用户。当用户与被侵权人是同一主体时，侵权作品并非源自实施侵权行为的第三人，而是直接产生于生成式人工智能。例如，用户在查询个人简介时，发现生成式人工智能输出了包含其敏感个人信息的内容。即便在用户与被侵权人并非同一主体的情形中，也可能不存在实施侵权行为的用户。例如，用户输入的提示词本身不违法也不具有诱导侵权的性质，但生成式人工智能所输出的内容侵犯了他人合法权益。直接侵权用户的缺失使生成式人工智能作品侵权与《民法典》第 1195 条所设计的三方主体架构有所差异。

第四，生成式人工智能的内容输出具有封闭性，侵权作品的生成和传播阶段分离。由于生成式人工智能仅向输入提示词的用户输出内容，潜在的侵权信息并不会直接向不特定第三人公开。因此，在用户与被侵权人不同时，受害人无法直接通过服务提供者发现侵权事实；仅在用户通过其他方式自行公开输出内容时，受害人才可能知悉侵权事实。[10]生成式人工智能服务提供者在接到通知后，有能力采取的措施仅限于删除、屏蔽已有和未来输出，而无法完全删除、屏蔽通过其他途径公开的侵权信息。生成式人工智能服务提供者封闭性的输出机制决定了其仅是侵权信息的生成者，而非侵权信息的传播者。

生成式人工智能独特的信息生产与传播特征，决定了生成式人工智能作品侵权不能直接适用针对传统网络侵权的“通知”规则：一是在法律结构上，生成式人工智能作品侵权可能仅存在两方主体而非三方主体，《民法典》规定的“转通知”和“反通知”规则可能无法适用；二是在侵权行为的判断上，服务提供者在收到“通知”后，需要先查明被控侵权内容是源于生成式人工智能服务还是用户，相比“通知”规则中的网络服务提供者，对构成侵权的证据需要进行更深入的审查；三是在接到“通知”后采取的措施上，相比传统“通知”规则以“通

知—删除”为核心，生成式人工智能服务提供者可能难以直接删除侵权信息，而主要应当采取“通知—屏蔽”的手段预防侵权，其应对侵权的“必要措施”显然更为复杂。

三、“通知”规则在生成式人工智能作品侵权中的类推适用

生成式人工智能作品侵权不能直接适用“通知”规则，但应当类推适用“通知”规则。所谓“类推适用”，是指在特定案件缺乏明确法律规定时，裁判者援引与该案件具有相似法律评价基础的规定，将其适用于尚无明确规定的情形。[11]类推适用的本质是“同类事物相同对待”，在对法律评价有决定性意义的方面，两类事实构成彼此类似，因此应被同等评价，且“不同之处在这里不能排除这种法定评价”。[12]因此，能否类推适用，关键在于相似性的判定。[13]生成式人工智能作品侵权与传统网络侵权在主体、价值、情境三个方面存在相似性，符合类推适用“通知”规则的条件。

（一）主体相似性：“技术中立”的服务提供者

《民法典》第 1195 条的“通知”规则的适用对象是“网络服务提供者”。生成式人工智能服务提供者是否属于“网络服务提供者”，现行法律规范并不明确。我国 2023 年发布的《生成式人工智能服务管理暂行办法》第 22 条将“生成式人工智能服务提供者”定义为“利用生成式人工智能技术提供生成式人工智能服务（包括通过提供可编程接口等方式提供生成式人工智能服务）的组织、个人”，似乎将其定义为一种特殊的“网络服务提供者”。然而，该文件第 9 条又规定“提供者应当依法承担网络信息内容生产者责任，履行网络信息安全义务”，似乎又将其定义为“网络内容生产者”。[14]我国有学者指出，《生成式人工智能服务管理暂行办法》等规范具有公法性质，不能直接作为生成式人工智能服务提供者私法地位的判断依据。[15]

从“网络服务提供者”概念的本质特征出发，生成式人工智能服务提供者与《民法典》第 1195 条规定的“网络服务提供者”具有高度相似性。[16]网络服务提供者之所以适用“通知”规则，是因为其提供的服务具有“技术中立性”。当服务具有技术中立性，“不主动支持侵权活动，不实质上促进侵权发生或扩大”时，网络服务提供者不应承担过重的审查义务，受到“通知”规则的保护。[17]生成式人工智能服务作为一种新型的信息处理与传递中介，其与传统的网络平台在结构上虽有差异，但其本质仍然是一种中立的信息传播方式。DeepSeek、ChatGPT 等生成式人工智能既不主动输出任何内容，也不预存任何即将输出的内容，其并非严格意义上的“智能体”，而是基于大语言模型的概率预测工具。[18]其在用户输入“提示词”后，通过计算提示词与训练语料中语言模式的关联，生成与之最可能匹配的响应。因此，其本质是基于既有语料进行预测的自动化信息处理工具，是信息传播链条中的中立节点。[19]这与传统网络平台的特征相同，二者都只是在系统中预先设置算法，并不采取积极行为干涉信息发布。[20]

比较法上也广泛认可生成式人工智能服务提供者具有“网络服务提供者”的技术中立性特征。在欧盟，学说争议主要在于生成式人工智能服务提供者是否是《数字服务法》（DSA）规定的适用避风港规则的网络“托管服务”提供者。有学者指出，虽然在文义解释上，生成式人工智能服务并非纯粹的托管服务，但从目的解释出发，“托管服务”应被解释为包括一切中立、自动、被动的网络服务。[21]例如，搜索引擎作为信息中介，也不完全符合托管服务的定义，但法院一直以来将其视为一种“托管服务”提供者。在 2010 年的 Google Search 案中，法院认为，为了符合托管服务的定义，服务提供商必须扮演中立角色，即“仅仅是技术性的、自动的和被动的”（merely technical, automatic and passive），并且“对其存储的数据缺乏了解或控制”。只要服务提供者对其服务中的数据不具有控制力，就可以被视为托管服务。[22]欧盟《数字服务法》本身也提到，搜索引擎也应当获得责任豁免。[23]按照这一逻辑，生成式人工智能服务提供者也符合“对其存储或生成的内容缺乏认知和控制”的标准，因

为这些内容是通过技术性、自动化且被动的方式生成的。因此，生成式人工智能服务提供者也应当适用欧盟《数字服务法》规定的避风港规则。[24]

