



数字科技与人工智能

**Digital Technology  
and Artificial Intelligence**

每月资讯 2025 年 1 月

上海市律师协会数字科技与人工智能专业委员会

上海市律师协会  
数字科技与人工智能专业委员会  
每月资讯  
(2025 年 1 月)

主任

张逸瑞（北京市金杜律师事务所上海分所）

副主任

吴卫明（上海市锦天城律师事务所）

徐凯（上海市君悦律师事务所）

编委会

本期责任编辑：史宇航、方懿

# 目录

新规概览.....	1
1. 《人工智能安全标准体系（V1.0）》（征求意见稿）.....	1
2. 《广州市智能网联汽车创新发展条例》.....	1
3. 《上海市智算中心建设导则（2025 年版）》.....	1
4. 《国家数据基础设施建设指引》.....	2
5. 《关于完善数据流通安全治理更好促进数据要素市场化价值化的实施方案》.....	3
6. 《关于加强互联网数据中心客户数据安全保护的通知》.....	3
7. 《个人信息出境个人信息保护认证办法（征求意见稿）》.....	4
域外规范.....	5
1. 英国政府发布《人工智能机会行动计划》.....	5
2. 美国参议员提出《2025 年美国人工智能能力与中国脱钩法案》.....	5
3. 美国政府发布《人工智能扩散暂行最终规则》.....	6
4. 欧洲数据保护委员会发布《关于假名化的 01/2025 号指南》.....	7
5. 美国联邦贸易委员会最终通过《儿童在线隐私保护规则》修正案.....	7
案例研讨.....	9
域内案例.....	9
1. 爱奇艺起诉 MiniMax 版权侵权.....	9
2. AI 一键生成图片的版权归属.....	9
3. AI 侵犯版权的平台责任认定.....	10
域外案例.....	12
1. LinkedIn 被指控利用私信训练 AI.....	12
2. DeepSeek APP 在意大利下架.....	12
实务研究.....	14
1. 人工智能专利客体适格性的中美比较研究.....	14
2. 机遇与困境并存：浅谈自动驾驶汽车行业的数据共享.....	14
3. 美国“数据脱钩”新规——中国企业应对 14117 最终规则之十问十答.....	15
4. 美商务部为防止人工智能技术扩散发布框架规则.....	16
5. 企业数据确权的逻辑反思与规则重构——基于成本收益视角.....	16
数字科技产品发展.....	18
1. “天工大模型 4.0”o1 版和 4o 版正式上线天工 APP 和网页.....	18
2. 科大讯飞发布全国产算力平台上唯一的深度推理大模型——讯飞星火 X1.....	18
3. IBM 携手欧莱雅推出首个 AI 模型：助力化妆品研发.....	19
4. DeepSeek-R1 发布，性能对标 OpenAI o1 正式版.....	19
5. 月之暗面发布 Kimi k1.5 多模态思考模型.....	20
6. OpenAI 发布首个智能体 Operator.....	20
7. 百川智能发布 Baichuan-M1-preview 及 Baichuan-M1-14B 大模型.....	21
8. OpenAI 上架推理模型 o3-mini.....	22
9. 智谱发布全球首个面向公众、回车即用的 AI 电脑智能体 GLM-PC.....	22

# 新规概览

## 1. 《人工智能安全标准体系（V1.0）》（征求意见稿）

发布机构：全国网络安全标准化技术委员会

公布/生效时间：2025 年 1 月 26 日

内容概要/法规、政策文件的原文：

为积极响应《全球人工智能治理倡议》，支撑落实《人工智能安全治理框架》，充分发挥标准对人工智能技术应用和产业规范的引领作用，持续完善人工智能安全标准体系建设，全国网络安全标准化技术委员会秘书处组织编制了《人工智能安全标准体系（V1.0）》（征求意见稿）。

来源：全国网络安全标准化技术委员会，

<https://www.tc260.org.cn/front/postDetail.html?id=20250124171028>。

## 2. 《广州市智能网联汽车创新发展条例》

发布机构：广州市人大常委会

公布/生效时间：2025 年 1 月 20 日

内容概要/法规、政策文件的原文：

广州市第十六届人民代表大会常务委员会第三十三次会议于 2024 年 11 月 29 日通过的《广州市智能网联汽车创新发展条例》，业经广东省第十四届人民代表大会常务委员会第十五次会议于 2025 年 1 月 12 日批准，现予公布，自 2025 年 2 月 28 日起施行。

来源：广州人大，

[https://www.rd.gz.cn/xwdt/content/post\\_257533.html](https://www.rd.gz.cn/xwdt/content/post_257533.html)。

