责任编辑:杨召奎 张才
E-mail:grrbjjxwb@sina.com
工人日报

互联网从业者直言:办公室里一半人在聊“养龙虾”,一半人在学怎么“养龙虾”

“养龙虾”热潮之下,如何守好安全底线?

本报记者 秦亦姝

“最近办公室里,一半人在聊‘养龙虾’,一半人在学怎么‘养龙虾’。”3月13日,北京某互联网公司产品经理李垚告诉记者,同事们热议的“养龙虾”,并非现实生活中的水产养殖,而是对近期发布的开源AI智能体框架OpenClaw的个性化训练与部署。

因为图标是一只红色龙虾,OpenClaw被大家称为“龙虾”。与普通AI不同,它能够通过整合调用通信软件和大语言模型,在用户电脑上自主执行文件管理、邮件收发、数据处理等复杂任务。

这只“龙虾”为何能掀起全民热潮?“养龙虾”又有哪些安全风险?《工人日报》记者对此展开了调查采访。

多地出台“龙虾”的相关支持政策

作为今年开年第一个引起全民关注的AI智能体,“龙虾”究竟有何特殊之处?

“普通AI的核心模式是对话式,用户提问后仅能得到答案或操作步骤,而‘龙虾’是典型的‘行动派’。用户只需提出任务目标,它便能直接操作各类工具完成整个流程。”曾就职于一线互联网大厂的科技博主“跟着阿亮学AI”向记者举例说,如果让其整理重要邮件,它会自动打开邮箱、筛选内容并撰写回复草稿,“全程无需用户动手”。

北京大学AIIT数字创意实验室AI工程师于静雯表示:“与ChatGPT等大语言模型不同,OpenClaw并非简单的聊天机器人,而是一个能够获得本地操作系统权限、调用各种工具、并按照自然语言指令规划步骤、自动执行复杂任务的‘数字员工’。”

“以往的AI大模型即便技术再成熟,也始终局限于各自的领域,无法实现跨领域的协同运作,而‘龙虾’的核心优势在于其打通了不同领域的大模型壁垒,真正调动起所有大模型的功能与价值。”于静雯解释道,“因此,可以说OpenClaw对于AI行业来说,是具有桥梁性、纽带性的颠覆性创新。”

热潮之下,不少地方积极响应。据不完全统计,截至3月12日,深圳龙岗区、无锡高新区、合肥高新区、苏州常熟市、南京栖霞高新区、杭州萧山区等多地出台“龙虾”的相关支持政策,还有一些地方政府推出面向公众的“小龙虾”免费部署服务。

“龙虾”暗藏多重安全隐患

全民“养虾”的热情之下,第一批尝试者的体验却并非都是好评。

“整体来说感觉不如网上宣传得那么神奇。”李垚坦言,用好“龙虾”需要开放电脑上各类应用的控制权限,出于谨慎,他没有打开过多权限,因此觉得“效果有限”。

于静雯分析,OpenClaw的核心能力在于对各类应用、工具的操作与控制。而想要实现这一功能,使用者必须向其开放大量的应用授权,包括邮箱、办公软件、各类平台后台等。“这就好比你想请人把家打扫干净,就得把家里所有房间的钥匙交给对方。”她比喻道,相应地,全量的应用授权可能会给部署“龙虾”的个人和企业带来数据泄漏风险。

3月10日,国家互联网应急中心发布的《关于OpenClaw安全应用的风险提示》(以下简称《提示》)中明确指出,为实现“自主执行任务”的能力,该应用被授予了较高的系统权限。然而,由于其默认的安全配置极为脆弱,攻击者一旦发现突破口,便能轻易获取系统的完全控制权。

《提示》显示,截至目前,OpenClaw已公开曝出多个高中危漏洞,一旦这些漏洞被网络攻击者恶意利用,则可能导致系统被控、隐私信息和敏感数据泄露的严重后果。“对于个人用户,可导致隐私数据(如照片、文档、聊天记录)、支付账户等敏感信息泄露;对于企业,可导致核心业务数据、商业机密泄露,造成难以估量的损失。”于静雯分析说。

