



端侧大模型迎来发展政策东风 专家建议

在技术创新与隐私安全之间寻求平衡

□ 本报记者 张维

人工智能热浪持续涌动。今年初,DeepSeek模型凭借其卓越的推理效率与开源生态成为中国自主创新的重要标杆;宇树科技舞蹈机器人亮相春晚,成就人工智能佳话;在刚刚闭幕的全国两会上,《政府工作报告》多次提及“智能”一词,“大模型”则首次被写入,众多代表委员为人工智能产业发展及相关制度政策完善建言献策。

“中国已经成为全球人工智能专利的最大拥有国。”国家知识产权局局长申长雨近日表示,国家知识产权局将进一步加强人工智能知识产权保护,推动建立人工智能大模型领域专利池,助力人工智能企业创新发展。

随着人工智能大模型的快速发展及普及应用,尤其是那些与老百姓关系密切的端侧大模型(即在用户设备端,如智能手机、物联网设备等上运行的AI模型)的兴起,与之相关的隐私与安全等新挑战,也浮出水面。对外经济贸易大学法学院教授张欣告诉《法治日报》记者,如何在技术创新与隐私安全之间寻求平衡,如何协调用户体验与数据安全的关系,如何构建负责产业生态,是当下需要关注的问题。

科技创新为产业注入活力

支持大模型广泛应用,大力发展人工智能手机和电脑等,被写入了今年的《政府工作报告》。这也是“人工智能手机和电脑”第一次进入《政府工作报告》。

过去的一年,是人工智能手机大规模布局的第一年。为此,2024年,亦被誉为“AI手机元年”。

只需要说一句话,AI就可以直接操作你的手机屏幕下单一杯咖啡,口味还是你喜欢的,因为它知道你常用的外卖软件、你常喝的咖啡口味,并通过手机定位找到离你最近的店铺下单。

图片美化做得也是如此贴心便捷。AI手机可以直接从拍照之前的AI场景识别,对主体识别到拍

核心阅读

应充分利用现有法律资源,区分近期和中远期处理方式,综合运用技术和制度政策等多种手段促进端侧大模型规范发展。



摄时的AI图像处理,再到后期的AI闭眼修发、AI路人消除,AI一键美颜全面介入。

……

诸多优势使得AI手机备受青睐,许多厂商争先布局AI手机,开辟新的赛道。

数据显示,2024年我国智能手机出货量达2.8亿部,同比增长4.7%,预计2025年将进一步攀升至3.0亿部,AI技术渗透与换机需求释放成为关键驱动力。高端化与AI功能渗透成为增长引擎,例如搭载AI功能的机型在高端市场占比已超40%,推动平均售价提升约8%。

今年的AI手机在政策利好和技术加持下,势必

迎来新的一波发展热潮。从技术上而言,如张欣所说,“从Microsoft的Phi系列到DeepSeek-R1的重磅亮相,端侧大模型正以前所未有的速度迈向轻量化、高性能与低功耗的新阶段,DeepSeek等大模型的开源特性有效降低了产业准入门槛,为AI手机的普及奠定了坚实基础”。

国际知名会计师事务所德勤预计,今年有望迎来“换机潮”,到年底,人工智能手机出货份额将超30%。

“AI手机是大模型创新与应用的重要领域,大模型的快速发展为智能终端产业注入了新的活力。”中国信息通信研究院互联网法律研究中心主任何波在近日对外经济贸易大学举办的“边缘计算新纪元:端侧大型语言模型的应用、风险与治理前瞻”研讨会上说,应当看到端侧大模型在提升处理能力、改善用户体验方面的积极价值,这种创新探索值得肯定和鼓励。