## 3. 《上海市智算中心建设导则（2025 年版）》

发布机构：上海市经济和信息化委员会

公布/生效时间：2025 年 1 月 10 日

内容概要/法规、政策文件的原文：

为进一步贯彻落实国家加快推进新型基础设施，赋能新型工业化，推动新质生产力发展的重要指示精神及《上海市进一步推进新型基础设施建设行动方案（2023-2026 年）》等政策文件要求，加快推进本市智能算力信息基础设施建设发展，形成本市智能算力高质量发展格局，在规划与选址、建筑与配套、规模与功能、AI 基础设施架构、集约高效、安全可靠、绿色节能、论证、评估与监测以及边缘智算中心等方面规范本市智算中心建设。上海市经济和信息化委员会组织编制了《上海市智算中心建设导则（2025 年版）》。

智算中心报建单位应依据本建设导则要求，加强可行性研究，认真制定项目方案和建设计划，科学设定或选取项目选址规模、功能定位、技术方案、耗能工艺、服务对象等，严格执行本市对智算中心全生命周期管理的要求。

来源：上海市经济和信息化委员会，

<https://www.sheitc.sh.gov.cn/cyfz/20250110/ff2f312248604845a82ec542fc0dd50e.html>。

#### 4. 《国家数据基础设施建设指引》

发布机构：国家发展改革委、国家数据局、工业和信息化部

公布/生效时间：2025 年 1 月 1 日

内容概要/法规、政策文件的原文：

按照党中央、国务院决策部署，国家发展改革委、国家数据局、工业和信息化部在充分调研的基础上，组织编制了《国家数据基础设施建设指引》，力争在当前情况下，说清楚数据基础设施的概念、发展愿景和建设目标，指导推进数据基础设施建设，推动形成横向联通、纵向贯通、协调有力的国家数据基础设施基本格局，打通数据流通动脉，畅通数据资源循环，促进数据应用开发，培育全国一体化数据市场，夯实数字经济发展基础，为数字中国建设提供有力支撑

来源：国家数据局微信公众号，

<https://mp.weixin.qq.com/s/aNRdWkr8zredPNbuqrP-zQ>。

## 5. 《关于完善数据流通安全治理更好促进数据要素市场化价值化的实施方案》

发布机构：国家发展改革委等六部门

公布/生效时间：2025 年 1 月 6 日

内容概要/法规、政策文件的原文：

为深入贯彻党中央、国务院决策部署，落实《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》

《关键信息基础设施安全保护条例》《网络数据安全条例》，推动高质量发展和高水平安全良性互动，国家发展改革委、国家数据局、中央网信办、工业和信息化部、公安部、市场监管总局制定了《关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案》

来源：国家发展和改革委员会，

[https://www.ndrc.gov.cn/xxgk/zcfb/tz/202501/t20250115\\_1395692.html](https://www.ndrc.gov.cn/xxgk/zcfb/tz/202501/t20250115_1395692.html)。

## 6. 《关于加强互联网数据中心客户数据安全保护的通知》

发布机构：工业和信息化部

公布/生效时间：2025 年 1 月 13 日

内容概要/法规、政策文件的原文：

工业和信息化部近日印发通知，部署加强互联网数据中心（IDC）客户数据安全保护。针对典型业务场景，提出明确安全责任界面、强化制度建设和组织保障、加强客户管理、加强客户数据安全保障、做好事件应急处置等工作要求。引导各通信管理局、基础电信运营企业和有关互联网数据中心企业做好 IDC 客户数据安全保护工作，推动 IDC 业务安全有序发展。

来源：工业和信息化部，

[https://www.miit.gov.cn/jgsj/waj/wjfb/art/2025/art\\_0ba3ad6a2bb94d0c9c0e466f](https://www.miit.gov.cn/jgsj/waj/wjfb/art/2025/art_0ba3ad6a2bb94d0c9c0e466f)

[db8ca48d.html](#)。

## 7. 《个人信息出境个人信息保护认证办法（征求意见稿）》

发布机构：国家互联网信息办公室

公布/生效时间：2025 年 1 月 3 日

内容概要/法规、政策文件的原文：

为促进个人信息高效便利安全跨境流动，规范个人信息出境个人信息保护认证工作，根据《中华人民共和国个人信息保护法》等法律法规，国家互联网信息办公室起草了《个人信息出境个人信息保护认证办法（征求意见稿）》，现向社会公开征求意见。

来源：国家互联网信息办公室，

[https://www.cac.gov.cn/2025-01/03/c\\_1737600915141373.htm](https://www.cac.gov.cn/2025-01/03/c_1737600915141373.htm)。

# 域外规范

## 1. 英国政府发布《人工智能机会行动计划》

内容概要：

2025 年 1 月 13 日，英国科学、创新与技术部（Department for Science, Innovation and Technology）向议会提交《人工智能机会行动计划》（AI Opportunities Action Plan），提出 50 项建议，该行动计划随即得到英国政府回应，除了其中一项建议为部分同意外，其余均为同意。