在美国，生成式人工智能服务提供者是否可以适用《美国法典》第 47 章第 230 条的豁免规则存在理论分歧。[25]根据该规定，只有“信息内容提供者”可能承担内容侵权的责任，计算机“服务提供者”不对内容侵权负责。如果进行严格的文义解释，生成式人工智能服务提供者确实“提供”了内容。[26]不过，根据美国法院的判例，作为“信息内容提供者”，相关主体必须“直接参与开发”或“实质性地促成”（materially contribute）被诉非法内容，[27]而“不仅仅是该内容的被动传递者”。[28]也有学者认为，仅在网站“采取明确行动确保内容生成”时才无法免责。[29]由于生成式人工智能服务提供者只是根据用户提供的命令或素材再现或重新包装语料库的内容，[30]因此可能仍作为“服务提供者”享有侵权责任豁免。更多的学者认为，生成式人工智能服务提供者不应享有完全的侵权责任豁免，而是应当类推适用《数字千年版权法》（DMCA）的避风港规则，在符合“通知—删除”条件的情况下才能免除责任。[31]

总之，从主体角度观察，生成式人工智能服务提供者与网络服务提供者在本质上具有相似性，即不控制、也不应控制服务中的内容，具有技术中立性。

（二）价值相似性：技术发展与权益保护的平衡

“通知”规则有助于在网络服务提供者、权利人等主体之间实现复杂的利益平衡，特别是技术利用与权益保护之间的平衡。在生成式人工智能作品侵权场景下，也存在相似的价值目标和利益平衡需求。

第一，“通知”规则旨在维护网络服务提供者的行为自由。“通知”规则的基本假设是，“本身不组织、筛选所传播信息的网络服务提供者通常必须借助于技术手段才能对通过其系统或网络的信息加以监控，但技术手段本身有局限性；网上信息数量太大，内容又在不断变化、更新，要求监控能力有限的网络服务提供者逐条甄别信息的合法性根本不可能”。[32]因此，法律不应当给网络服务提供者施加进行审查并予以预防和制止的一般性义务，否则就会迫使网络服务提供者花费大量的人力、物力和财力审查网络信息内容，从而显著提高运营成本，不仅可能推高服务价格，还会妨碍信息自由流通，违背网络技术发展的初衷与价值取向。[33]

第二，“通知”规则旨在保护被侵权人的合法权益。网络服务提供者通常具有更充分的技术手段和信息能力来预防和制止侵权行为。如果不采取“通知”规则，权利人只能向法院或有关部门寻求救济，此种方式不仅无法快速地预防和制止侵权行为、防止损害的发生或扩大，也增加了当事人的讼累和司法机关、行政机关的负担。依据“通知”规则，权利人只要能够提供构成侵权的初步证据，就可以要求网络服务提供者采取必要措施。这有利于服务提供者及时发现侵权信息，迅速采取措施预防和制止侵权行为。[34]

第三，“通知”规则具有维护信息自由、促进技术创新等作用，有助于实现公共利益。欧盟 2022 年通过、2024 年正式实施的《数字服务法》第 6 条也规定了以“通知”规则为核心的避风港规则。[35]该法在序言部分（recitals）指出，有关中介服务提供者的责任规则旨在平衡不同类型的利益，包括言论和信息自由、经营自由、维持高水平的消费者保护，以及促进创新和经济增长。[36]美国法院的判例也表明，如果网络服务具有“实质性非侵权用途”（substantial non-infringing use），服务提供者不介入技术的具体使用，就应当维护其“网络中立”性，即避免通过对其施加过高的注意义务促使其审查被传播的网络内容，破坏网络的自由环境，从而实现“市场自由竞争、信息自由流动、言论自由表达”等价值。[37]可见，“通知”规则不仅能有效平衡网络服务提供者与权利人之间的利益，还有助于公共利益的实现。

“通知”规则所体现的价值理念适用于生成式

人工智能作品侵权。生成式人工智能依赖于大规模训练数据和复杂算法，其抓取的数据是海量的，生成的内容具有高度的不确定性和即时性，服务提供者往往难以预先判断某一具体输出是否构成侵权。[38]法谚指出，“法律不强人所难”（Lex non cogit ad impossibilia）。如果要求生成式人工智能服务提供者在作品生成前进行全面事前审查，不仅技术上难以实现，也不利于人工智能服务的利用和技术发展。广州互联网法院在裁判中就指出：“考虑到生成式人工智能产业正处于发展的初期，需要同时兼顾权利保障和产业发展，不宜过度加重服务提供者的义务”，服务提供者应当履行的是“合理的、可负担的”注意义务。[39]只有要求服务提供者在接到权利人通知后再启动必要的处理机制，才具有技术上的可行性与责任上的合理性。“通知”规则一方面降低了服务提供者的负担（特别是原则上免除事前审查义务），为生成式人工智能服务提供者提供了明确的行为规则与责任边界；另一方面有助于为权利人提供及时有效的救济途径，高效地保护了可能受到权益侵害的民事主体，在权益保护与鼓励技术运用和发展的双重目标之间实现了合理平衡。

（三）情境相似性：“通知”在过错判断中的功能趋同

“通知”规则在生成式人工智能作品侵权与网络侵权场景中，都用以解决“过错”的判断问题，并且通过对“过错”内涵的细化、合理设置注意义务实现技术创新与权益保护的平衡。“通知”规则针对的情境是，在用户利用网络服务实施侵权行为侵害他人权利时，网络服务提供者的“过错”难以判断，因此需要借助“通知”规则来认定其过错。与传统网络侵权类似，生成式人工智能作品侵权中的“过错”判断也是一项难题。“通知”规则提供了一种判断生成式人工智能服务提供者是否存在过错的可行路径。

《民法典》第 1195 条的“通知”规则并非单纯的免责事由，而是判断网络服务提供者过错的法定义务规则。[40]如果网络服务提供者在接到通知后未采取相应措施，就存在过错。该规则在性质上属于过错责任的一种特殊表现形式，与《民法典》第 1165 条规定的过错责任的一般条款属于一般规范与特别规范的关系。[41]“通知”规则将过错认定的“标准”（standard）细化为“规则”（rule）形式，当行为主体选择在规范范围内开展相关活动时，便可获得较为确定的免于被追究责任的预期，相反则需要承担责任。[42]生成式人工智能具有“黑箱”问题，这也导致对生成式人工智能服务提供者过错的判断较为困

难。生成式人工智能通过对用户提示词的语义分析，基于大规模语料训练出的概率模型，预测最可能的词语组合，从而逐步生成完整的文本内容。无论开发者还是使用者，目前都难以充分解释或预测其基于算法作出决策的具体过程。[43]“通知”规则的类推适用有利于使生成式人工智能服务提供者的注意义务具体化，即通过设定外在的行为义务解决“黑箱”问题：在收到“通知”之前，服务提供者仅负担较低程度的注意义务；在收到“通知”后，服务提供者就应当依法采取一系列“必要措施”，否则就可能存在过错。

总之，生成式人工智能作品侵权与网络侵权在主体、价值、情境三个方面均存在相似性，因此应当类推适用“通知”规则。事实上，主体、价值、情境三个方面的相似性也存在相互关联：作为主体的服务提供者的技术中立性意味着，不应对其施加过重的注意义务，而应当合理平衡技术利用和权利人的权益保护，而这种平衡正是通过对“过错”内涵的细化、合理设置注意义务实现的。生成式人工智能作品侵权与网络侵权本质上的相似性，使其契合“通知”规则的基本思想和法律理由（ratio legis）。这构成了生成式人工智能作品侵权应当类推适用“通知”规则的根本理由。[44]

