数字科技与人工智能

Digital Technology and Artificial Intelligence

每月资讯 2025 年 3 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 3 月）

目 录

新规概览

1. 《中华人民共和国网络安全法（修正草案再次征求意见稿）》

发布机构：国家互联网信息办公室

公布/生效时间：2025 年 3 月 28 日

内容概要：

2025 年 3 月 28 日，国家互联网信息办公室发布《中华人民共和国网络安全法（修正草案再次征求意见稿）》，向社会公开征求意见至 2025 年 4 月 27 日。公众可通过电子邮件或信函方式提交意见。此次修订重点强化网络安全法律责任，加大对违法行为的处罚力度。此次修订旨在做好《网络安全法》与《数据安全法》《个人信息保护法》《行政处罚法》等相关法律的衔接协调，完善法律责任制度，保护个人、组织在网络空间的合法权益，维护国家安全和公共利益。

来源：中国网信网

https://www.cac.gov.cn/2025-03/28/c_1744779434867328.htm

2. 《人脸识别技术应用安全管理办法》

发布机构：国家互联网信息办公室、公安部

公布/生效时间：2025 年 3 月 13 日

内容概要：

2025 年 3 月 13 日，国家互联网信息办公室、公安部联合公布《人脸识别技术应用安全管理办法》，自 2025 年 6 月 1 日起正式施行。该《办法》共二十条，对人脸识别技术应用的基本要求、处理规则、安全规范和监督管理等作出全面规定。《办法》明确要求，应用人脸识别技术处理人脸信息应当遵守法律法规，尊重社会公德和伦理道德，履行个人信息保护义务，不得危害

国家安全、损害公共利益或侵害个人合法权益。其中特别规定，处理人脸信息应当具有特定目的和充分必要性，采取对个人权益影响最小的方式，并取得个人单独同意。根据《办法》，处理人脸信息达到 10 万人的组织需向省级以上网信部门备案。网信部门将会同公安机关建立协同监管机制，共同规范人脸识别技术应用。

来源：中央人民政府网站

https://www.gov.cn/zhengce/zhengceku/202503/content_7016075.htm

3. 《人工智能生成合成内容标识办法》

发布机构：国家互联网信息办公室、工业和信息化部、公安部、国家广播电视总局

公布/生效时间：2025 年 3 月 14 日

内容概要：

2025 年 3 月 14 日，国家互联网信息办公室、工业和信息化部、公安部、国家广播电视总局联合发布《人工智能生成合成内容标识办法》，将于 2025 年 9 月 1 日起施行。《标识办法》共十四条，明确了人工智能生成合成内容的标识形式、责任主体、技术要求和监管措施等内容。其中规定，服务提供者应当对生成合成内容采取显式标识或隐式标识，确保用户可识别或技术可溯源，并禁止任何组织或个人恶意篡改、伪造或隐匿标识。

同时，配套强制性国家标准《网络安全技术人工智能生成合成内容标识方法》及《服务提供者编码规则》将于 2025 年 9 月 1 日与《标识办法》同步实施，为标识工作提供技术指引。

来源：中国网信网

https://www.cac.gov.cn/2025-03/14/c_1743654685899683.htm

4. 《网络安全标准实践指南——个人信息保护合规审计专业机构服务能力要求（征求意见稿）》

发布机构：全国网络安全标准化技术委员会秘书处

公布/生效时间：2025 年 3 月 3 日

内容概要：

2025 年 3 月 3 日，全国网络安全标准化技术委员会秘书处发布《网络安全标准实践指南——个人信息保护合规审计专业机构服务能力要求（征求意见稿）》，公开征求意见至 2025 年 3 月 17 日。该《实践指南》从五个方面规范了专业机构提供个人信息保护合规审计服务的能力要求，包括基本条件、管理体系、技术能力、人员能力、场所与设备资源能力。该《实践指南》可用于规范专业机构个人信息保护合规审计活动，为个人信息保护合规审计专业机构认证提供依据。

来源：全国网络安全标准化技术委员会官网

https://www.tc260.org.cn/front/postDetail.html?id=20250303215420

5. 《工业和信息化领域人工智能安全治理标准体系建设指南（2025）（征求意见稿）》

发布机构：工业和信息化部人工智能标准化技术委员会

公布/生效时间：2025 年 3 月 27 日

内容概要：

2025 年 3 月 27 日，工业和信息化部人工智能标准化技术委员会发布《工业和信息化领域人工智能安全治理标准体系建设指南（2025）（征求意见稿）》，面向社会公开征求意见，意见反馈截止时间为 2025 年 4 月 15 日。《指南》旨在贯彻落实国家人工智能发展战略，加快构建人工智能安全治理标准体系，

推动产业高质量发展和高水平安全协同推进，夯实标准对推动技术进步、促进企业发展、引领产业升级、保障产业安全的支撑作用，更好推进人工智能赋能新型工业化，加速迈向制造强国和网络强国。