该行动计划提出其中一项重要任务为“培养、留住和吸引下一代 AI 科学家和创业者”。对此，该行动计划指出，如果能让英国同时拥有世界一流的 AI 研究和全球领先的 AI 应用生态系统，就必须成为精英人才的首选之地。在未来 5 年，英国必须做好准备，在各个技术领域增加培训数万名 AI 专业人员，以满足预期需求，并积极增加英国在全球顶尖 1000 名 AI 研究人员中的占比。

从长远来看，政府需要建立一个更深层次的 AI 技能和人才库，以推动 AI 产品在经济各领域的开发、推广和应用。设定一个短期目标，即到 2030 年培养数万名 AI 专业人才，这将有助于弥合预计存在的供需缺口。这会使英国与法国等国家保持同步，法国的国家 AI 委员会估计，未来 10 年法国的 AI 毕业生数量需要增加两倍才能满足预估需求。

来源：国际与比较教育研究所，

<https://mp.weixin.qq.com/s/3auO5Bhob-Y1VkeC7kMf8Q>。

## 2. 美国参议员提出《2025 年美国人工智能能力与中国脱钩法案》

内容概要：

2025 年 1 月底，美国参议员乔希·霍利（Josh Hawley）提出了一项法案，旨在阻止该软件在美国下载或使用，理由是可能将其集成到该国计算机系统中会带来国家安全风险，该法案名称为《2025 年美国人工智能



能力与中国脱钩法案》(Decoupling America's Artificial Intelligence Capabilities from China Act of 2025)。

据霍利称,使用中国开发的人工智能可能会使敏感数据和关键基础设施暴露于中国政府的利益之下。这一立场契合了美国和中国在科技领域更广泛的紧张关系,这一紧张关系在对华为和 TikTok 等公司实施的禁令中已经显而易见。该方案的内容是阻止美国个人和实体在中国进行 AI 研究、转让 AI 相关知识产权或投资中国 AI 企业,并对违反规定的行为处以严厉罚款和处罚。

来源:清华大学智能法治研究院,

<https://mp.weixin.qq.com/s/Mdr6zuw2W5rXyScHRhZ-7w>。

### 3. 美国政府发布《人工智能扩散暂行最终规则》

内容概要:

1月13日,拜登政府正式发布了《人工智能扩散暂行最终规则》(Interim Final Rule on Artificial Intelligence Diffusion),该规则详尽地规定了对全球 AI 芯片出口的限制措施,并于发布当天即刻生效。新规的详细内容于1月15日刊载于《联邦公报》,公众有120天的时间提交反馈意见。在此期限内,相关出口商和供应商无需遵守本规则的任何变更内容。

新规定长达168页,其核心目的是通过严格控制出口 AI 芯片及相关技术,实现对先进 AI 技术和 CPU 芯片的全球分布进行管理。根据新规定,美国将全球划分为三个不同“层级”的区域,并据此决定哪些国家和地区能够自由获取先进的 AI 技术和 CPU 芯片。

来源:赛博研究院,

<https://mp.weixin.qq.com/s/HG-gWzM3pNLFCvcfo99Jqg>。

#### 4. 欧洲数据保护委员会发布《关于假名化的 01/2025 号指南》

内容概要：

2025 年 1 月 17 日，欧洲数据保护监督机构（EDPB）发布了《关于假名化的 01/2025 号指南》。EDPB 明确假名化在 GDPR 合规中的应用。

指南提供了两项重要的法律澄清：假名化数据，如果可以通过使用额外信息归因于个人，则仍然是与可识别的自然人相关的信息，因此仍然是个人数据。换言之，如果数据控制者或其他人能够将数据关联回个人，那么它仍然是个人数据。但是，假名化可以降低风险，并在满足 GDPR 所有其他要求的前提下，更容易以合法利益作为法律基础（GDPR 第 6(1)(f) 条）。同样，假名化有助于确保与原始目的的一致性（GDPR 第 6(4) 条）。指南还解释了假名化如何帮助组织履行其与实施数据保护原则（GDPR 第 5 条）、默认情况下的数据保护设计（GDPR 第 25 条）和安全（GDPR 第 32 条）相关的义务。最后，指南分析了在使用假名化时采取的技术措施和保障措施，以确保保密性并防止未经授权的个人身份识别。

来源：清华大学智能法治研究院，

<https://mp.weixin.qq.com/s/3pq2cRB6-kQjM0e58-fSbg>。

#### 5. 美国联邦贸易委员会最终通过《儿童在线隐私保护规则》修正案

内容概要：

2025 年 1 月 16 日，美国联邦贸易委员会（Federal Trade Commission，下称“FTC”）全票通过了对《儿童在线隐私保护法案》（Children’s Online Privacy Protection Rule，下称“COPPA”）的重大修订。这标志着自 2013 年以来 COPPA 的首次重大更新，代表着为应对不断变化的数字环境和日益增长的对儿童数据在线安全重视所做出的巨大努力。COPPA 规则的最终修正案（修订规则）将在联邦公报上公布 60 天后生效。