四、“通知”规则在生成式人工智能作品侵权中的具体适用

（一）类推适用“通知”规则下注意义务的具体内容

在将“通知”规则类推至生成式人工智能作品侵权之后，服务提供者是否存在过错，便可围绕“通

知—必要措施”这一程序进行判断：权利人发出的“合格通知”启动了服务提供者的注意义务，而服务提供者对该通知所涉内容采取的“必要措施”的及时性与充分性，则成为衡量其是否尽到合理注意义务的核心指标。以下分别从“合格通知”的认定标准以及通知后“必要措施”的类型与适当性判断两方面，探讨生成式人工智能作品侵权类推适用“通知”规则的具体内容。

1. “合格通知”的判断标准

《民法典》第 1195 条规定，权利人发出的“通知应当包括构成侵权的初步证据及权利人的真实身份信息”。有学者认为，有效通知应当包括以下内容项：侵权行为实施主体信息、侵权事实、权利人身份信息等。[45]在用户与受害人不同的情况下，由于受害人难以知晓侵权作品的产生是输入“提示词”的用户造成的，还是生成式人工智能造成的，因此难以确定“侵权行为实施主体信息”；受害人也难以通过公开渠道获取足以定位侵权内容的信息，如特定账户或链接等。[46]因此，在判断通知是否合格时，不应要求权利人详尽描述侵权信息。即使通知未具体指明涉嫌侵权的主体或侵权内容的定位信息，只要提供了足够的信息使生成式人工智能服务提供者能够定位侵权作品、采取必要措施，就属于有效通知。[47]权利人在发出通知时，为了更好地让生成式人工智能服务提供者履行必要措施预防侵权，还可以在通知中提供关键词或侵权比对信息（如权利人可以提供其享有著作权的作品作为比对素材），便于服务提供者实施过滤、屏蔽等必要措施。

“合格通知”应当包括构成侵权的初步证据。对于不易识别的侵权行为，服务提供者应以“正常理性人”标准，结合一般专业知识判断是否支持权利请求。[48]例如，针对可能侵犯名誉权的输出内容，如果输出内容在人工智能的训练数据、互联网资源以及用户的提示词中都无法找到时，生成式人工智能服务提供者就可以确认相关内容不存在任何支撑，此时应当及时采取必要措施。[49]若按照一个正常理性人标准，生成式人工智能服务提供者无法识别出被举报内容的不法性，则其不应直接采取过滤、屏蔽等措施。这是因为其违法判定能力有限，既没有确认某一行为是否属于侵权行为的权力，也缺乏相应的专业知识和能力，不应由其代替法院对侵权纠纷进行裁决。[50]在这种情形下，服务提供者可能会承担有限的标识义务，例如在生成相关内容时提示用户潜在的侵权风险或相关内容已被他人投诉。

2. 接到通知后应当采取的必要措施

根据“通知”规则，网络服务提供者应当在接到合格通知后采取删除、屏蔽、断开链接等必要措施。“必要措施”的具体内容要根据服务的类型、受侵害权利的类型、侵权行为的性质、技术发展水平等因素进行衡量确定。[51]在生成式人工智能作品侵权场景中，服务提供者应采取补救性与预防性“必要措施”，其中预防性措施更为关键。

第一，生成式人工智能服务提供者可以采取的主要措施是通过内容过滤机制屏蔽侵权内容。在生成式人工智能领域，“通知—删除规则”（notice-and-takedown）很大程度上被“通知—屏蔽规则”（notice-and-staydown）取代。[52]此处的屏蔽措施不同于“接到通知后屏蔽通知所载的特定侵权链接”，而强调在接到通知后，服务提供者阻止侵权信息再次生成。服务提供者不仅要处理通知所载的具体侵　权内容，还要过滤、屏蔽相似的侵权内容。例如，在通过关键词过滤侵权“奥特曼”作品时，如果仅屏蔽“奥特曼”而不屏蔽“迪迦”（“奥特曼”系列中的一个著名角色），就属于未尽到注意义务。[53]服务提供者主要可通过两种方式实现过滤、屏蔽：一是“输入提示词过滤”，即在提示词违法或可能引发侵权时拒绝输出内容；二是“输出内容过滤”，即在提示词合法但生成内容具侵权风险时，拒绝输出内容或通过技术手段调整输出内容。需要注意的是，以上两种方案均依赖技术自动识别，现有技术可能无法做到完全杜绝侵权内容的生成。只要服务提供者在现行技术方案下尽到了合理努力、采取合理的算法进行过滤，就应当认为其尽到了注意义务，不应就无法控制的风险承担

责任。[54]在面临海量信息的情况下，过滤、屏蔽措施的合理性判断不是结果主义的，不能因为服务提供者采取了合理措施后仍然小概率偶发性地出现侵权内容，就要求其承担侵权责任。[55]只要其采取的技术方案具备合理性，服务提供者就不应承担责任。[56]

第二，生成式人工智能服务提供者还可以采取一系列其他的“必要措施”预防侵权。虽然“删除、屏蔽、断开链接等必要措施”是一种列举加概括的规定，但“必要措施”未必是与“删除、屏蔽、断开链接”程度相当的措施，而可以被解释为这些列举性措施以外的其他必要措施。[57]生成式人工智能服务提供者可以采取的其他必要措施是多样化的。例如，服务提供者可以对存在侵权风险的内容进行标识、风险提示。在特定内容有侵权风险，但过滤、屏蔽相关内容不可行或相较侵权风险过于严厉时，服务提供者可以将内容可能侵权的事实告知使用人工智能生成该内容的用户，提醒用户谨慎使用或不得向他人传播侵权内容等，以避免损害后果扩大。目前已有搜索引擎平台采用类似策略，在呈现疑似侵权搜索结果时附加相关投诉信息或法院裁判链接。[58]又如，服务提供者可以对侵权用户采取管理措施。在特定用户频繁输入侵权提示词或诱导输出侵权内容时，服务提供者可以根据侵权用户的侵权程度、次数和主观恶性等因素，采取警告、限制适用、暂停服务和关闭账户等手段。