来源：“工信部人工智能标准化技术委员会”微信公众号

https://mp.weixin.qq.com/s/PxhkZiDJXMDwI7jhucSmtg

6. 《工业互联网安全分类分级管理办法》

发布机构：工业和信息化部

公布/生效时间：

内容概要：

2025 年 3 月 20 日，工业和信息化部正式发布《工业互联网安全分类分级管理办法》（工信部网安〔2024〕68 号）。《办法》共五章二十二条，明确将工业互联网企业分为联网工业企业、平台企业、标识解析企业三类。并要求企业根据规模、业务范围、数据重要性等要素自主定级，由高到低分为三级、二级和一级，并通过全国管理平台完成信息登记。其中规定，三级企业需每年至少开展一次安全评测，二级企业每两年至少评测一次，企业发生网络安全事件时应立即启动应急预案并向主管部门报告。

来源：工业和信息化部官网

https://www.miit.gov.cn/jgsj/waj/wjfb/art/2025/art_72d3dab25147424590861126 3f50b096.html

7. 《卫星网络国内协调管理办法（暂行）》

发布机构：工业和信息化部

公布/生效时间：2025 年 3 月 4 日

内容概要：

2025 年 3 月 4 日，工业和信息化部正式印发《卫星网络国内协调管理办法（暂行）》（工信部无〔2025〕52 号），自 2025 年 5 月 1 日起实施。《办法》共六章三十三条，明确了国内协调的基本原则、程序流程和完成形式，旨在提升卫星频率轨道资源协调效率，维护空中电波秩序。其中规定，卫星操作单位应依据国际电信联盟《无线电规则》和国内协调列表开展频率协调工作。该办法的出台将显著降低航天企业协调成本，促进卫星频率轨道资源的高效开发利用。

来源：工业和信息化部官网

https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2025/art_01e8245a456448f1b0897f548487c3c2.html

8. 《上海市网络数据分类分级和重要数据目录管理办法（征求意见稿）》

发布机构：上海市互联网信息办公室

公布/生效时间：2025 年 3 月 28 日

内容概要：

2025 年 3 月 28 日，上海市互联网信息办公室会同市数据局联合发布《上海市网络数据分类分级和重要数据目录管理办法（征求意见稿）》，面向社会公开征求意见，意见反馈截止时间为 2025 年 4 月 28 日。《办法》旨在健全网络数据分类分级制度及重要数据目录管理机制，保障网络数据安全，促进网络数据开发利用。《办法》共六章二十四条，对网络数据分类分级制度、重要数据目录管理机制以及公共数据安全管理等方面作出具体规定。

来源：“网信上海”微信公众号

https://mp.weixin.qq.com/s/sg10kB6ahFsPTpbv4rmOCA

9. 《北京市数据跨境流动便利化综合配套改革实施方案》

发布机构：北京市互联网信息办公室、北京市商务局、北京市政务服务和数据管理局

公布/生效时间：2025 年 3 月 27 日

内容概要：

2025 年 3 月 27 日，北京市互联网信息办公室、北京市商务局、北京市政务服务和数据管理局联合印发《北京市数据跨境流动便利化综合配套改革实施方案》。该《方案》旨在建立高效便利安全的数据跨境流动机制决策部署和北京市委、市政府关于持续深化数据跨境流动便利化改革任务要求，迭代升级北京市数据出境政策措施，健全完善服务管理体系。《方案》围绕持续优化数据跨境流动政策、应用、服务、技术、生态、监管等 6 个方面，重点提出了 24 项创新政策举措。

来源：北京市商务局网站

https://sw.beijing.gov.cn/sy/nsjg/zdcxc/tzgg/202503/t20250327_4046627.html

域外规范

1. 欧盟委员会发布《通用人工智能实践准则》第三版草案

内容概要：

2025 年 3 月 11 日，欧盟委员会正式发布《通用人工智能实践准则》第三版草案，开启最终征求意见阶段。该草案在整合前两轮公众意见的基础上，形成了更为精简的结构，设定 2 项适用于所有通用 AI 模型提供商（GPAI）的透明度与版权基础承诺，以及 16 项专门针对系统性风险 AI 模型的安全专项承诺。委员会人工智能办公室将同步发布配套指南，就通用人工智能模型的定义、责任价值链条、免费和开源许可下提供的模型的豁免等问题作必要的澄清。该准则最终版预计将于 2025 年 5 月定稿。

来源：英国议会官网

https://bills.parliament.uk/bills/3942

2. 英国《人工智能（监管）法案》通过一读

内容概要：

2025 年 3 月 4 日，英国议会正式提交《人工智能（监管）法案》，并于同日在上议院完成一读程序。该法案提出设立专门的人工智能监管局，统筹人工智能监管工作，确保各监管机构之间协调一致，开展监管空白分析，并通过测试平台与监管沙箱支持 AI 创新。法案确立了 AI 监管的基本原则，包括安全性、透明度、公平性和问责制，并要求企业指定专门的人工智能负责人，以确保人工智能的道德使用及数据公正性。《法案》将人工智能定义为能够感知环境、解读数据并做出决策的技术，包括生成式人工智能模型。该法案后续将进入议会二读及委员会审议阶段。