数据安全风险持续增加

对于创新,要肯定,要鼓励,更要拿出实际行动保护。

“人工智能作为新兴领域,哪些技术需要保护,应采取什么策略进行保护,如何借助知识产权提升企业的竞争力,需要我们认真思考。”申长雨说。

为做好人工智能领域的知识产权保护,申长雨赴浙江调研了初创型科技企业知识产权保护工作,并举行了初创型科技企业知识产权保护工作座谈会,听取企业有关意见和建议。

对于相关技术的迅速演进与创新部署所带来的一系列治理挑战,也要做好积极应对。

北京航空航天大学法学院副教授赵精武发现,各手机厂商纷纷推出智能助手升级版,增加了精准搜索、跨设备操作等功能。然而,这些创新也伴随着隐私风险。他举例说,一些AI手机系统中默认开启的“增强视觉搜索”功能虽有隐私保护功能,但仍可能在处理照片过程中泄露敏感信息。

“未来数据安全风险将持续增加。”赵精武说,整个生态链中参与主体众多,包括手机厂商、应用开发者和第三方服务提供商,各方在数据收集、使用、共享过程中尚未形成明确的责任边界。手机厂商作为硬件和操作系统提供者,具有获取基础用户数据的先天优势,能够收集用户的操作系统版本、设备型号以及使用习惯和位置信息;应用开发者则关注用户的浏览历史、点赞评论等行为数据,实现定制化推送;第三方服务提供商则可能大量接触用户语音类数据,为实现定制化服务进行数据分析。

用户数据权限获取的必要性界限模糊问题,在赵精武看来需要特别注意。尤其是,随着人机交互内容可能被用作模型训练数据,其中将包含更多敏感个人信息。

在北京大学法学院副院长戴昕看来,端侧大模型所面临的数据安全和隐私保护问题本质上是传统问题的量级扩大,而非全新挑战。“我们在既有网络环境中面临的数据安全和保护问题,例如过度收集、权限滥用、隐蔽教育、云端数据传输风险在端侧大模型时代只是变得更加严重和复杂,解决难度更高。”

中国社会科学院法学研究所副研究员唐林森认为,端侧大模型环境下数据保护机制存在三大缺陷:首先,知情同意更加流于形式,因为AI手机对数据的采集和处理完全无孔不入且实时进行,通常通过一次性授权实现一揽子权限获取;其次,数据授权机制中存在多方主体责任划分不清问题,风险出现时可能相互推诿;第三,用户权利难以实现,特别是当数据用于模型训练时,用户实际上无法知晓数据使用情况,也无法实现定向删除,使得个人信息保护法规定的查阅删除权形同虚设。

多种手段促进规范发展

关于AI手机带来的风险,一个形象的比喻,“普通用户可能把手机视为一个上锁的笔记本,而无障

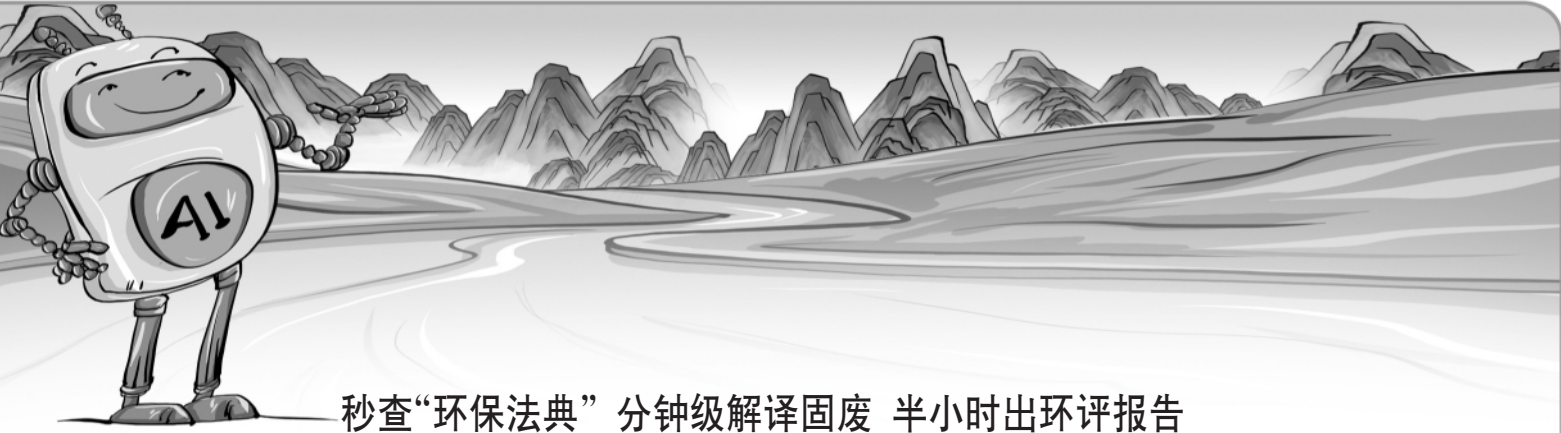
碍权限的开启相当于将所有抽屉一次性全部打开,这远超出了用户的合理预期。”中国人民大学法学院教授,未来法治研究院副院长丁晓东说。