除其他事项外，修订后的规则引入了新的同意要求和保留义务，并对运营商提出了更精细的安全要求，包括第三方尽职调查、安全控制的定期测试和监控，以及年度风险评估和安全计划评估。修订后的规则还更新了 COPPA 安全港计划的要求。

来源：数据法律资讯，

<https://mp.weixin.qq.com/s/AaWCJURs7IBiTLXfCIVFIA>。

# 案例研讨

## 域内案例

### 1. 爱奇艺起诉 MiniMax 版权侵权

时间：2025 年 1 月 6 日

内容概要：

国内知名视频流媒体平台爱奇艺已向上海市徐汇区人民法院正式提起诉讼，指控国内 AI 初创企业 MiniMax 在 AI 模型训练及内容生成流程中涉嫌侵犯其版权。

在 MiniMax 旗下的海螺 AI 创意视频平台上，用户可以通过上传图片 and 文字进行视频的生成创作。爱奇艺指控 MiniMax 未经授权使用其享有版权的素材进行训练，导致生成的内容构成对爱奇艺版权的侵犯。

来源：科创板日报，

[https://mp.weixin.qq.com/s/SszrnZq1BL\\_8sXvCdn7dCQ](https://mp.weixin.qq.com/s/SszrnZq1BL_8sXvCdn7dCQ)。

### 2. AI 一键生成图片的版权归属

时间：2024 年 1 月 15 日

案号：（2024）鄂 0192 知民初 968 号

审理法院：湖北省武汉东湖新技术开发区人民法院

内容概要：

原告王某是人工智能生成内容的创作者，其在小红书注册有相关账号。2024 年 5 月 17 日，王某在小红书首次发布含有其利用 AI 创作的作品的笔记，平台截图显示，该笔记有 3.5 万点赞、6478 收藏、661 条评论。

2024 年 6 月 20 日，王某发现武汉某科技有限公司通过抖音账号发布 AI 绘画训练营广告，用于 AI 绘画售课。该广告中引用图片与自己用 AI 创作的图片一致。

王某主张，案涉图片由其利用“某 AI”APP 创作而成。在创作期间，使用者需预先在头脑中构思画面，精心撰写并输入关键词，反复调整，以此把

控出图效果。即便提交相同关键词，生成的图片也不尽相同。王某于 5 月 26 日对该作品进行了版权登记。因此，王某认为被告公司的行为侵犯了自己对案涉图片享有的著作权，因而向法院提起诉讼。

案件结果：

法院认为，原告使用 AIGC 软件生成的被诉图片与通常人们见到的照片、绘画无异，显然属于艺术领域，具有一定的表现形式，受到著作权法的保护。从被诉图片的呈现与原告上述创作过程的关联性来看，原告使用的关键词均与画面的元素及效果对应，生成的图片和原告的创作活动之间具有一定的“映射性”。在原告设置调整关键词、参数、风格光影效果并挑选图片最终获得被诉图片的过程中，原告对生成作品具有一定程度的“控制和预见”，创作过程反映了原告的构思、创作技法、审美选择，体现了原告的个性化表达。故，被诉图片凝结了原告的智力劳动成果，应予保护。

被告未经许可使用被诉图片作为配图发表在自己的账号作为售课推广，使公众可以在其选定的时间和地点获得被诉图片，侵害了原告就被诉图片享有的信息网络传播权，应当承担停止侵权和赔偿损失的侵权责任。

来源：湖北高院，

<https://mp.weixin.qq.com/s/SwgQTxzCqZP4XpRAVpmoeA>。

### 3. AI 侵犯版权的平台责任认定

时间：2025 年 1 月 10 日

案号：(2024)浙 0192 民初 1587 号（一审）、(2024)浙 01 民终 10332 号（二审）

审理法院：杭州互联网法院（一审）、杭州中级人民法院（二审）

内容概要：

奥特曼系列作品著作权人圆谷制作株式会社将相关权利独占授权给原告上海某文化发展公司。被告杭州某智能科技公司是触手 AI 平台的运营主体，该平台功能众多，用户能通过上传图片等方式利用其训练和分享奥特曼 AI 模型，并可再利用奥特曼 AI 模型生成与原告奥特曼形象构成实质性相似的作品。被告系生成式人工智能服务提供者，其对部分服务收费，但在

平台用户服务协议中声明对用户上传素材及生成内容不加审核，还主动引导用户发布生成内容。原告认为被告的行为侵犯其享有的信息网络传播权，同时违反反不正当竞争法的诚信原则，给其合法权益造成严重损害，故诉至杭州互联网法院。

