Tel:0311-88629205 责编:张凌波 美编:魏娟

把离职员工“炼化”成数字人继续干活?

——AI 应用的合规边界与权益困境剖析

新华社北京 4 月 27 日电 4 月 27 日,《新华每日电讯》发表题为《把离职员工“炼化”成数字人继续干活? ——AI 应用的合规边界与权益困境剖析》的报道。

近日,一个名为“同事.skill”的开源项目在技术社区 GitHub 上爆火。功能是把离职同事的飞书消息、钉钉文档、邮件、截图等“原材料”投喂给 AI,再加上几句对其性格的主观描述,就可生成一个能够替他继续工作的 AI 分身,网友戏称这一过程为“炼化”。

被裁员后,还要把在职期间学到的技能、业务逻辑,甚至原属于自己的语言风格、为人处事的方法留下,为公司永久工作? 这项技术在网络社交平台上引发广泛讨论。

训练 AI 分身,数据从何而来、可以使用到何种程度? 如何强化知识产权保护、明确技术伦理边界,让 AI 发展的成果惠及更多劳动者?新华每日电讯记者多方采访,深入剖析该现象。

(AI 生成图片)

离职员工的“赛博永生”

最近,“把前同事‘炼化’(或蒸馏)成 AI Skills”成为舆论热点。此技术可提取人的工作经验、沟通风格、决策逻辑等隐性信息,使 AI 分身一定程度具备人的思维能力,同时完成特定工作任务。

“以前的离职,是工位清空、移交工作,学到的本领、积累的经验还是自己的;现在的离职,仿佛把灵魂留在了公司,实现‘赛博打工’、永不下班。”还有网友“整活”,将前任、老板生成数字人,试图“求虐”。

不少受访者认为,“炼化”同事不仅侵犯了劳动者的知识产权,而且各类数据被收集后,AI 将不再是可靠的工作助手,而是可能被用作“优化”自己的工具。为了提前杀死自己的“数字分身”,有的网友尝试给自己“投毒”,“只要我代码写得够烂,AI 就只能学到一堆垃圾,公司也只能得到垃圾代码”。

还有网友制作了“反同事.skill”,与“克隆”他人相反,它通过将真正重要的核心知识替换为看似正确但无实质内容的“正确的废话”,来保护自己的知识不被轻易复制。

“赛博永生”暗藏隐忧

受访专家认为,“同事.skill”看似是能够短时间大幅提升生产力的工具,实则暗藏多重隐忧。

首先是劳动者隐私使用权限和知识产权问题。青岛黄海学院教授孙在福认为,当前,个体在职场中积累的经验、习惯到底更偏重属于公司财产还是劳动者本人知识产权,在法律上尚属模糊地带。员工带入职场的个人经验、外部学习成果、非职务发明、个人方法论被“克隆”,将构成对员工个人智力成果的侵害。一旦 AI 生成内容出现侵权、错误、泄密,现有法律无法清晰界定责任主体,最终形成“谁都负责、谁都不负责”的法律真空。

其次,“同事.skill”的迭代发展带来了职业替代焦虑。山东师范大学副教授刘溪认为,若该技能无序发展,可能直接导致企业对某些岗位的人力需求大幅缩减,进而引发调岗降薪、优化裁员等一系列问题。

再次,人才培养很有可能追不上科技的步伐。随着 AI 持续发展,技能迭代周期可能从 10 年缩短至 2 到 3 年,“一技终身”将成为历史。同时,职业教育模式可能从长期学历教育转向短周期、模块化、微证书教育,并要求学员从一次性教育转向终身学习、持续更新、动态适配。

让 AI 成为人类的羽翼

“人工智能发展越来越好,普通劳动者该如何享受到这份时代的红利? ”不少受访者都有这种困惑。

不可否认,AI 的发展在替代部分基础岗位的同时,会同步创造新的就业岗位,如 AI 训练师、提示词工程师、数字员工管理员、算法合规审计师等。这些新岗位数量有限,目前不能完全承接被替换的劳动力,技术发展速度与新岗位诞生速度、新保障体系构建速度之间的“赛跑”,将需要一个较长时间的调和。

一方面,培养 AI 不可替代的竞争力、学会用 AI 处理问题,才能让 AI 成为人类的羽翼。刘溪认为,当 AI 逐步承担“如何做”的执行工作,“做什么”与“为何做”的决策价值更加突出。高校应及时进行专业和课程调整,加强人文社科与伦理教育,提升学生的问题定义能力、价值判断能力和综合审美能力。

孙在福认为,企业可以采取“人机耦合”的选择,即利用 AI Skill 处理标准化、重复性的基础任务,将人类员工从繁琐劳动中释放出来,转而聚焦于高价值的战略决策、情感沟通与复杂问题的综合处理。

当“能力算法化”成为无法避免的趋势,劳动者可以尝试将自身的专业技能、工作经验、决策逻辑封装为可复用的 AI Skill,以订阅授权、调用分成的方式,为多家企业提供远程服务,实现“一人服务多家企业”的灵活就业模式,将自身劳动价值最大化。