针对未来监管趋势,赵精武预测平台规则将表达得更加显著,提示将做得更加到位,以确保符合个人信息保护法要求。“随着个人信息合规审计新规出台,手机应用合规审计将更加关注最小必要原则、业务相关性、用户知情权、禁止强制捆绑以及动态申请等要求。特别是高敏感权限(如剪贴板、通知栏监听)、非主动用户行为弹窗和权限撤销功能将成为审计重点。”赵精武说。

端侧大模型不仅涉及个人信息保护问题,还关系到更广泛的内容安全与数据安全。“如果硬件部署的大模型能够调动手机内的个人信息和数据,这种风险将超越个人层面,对整体数据安全构成威胁。”丁晓东说。

丁晓东建议,在支持人工智能发展的同时确保安全与合规:第一重授权是应用厂商层面,端侧大模型必须首先获得应用厂商的明确授权或许可;第二重授权是用户层面。丁晓东强调必须获得用户明确授权,且应采用“选择加入”而非“默认启用”的机制,授权应当非常明确,用户必须主动参与决策过程。还需要建立合同之外的保障,不能让用户一揽子授权后,因信息融合导致隐私侵扰或个人信息泄露。

何波认为,要统筹好守正与创新的关系。端侧大模型并非完全“裸奔”,现有法律法规已对相关安全问题有所规定,也同样适用于AI手机监管。例如,网络安全法、数据安全法、个人信息保护法都为监管端侧大模型提供了法律依据,今年1月1日起施行的《网络数据安全管理条例》进一步对涉及自动化工具、生成式人工智能等新兴技术的数据处理活动作出特殊规定,因此应充分利用现有法律资源,区分近期和中远期处理方式,综合运用技术和制度政策等多种手段促进端侧大模型规范发展。



秒查“环保法典” 分钟级解译固废 半小时出环评报告

人工智能在生态环境监管领域“大显身手”

全面推进美丽中国建设

□ 本报记者 张维

秒查“环保法典”,追踪“历史病历”,智能识别固体废物倾倒线索,环评报告表编制时间缩短至30分钟左右……

记者近日从生态环境部获悉,DeepSeek等人工智能技术正在为生态环境部门守护绿水青山装上“智慧大脑”,在生态环境监测、执法、环评、宣教等领域“大显身手”,全方位赋能生态环保。

智能识别违法线索

有了AI智能识别固体废物倾倒线索,解译耗时已缩短至“分钟级”。

据了解,非法倾倒、堆存的固体废物,占地面积通常在几十至几千平方米之间,属于典型的小尺度目标。根据最小成像单元原理,这些目标只能通过高分辨率卫星影像进行识别,而高分辨率卫星影像谱段数量普遍较少,限制了固体废物光谱特征分析潜力,一定程度上增加了解译难度。