被告辩称，原告提交的权属来源链条不完整，无法确认本案是否涉及其他权利人的独占使用权。某公司本身不提供训练数据，没有实质侵权行为，用户创作未用于商业用途，积分充值是正常经营行为，平台算法模型合规备案，且有多处提醒用户合法创作，平台也有反馈处理和例检机制。涉案 AI 行为不符合信息网络传播权控制的特定行为，也不构成不正当竞争，且被告已采取屏蔽措施，原告主张的损失过高且无依据。

案件结果：

2024 年 9 月 25 日，杭州互联网法院作出一审判决，认为涉案奥特曼动漫形象属美术作品，圆谷制作株式会社享有著作权，其授权原告相关权利，原告有权提起诉讼。被告虽提供生成式人工智能服务，但侵权图片训练素材由用户上传，且无证据表明其与用户共同提供作品，不构成直接侵权，但其怠于采取符合侵权损害发生时技术水平的必要措施来预防侵权，未尽到合理注意义务，构成帮助侵权。被告商业模式提供个性化服务，技术中立，用户合法创作不侵害权益，未扰乱市场竞争秩序，故被告不构成不正当竞争。2024 年 12 月 30 日，杭州市中级人民法院作出二审判决，驳回上诉，维持原判。

来源：网络法实务圈，

<https://mp.weixin.qq.com/s/TSSUlgo68TVWRmaGoq3kFQ>。

## 域外案例

### 1. LinkedIn 被指控利用私信训练 AI

时间：2025 年 1 月 23 日

内容概要：

2025 年 1 月 23 日，多家媒体报道，LinkedIn Premium 用户正在起诉这家全球最大的职业社交网站，指控其未经用户同意，将与第三方共享他们的私信，以用于训练人工智能模型。据在加利福尼亚州联邦法院提起的拟议集体诉讼指控，去年 8 月，LinkedIn“表面上”为用户提供了启用新隐私功能的能力，该功能决定用户的个人数据是否可以被共享，但默认开启了权限。诉讼还指控这家微软旗下的公司在一个月后通过更改其隐私政策来隐瞒其行为，新政策中表示用户信息可能会被披露用于 AI 训练目的。

LinkedIn 的一位发言人告诉 BBC 新闻，“这些指控是虚假的，毫无根据”。诉讼文件还指出，LinkedIn 更改了其“常见问题”部分，表示用户可以选择 not 共享用于 AI 目的的数据，但这样做不会影响已经进行的训练。“LinkedIn 的行为……表明其试图掩盖痕迹的模式，”诉讼称“这种行为表明，LinkedIn 完全意识到其已违反了合同承诺和隐私标准，并旨在尽量减少公众审查。”

来源：清华大学智能法治研究院，

[https://mp.weixin.qq.com/s/I-En6Qk1qv1\\_krg9o-7aFw](https://mp.weixin.qq.com/s/I-En6Qk1qv1_krg9o-7aFw)。

### 2. DeepSeek APP 在意大利下架

时间：2025 年 1 月 29 日

内容概要：

2025 年 1 月 29 日，在意大利当局要求 DeepSeek 提供有关该公司如何处理用户数据的信息数小时后，DeepSeek 已不在意大利地区苹果的 AppStore 和谷歌的 Play Store 上提供。

意大利数据保护机构周二表示，正在向 DeepSeek 寻求有关其使用个人

数据的解释。意大利监管机构 **Garante** 表示, 希望了解收集了哪些个人数据、从哪些来源收集、用于什么目的、基于什么法律依据, 以及是否存储在中国。Garante 在一份声明中表示, DeepSeek 及其附属公司有 20 天的时间答复。

来源: 云头条,

<https://mp.weixin.qq.com/s/zLY2uQdjS8i5546y1NG7bw>。



# 实务研究

## 1. 人工智能专利客体适格性的中美比较研究

作者：金杜研究院-马俊豪、姜鹏义

时间：2025 年 1 月 15 日

内容概要：

2024 年 12 月 31 日，中国国家知识产权局发布了《人工智能相关发明专利申请指引（试行）》（下称“《指引》”），意在进一步明确和细化我国现行专利法律制度框架下人工智能领域的专利审查政策，回应创新主体普遍关切的热点法律问题。文章以此为背景，对中美人工智能专利客体适格性展开比较研究。中国将人工智能相关专利申请分为四类，《指引》对人工智能方案客体审查基准进行细化，为申请人提供明确指导；美国专利主题适格性标准源于专利法第 101 条，采用 Mayo/Alice 测试判断，但该测试在软件和算法领域主观性强、标准不明确，为此美国提出相关法案，USPTO 也多次更新指南。中美在判断专利客体适格性时都强调技术性，完善评判基准的趋势都是将抽象概念与实际技术应用相结合。最后文章指出，中美都重视人工智能行业发展并完善相关法规，但美国实践经验更丰富，创新主体进行境外专利布局时需深入了解目标国家审查标准和判例，灵活调整策略以保护自身利益。