北京市汉鼎联合律师事务所执业律师周子川表示,为完成用户指令,“龙虾”在没有控制权限的情况下,可能在全网直接或间接收集大量各类数据,其获取数量、访问权限、数据敏感程度等,往往超出用户控制范围,严重的可能构成非法获取计算机信息系统数据罪、侵犯公民个人信息罪。

“此外,目前很多用户为了图便利,找第三方花钱部署‘龙虾’,但这些第三方未必具备安全防护条件,极易导致设备数据暴露,攻击者可通过恶意代码执行等方式远程控制设备,窃取敏感信息。”周子川补充道。

热潮之中,更需守好安全底线

今年的政府工作报告提出,深化拓展“人工智能+”,促进新一代智能终端和智能体加快推广,推动重点行业领域人工智能商业化规模化应用,培育智能原生新业态新模式。

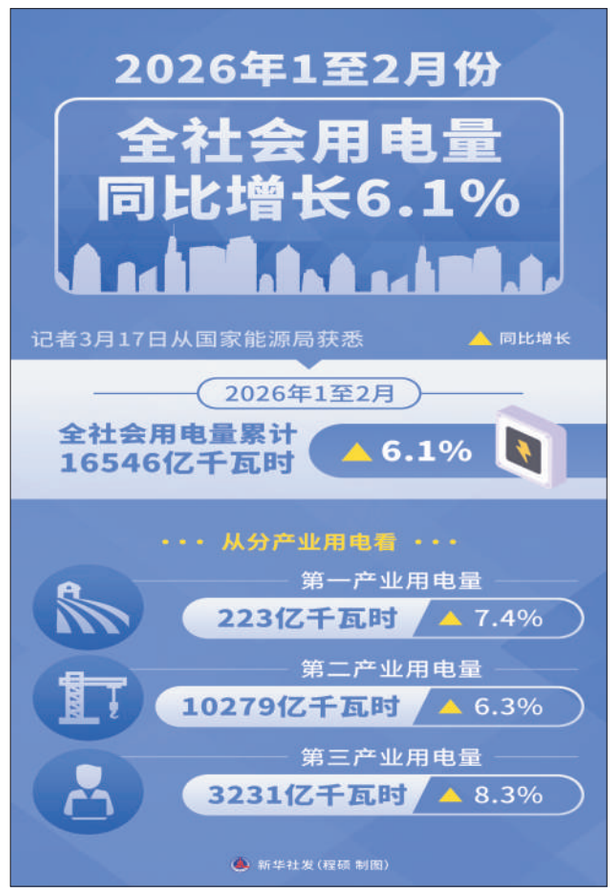
“‘龙虾’的出现,为AI智能体的落地应用提供了新路径。若能规范使用,就能很好发挥现有AI智能体的作用,大幅提升个人和企业的工作效率。”于静雯表示,推动“龙虾”良性发展,关键在于平衡便利与安全。

“‘龙虾’等AI智能体呈现出的新技术特征,使现有的关于AI的法律问题更加复杂。”周子川举例说,如最重要的“权责归属模糊”问题,当“龙虾”等AI智能体基于用户指令执行操作并造成侵权或其他违法违规行为时,开发者、部署者、使用者之间如何归责、确定责任的大小,需要法律进一步明确。

对于AI产品的开发者和服务提供者,周子川建议,一方面,应积极履行个人信息保护法等规定的合规义务,如数据处理日志满足日志留存和可追溯的要求。另一方面,在具体操作中也应增强法律合规意识,如加强AI权限管理、加强提示词审核等,降低安全风险。

国家互联网应急中心发布的《提示》也给出具体建议:相关单位和个人用户在部署和应用OpenClaw时,应对运行环境进行严格隔离,使用容器等技术限制OpenClaw权限过高问题,同时严格管理插件来源,持续关注补丁和安全中心。

“用户在‘养龙虾’前,首先要全面评估其价值与风险,判断自己是否真的需要它解决问题,再决定是否部署。”于静雯提醒,使用过程中,也务必做好数据分区和隐私保护,“不盲目跟风,将自己的隐私和数据安全暴露于风险之中”。