同时,在“清废行动”前,相对于生态、水、大气等环境监测领域,固体废物识别属于新兴领域,相关研究应用较少,现成的技术方法和应用示例有限。为更加及时高效发现问题,生态环境部卫星环境应用中心(以下简称卫星中心)利用基于神经网络的语义分割算法SFE-YOLO等深度学习模型研究建立基于AI的固体废物物机交互解译技术方法,初步实现遥感影像处理、固体废物识别、问题图斑导出等自动化作业。

“通过不断优化解译规则,迭代解译算法,固体废物执法工作得以迈向智能化和高效化,解译耗时从‘小时级’缩短至‘分钟级’,解译准确度由长江经济带‘清废行动’的50%提升至黄河流域‘清废行动’的70%以上。”卫星中心有关负责人介绍说。

技术的进步在推动固废排查工作开展更加精准高效的同时,还能够促使地方从“被动接收”向“主动监管”转变。

2023年至2024年,辽宁省生态环境厅在全国范围内首创省级“清废行动”,联合卫星中心发挥遥感、GIS与信息化技术优势实现固废点位“排查—核实—整治—回头看”全过程的数字化、智能化管理。

2024年,山东省生态环境厅联合卫星中心研究构建面向山东特色的固体废物“AI+遥感”融合的人机交互识别技术方法,强化固体废物识别的针对性与准确性,提升排查效率。

环境问题“有迹可循”

AI对于执法监管的助力还不止于此。

AI能秒级锁定人类活动热源区,赋能海洋温排水遥感监测。国家海洋环境监测中心有关负责人说,借助包含标准文件、管理方法及核电、火电行业专业信息的知识库,以及基于知识图谱的智能检索系统,监测人员只需输入有效关键词即可秒级锁定引起温升的人类活动区域,彻底告别“翻资料半小时,找答案一分钟”的低效工作模式。“面向海洋生态环境保护的智能热源区快速定位,这种高效的工作模式有利于破解‘大海捞针’难题,准确掌握沿海热源分布。”该负责人说。

AI还能高效判别排水口。通过自动检索网络公开资源和接收人工投喂的精准专业信息,AI平台可全面总结分析电厂排水口的地理信息与图像特征。当监测人员输入影像时,AI助手可智能辅助识别进出水口特征,提供专业判断依据和分析结果,从而整合多源信息有效识别温排水入海途径。

在生态环境监测领域,AI也在扮演重要角色。针对标准查询繁琐、污染溯源低效、报告审核耗时等痛点,江苏省常州市环境监测中心近日尝试将DeepSeek-R1大模型与本地化Dify平台深度融合,打造三大“智能利器”。这三大“智能利器”分别是:

秒查“环保法典”。输入“监测站房巡检要求”“无组织排放标准”等模糊问题,AI自动匹配72份大气标准文件,精准定位条款并标注来源,解决“翻文件半小时,找答案一分钟”的难题。

追踪“历史病历”。例如,输入“钟楼国控站点问题”,AI瞬间调取200余份历史报告,结合气象、排放数据,5秒生成污染成因分析及整改建议,让环境问题“有迹可循”。

智检“监测报告”。上传监测报告,AI自动揪出“错别字、单位错误、逻辑漏洞”,还能主动建议补充数据分析,审核效率提升70%,报告质量显著提高。

广东省深圳生态环境监测中心站此前完成DeepSeek 671B大模型的本地化部署,其开发的“监测智能助手矩阵”涵盖四大核心模块,包括监测知识助手、业务培训助手、环境质量助手以及“深测”智能大屏助手。尤其值得一提的是,环境质量助手依托5年历史数据与12类智能分析模块,融合多模态生成技术与GraphRAG图谱,将环境质量报表报告编制从“小时级”压缩至“分钟级”。