第三，生成式人工智能服务提供者采取的“必要措施”应当与通知所载的侵权行为性质相符合。当权利人所通知的侵害较为严重、侵害行为较为容易辨别、采取必要措施并不会妨碍其他合法活动时，服务提供者应当采取过滤、屏蔽等较为严厉的措施。当通知所载的侵权行为真实性存疑、侵权的实际概率较低，采取措施可能激励不实举报、威胁与妨碍合法活动时，服务提供者就应当采取风险提示等较为柔和的措施，甚至不采取措施。在综合考虑相关因素后，服务提供者所采取的措施具有合理性的，应认定其已尽合理注意义务。这与《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》（法释[2020]17号）第 4 条和《最高人民法院关于审理涉电子商务平台知识产权民事案件的指导意见》（法发[2020]32号）第 10 条所体现的思路一致，即法律应当从整体上判断服务提供者采取的措施或处理方案的合理性。服务提供者只需善意地采取整体合理的应对措施，无需对每一侵权通知都作出“完美响应”。[59]杭州互联网法院在裁判中也指出，应综合考量“生成式人工智能服务的性质、当前人工智能技术的发展水平、避免损害的替代设计的可行性与成本、可以采取的必要措施及其效果、侵权责任的承担对行业的影响等因素，通过动态地调整过错的认定标准，将平台注意义务控制在合理的程度”。[60]这有助于避免服务提供者因“寒蝉效应”采取过度的措施，影响生成式人工智能技术的运用和发展。[61]

需要特别注意的是，生成式人工智能服务提供者与传统网络服务提供者在接到“通知”后能采取的措施存在不同。一方面，生成式人工智能服务提供者难以通过“删除语料库中被训练素材”或“调整模型参数”避免侵权行为。这是因为，在完成模型参数训练后，内容生成过程、输出结果往往难以解释和验证，服务提供者无法识别特定训练数据与侵权内容的稳定关联，事后删除语料内容也无法对已训练完成的模型的输出内容产生影响。只有用剔除侵权作品后的新语料数据集对该模型加以再次整体训练，才可能真正有效改变模型参数，但从产业实际和技术成本角度出发，这是无法实现的。[62]另一方面，生成式人工智能服务提供者删除特定用户账号中的侵权内容或断开侵权内容的链接存在可行性，但在部分情况下也难以实施。如果特定侵权作品存储在服务器中，服务提供者当然可以采取断开链接、删除等措施。如果特定侵权作品存储在用户本地设备而非服务器中，或者用户已通过其他途径保存、传播了侵权作品，人工智能服务提供者就难以直接删除侵权内容。此时，服务提供者可采取提示用户侵权风险、建议用户删除或停止传播相关内容等“必要措施”，履行注意义务。[63]

（二）“通知”规则与“知道或应知”规则的衔接适用

《民法典》第 1197 条在“通知”规则之外规定了“知道或应知”规则，即“网络服务提供者知道或者应当知道网络用户利用其网络服务侵害他人民事权益，未采取必要措施的，与该网络用户承担连带责任”。该条规定了“知道或应知”侵权行为而不采取必要措施构成过错。由于引入了违反注意义务的应知，我国的“知道或应知”规则与美国法上的“红旗规则”不同，呈现出过错责任一般条款的结构。[64]根据《民法典》第 1197 条，在没有接到通知的情况下，网络服务提供者如果知道或者应当知道生成的内容侵犯了他人权利，而未采取适当措施，也应当承担责任。可见，侵权通知不是服务提供者承担责任的唯一条件。[65]“知道或应知”规则是过错判断的一般规则，而“通知”规则规定了有效通知构成“知道”，具有特殊性。[66]

在类推适用“知道或应知”规则判断生成式人工智能服务提供者的过错时，应当考虑生成式人工智能的特殊性。在网络侵权中，网络服务提供者知道或应当知道的对象通常是已经发布的侵权信息，而生成式人工智能作品侵权的原因具有多样性，因此判断服务提供者“知道或应知”也较为复杂：一方面，生成式人工智能具有用户交互性，在用户上传语料或者输入提示词本身侵权或具有诱导侵权的高度可能性时，服务提供者就有可能知道或者应当知道侵权行为很可能发生；另一方面，生成式人工智能依赖海量的训练数据，对于语料库中涉嫌侵权的信息，服务提供者可能在技术上难以通过合理的成本进行筛查，因此应当降低其识别语料库中侵权信息的注意义务，不应因为语料库中存在侵权信息，就当然认定服务提供者知道或者应当知道侵权行为。

生成式人工智能服务提供者不承担普遍的审查义务，但在未接到针对特定侵权行为的通知时仍负有一定的注意义务。第一，对于明显构成侵权的信息，如敏感个人信息、含有明显违禁词的信息等，如果以一般理性人标准来看足以判定构成侵权，应认为服务提供者对此类信息“应知”，服务提供者应当采取适当措施。

第二，“防止侵权行为再次发生”包含了防止未来侵权的注意义务，在接到权利人的通知后，服务提供者需要通过合理的过滤、屏蔽手段，防止类似侵权行为的发生。在先通知构成了对未来类似侵权的注意义务来源。[67]2019 年欧盟通过的《单一数字市场版权指令》第 17 条就指出，在线内容分享服务提供者应“尽最大努力防止侵权行为的再次发生”。虽然该条明确否定了“一般性的监控义务”，但在实践中，服务提供者几乎无法回避一定程度的过滤或审查义务。[68]

第三，从增进社会整体福祉的法经济学视角出发，在特定情形下，服务提供者亦应承担一定的事前注意义务。如果在考量服务提供者对内容的控制力、生成内容的类型、侵权的明显程度以及侵权的频率等因素后，服务提供者相比生成内容的接收者（包括用户和第三方）能以更低成本识别侵权行为，那么要求服务提供者通过技术进行有限审查更能减少社会成本。事前注意义务的标准不宜过高，其合理边界可以被划定为“采取与网络服务提供者的技术能力相适应的预防措施”。这种注意义务会随着生成式人工智能技术的不断提升尤其是防范措施的日渐成熟而逐渐提高。[69]目前，《生成式人工智能服务管理暂行办法》等公法规范规定了人工智能服务提供者在特定情形下的事前注意义务。若上述规范被视为 “保护性法律”，则服务提供者应在其适用范围内承担相应注意义务。[70]不过，应当明确区分有限的事前注意义务与全面的事前审查义务：前者仅要求服务提供者在其技术能力允许的范围内，对高风险内容进行有针对性的预防措施，而非对所有生成内容进行普遍性的事前审查。

第四，生成式人工智能服务提供者主动采取的过滤筛查等手段，不应使其承担额外的侵权风险。在实践中，不少服务提供者会在没有法定审查义务的情况下主动对潜在侵权内容进行过滤。如 ChatGPT 的服务提供者 OpenAI 设立了内容审核机制，当接收到提示词时，审核端点会评估内容是否

涉及色情、仇恨、暴力或宣扬自残等，这减少了产品输出侵权内容的可能性。[71]如果善意的主动审核会使服务提供者陷入“知道或应知”侵权的状态，反而可能导致承担更多责任，那么就不利于鼓励其采取必要措施预防侵权。因此，美国与欧盟都规定了“好撒玛利亚人”条款（good Samaritans），服务提供者进行善意审核时不会被排除在避风港规则之外。[72]《民法典》没有规定这一特殊条款，但是在解释上，如果服务提供者已经采取了与注意义务相符甚至更有效的预防措施，就不存在过错，因此也不应承担责任。对《民法典》第 1197 条进行恰当解释，并不会出现服务提供者“做多错多”的悖论。[73]