来源：英国议会官网

https://bills.parliament.uk/bills/3942

3. 土耳其《网络安全法》正式生效

内容概要：

2025 年 3 月 19 日，土耳其《网络安全法》正式生效。该法律将"网络安全"定义为保护网络空间信息系统免受攻击、确保数据机密性、完整性和可用性的一系列活动，涵盖关键基础设施、网络事件、网络威胁情报等核心概念。《网络安全法》适用于公共机构、组织及网络空间运营的个人，要求相关主体向总统府提供数据，并从认证实体采购网络安全产品。违规行为将面临刑事处罚，包括监禁和罚款，未履行义务或未获必要批准的主体将受到特定制裁。总统府将与多方合作提升网络成熟度并加强监管执行。

来源：土耳其官方公报网站

https://www.resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm

4. 西班牙政府批准《人工智能治理法》草案

内容概要：

2025 年 3 月 11 日，西班牙数字化与公共职能部公布《人工智能治理法》草案，旨在确保人工智能技术的伦理、包容和有益使用。该草案将西班牙法律与已生效的欧盟《人工智能法案》相衔接，同时设立创新支持机制，包括提前建立欧盟要求的"沙盒"测试环境。

该《治理法》明确禁止六类 AI 应用，包括“潜意识技术操纵决策、利用弱点、生物特征分类歧视、社会评分、犯罪风险评估、用于晋升或解雇”。同时《治理法》要求高风险 AI 系统（如医疗诊断、关键基础设施、边境管控等）必须履行配备风险管理系统和人工监督机制等一系列义务。

来源：西班牙政府数字化转型与公共职能部官网

https://digital.gob.es/comunicacion/notas-prensa/mtdfp/2025/03/2025-03-11

案例研讨

域内案例

1. 国家网络安全通报中心通报大模型工具 Ollama 存在安全风险

时间：2025 年 3 月 3 日

内容概要：

据清华大学网络空间测绘联合研究中心分析，开源跨平台大模型工具 Ollama 在默认配置下存在严重安全隐患。该工具默认开放的 11434 端口无鉴权机制，可能导致 DeepSeek 等大模型面临未授权访问、数据泄露及算力盗取等风险。通报详细披露了三类高危漏洞：攻击者可绕过认证直接调用模型服务甚至删除模型文件；通过/api/show 等接口可提取模型 license 等敏感信息；CVE-2024 系列漏洞可能引发数据投毒、参数窃取、恶意文件上传等攻击。

研究中心提出五项加固建议，包括限制端口访问范围、配置防火墙规则、实施 API 密钥管理、禁用危险操作接口、历史漏洞修复等，并呼吁用户加强隐患排查，及时进行安全加固。国家网络与信息安全信息通报中心将持续监测相关风险。

来源：“国家网络安全通报中心”微信公众号

https://mp.weixin.qq.com/s/n7PyLykK7MlO3re2oOyY5w

2. 国家计算机病毒应急处理中心通报 15 款违规移动应用

时间：2025 年 3 月 7 日

内容概要：

国家计算机病毒应急处理中心近期依据《网络安全法》《个人信息保护法》等法律法规，监测发现 15 款移动应用存在隐私不合规行为。主要问题包括：

未显著告知个人信息处理规则（涉及《车进京》等 6 款 App）、未完整说明第三方数据收集范围（涉及《代驾宝》等 11 款 App）、未获单独同意向第三方提供信息（涉及《九拍教师》等 3 款 App），以及未提供便捷的撤回同意方式（涉及《草莓恋爱》等 14 款 App）。其中，《货运达司机端》存在未经单独同意处理敏感个人信息的严重违规行为。中心提醒用户谨慎下载相关应用，注意阅读隐私政策，限制非必要权限授权，并定期清理隐私数据。

来源：国家计算机病毒应急处理中心网站

https://www.cverc.org.cn/zxdt/report20250307.htm

3. “3·15 晚会”央视曝光多款"精准获客"软件非法窃取个人信息

时间：2025 年 3 月 15 日

内容概要：

央视新闻调查发现，市场上多家科技公司销售的"获客软件"涉嫌非法窃取用户个人信息。云企智能、绿信科技等公司通过爬虫技术嵌入主流互联网平台，在用户不知情的情况下抓取电话号码、微信号等个人敏感信息。其中"云客引流"软件可在 1 分钟内抓取 6 位用户完整信息，"点点蚁"软件则能监控同行直播数据并窃取用户资料。调查显示，这些公司不仅窃取基础联系方式，还通过类型化和标签化的方式对用户进行数字画像。比如启科科技有限公司将用户划分为 9 类，设置多达 3800 个个性化标签，关联的互联网网站数量超过 2 亿个，品牌类型也涵盖 6 万个互联网品牌及 2000 个手机品牌，每日处理数据量达百亿条，将用户的工作、生活等习惯数据商业化。调查还指出，通过接入运营商后台实时数据，启科科技有限公司非法获取拨打 400 电话或访问特定网站用户的手机号码，并以每条约 6 元人民币的价格对外售卖，构建所谓“精准获客”服务。