来源：金杜研究院，

[https://mp.weixin.qq.com/s/ZcuRjuQ\\_0\\_PVrJM0qNJsew](https://mp.weixin.qq.com/s/ZcuRjuQ_0_PVrJM0qNJsew)。

## 2. 机遇与困境并存：浅谈自动驾驶汽车行业的数据共享

作者：金杜研究院-宋海燕、王筠毅

时间：2025 年 1 月 21 日

内容概要：

汽车行业正从传统机械交通工具向智能移动空间转变，数据是自动驾驶产业发展的关键，但当前数据共享面临困境。美国国家公路交通安全管

理局发起 AV TEST 计划，拨款打造数据共享中心，后又推出 AV STEP 计划，旨在提高透明度、增强公众信任，不过二者均存在企业参与度不高的问题；德国汽车行业龙头企业合资搭建 Catena-X 数据生态系统，通过标准化、保障安全、建立信任和开展国际化合作，推动数据共享，其模式还被推广到其他制造业领域。我国自动驾驶汽车数据共享模式包括行业协会联合车企建立的 VDBP 平台以及各地数据交易所的汽车数据专区，但都面临交易量少等问题。未来，我国自动驾驶汽车数据产业需统一行业数据流通规则、标准，并给予汽车数据交易财政补贴，以此促进数据共享，释放自动驾驶技术潜力。

来源：金杜研究院，

<https://mp.weixin.qq.com/s/lHP3ilKj4T0gsQZCtcNtZg>。

### 3. 美国“数据脱钩”新规——中国企业应对 14117 最终规则之十问十答

作者：金杜研究院-赵新华、王哲峰等

时间：2025 年 1 月 24 日

内容概要：

美国出台的《14117 最终规则》旨在防范敏感个人数据流动带来的国家安全风险，改变了其长期奉行的“数据跨境自由流动”原则。该规则于 2025 年 4 月 8 日生效，部分义务于 10 月 6 日实施，其影响范围广泛，对开展海外尤其是美国业务的中国企业以及境外跨国公司与中国关联公司的业务往来均有不同程度的限制，跨境电商、AI 等多个行业将受到冲击。规则重点规制涉及特定数据的交易，明确了美国人、受关注国家和受规制主体的范围，详细规定了受规制的数据类型、禁止和限制的交易类型，也提供了一般许可与特别许可等合规路径。违反该规则将面临民事或刑事处罚。相关企业应梳理业务、采取合规措施、加强数据管理并关注法规动态，中国企业还需注意避免违反中国数据保护法规。

来源：金杜研究院，

<https://mp.weixin.qq.com/s/meb5XM7F17ZQ-Kj75mhHxw>。

#### 4. 美商务部为防止人工智能技术扩散发布框架规则

作者：中伦视界-张国勋等

时间：2024 年 1 月 15 日

内容概要：

2025 年 1 月 13 日，美国商务部产业与安全局（BIS）发布《人工智能扩散框架》临时最终规则，修订《出口管理条例》，一方面新增对人工智能模型权重的限制，如管控特定训练次数的模型参数、设定外国直接产品规则等，同时对开源等部分模型权重未设许可要求并新设许可例外；另一方面针对先进计算物项按国家和地区划分三个级别实施不同管控措施，各级别在许可审查政策、限额及许可例外等方面规定各异。该规则于发布日生效并设有过渡期条款，建议中国企业密切跟踪规则进展、优化全球业务布局并应对 IaaS 服务商合规问询，以满足合规要求。

来源：中伦视界，

<https://mp.weixin.qq.com/s/AYpmVVrVN7BgJCi2qGDNjQ>。

#### 5. 企业数据确权的逻辑反思与规则重构——基于成本收益视角

作者：牛梦倩

时间：2025 年 1 月 2 日

内容概要：

文章从成本收益视角对企业数据确权进行反思并提出利用和保护策略。企业数据作为重要生产要素，其确权在实务界和理论界引发诸多讨论。但基于成本收益分析，确权存在问题：概念层面，学界对“企业数据”概念界定混乱；收益方面，数据市场交易量小，“定分止争”效益微薄；成本层面，会增加利用成本和执法“识别”成本。因此，当前企业数据确权预期成本小于预

期收益，不利于企业数据发展。对此，应采取以下策略：建立和完善企业数据互操作框架，统一数据对接程序，推动数据共享流通；把握企业数据跨境流动安全红线，实现数据设施“本土化”和传输“保密化”；推动企业数据治理公私合作，探索行业自治，政府提供良好发展环境，实现“软”性监管。