总之，《民法典》第 1197 条与第 1195 条中的“必要措施”，均包括与技术能力相适应的必要过滤、屏蔽措施。在未接到通知时，生成式人工智能服务提供者也负有一定的注意义务，该规则实质上设定了有限的审查和预防侵权的作为义务。[74]

五、结论

生成式人工智能技术的发展推动了信息传播模式的变革，其潜在的侵权可能性也对既有侵权责任规则提出了新的挑战。虽然生成式人工智能作品侵权与传统网络侵权在结构上存在一定差异，但生成式人工智能服务提供者与传统网络服务提供者在本质上具有相似性，因此可以类推适用《民法典》规定的“通知”规则。在生成式人工智能作品侵权案件中类推适用网络侵权的“通知”规则，一方面有助于在过错责任原则的基础上，合理设定服务提供者的注意义务，防止因不当加重服务提供者的侵权责任而影响人工智能技术的运用和创新；另一方面有助于结合“知道或应知”规则，使人工智能服务提供者采取事前与事后必要措施，保护被侵权人的权益。随着人工智能过滤审核机制等技术的发展，事前与事后注意义务标准也应根据“现有技术水平”持续调整，以实现权益保护与技术发展之间的动态平衡，最终服务于社会总福利的最大化。

数智司法鉴定的关键要素——以特征比对型鉴定的核心环节为视角

此处删除了原文脚注，全文请参见《数字法治》2024 年第 6 期，转载或引用请注明出处。

作者：李学军，宋华秋

内容提要：司法鉴定的内涵、外延以及鉴定意见的生成机理，关乎鉴定规制及其证据审查，可谓鉴定知识体系的关键要素。步入数智时代，传统鉴定经数智化转型形成鉴定的新样态即数智鉴定，但数智鉴定的内涵与外延并不明确，因此亟待理论探析。明确上述关键要素的价值，不仅在于对数智鉴定形成理论性认识，还在于揭示数智鉴定的双刃剑效应。换言之，数智鉴定虽具备一定的效能优势，但也呈现出传统鉴定中不曾有过的可靠性风险以及侵权隐忧。

我们正处于以大数据为“食粮”、以算法为“大脑”的人工智能时代。

自我国于 2017 年通过《新一代人工智能发展规划》，将人工智能上升为国家战略起，司法领域便加快了数字智能化步伐。而服务于司法、为司法公正的实现提供重要证据的司法鉴定（亦可简称为“鉴定”），即在诉讼中鉴定人运用科学技术或者专门知识对诉讼涉及的专门性问题进行鉴别和判断并提供鉴定意见的活动，自然也不例外地被人工智能技术所青睐。随着算法的嵌入，早期的指纹自动识别系统（Automation Fingerprint Identification System，AFIS）[1]得以升级优化，基因型概率（分型）软件（Probabilistic Genotype Soft-ware，PGS）[2]、法医表型特征分子刻画技术、硅藻自动化识别及分类技术、人脸识别技术（Facial Recognition Technology，FRT）、虹膜识别技术等新技术或系统，更辅助鉴定人顺畅、快捷完成司法鉴定——无疑，因“数”有“法”进而“智慧”的“数智司法鉴定”已经更加客观、高效、高能。与此同时，大量算法与鉴定人共同参与生成的“数智鉴定意见”正步入法庭，成为诉讼中难以回避的话题——其生成机理及其可靠性隐患等审查判断细节，均关乎案件事实认定的准确性，影响当事人的人身权、财产权等权益。

从域外视角来看，以算法辅助专家证人生成证据的司法实践正在不断增加，而与司法鉴定密切关联的法庭科学界更出现了关于“自动法庭科技”（Automated forensic techniques）[3]“法庭算法”（Forensic algorithms）[4][5]等相关讨论；同时还有立法机构提出了《法庭算法正义法案（2021）》（JusticeinForensicAlgorithmsActof2021）等。目光回到国内则发现，既有学者提出了构建“大数据司法鉴定（平台）”[6]“智慧司法鉴定”[7]的设想，也有关于“大数据证据”[8]“算法证据”[9]“人工智能证据”[10]等新型证据的研究。诚然，这些研究直接或间接地涉及鉴定的数智化，[11]但鲜有聚焦鉴定过程本身，既未道明其与传统鉴定意见生成机理的不同及其价值，亦未全面展现数智司法鉴定带来的机遇及隐忧。事实上，唯有明晰鉴定意见的生成机理，抽象出鉴定的要素及结构，打破鉴定意见“客观真实”的迷信崇拜，方能有利于对其开展有效的审查判断。[12]因此，关注司法鉴定的核心环节，即从检材、样本的检验及其鉴定结果转化为鉴定意见的过程，极为重要。基于此，笔者拟以司法鉴定的核心环节为切入点，揭示司法鉴定数智化的规律，并廓清数智司法鉴定的含义和类型，进而分析数智司法鉴定带来的机遇与挑战。

一、司法鉴定核心环节的数智化转型

司法鉴定的核心环节即鉴定意见的生成过程。随着数智技术介入司法鉴定，鉴定意见的生成机理正在迭代。从鉴定人的认知决策地位来看，司法鉴定核心环节的数智化，意味着数智技术正部分发挥着鉴定人原有的权能，而鉴定人在鉴定中的专属地位则相对下降。明晰该机理转变，无疑有助于准确把握数智司法鉴定的概念由来及其优劣。

（一）以特征比对法鉴定为代表

鉴定涉及众多环节，如鉴定的委托、受理、鉴定的展开及鉴定意见的生成等，同时还涉及不同的鉴定方法。无疑，鉴定的展开及鉴定意见的生成是鉴定的核心环节，而所用的鉴定方法终归可概括性

地分为比对鉴定法和非比对鉴定法。因此，本文将聚焦于鉴定展开及鉴定意见生成这一核心环节的机理进行探析，并结合鉴定展开或具体施行时最常见、最广泛使用的鉴定方法即比对法，来研究鉴定的数智化转型。诚然，我国现有法律规定及相关法规、规章等已明确，当下的司法鉴定包括法医类鉴定、物证类鉴定、声像资料鉴定和环境损害鉴定这四大类鉴定，以及该四大类以外的司法会计鉴定、知识产权鉴定这些鉴定类型；但从如上概括性的鉴定方法来分类，也可将当下的司法鉴定分为比对型鉴定以及非比对型鉴定。