守护人的主体地位

在人机协同时代,如何守护人的主体地位与不可替代性? 受访专家认为,当前,应在法律法规、伦理审查、行业自律等方面发力,保护劳动者合法权益,为人机协同发展打下坚实基础。

——补齐法律短板,实现刚性约束。孙在福建议,在个人信息保护法框架下进一步明确:员工的工作行为模式、沟通风格、判断偏好、思维逻辑属于个人信息乃至敏感个人信息,企业用于 AI 训练必须取得单独书面同意。劳动关系终止后,企业应在规定期限内删除用于 AI 训练的个人痕迹数据。

——强化伦理审查,降低劳动者维权成本。孙在福建议,面向企业的“同事.skill”类系统上线前,应向网信、人社、市场监管部门进行备案与伦理评估,重点检查数据授权合法性、采集范围必要性、劳动权益保障情况。

——完善行业自律,形成柔性约束补充。刘溪建议,行业协会可牵头,联合法律机构、劳动保护组织制定自律公约,倡导行业自律,抵制贬损人类职业价值、加剧就业失衡的恶性算法竞争,确保技术进步始终运行在文明与法治的轨道上。

面对“Skill”,普通人如何保护自己

新华社北京 4 月 27 日电 4 月 27 日,《新华每日电讯》发表题为《面对“Skill”,普通人如何保护自己》的评论。

近来,在智能体生态中,一种叫做“Skill(技能包)”的插件正变得越来越流行——它就像智能体的“技能卡”,安装一个,就多练出一项“本领”。听上去很方便,但你可能没有意识到:随手下载安装的插件,可能正在让你的数据、财产甚至个人安全暴露在风险之中。

Skill 插件可能带来哪些法律风险?

首先是个人信息与隐私泄露。插件在运行时,往往需要获取你的文件、浏览器信息,甚至系统权限。一个恶意的 Skill 完全有能力在后台悄悄读取你的通讯录、聊天记录,并将这些敏感信息传输至外部服务器。作为受害者,你有权依据民法典第 1034 条和个人信息保护法第 69 条,要求侵权方承担民事赔偿责任。

其次是遭遇财产损失与网络诈骗。恶意插件可能会伪装成“办公自动化”等正常功能,利用智能体的自主执行能力,在用户毫不知情的情况下完成虚假交易或资金转移。这些行为可能构成刑法规定的盗窃罪、诈骗罪或破坏计算机信息系统罪。

第三是追责困难。大多数开源 Skill 插件的许可证通常包含“不提供任何保证”的免责声明。这意味着,如果出了问题导致你遭受损失,你很可能无法直接向开发者索赔。而开源平台的用户协议中,通常也会声明平台不对用户上传的内容承担审核责任。在这种情况下,你的损失可能面临“找不到人赔”的困境。

第四是数据安全合规的风险。如果你是企业用户,使用来路不明的 Skill 插件可能导致企业数据泄露,进而触发数据安全法和网络安全法上的合规责任。即便你本人是受害者,企业也可能因为未能履行数据安全管理义务而面临行政处罚。

面对“Skill”,普通人如何保护自己?以下几点建议,或许能帮助你在享受 AI 便利的同时,降低法律风险:

首先,选择插件时要多一分“审慎”。不要看到功能介绍吸引人就直接安装。下载 Skill 插件之前留意以下几点:开发者是否有真实可查的身份或组织背景? 下载量、用户评价和社区讨论如何? 是否有其他用户反馈过安全问题? 来源不明、下载量极低、缺乏社区维护的,风险通常更高。

其次,关注权限请求,坚持“最小授权”原则。安装时,注意它申请了哪些权限。一个帮你整理待办事项的 Skill 插件,不应该需要访问你的浏览器密码或文件系统根目录。如果权限请求明显超出其功能所需,果断拒绝安装。

第三,避免在敏感场景中使用未经验证的插件。涉及银行账户、加密货币钱包、企业内部系统等敏感操作时,尽量只使用经过官方认证或广泛验证的 Skill 插件。不要让智能体在无人监督的情况下,使用不熟悉的 Skill 插件处理涉及资金或重要数据的任务。同时,要定期检查你的智能体里装了哪些 Skill 插件。不再使用的及时卸载,发现异常行为时,立即停用。

第四,也是相当重要的,注意保留证据、及时维权。如果你因使用 Skill 插件遭受了损失,第一时间保存相关证据:包括下载页面截图、许可证内容、异常行为的日志记录、财产损失的凭证等。这些证据在后续维权中至关重要。

技术的进步总是跑在法律前面。AI 智能体和 Skill 插件生态正处于快速发展期,相关的法律规范和监管框架还在不断完善中。在制度尚未完全跟上的窗口期,每个用户多一分警觉和审慎,就多一分安全。

请记住:便利和风险往往是一枚硬币的两面——在享受 AI 提升效率时,也不要忘了为自己的数据和财产加一道锁。