北京花粉防控加快向“科技赋能”转型

未来将采用机器人进行自动喷洒

本报讯 (记者徐新星 实习生曹硕)记者3月15日从北京市园林绿化局获悉,经市园林、气象部门专家结合北京市植物生长规律及未来气象条件综合研判,今年春季柏科花粉始期为3月8日左右,3月中旬前后将逐步进入散粉高峰期。为全力降低致敏花粉对市民日常生活的影响,北京市园林绿化局已经全面启动2026年全市致敏花粉综合防治工作,与气象、卫健、城管等部门建立联防联治机制,通过精准化防控、系统化治理、长效化建设的全链条举措,积极应对春季花粉高发挑战。

为实现精准施策、靶向防控,北京市园林绿化局依托第十次园林绿化资源普查数据,完成了五环内圆柏株数核算,并绘制形成“五环内圆柏密度空间分布图”,为防控作业提供精准的空间导航。经核查,五环内圆柏雄株16.8万株,重点分布区域集中在东城区天坛街道,西城区陶然亭街道、什刹海街道,海淀区四季青镇、海淀镇、东升镇,朝阳区小红门街道等区域,为后续分区域、分等级落实精准防控划定了核心范围。

据北京市园林绿化局科技处处长姜英淑介绍,2026年全市致敏花粉防治工作加快从“人海战术”向“科技赋能”转型。北京市园林绿化局联合在京科研院所持续推进花粉防治科技攻关,成功研发花粉固定剂、花粉控制剂等新型环保生物制剂,有效提升作业效率与防控精度。同时,持续总结推广成熟防控技术,逐步扩大科技防控覆盖范围。此外,该局同步下发《北京市花粉防治技术手册》,指导各区科学、精准开展综合防治工作。

未来,北京市园林绿化部门还将采用机器人进行自动喷洒,这是目前正在研发的一个项目,能够通过机器人夜间喷洒避开白天游人高峰期,达到防治效果,并减少人力、物力、财力消耗。

武汉:汉阳“双子塔”玻璃幕墙完工

本报讯 (记者张翀)日前,由中国铁建大桥局承建的湖北交投实业总部项目玻璃幕墙全面完工。该项目以190.5米和220米的高度,成为武汉市汉阳区在建第一“双子塔”高楼,为武汉城市天际线再添新地标。