所谓比对型鉴定，即以被鉴定客体的相关特征为重心，通过比较检材（需断定真伪或出处的客体）特征与样本（供鉴定真伪或出处的客体）特征之异同，即比较法（Feature comparison methods）而具体施行的鉴定——诉讼中最常出现的鉴定需求即种属认定与同一认定型鉴定便是此类比对型鉴定。而该比对型鉴定，表述为“特征比对型鉴定”更为明晰，因为，“特征比对”系此类鉴定中必不可少的判断依据及鉴定手法：一方面，种属认定、同一认定型鉴定时，均涉及分别检验、比较检验和综合评断这三个环节，而“特征”的“比较”正是其中的关键方法；另一方面，在域外，特征比对法已被法庭科学界格外重视。例如，美国的总统科技顾问委员会（President's Council of Advisors on Science and Technology，PCAST）曾于 2016 年发布关于保障法庭科学证据有效性（The validity of forensic evidence）的报告，其即以“特征比对法”为基础的鉴定为核心，来作为刑事司法中法庭科学技术的代表。[13]更重要的是，特征比对型鉴定是鉴定实务中常见的一种鉴定，因而可作为鉴定的典型代表。指印鉴定、DNA 分型、笔迹鉴定、工具痕迹鉴定、足迹鉴定等鉴定，便是特征比对型鉴定的具体体现，并很大程度上受当下大数据、人工智能、算法等科技的影响。基于此，本文以特征比对型鉴定为鉴定的代表，以其核心环节即鉴定意见的生成机理为视角，阐释其数智化转型的过程。

（二）传统鉴定意见的生成机理

在数智算法用于鉴定之前，鉴定人对于鉴定意见的生成有着专属地位：专家运用物理、化学、生物等专门知识和技术手段开展各种鉴定。例如，在手印鉴定中，技术专家可能会利用专用粉末、化学试剂或特定光源来找寻、标识送检指纹的潜在特征。在 DNA 分型中，专家可能会运用 DNA 提取技术、聚合酶链反应（PCR）技术和测序技术等手段，获得鉴定对象（检材、样本）的 DNA 图谱。在人脸比对鉴定中，技术专家可能会使用摄影技术、图像处理技术来提取和强化人脸图像的特征。

这些示例中用于手印鉴定、DNA 鉴定和人脸比对等鉴定的技术手段，尽管在技术原理上千差万别，获得的鉴定结果在形式上也表现不一，但其发挥的作用相似——即展现出了鉴定对象的特征——在此基础上，鉴定人再从这些经强化的图像、音视频、数据或图谱等鉴定结果中筛选出具有鉴定价值的特征，进而作出鉴定意见。[14]换言之，此等鉴定意见的生成过程中，人与技术存在认知与决策的分工，且技术手段本身并没有参与特征选择以及特征比对分析等鉴定的核心检验环节——即鉴定人，居于技术手段之上实为鉴定检验决策的主角。因此，传统鉴定意见的生成机理实质上表现为“鉴定人全局主导”的结构。

（三）鉴定意见生成机理的数智化

上述既有的鉴定意见生成机理，较好地抽象出传统鉴定的要素和结构。但是，随着数智技术深度融入司法鉴定，该生成机理的适用性受到挑战。一是难以解释越来越多鉴定中出现的算法要素。即算法不仅用于呈现被检验的指印、笔迹、DNA 等所含客体特征，还用于自动识别、比对客体特征，显然，既有的传统鉴定生成机理无法反映这些现象。二是难以体现人与算法的交互情况，进而无法提示数智司法鉴定隐藏的可靠性风险、无法为所形成的鉴定意见提供审查判断的分析框架。因此，有必要顺应数智技术潮流并更新数智鉴定意见的生成机理。

数智鉴定与传统鉴定的最大区别在于算法介入了检验（阶段），这导致鉴定人的专属地位受到冲击。在鉴定时，识别特征并对特征进行比较检验，通

常被认为是鉴定人的能力专权。但是，当算法介入司法鉴定时，这种传统鉴定模式将被打破：数智算法技术不仅发挥辅助鉴定人的作用，而且实质性参与检验的决策——其具体体现在以下三方面。

1. 特征识别自动化

自动化是运用技术、程序、机器人技术或流程来“代替人的体力或脑力劳动”[15]；自动识别特征，便是运用算法等技术手段，在人力投入最小的情况下实现特征识别。一方面，算法可自动识别人类可感知特征，即对于图像、声音等可通过人的感官识别的特征，算法能自动识别。另一方面，算法亦可自动识别人类难以直接感知的特征。鉴定时，图像（如笔迹的字形、字体以及运笔、连笔特征等）、语音（说话人的音高、嗓音、节奏信息等）等信息能被人的眼睛、耳朵等感官直接捕获，并用于比对分析进而得出可靠的鉴定意见。但是，人的感官捕获的信息有限，如笔迹中潜藏的书写速度、压力和时序等动态特征，语音中蕴含的共振峰、音强、基频率信息等，难以被人眼或人耳所直接感知。随着数智技术的嵌入，上述原本无法或难以“肤浅”反映在客体上的特征，可被算法驱动的传感器（如同人的“机器感官”）所识别并记录，进而具备可用性。例如，搭载有动态签名识别算法的电子化签名系统，不仅能记录笔迹的静态图像信息，还能通过电子屏板准确捕捉笔迹形成的动态特征。而说话人自动识别系统则能识别上述人耳难以识别的声学特征参量。这无疑扩大了可用于比对、分析的特征疆域。

2. 比对分析自动化

被算法提取或识别的特征，将被用于自动比对或分析。换言之，算法已经介入鉴定的比对/分析这一重要环节。自动比对，是指匹配算法（Matchers）将检材特征与数据库中存档的样本特征进行自动化比对，筛选出数据库中最为相似的一系列待检样本，并将其按照相似性高低顺序进行排列（这个待筛选列表可以看成“机器意见”）。在数智算法的参与下，重复枯燥的比对负担从专家肩上卸下，鉴定效率大幅提升。

算法不仅可用于自动比对，还能用于自动分析其他专门问题。与自动比对类似，自动分析便是模拟人分析问题的流程，以实现在人的最少参与下得出分析“意见”。用算法进行自动分析的重要性日益提升，以混合 DNA 分型为例便可证实这一点。混合 DNA 分型，是指对来自两人或更多人的 DNA 混合物进行分析以确认其各自身份。其与传统 DNA 分型的主要差别不在于分离提取技术，而在于 DNA 图谱的解读难度。对于传统 DNA 分型，人工解读图谱并计算出检测对象的基因型被证明是可靠的。若使用数智方式分析，则能提升解读效率。然而，对于混合 DNA 图谱分析，人类专家面临一系列分析难题：混合 DNA 由多少人组成；各组分 DNA 的比例是多少；各自的基因型是什么；等等。[16]对于简单的混合 DNA（两组分混合 DNA 并满足特定条件）[17]，这些问题一般也可由专家解析 DNA 图谱后解答。但若混合 DNA 的组分变得复杂（例如，涉及三人的 DNA 混合斑），混合 DNA 图谱的解读难度便陡增[18]——此时，人工分析不仅耗时费力，而且专家之间的意见也可能具有显著差异。基于此，实务鉴定专家通常拒绝就此混合 DNA 进行分析检验并出具分析报告，或不得不借力于基因型概率（分析）软件（PGS），自动分析混合 DNA 图谱并给出“鉴定结果”即“机器意见”。