来源：“央视新闻”微信公众号

https://jingji.cctv.com/2025/03/15/ARTIaF2Ob26FiBOhi4qJDsVd250315.shtml

4. 上海启动“清朗浦江·2025”网络生态治理旬行动

时间：2025 年 3 月 20 日

2025 年 3 月 20 日，上海市委网信办联合市互联网业联合会、上海报业集团等单位在长宁区启动“清朗浦江·2025”网络生态治理旬行动。此次行动以“惠企为民，凝聚向上力量”为主题，重点针对涉企侵权信息、自媒体和 MCN 机构运营乱象、网络暴力、未成年人网络保护、网络金融信息乱象等五大领域开展专项整治。行动期间同步推出 40 多项主题日和平台开放日活动，全面展示上海网络生态治理成果。

来源：上海市政府网站

https://www.shanghai.gov.cn/nw15343/20250321/d2fa710ff41d4513a0cdc40687f64d57.html

5. 上海市网信办联合多部门整治“标题党”房地产类自媒体不实信息

时间：2025 年 3 月 25 日

2025 年 3 月 25 日，上海市网信办联合市房管局、市公安局网安总队等部门，对“锐哥经济思维”“上海珑铮新房”等 98 个违规自媒体账号实施阶段性禁言处置，并清理相关违法违规信息 900 余条。此次行动针对部分房地产类自媒体为博取流量，发布“上海市中心房价要崩了”等不实标题党信息，扰乱市场秩序的行为。

约谈指出，当前上海房地产市场总体呈现回稳向好态势，1-2 月商品住房市场“淡季不淡”，3 月上旬新增购房委托量等指标已回升至 2023 年以来高位。相关部门要求自媒体严格遵守《网络信息内容生态治理规定》等法规，不得发布虚假交易信息、编造涨跌数据，严禁以“房价暴跌”等煽动性标题制造恐慌。

来源：“网信上海”微信公众号

https://mp.weixin.qq.com/s/JzfnwHWQ7PNaJHmSS_XufA

6. 四部门联合开展 2025 年个人信息保护系列专项行动

时间：2025 年 3 月 28 日

2025 年 3 月 28 日，中央网信办联合工业和信息化部、公安部、市场监管总局发布公告，宣布将针对六类重点问题开展个人信息保护专项行动。此次行动聚焦 App、SDK、智能终端等常用服务产品，以及公共场所人脸识别、线下消费等生活场景中的个人信息保护问题。专项行动重点整治内容包括：App 未提供个人信息收集规则或超范围收集信息；SDK 违规调用非必要权限；智能终端违法违规收集使用个人信息；公共场所违法违规收集使用人脸识别信息；线下消费场景违法违规收集使用个人信息；以及网络借贷、求职招聘等领域的个人信息违法犯罪活动。相关部门将对拒不整改的行为依法从严处理，并根据实际需要动态调整治理重点，切实保障公民个人信息安全。

来源：中国网信网

https://www.cac.gov.cn/2025-03/28/c_1744867353112759.htm

域外案例

1. 英国 ICO 启动对 TikTok 等平台针对儿童隐私保护的调查

时间：2025 年 3 月 3 日

英国信息专员办公室（ICO）近日宣布对 TikTok、Reddit 和 Imgur 三家社交媒体平台展开调查，重点关注其对英国儿童用户个人信息的保护措施。此次调查是 ICO 推动企业落实儿童在线隐私保护工作的重要组成部分，旨在评估相关平台是否违反数据保护法规。

调查重点包括：TikTok 平台对 13-17 岁英国青少年个人信息的算法推荐使用情况；Reddit 和 Imgur 平台的年龄验证措施实施情况。信息专员 John Edwards 强调，社交媒体平台必须严格遵守数据保护法，绝不能以牺牲儿童隐私为代价获取商业利益。自 2021 年《儿童守则》实施以来，ICO 已推动 X 平台、Sendit 等多家企业改进儿童隐私保护措施，包括停止向未成年人展示广告、关闭地理位置共享默认设置等。

来源：英国信息专员办公室网站

https://cy.ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/02/investigations-announced-into-how-social-media-and-video-sharing-platforms-use-uk-children-s-personal-information/