武汉夏热冬冷的气候,使幕墙材料热胀冷缩效应明显,与超高层结构自身的变形叠加,极易影响密封性和结构安全。面对挑战,项目团队深入论证,优化方案,保障安全质量。

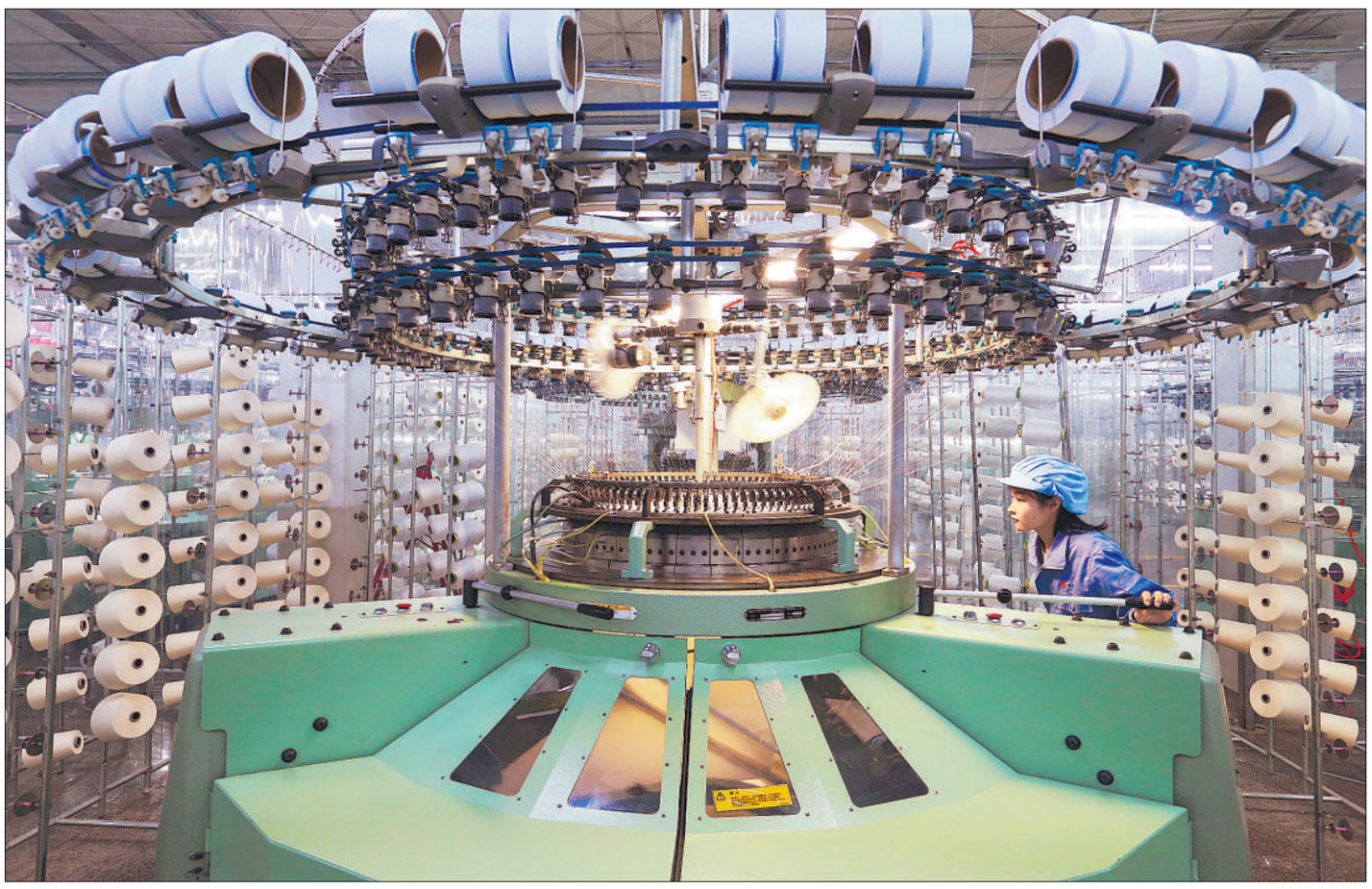
施工过程中,项目团队严格执行“自检、互检、专检”制度,对幕墙垂直度、密封性等关键指标进行全程监测。同时,积极运用“智慧工地”等信息化平台,推动安全管理数字化、可视化,实现了对现场作业风险的精准防控与高效监管。

秦皇岛:高端层压装备启运出海

本报讯 (特约记者朱润胜 通讯员王继军 李佳新)日前,由秦皇岛晟成自动化设备有限公司自主研发的全球首台(套)电磁加热多层层压机完成总装调试,顺利启运发往海外。

该设备可实现太阳能光伏电池组件进料、层压、出料全流程自动化连续生产,并能灵活组线,相关技术在行业内乃至全球均属首创,装备技术成果经评定为“国际先进”,成功入选河北省重点领域首台(套)重大技术装备目录。

公司总经理李硕鹏表示,此次设备发往海外,是我国高端层压装备首次以“全球首创”身份亮相国际市场,将带动我国光伏、新材料等产业链上下游协同出海。



开足马力 赶制订单

3月16日,山东青岛一家纺织企业,员工在生产出口海外市场的面料产品。

今年以来,青岛市即墨区的纺织服装企业一派忙碌景象,工人们开足马力赶制订单,抢抓生产,满足市场需求。

本报通讯员 梁孝鹏 摄

民营企业家谈AI赋能产业发展

“人工智能+”如何加出更多“强劲增量”?

