“养龙虾”热潮之下，如何守好安全底线？

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。”

□ 文/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’。”近日，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？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