来源：上海市法学会 东方法学，

<https://mp.weixin.qq.com/s/M4yqCz4hEJbAFfulfCaCeA>。

# 数字科技产品发展

## 1. “天工大模型 4.0” o1 版和 4o 版正式上线天工 APP 和网页

发布企业：昆仑万维集团

时间：2025 年 1 月 6 日

内容概要：

2025 年 1 月 6 日，昆仑万维「天工大模型 4.0」o1 版（Skywork o1）和 4o 版（Skywork 4o）正式上线天工网页和 APP，面向用户免费开放。Skywork o1 在逻辑推理任务性能上大幅提升，通过推理反思能力训练、推理能力强化学习、推理 planning 等自研训练方案，以及 PRM 优化、基于 Q\*算法的推理系统优化、提出 Step-DAPO 算法等升级举措，在数学、代码和逻辑推理基准测试中表现出色，逼近 o1-mini 且显著优于行业常规通用大模型。Skywork 4o 赋能的 Skyo 语音助手采用多模态 LLM 端到端建模，具有极低响应延迟、语音多维度理解、拟真人自然回复等特性，为用户带来流畅自然的对话体验。

来源：昆仑万维集团，

<https://mp.weixin.qq.com/s/bSLAcicOIbj2BMPavlv4wg>。

## 2. 科大讯飞发布全国产算力平台上唯一的深度推理大模型——讯飞星火 X1

发布企业：科大讯飞

时间：2025 年 1 月 15 日

内容概要：

2025 年 1 月 15 日，科大讯飞举办发布会，带来多项重大成果。发布了基于全国产算力的深度推理大模型讯飞星火 X1，其中文数学能力国内领先，在多类测试中成绩优异，已率先应用于教育、医疗领域。讯飞星火 4.0Turbo 底座能力也实现升级，在数学、图文识别、长文本等方面能力显著提升，还

首发混域知识搜索技术，行业能力全面增强。此外，科大讯飞发布了业界首个端到端语音到语音同传大模型，技术测试领先竞品，全系产品翻译能力得以提升，并计划在 2025 年推出翻译机商务套装，满足不同商务场景需求。

来源：安徽省科技厅，

<https://mp.weixin.qq.com/s/Csz0RRcQjkU0CxUxEB5mDQ>。

### 3. IBM 携手欧莱雅推出首个 AI 模型：助力化妆品研发

发布企业：IBM 中国

时间：2025 年 1 月 20 日

内容概要：

IBM 与欧莱雅宣布合作成果，双方利用 IBM 的生成式人工智能技术和行业专长，开发业内首个基于化妆品配方的 AI 基础模型，旨在从化妆品配方数据中挖掘关键洞察，助力欧莱雅使用可持续原材料，减少能源和材料浪费，提升研发与创新能力，满足业绩和消费者满意度提升需求。该模型将辅助欧莱雅全球 4000 多位研究人员开展多项工作，IBM Consulting 还会帮助其重塑配方研发流程。此次合作有望开创 AI 在美妆、化学和科技交叉领域的创新，助力欧莱雅实现“2030 承诺”，推动其迈向创新与可持续发展共荣的未来。

来源：IBM 中国，

[https://mp.weixin.qq.com/s/ufpW\\_7JcPnLvE4AWL2aYxQ](https://mp.weixin.qq.com/s/ufpW_7JcPnLvE4AWL2aYxQ)。

### 4. DeepSeek-R1 发布，性能对标 OpenAI o1 正式版

发布企业：DeepSeek

时间：2025 年 1 月 20 日

内容概要：

2025 年 1 月 20 日，DeepSeek 正式发布 DeepSeek-R1 并同步开源模型权重，上线 API 且开放思维链输出，DeepSeek 官网与 App 同步更新。该模型在数学、代码、自然语言推理等任务上性能对标 OpenAI o1 正式版，其

训练技术全部公开。同时，通过 DeepSeek-R1 蒸馏的 6 个小模型也开源给社区，其中 32B 和 70B 模型多项能力对标 OpenAI o1-mini。此外，DeepSeek 调整协议授权，模型开源 License 统一使用 MIT，产品协议明确可“模型蒸馏”。DeepSeek-R1 API 服务定价为每百万输入 tokens 1 元（缓存命中）/4 元（缓存未命中），每百万输出 tokens 16 元，调用指南可参考官方文档。