本报记者 于灵歌 罗娟

今年的政府工作报告首次提出打造智能经济新形态,并提出“促进新一代智能终端和智能体加快推广”“支持人工智能开源社区建设”“实施超大规模智算集群、算电协同等新基建工程”等具体路径。

在3月6日举行的十四届全国人大四次会议经济主题记者会上,国家发展和改革委员会主任郑栅洁表示,将深化“人工智能+”行动,“十五五”末人工智能相关产业规模将增长到10万亿元以上。

智能经济的浪潮中,人工智能如何加速从“技术概念”转化为“现实生产力”?《工人日报》记者采访了3位民营企业家。

持续创新,深化应用场景

工业和信息化部部长李乐成3月5日在十四届全国人大四次会议首场“部长通道”上说,今年将大力推动“人工智能+制造”,深度挖掘高价值应用场景,培育一批高水平典型应用,打造一批特色智能体。

“要推动‘人工智能+制造’,对于传统制造业而言,持续创新和提升自身水平至关重要。”格力电器董事长董明珠代表表示。

董明珠代表介绍,格力电器坚持自主创新,自2016年起将人工智能技术引进到工业制造领域,如今拥有了“领航级”智能工厂。去年,格力电器自主研发的“AI动态节能科技”技术获评国际领先,目前已经成功应用到空调产品中,能为消费者带来更好的节能、舒适体验。

“人工智能与制造业的深度融合,有效提升了生产效率、制造精度,有利于推出高品质产品,满足消费者对美好生活的向往。”董明珠代表说。

不只是制造业,从教育到医疗,从办公到日常生活,AI正加速从“工具”向“伙伴”转变。

“多地实践已充分证明,AI技术可有效助力家庭医生优化履约管理、实现慢性病精准管理、为居民提供个性化健康服务。”科大讯飞董事长刘庆峰代表以AI在医疗场景的应用向记者举例说,“比如,承载着星火医疗大模型能力的‘讯飞晓医’APP越来越得到用户的认可。未来,我们将把大模型底座能力的突破转化为行业应用的领先优势,持续推动应用场景的拓展与深化。”

新业态新模式释放增长新动力

一人公司、智能体、人机协同……当前,人工智能催生了大量新业态、新模式,为经济增长注入了新动力。

技术突破首先带来工作场景的重构。“当前,AI正从根本上释放个体能力,带来生产力的跃升。”刘庆峰代表举例,科大讯飞也涌现出一批“超级团队”,团队仅凭1名产品经理加2名前端开发人员,就完成了专家评估需15人开发3个月的任务,日产10万行高质量代码。“AI能够让一个人完成过去一个团队才能做到的事。”他说。

刘庆峰代表认为,未来3至5年,AI将在数字内容、科研创新等领域持续催生AI训练师、行业解决方案专家、人机协同运营官、智能系统运维师、数据治理与安全专员等新岗位。“这些岗位高度依赖AI技术与行业经验的深度融合,其核心在于通过人机协同创造更高价值。”刘庆峰代表说。

360集团创始人周鸿祎委员表示,人工智能已从“大模型能力竞争”迈向“智能体规模应用阶段”。

“今年以来,智能体正在从概念走向实干。”周鸿祎委员认为,目前,大模型已进化成能干活的“数字员工”,每一秒都在消耗推理算力。随着百亿级智能体进入产业场景,推理算力的重要性日益凸显。他建议,优化推理算力布局,夯实人工智能产业发展底座。

加速成果转化,改善创新生态

工信部数据显示,2025年,我国人工智能核心产业规模超过1.2万亿元,企业数量超过6200家。推动人工智能这个“关键变量”成为经济高质量发展的“强劲增量”,还存在哪些堵点和挑战?

周鸿祎委员在调研中发现,智能体规模化落地仍面临一些挑战:技术转化门槛较高,安全保障能力不足,复合型人才储备不足。对此,他建议,平台集成模型与行业工具,提供全流程服务,支持中小企业低成本构建垂直领域智能体。同时,坚持“智能体技术普惠+懂AI懂业务的人才培育”双轮驱动,加速推进“人工智能+”行动落地。

“部分企业尤其是中小企业面临的挑战也不容忽视。”刘庆峰代表表示,一方面,部分企业缺乏AI技术应用的资金、人才和技术储备,难以快速实现数字化转型;另一方面,部分AI产品脱离实际应用需求,陷入“玩具级”困境,未能真正融入产业场景、创造实际价值。