2. 西班牙数据保护局对西甲联盟未能执行 DPIA 处以 100 万欧元罚款

时间：2025 年 3 月 8 日

西班牙数据保护局（AEPD）公布 PS/00484/2023 号处罚决定，对西甲联盟（LaLiga）处以 100 万欧元罚款。该处罚针对西甲联盟在足球场实施生物识别门禁系统前未按要求进行数据保护影响评估（DPIA），违反了《通用数据保护条例》（GDPR）第 35 条规定。

AEPD 在裁决中指出，生物识别系统对公民基本权利和自由具有高度侵入性，必须事先进行 DPIA 以评估相关风险。根据处罚决定，西甲联盟需在完成有效 DPIA 前暂停生物识别数据处理，并将此要求通知其关联机构。该案源于西班牙体育反暴力委员会要求球场使用生物识别门禁系统后收到的多起投诉。AEPD 强调，即便是基于安全考虑的数据处理，也必须严格遵守 GDPR 规定的评估程序。

来源：DataGuidance 官网

https://www.dataguidance.com/node/642899

3. 纽约州总检察长就数据泄露事件对多家保险公司提起诉讼

时间：2025 年 3 月 10 日

2025 年 3 月 10 日，纽约州总检察长宣布已向纽约州最高法院提起诉讼，指控 National General Holdings Corp.等 10 家保险公司因数据泄露事件违反《普通商业法》和《纽约州行政法》。该事件导致近 20 万消费者个人信息泄露，其中包括约 16.5 万纽约州居民。

总检察长认为，这些公司在第一次数据泄露后未及时向受影响用户和相关纽约州政府机构发出通知，违反了州的数据泄露通知法。同时，这些公司在数据安全方面存在严重不足，包括行政和技术防护措施不到位、访问控制薄弱、对安全事件缺乏有效监测和响应机制等问题。总检察长要求法院禁止这些公司继续违反纽约州法律，责令公司向受影响居民发出合规通知，并按每项违规行为处以 5000 美元民事罚款。

来源：纽约州总检察长办公室网站

https://ag.ny.gov/press-release/2025/attorney-general-james-sues-national-general-and-allstate-insurance-failing

4. 卢森堡法院维持对亚马逊非法数据处理行为处以 7.46 亿欧元罚款的决定

时间：2025 年 3 月 18 日

2025 年 3 月 18 日，卢森堡行政法院作出裁决，维持国家数据保护委员会（CNPD）2021 年对亚马逊欧洲核心公司（Amazon Europe Core S.àrl）处以 7.46 亿欧元罚款的决定。该处罚针对亚马逊基于兴趣的广告目的处理个人数据时，违反《通用数据保护条例》（GDPR）多项规定的行为。

法院认定亚马逊存在三项主要违规：未建立合法数据处理基础、未履行透明度义务、侵犯用户数据主体权利。具体表现为未向用户充分告知数据处理情况，且未保障用户访问、更正、删除及反对处理个人数据的权利。尽管亚马逊于 2021 年 10 月提出上诉，法院经审理后驳回其全部诉求，该裁决仍可被进一步上诉。

来源：卢森堡国家数据保护委员会网站

https://cnpd.public.lu/en/actualites/national/2025/03/amazon-decision.html

5. 英国 ICO 对 Advanced 公司数据泄漏事故处以 307 万英镑罚款

时间：2025 年 3 月 27 日

英国信息专员办公室（ICO）近日宣布对软件供应商 Advanced Computer Software Group Ltd 处以 307 万英镑罚款，因其未能有效保护客户个人信息导致数据泄露事件。该处罚源于 2022 年 8 月 Advanced 子公司遭受的勒索软件攻击，事件导致 79,404 人个人信息泄露，其中包括 890 名居家护理人员的敏感信息。ICO 调查发现，Advanced 存在多项安全漏洞：未全面实施多因素认证（MFA）、缺乏系统漏洞扫描及补丁管理不足。信息专员 John Edwards 强调，处理敏感医疗信息的组织必须采取更严格的安全措施。尽管 ICO 最初拟处罚 609 万英镑，但考虑到 Advanced 事后积极与 NCSC、NHS 等机构合作

降低风险，最终罚款金额减半。ICO 同时发布安全指南，敦促所有组织全面实施多因素身份验证等防护措施，以应对日益严峻的网络威胁。

来源：英国信息专员办公室网站

https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/03/software-provider-fined-3m-following-2022-ransomware-attack/

6. 苹果公司因滥用支配地位被法国竞争管理局罚款 1.5 亿欧元

时间：2025 年 3 月 31 日

内容概览：

法国竞争管理局 3 月 31 日宣布对美国苹果公司处以 1.5 亿欧元罚款，原因是该公司滥用其在设备定向广告中的主导地位。法国竞争管理局指出，苹果公司于 2021 年 4 月发布“应用程序跟踪透明度”机制，宣称以保护个人数据为目标，但其实施方式“既无必要，也不适当”。该机制有偏袒苹果自身服务之嫌，损害了第三方应用程序利益。该机制使在 iPhone 和 iPad 上使用第三方应用程序流程变得过于复杂，显示了苹果对自身应用程序和第三方应用程序的“不对称”待遇，对小型应用程序发行商来说尤为有害。法国竞争管理局表示，此次处罚针对的是 2021 年 4 月至 2023 年 7 月之间苹果的违规行为。除罚金外，该局还要求苹果公司连续七天在其网站上发布该处罚决定的摘要。