环评报告30分钟出

让环评“拥抱”智能化手段,为生态环境治理体系和治理能力现代化建设注入全新活力,已成为各地开展环评改革工作的重要关注点。

数字乡村强农惠农富农专项行动启动

本报讯 记者刘欣 近日,中央网信办、农业农村部、商务部、中国人民银行联合印发《关于开展数字乡村强农惠农富农专项行动的通知》(以下简称《通知》),在浙江省、安徽省、福建省、山东省、河南省、重庆市、四川省、陕西省等8个重点省(市)部署开展数字乡村强农惠农富农专项行动。

《通知》明确了行动目标,通过两年左右时间,重点省(市)数字乡村建设取得突出进展。农业生产信息化水平进一步提升,乡村新产业新业态持续壮大,农村网络零售额稳步增长,城乡数字鸿沟加速弥合,基本公共服务更加均质可及,乡村治理效能显著提高,农村集体经济和农民实现“双增收”,带动全国数字乡村发展迈上新台阶。重点省(市)结合所辖县(市、区)经济基础、资源禀赋、参与意愿等实际情况,确定纳入专项行动范围的县(市、区)比例。

《通知》部署了6项重点任务。一是大力推进智慧农业发展,包括积极打造智慧农业发展高地,加快5G

与智能农机深度融合等内容。二是培育壮大新产业新业态,包括深化“数商兴农”,因地制宜发展乡村新业态,开展乡村旅游数字提升行动等内容。三是建强乡村数字基础设施,包括按需推进农村5G网络和千兆光网建设,完善农村寄递物流体系等内容。四是深化数字惠农便民服务,包括构建线上线下相结合的乡村信息服务体系,深化实施金融科技赋能乡村振兴示范工程等内容。五是打造智慧乡村治理体系,包括推进涉农数据汇聚共享和开放开发,深化整治“指尖上的形式主义”,切实为基层减负赋能等内容。六是拓宽农民增收致富渠道,包括进一步完善联农带农机制,有效增加农民经营性收入,因地制宜发展新型农村集体经济等内容。

下一步,中央网信办将会同有关部门,重点省(市)建立完善工作机制,加强政策支持、人才保障、跟踪监测和宣传推广,营造各地互学互鉴、共促共进的良好氛围。

中国人民银行部署2025年金融法治工作

本报讯 记者李立娟 近日,中国人民银行召开2025年金融法治工作会议。会议深入贯彻党的二十届三中全会和中央经济工作会议精神,按照中国人民银行工作会议部署,总结工作,分析问题,研究部署2025年金融法治工作。

会议认为,2024年中国人民银行不断提升依法行政水平,加快推进金融领域重点立法修法,金融稳定法草案经全国人大常委会第二次审议,反洗钱法完成修订。出台《中国人民银行行政处罚裁量基准适用规定》,修订行政许可事项清单,依法合规开展执法检查检查和行政处罚。认真贯彻落实新修订的行政复议法,依法开展行政复议应诉,扎实做好法律顧問、法治研究和普法宣传,为中央银行高效履职提供坚强法治保障,有力支持金融服务实体经济和防范化解金融风险。

会议要求,做好金融法治工作,全面深化法治央行建设,要坚持和加强党的领导,加快完善金融法律法规体系,推进修订中国人民银行法,配合金融稳定法后续审议工作。持续完善依法行政制度,提升行政执法规范性有效性,坚持“过罚相当”,依法实施行政处罚。依法高效办理行政复议应诉案件,做好法律服务保障,提高法治研究对中心工作的支持,巩固拓展金融普法宣传,锻造忠诚干净担当的高素质专业化法治人才队伍。

当前正值春耕备耕时期,安徽省阜南县公安局森林大队、县农业综合执法大队联合开展种子、化肥和农药等农资产品检查,严防假冒伪劣产品流入市场,筑牢春耕生产“第一道防线”。因为近日阜南县公安局森林民警联合农业执法人员在该县田集镇一农资销售点检查农资产品。

本报通讯员 吕乃明 摄