来源：DeepSeek，

<https://mp.weixin.qq.com/s/atKyfC5l-BaStje8-F3FGQ>。

## 5. 月之暗面发布 Kimi k1.5 多模态思考模型

发布企业：月之暗面 Kimi

时间：2025 年 1 月 20 日

内容概要：

2025 年 1 月 20 日，Kimi 发布全新 SOTA 模型 k1.5 多模态思考模型，这是其 k 系列强化学习模型连续第三个月的重磅升级。该模型在 short-CoT 模式下，数学、代码、视觉多模态和通用能力大幅超越全球范围内短思考 SOTA 模型；在 long-CoT 模式下，数学、代码、多模态推理能力达到长思考 SOTA 模型 OpenAI o1 正式版的水平。同时，Kimi 首次公开模型训练技术报告，介绍了 k1.5 模型设计和训练的关键要素，包括长上下文扩展、改进的策略优化、简洁的框架、多模态能力，还提出了用 Long-CoT 技术改进 Short-CoT 模型的 long2short 方法。k1.5 多模态思考模型的预览版将陆续在 Kimi.com 网站和 Kimi 智能助手 app 灰度上线。

来源：月之暗面 Kimi，

<https://mp.weixin.qq.com/s/BmOKGKjXP2tjmPyNdU0Hqg>。

## 6. OpenAI 发布首个智能体 Operator

发布企业：OpenAI

时间：2025 年 1 月 23 日

内容概要：



2025 年 1 月 24 日消息，美国初创公司 OpenAI 于周四突然举行直播活动，推出首款 AI 代理工具 Operator，它由 CUA 模型驱动，结合了 GPT-4o 的视觉能力与强化学习实现的高级推理，能像人类一样使用网页浏览器，在有限监督下按设定完成任务。目前美国的 ChatGPT Pro 用户已可使用其“研究预览版”，未来会拓展至更多区域的 Pro 用户及 ChatGPT Plus 用户。OpenAI 还计划在未来发布更多 AI 代理。在演示案例中，Operator 能完成饭店预订、按购物清单买菜等任务，不过它与人类仍存在差距，后续会持续改进。

来源：财联社，

[https://mp.weixin.qq.com/s/Ww4dkuzrsXQ\\_pNMOORJNew](https://mp.weixin.qq.com/s/Ww4dkuzrsXQ_pNMOORJNew)。

## 7. 百川智能发布 Baichuan-M1-preview 及 Baichuan-M1-14B 大模型

发布企业：百川智能

时间：2025 年 1 月 24 日

内容概要：

2025 年 1 月 24 日，百川智能发布两款新模型，国内首个全场景深度思考模型 Baichuan-M1-preview 和行业首个开源医疗增强大模型 Baichuan-M1-14B。前者是国内目前唯一同时具备语言、视觉和搜索三大领域推理能力的模型，多项能力超越 o1-preview，还解锁“医疗循证模式”，已上线百小应；后者是 Baichuan-M1-preview 的小尺寸版本，医疗能力超越 Qwen2.5-72B，与 o1-mini 相近。为实现“医疗循证模式”，团队自建循证医学知识库并进行证据分级。Baichuan-M1-14B 通过多管齐下优化医疗能力，其开源将推动 AI 医疗领域发展，助力构建医疗健康生态。

来源：百川智能商业服务，

<https://mp.weixin.qq.com/s/uOdNLZILBXdoWarqwkIx6A>。



## 8. OpenAI 上架推理模型 o3-mini

发布企业：OpenAI

时间：2025 年 1 月 31 日

内容概要：

2025 年 1 月 31 日，OpenAI 正式推出推理模型 o3-mini，这是 ChatGPT 首次向免费用户开放推理模型。o3-mini 是 OpenAI 推理系列中最新且具成本效益的模型，在编码评估、数学能力测试等方面性能出色，支持函数调用、结构化输出等功能，还能让开发者选择低、中、高三级推理强度。目前该模型已在 ChatGPT 和 API 中上线，付费用户使用权限提升，且它集成搜索功能，通过网络资源链接提供最新答案，未来有望推动人工智能领域的发展。

来源：每日经济新闻，

<https://news.qq.com/rain/a/20250201A01L4G00>。

## 9. 智谱发布全球首个面向公众、回车即用的 AI 电脑智能体 GLM-PC

发布企业：OpenAI

时间：2025 年 1 月 23 日

内容概要：

智谱推出的 GLM-PC 是全球首个面向公众、回车即用的电脑智能体，基于智谱多模态大模型 CogAgent 开发。自发布内测以来，其不断升级，新增“深度思考”模式、逻辑推理和代码生成功能，并支持 Windows 系统。它借鉴人类左右脑分工模式，将 CogAgent 与代码模型 CodeGeex 深度融合，“左脑”负责逻辑推理与任务执行，具备规划、循环执行、动态反思纠错优化等能力；“右脑”专注感知与交互，能进行 GUI 图像理解、用户行为认知等。这种左右脑协作模式让 GLM-PC 在处理复杂逻辑和开放性问题上表现出色，可完成多种复杂任务。此外，智谱还开源了 CogAgent-9B-20241220 以促进相关研究，目前正与联想、华硕等合作推动 AIPC 创新发展。

来源：智谱，

<https://mp.weixin.qq.com/s/87pYtSG9bpgYNZi5UGNnIg>。