来源：法国竞争管理局网站

https://www.autoritedelaconcurrence.fr/en/press-release/targeted-advertising-autorite-de-la-concurrence-imposes-fine-eu150000000-apple

实务研究

1. 论数据纠纷的可仲裁性

作者：金杜研究院-宁宣凤、刘迎

时间：2025 年 3 月 7 日

内容概要：

随着数字经济的快速发展，数据已成为关键生产要素，数据市场的扩大也带来了数据相关争议的显著增长。仲裁因其灵活、高效、保密和国际可执行性等特点，被认为更契合数据市场的纠纷解决需求。然而，仲裁作为一种替代性争议解决机制，其适用范围受到法律上的限制，数据争议是否可仲裁，关键在于争议本身的法律属性和是否符合《仲裁法》所规定的可仲裁事项。

文章围绕数据争议的可仲裁性展开系统分析，并对五类典型数据争议进行了适用性评估，包括：数据权益侵权、商业秘密纠纷、数据垄断、公共数据授权运营，以及个人信息侵权。仲裁在程序效率、保密机制等方面具有独特优势，尤其适应数据争议对时效性与信息保护的双重需求。目前，已有仲裁机构设立专门的数据仲裁机制，仲裁将在未来数据要素治理中发挥更积极作用。企业在开展数据业务时，可以结合自身业务特点，将仲裁列入数据纠纷的争议解决备选范畴。

来源：金杜律师事务所官网

https://www.kwm.com/cn/zh/insights/latest-thinking/the-arbitrability-of-disputes-over-data-issues.html

2. AI 开拓者指南：GenAI 产品应用 TIPs——从采购到使用（使用篇）

作者：金杜研究院-张逸瑞、张一凡

时间：2025 年 3 月 5 日

内容概要：

文章聚焦企业在使用生成式人工智能（GenAI）产品过程中的合规风险与管理要点。文章指出，企业在实际应用中面临商业秘密泄露、个人信息保护义务、生成内容（AIGC）侵权与权属不明、数据跨境传输等多重法律挑战。基于部署模式不同，企业在特定场景下可能被认定为个人信息处理者，需履行相关法定义务。

同时，文章结合实践提出应对建议，包括加强内容审查、明示授权机制、合同安排中明确 AIGC 权属与责任划分、强化数据分级管理与安全防控等。文章认为，企业应建立覆盖数据、人员与合同管理的内部制度，以实现 GenAI 产品的安全、合规使用，逐步构建起完整的风险防控体系，保障其商业可持续性。

来源：金杜律师事务所官网

https://www.kwm.com/cn/zh/insights/latest-thinking/guide-for-ai-practitioners-tips-for-deployment-of-genai-applications.html

3. 中国药品试验数据保护新规——鼓励创新与规范仿制

作者：葛永彬、董剑平

时间：2025 年 3 月 25 日

内容概要：

2025 年 3 月，国家药监局发布《药品试验数据保护实施办法（试行）》及配套工作程序，标志着我国药品试验数据保护制度进入实质落地阶段。新规以“鼓励创新、规范仿制”为核心导向，确立了按药品创新程度设定差异化保护期的分类保护机制，采用“不受理、不批准”的行政措施直接赋予数据保护效力，并创新性引入“境外已上市、境内未上市”药品的动态保护期算法及首

仿激励规则。在保护内容方面，仅限于申请人提交的“自行取得、未披露”的完整试验数据，明确排除常规 BE 和免疫原性数据，强化了数据合规管理的边界。

制度设计兼顾原研药保护与仿制药可及，有望推动我国医药产业从“仿制主导”走向“创新驱动”。对企业而言，新规释放出强化药品数据合规性管理、重塑产品管线保护策略的明确信号。原研企业应提前布局核心试验数据的合规留存与披露控制，争取最大化数据保护利益；仿制药企业则需关注数据保护期动态变化，优化首仿策略，合理安排上市路径与审评节奏。新规不仅是知识产权规则的制度补强，更为医药企业提供了政策确定性与竞争路径指引。