“人工智能的发展是一场长期的探索,机遇与挑战并存,堵点与希望同在。只要坚持自主可控、软硬一体、行业纵深、个性化的发展方向,持续深化技术创新、强化场景落地、构建开放生态,就一定能加速AI科技成果转化,让AI技术真正成为推动高质量发展的强大引擎。”刘庆峰代表说。

“制造业是国家根基,工人是产业脊梁。面对AI浪潮,企业要扛责任,劳动者要练‘硬功’,来面对技术革新的时代与潮流。”董明珠代表表示,格力电器目前已经拥有近2万名研发人员,近8万名员工,“我们也将继续坚持自主培养人才的理念,锻造中国制造强大的自主创新能力”。

李乐成表示,我国产业门类齐全、创新人才众多,尤其创新生态在不断改善,必将有更多的世界级智能产品在这块热土上生产出来。

宁夏出台14项举措支持数字消费发展

本报讯 (记者马学礼 李静楠)近日,宁夏回族自治区商务厅、区发改委、区工信厅等7部门联合印发《大力发展数字消费共创数字时代美好生活三年行动方案(2026—2028年)》(以下简称《行动方案》),提出14项具体举措,充分发挥“人工智能+”等数字技术对消费市场的赋能作用,推动数字技术与消费各领域深度融合,打造具有宁夏特色的数字消费生态体系,使数字消费成为拉动宁夏消费增长的新引擎。

根据《行动方案》,宁夏将聚焦智能家电、智能家居、智能机器人、可穿戴设备、智能安防等,鼓励企业研发适配宁夏城乡消费场景的定制化新型数字产品;大力发展在线教育、远程诊疗、智慧景区、数字养老、智慧家政等服务消费业态,打造智能辅助诊断、健康画像等“人工智能+医疗健康”应用场景;鼓励大型商场、连锁超市、特色门店等实体商业数字化转型,发展“即时零售”“社区团购”“直播电商”等新业态,同时大力发展农村电商,深入实施“村播计划”和“溯源直播”,推动枸杞、葡萄酒、滩羊等特色产品全渠道数字化营销。

在增强数字消费发展内生动力方面,宁夏计划实施农村电商高质量发展工程和“互联网+”农产品出村进城工程,打造一批产加销一体的网货生产供应中心项目,培育县域数字消费品牌企业和区域特色数字消费品牌。

青海部署开展重点领域价格监管行动

本报讯 (记者邢生祥)近日,青海省召开重点领域监管“价格利剑·2026”行动安排部署会,即日起至2026年10月底,集中开展重点领域监管“价格利剑·2026”行动,旨在营造透明公平的营商环境。

在涉企收费专项整治方面,青海将聚焦政府部门及下属单位、行业协会商会、电子政务平台等领域,开展涉企收费检查。聚焦电网环节价格监管,重点查处供电企业不落实价格优惠政策的行为。医疗服务价格专项检查方面,检查医疗机构是否按规定的医疗服务项目和标准收费,有无自立项目、自定标准、分解项目收费以及不按规定提供服务并收费的行为。

在网络平台价格专项检查方面,青海将重点检查本地注册登记经营的平台经营者、平台内经营者是否在显著位置公示收费项目(如佣金、配送费)、计价单位和收费标准;促销划线价是否有依据、是否存在虚构原价、先涨后降等价格欺诈行为;平台是否干预商家定价、强制商家调价或开通“自动跟价”系统及其他价格违法行为。

在酒店住宿业价格专项检查方面,重点检查是否严格执行明码标价规定,是否明码标价、是否在标价之外加价出售或收取任何未标明的费用。促销活动中标示的“原价”“划线价”是否真实,是否以低价招徕顾客却以高价结算,或以“房源紧张”等为由单方面毁约等情况。

本报社址:北京市东城区安德路甲61号 邮政编码:100718 定价:全年352元 每季88元 2月29.26元 其余月29.34元 零售:逢4版0.56元 逢8版1.12元 广告经营许可证京东工商广字0184号 工人日报社印刷厂印刷