需要说明的是，不论是自动比对，抑或自动分析，并不意味着此环节没有鉴定人等专家的参与。算法的可靠应用，离不开鉴定人等专家事先设定算法相关参数或假设，确认输入的检材数据适用于特定算法。[19]因而从本质上说，算法自动比对分析后得出的“鉴定结果”，是一种“算法分析与人类知识交互的意见性结论”。[20]

3. 鉴定人核验

对于上述算法功能，即自动识别特征并自动比对分析，可统称为自动化决策。[21]需要注意的是，尽管自动化决策可给出诸如认定同一等“鉴定结果”，但该鉴定结果并不意味着认定同一的“鉴定意见”。[22]通常而言，算法会根据输入的检材数据，按照检材与样本相似程度高低或其他标准，返回一个（可疑人员）“候选名单”（Candidate list），鉴定人

再依据传统比较检验方法，认定检材与样本是否源于同一人。[23]而对于超出鉴定人认知能力范围的鉴定（如复杂的混合 DNA 分型，或“少笔画签名”的真伪鉴定），算法似乎“主宰”了鉴定意见的生成，鉴定人核验“机器意见”也似乎不具有可行性。其实，即便如此，鉴定人也有发挥核验作用的空间：在算法运行前，需要鉴定人设置相关参数或作出特定假设，并确保个案检材适用于算法的可靠性范围；在算法运行后，鉴定人也有必要验证算法是否正常运行，才能出具相关的鉴定意见。

简言之，由于算法技术的介入，数智司法鉴定意见的生成机理已不再是“鉴定人全局主导”结构，而与传统鉴定相比具有显著区别。数智鉴定意见的生成机理可概括为“自动化决策+鉴定人核验”。

二、数智司法鉴定的内涵与外延

数智鉴定是数智时代鉴定知识体系的新概念，前文已论及该概念的由来是鉴定实践的数智化转型。而明确一个概念的关键，从形式逻辑视角看，在于阐明其内涵与外延，这是对其进行理性认识的必经之路。

（一）数智司法鉴定的内涵

以大数据为“食粮”、以算法为“大脑”的人工智能介入司法鉴定后，不但变更了传统鉴定意见的生成机理，也进而影响到新型鉴定意见即“数智鉴定意见”[24]在诉讼应用中的审查判断，因此，有必要就前文反复使用的“数智司法鉴定”一词予以界定并就其特性展开探析。所谓数智司法鉴定，即鉴定人为了解决诉讼中的专门性问题，借助以数据为本、以算法为要的人工智能技术对相关鉴定对象展开检验、分析判断，并给出鉴定意见的专门性活动。无疑，“数”的强调、“智”的凸显，更有助于大家重视并在意人工智能对司法鉴定核心环节的深刻影响，以及对其所形成的数智鉴定意见展开审查判断时应注意的核心问题。

明确数智鉴定内涵的关键，在于阐释其特性。数智司法鉴定作为传统鉴定的迭代升级，自然承继着传统鉴定的基本属性，即大家通常认同的法定性、中立性、专门知识性和主观意志性等。[25]不仅如此，笔者在其他文章中已论证，数智鉴定的核心环节还存在人与技术之间的“耦合性”（简称人技耦合性）——该特性的探究，对鉴定意见可靠性风险的揭示与审查具有指导作用。简言之，人技耦合性的提出是为了反驳或警惕“人机协同”这种侧重于“技术助人”的单方面认识。因为，人与算法技术不仅有单向、正面影响的关系，还有技术对人的负面影响。例如，鉴定人可能轻信人工智能系统的判断导致错鉴，即后文将阐述的“自动化偏差”。换言之，在数智鉴定中，人与人工智能技术并不能以“人机协同”这种单向表述来概括，其实际存在一种双向互动关系，即耦合关系。因此，采用人技耦合性这种中立的表达表征数智鉴定的特性和内涵，更为全面并契合实际。

（二）数智司法鉴定的外延

前文已明确数智鉴定的内涵，进而需阐明其外延，即具有哪些具体类型？除了鉴定的法定类型外，从传统观点来看，有学者以鉴定学学科为分类标准，将鉴定分为法医学鉴定、物证技术学鉴定、司法会计学鉴定、环境损害鉴定、声像资料鉴定等。此外，也可按鉴定客体、鉴定程序等对鉴定予以分类。[26]上述传统分类共同构成了司法鉴定学的分类理论，这对于认识鉴定的外延，且对鉴定活动的具体展开无疑具有重要指导价值。

进入数智时代，作为关键变量的人工智能步入鉴定活动核心环节，乃人类历史上首次深度介入和承担人类认知功能的技术，其无疑为鉴定新类型的创设带来坚实的技术根基。但是，上述既有分类理论并未反映人工智能技术如何影响鉴定人行为或何以挑战传统鉴定范式。因此，以人工智能作为划分标准进而丰富鉴定的外延理论尤为必要。本文认为，可以人工智能介入鉴定的方式为标准，将数智鉴定分为“以人工智能为方法的鉴定”与“以人工智能产物为对象的鉴定”。

第一，人工智能介入鉴定人一方的工作，构成以人工智能为方法的鉴定。前文已述，人工智能介入特征比对型鉴定，形成了“自动化特征识别—特征比对—鉴定人核验”的鉴定模式。AFIS 耦合下

的指印鉴定、人脸识别系统耦合下的人像鉴定、PGS 耦合下的混合 DNA 分型等，均为此类鉴定。有别于传统鉴定，此类鉴定在鉴定实施的效能方面显著提升，本文第三部分将就此展开进一步的论述。

第二，人工智能介入鉴定对象的形成，则构成以人工智能产物为对象的鉴定。目前，此类鉴定有待规范化。近年来，人工智能中的深度学习技术被用于合成文本、图片、音频和视频等电子数据，构成了坊间广为流传的“深度伪造”（Deep Fake）之举。这种由生成对抗网络（Generative Adversarial Network，GAN）算法生成的电子材料具有“超拟真、反鉴别、快更迭”的功能特点，[27]导致实践中出现了“换脸”“仿声”的新型电信网络诈骗。[28]“深度伪造”不仅为新型犯罪治理带来挑战，也冲击着传统鉴定范式。详言之，“深度伪造”的出现，颠覆了实践中“眼见为实”的经验法则，冲击着传统鉴定中以感官为判断依据的范式。也就是说，对于“深度伪造”形成的视听资料，传统的特征识别方式，如眼观、耳听，极有可能被“深度伪造”特征所误导。因此，以人工智能产物为对象的鉴定，实际上也不得不借助智能识别算法的力量。对此，技术界已逐步推出相应的检测手段。[29]