来源：中伦律师事务所官网

https://www.zhonglun.com/research/articles/54330.html

4. 从竞争法角度看商用 AI 训练中的创新性对合法标准的影响——以美国判例汤森路透诉 Ross 公司侵权案为视角

作者：陈志军、陆勇洲

时间：2025 年 3 月 28 日

内容概要：

生成式人工智能采集数据进行模型训练，通过数据训练达到自主生成内容的目的，是当代科技创新的产物。本文围绕“AI 技术创新与数据持有权益的冲突”问题展开，聚焦生成式人工智能（GenAI）在数据采集和模型训练过程中的合法性边界，探讨如何在保护数据权益与促进技术创新之间取得平衡。文章以 2025 年美国特拉华州“Thomson Reuters 诉 Ross 公司”AI 数据侵权案为分析起点，指出法院在判断数据使用行为是否合法时，特别强调 AI 产品的“变革性”与其对原数据持有方市场的“潜在影响”，将其纳入不正当竞争审查视角。

在对比中美竞争法框架后，文章指出我国当前相关法律对数据采集仍以“合法来源、合法使用”为基本要求，但亦在实践中展现出对 AI 创新的包容审慎态度。结合现行立法与判例趋势，作者建议在反不正当竞争法中引入“技术创新缓冲空间”与“安全港”规则，对不直接损害市场秩序、具有创新性和公益性的数据使用行为给予有条件豁免，以推动 AI 技术与市场竞争的协调发展。

来源：中伦律师事务所官网

https://www.zhonglun.com/research/articles/54346.html

数字科技产品发展

1. 中国创业公司 Monica 发布全球首款通用型 AI Agent 产品 Manus

发布企业：Monica

时间：2025 年 3 月 6 日

内容概要：

2025 年 3 月 6 日，中国创业公司 Monica 正式发布全球首款通用型 AI Agent 产品 Manus。该产品在 GAIA 基准测试中取得 SOTA（State-of-the-Art）成绩，性能超越 OpenAI 同层次大模型。Manus 具备独立思考、规划并执行复杂任务的能力，能够直接交付完整成果，包括简历筛选、旅行规划、财务分析等多样化工作场景。

产品演示显示，Manus 可解压文件、异步处理任务、生成电子表格，并具备持续学习能力。目前该产品处于内测阶段，邀请码在二手平台被炒至 5 万元。Manus 由 Monica 公司开发，该公司创始人肖弘曾推出"壹伴助手"等产品，2022 年转型 AI 领域。业内预测 2025 年将成为 AI Agent 商用爆发年，谷歌、微软等科技巨头也已布局相关产品。

来源：央视网

https://news.cctv.com/2025/03/07/ARTIc3pdLCxmYpVt5ZLamBL1250307.shtml

2. 谷歌发布 Gemma 3 开源模型系列支持单 GPU 部署与多模态推理

发布企业：谷歌

时间：2025 年 3 月 12 日

内容概要：

2025 年 3 月 12 日，谷歌正式发布 Gemma 3 开源模型系列，包含 1B、

4B、12B 和 27B 四种参数规格，专为单 GPU 或 TPU 设备优化设计。Gemma 3 在 LMArena 人工评估中性能超越 Llama3-405B、DeepSeek-V3 等模型，支持 140 种语言处理、12.8 万 token 上下文长度及视觉推理能力，并首次提供量化版本以降低计算资源需求。该系列集成多模态理解功能，可分析图像、文本及短视频内容，同时支持函数调用实现自动化工作流。开发者可通过 Google AI Studio、Hugging Face 等平台获取模型，并依托 NVIDIA GPU、Google Cloud TPU 等硬件获得优化性能。

来源：谷歌网站

https://blog.google/technology/developers/gemma-3/

3. 智元机器人发布全球首个通用具身基座模型，珠海加速打造具身智能产业高地

发布企业：智元机器人

时间：2025 年 3 月 14 日

内容概要：

2025 年 3 月 14 日，智元机器人在珠海发布全球首个通用具身基座模型“智元启元大模型”（Genie Operator-1），并同步推出新一代人形机器人“灵犀 X2”。该模型具备强大的泛化能力，支持多机器人部署与持续学习，标志着具身智能向通用化、开放化方向迈出关键一步。发布会同期，珠海市联合华发集团等合作方启动“科技+好房子、康养、安防、泛零售”四大行业模型，推动具身智能在多场景中的应用落地。同时，珠海具身智能创新中心正式揭牌，将通过“一中心三平台”布局，打造涵盖供应链、应用示范、公众体验和人才生态的全链条产业支撑体系。

本次发布标志着珠海在人工智能与机器人产业领域的生态构建与技术集成进入新阶段。通过引入头部企业和高端人才，珠海正加速形成以“场景驱动+技术集成”为核心的具身智能产业高地，为中国乃至全球 AI 机器人技术发

展注入新动能。

来源：“珠海发布”微信公众号

https://mp.weixin.qq.com/s/kM2xDXVhGdAERgkdHVlYZQ

4. 腾讯发布混元 T1 正式版，推理能力达业界领先水平

发布企业：腾讯

时间：2025 年 3 月 21 日

内容概要：

2025 年 3 月 21 日，腾讯正式发布自研深度思考模型混元 T1 正式版。该模型采用创新的 Hybrid-Mamba-Transformer 融合架构，在 MMLU-PRO 基准测试中获得 87.2 分的优异成绩，仅次于行业领先的 o1 模型，在 CEval、AIME 等中英文知识及数学推理测试中同样表现优异。

混元 T1 具备三大技术突破：首先，作为工业界首个应用混合 Mamba 架构的超大型推理模型，显著降低了传统 Transformer 结构的计算复杂度；其次，通过专项优化实现解码速度提升 2 倍，大幅提高响应效率；第三，在超长文本处理方面展现出独特优势，有效解决长文推理中的上下文丢失问题。目前该模型已在腾讯云平台上线，定价为输入每百万 tokens1 元，输出每百万 tokens4 元，即将在腾讯元宝产品中灰度上线。

腾讯表示，混元 T1 已展现出强大的任务适应性，能够高效完成对齐任务、指令跟随任务和工具利用任务，标志着腾讯在大模型推理能力领域取得重要突破。企业用户现可通过腾讯云官网申请产品试用。

来源：“腾讯混元”微信公众号

https://mp.weixin.qq.com/s/38ilIogkFK8tbgRFDSXdSw

5. 深度求索发布 DeepSeek-V3-0324 大模型，代码能力对标 Claude 3.7

发布企业：深度求索

时间：2025 年 3 月 24 日

内容概要：

2025 年 3 月 24 日，中国人工智能初创公司深度求索（DeepSeek）正式发布 DeepSeek-V3 系列新版本 DeepSeek-V3-0324。该版本参数量达 6850 亿，在代码、数学和推理能力方面实现显著提升，其中代码生成能力已追平美国 Anthropic 公司最新发布的 Claude 3.7 模型。

据官方介绍，DeepSeek-V3-0324 具备三大核心升级：代码能力方面可一次性生成 800 行无错误的网页代码;数学与逻辑推理能力接近专业模型水平，能解决经典"4 升水壶问题"及 AIME 2025 竞赛题；采用 MIT 开源许可证，允许自由修改和商业化应用。清华大学教授沈阳指出，此次更新不仅展示中国 AI 技术实力，更为传言中的 DeepSeek-R2 或 V4 等重大版本发布奠定基础。该模型发布正值美国对华 GPU 出口限制背景下，其开源策略或将推动全球 AI 生态格局变化。

来源：深度求索官网

https://api-docs.deepseek.com/zh-cn/news/news250325

6. 昆仑万维发布全球首款音乐推理大模型 Mureka O1，引领 AI 音乐迈入个性化时代

发布企业：昆仑万维

时间：2025 年 3 月 26 日

内容概要：

2025 年 3 月 26 日，昆仑万维正式发布 Mureka O1 与 V6 两款 AI 音乐大模型。其中 Mureka O1 作为全球首款音乐推理大模型，采用自研 MusiCoT 技术，首次在音乐生成领域引入思维链（CoT）方法，在发音清晰度、乐段准确率等关键指标上超越行业标杆 Suno V4，实现中国 AI 音乐技术的全球领跑。

Mureka 系列模型具备三大创新突破：支持 10 种语言音乐创作及音色克隆功能，用户可上传声音样本生成个性化作品；通过自研 ICL 技术显著提升声场表现和人声质感；全球首次开放 API 服务与模型微调功能，开发者可基于私有数据训练专属音乐模型。目前该产品已覆盖全球 100 多个国家和地区，其开放生态战略将推动 AI 音乐创作进入个性化时代。

来源：“昆仑万维集团”微信公众号

https://mp.weixin.qq.com/s/1JPYXUwX-1JAVpz3IgygtQ

7. OpenAI 发布 GPT-4o 图像生成功能，多模态 AI 迈入实用新阶段

发布企业：OpenAI

时间：2025 年 3 月 25 日

内容概要：

2025 年 3 月 25 日，OpenAI 正式发布 GPT-4o 原生多模态图像生成功能，该功能将作为 ChatGPT 默认图像引擎，即日向 ChatGPT Free、Plus 等用户开放。此次升级突破三大技术边界：首次实现图像内文字精准渲染，可生成 logo、菜单等专业设计；支持单次处理 10-20 个对象的复杂构图；通过人类反馈强化学习（RLHF）优化，显著提升多轮交互的视觉一致性。

GPT-4o 图像生成采用 C2PA 元数据标识技术保障内容可追溯，同时建立内部检测工具防范滥用风险。尽管在非拉丁字符呈现、大尺寸图像裁剪等方面仍存在局限，但其在商业设计、科普插画等场景的实用表现已超越前代

DALL-E3。该功能后续将扩展至企业版及 API 接口，标志着 OpenAI 在多模态生成领域取得重要突破。

来源：OpenAI 网站

https://openai.com/index/introducing-4o-image-generation/