值得注意的是，虽然“深度伪造”已有检测技术应对，但理应与之配套的鉴定、审查规范却尚未跟进。截至目前，我国国家标准、行业标准、团体标准均未对此进行专门规制，[30]如何规范化开展“深度伪造”产物的鉴定，尚需进一步的学理探讨与实践摸索。尽管如此，从学理上提出以人工智能产物为对象的鉴定仍然有其价值，该分类有助于提示事实认定者留意“看起来真”的证据实际上存在被“深度伪造”的风险。因此，具体案件若涉及“深度伪造”的图像或音视频时，应进行专门性检验或鉴定，而非依赖于传统的感官判别。

综上所述，随着算法参与检验分析环节，司法鉴定实现了数智化转型，促生了数智鉴定的内涵与外延。一方面，鉴定意见的生成已具有人技耦合性，可称作数智司法鉴定；另一方面，鉴定中人工智能的介入创新了司法鉴定的类型理论。这为深入认识数智鉴定的“双刃剑”效应提供了本体基础。

三、数智司法鉴定的优势与隐忧

（一）数智司法鉴定的优势

司法鉴定的数智化是大势所趋，相对于传统司法鉴定而言具备一系列优势。

一是提升司法鉴定效率。在传统鉴定中，手动比对指印、比对人脸图像或计算 DNA 分型概率可能耗时数千小时未果，而借力于 AFIS、FRT、PGS 等数智技术耦合鉴定，可在当天甚至数分钟内便完成比对或分析。数智赋能后的鉴定效率提升可见一斑，对此不赘。

二是赋能司法鉴定意见一定的客观可靠性。除前文所述提高鉴定的效率外，鉴定的数智化还提高了鉴定意见的客观可靠性。鉴定是客观的原理、技术与鉴定人的主观能动判断的统一。鉴定人在鉴定中的干预越少，鉴定意见越趋向客观可靠。鉴定的数智化恰恰是比较法的客观可靠化——让机器和算法从事重复性的特征选择与比对分析，能在一定程度上降低鉴定人员的失误、偏见以及徇私带来的主观偏差，为司法鉴定意见的可靠性提供了一层保障。与此同时，方法趋于客观会提高“同案同鉴”[31]的可能性，进而有利于提高鉴定意见的可信度及鉴定机构的公信力。

三是数智司法鉴定有助于提高鉴定意见的可靠性。以人脸识别为例，工信部曾发布《促进新一代人工智能产业发展三年行动计划（2018—2020 年）》，支持生物识别等技术在安防、金融等重点领域的应用，并计划在 2020 年实现复杂动态场景下人脸识别有效检出率超过 97%，正确识别率超过 90%。相较于传统人工比对人脸图像而言，人工智能算法的准确性可谓达到“机智过人”的程度。在此类高性能人工智能耦合下，鉴定意见的可靠性也会随之提升。

四是数智司法鉴定还具有一定的超越性，即鉴定的边界因数据和算法的介入而得以拓展。例如，机器和算法的介入让“少笔画”（电子化）笔迹的鉴定成为可能。具体而言，对于“少笔画”的伪装签名（如鉴定“丁一”二字是否由本人书写），在传统

笔墨环境下，鉴定人难以甚至无法完成此种鉴定，因为传统条件下的笔画缺失，会导致笔迹特征反映不够充分，进而不具备鉴定条件。但在无纸化条件下进行电子化签名时，电子设备将记录书写人运笔的时序、压力、速度等特征，鉴定人若能从计算机中调取这些“原始数据”，使用“传统笔迹鉴定+电子数据分析”相结合的方法，便有了鉴别“少笔画”签名是否由本人书写的现实基础。又如前文所述，对于混合 DNA 鉴定，在 PGS 介入后，三人混合的 DNA 乃至更为复杂的混合 DNA，均能在对应智能分析软件的助力下发挥超越传统鉴定的证明效力。

（二）数智司法鉴定的隐忧

尽管司法鉴定的数智化具有上述效能优势，但是，更值得注意的是，司法鉴定的数智化也会引发一系列隐患或挑战，有待学界和实务界进一步规制或应对。

一是自动化偏差的存续。自动化偏差，是人们倾向于信任数智系统给出的结果而忽视与之冲突信息的认知偏差。这种偏差具有极强的迷惑性，即便是经验丰富且受过专门训练的专家也难逃此种偏差影响。其实，自动化偏差在数智技术普遍渗入司法鉴定前便被察觉，如发生于 2004 年的“马德里炸弹恐怖袭击案”中涉及一起典型的指印错鉴。该案中，涉案指印先后经美国 4 位专家（含一名法官委任的专家）鉴定，他们均在 AFIS 给出的“机器意见”基础上错将嫌疑人认定为布兰登·梅菲尔德（Brandon Mayfield）。之所以在数智时代再次强调自动化偏差，是因为自动化偏差不会随着数智技术的更新而消失，反而会因人工智能技术的迭代而更具隐蔽性。因此，数智鉴定若要可靠落地，需学界对此足够重视，并在将来对数智技术在鉴定中的前端设计、中端应用以及后端审查上，予以技术和规范层面的系统性规制。

二是证据新样态的审查挑战。相对于传统鉴定意见而言，数智鉴定意见的生成机理增加了算法因素而变得相对复杂。从算法层面看，如何审查数智司法鉴定中所用算法的可靠性、如何破解算法黑箱是传统鉴定不曾有过的问题；从鉴定人层面看，鉴定人面对的自动化偏差应如何避免或减轻、鉴定时与算法的交互操作应如何规范化并透明化更是应该重视的方向。因此，数智鉴定的出现同时带来了证据新样态的审查问题，这将是证据学界与司法实务人员不得不面对的重要问题。

三是隐私和个人信息保护问题。DNA、指纹数据、声纹数据等生物识别数据属于我国《个人信息保护法》规定的敏感个人信息，其关乎个人隐私、信息保护以及财产安全。对于将生物识别数据用于鉴定，我国相关法律法规有待明确细则。例如，2012 年修订的《刑事诉讼法》第 130 条（现为第 132 条）授权侦查机关提取生物样本。据此，指纹信息无疑可被收集到大数据库中用于鉴定。但声纹、人脸图像、DNA 信息等能否被依法收集并用于鉴定，目前未有明确规定。对于生物识别数据的安全存储和及时删除问题，我国已有部分国家标准予以规制，[32] 但此等规制也存在法律效力低和法律衔接问题，有待学界进一步回应。

（技术编辑：艾薇）