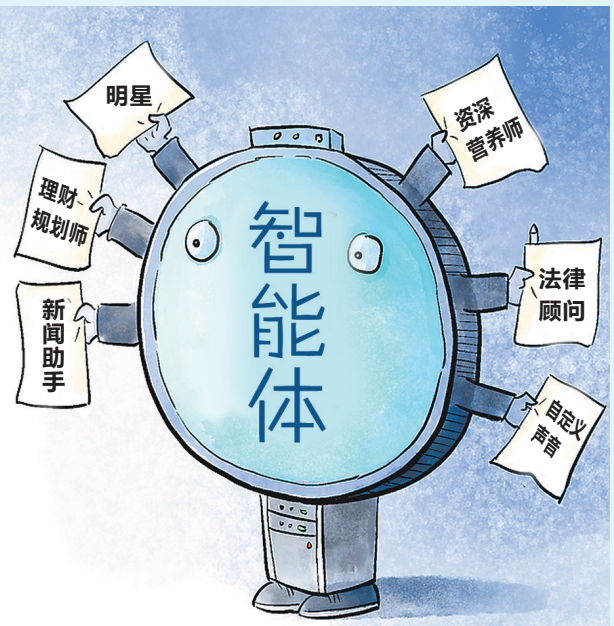
“您有法律问题,我来帮您解决”“心理学专家,回应你的心理和情绪问题”……伴随大模型飞速发展,面向个人用户的相关APP(应用)也愈发丰富。而在部分APP中,人们可能会注意到一个新奇的名字——“智能体”。

这些“智能体”顶着各种各样的名称,看似可以提供法律援助、心理咨询、职业规划等多种专业服务,但其背后的创建者是谁却无从知晓,一些智能体还涉嫌侵权、信息索取等问题。



(CFP)

“智能体”秒变各种身份

“自称”业内人士、假扮专家明星等,背后创建者是谁却无从知晓

创建“法律顾问”只需10秒“审核”

什么是“智能体”?这一概念在业界包含的内容较为复杂,且尚未达成统一的官方定义。但在面向个人用户的大模型APP中,智能体的呈现方式显得简单了许多。使用者可以点击APP中相应的功能按键,生成属于自己的智能体。

如今,利用大模型APP写文章、创作AI图像、AI视频、AI音乐等,已逐渐为人们所熟悉。APP中的智能体,大致可以理解成,AI创作的又一项进阶功能——创作一个“身份”。

在软件中,普通人几乎零门槛就能生成自己的“智能体”。记者点击某大模型APP的AI智能体创作功能,发现需要给自己的智能体“起个名”,并输入一段设定,还可以自定义AI智能体的声音、语种,以及选择是否公开。如果公开,所有人都可以与该智能体“对话”。

按照示例,记者尝试将智能体设定为“资深营养师”,描述内容设定为,“具有多年营养健康方面咨询经验,擅长通过饮食调节身体状态”,然后点击一键完善。就这样,一位“资深营养师”诞生了。软件还根据记者描述,自动为智能体添加了穿着白大褂的老年女性医师头像,以及开场白:“告诉我你的身体状况,我给你定制饮食方案。”

在另一款大模型APP中,“智能体”创建拥有一个单独的模块,可以设计自己的“分身”,也可以一句话简易创建。这次记者将身份设定为“法律顾问”,可为用户提供基本的法律咨询和建议,解答日常生活中可能遇到的法律问题。

以上智能体,记者均选择“公开发布”,确认发布前会出现浅色小字,提醒用户保护个人信息,确保未侵犯第三方权利。发布后会显示“待审核”字样,不过大约10秒即显示通过上架,可在平台中搜索找到。整个过程中,除了“起名”“描述”等步骤,系统未要求记者提供任何身份资质相关证明材料,基本上是“你怎么定义,我就怎么生成”。

此外,测试发现,软件暂未对一位用户可创建的智能体数量加以限制。除了个人身份,以机构、单位名称创建的智能体也能轻易通过。记者分别以“某日报”及“某日报新闻助手”的名义,尝试创建了智能体,同样是数秒创建,不需要任何证明材料。

为避免引起不必要的麻烦,记者将上述机构名称的智能体,设为不公开上架的私密状态。不过此前的“资深营养师”因公开发布,短短几小时内显示,已有“7人添加,8人聊过”。

身份随意仿冒 答案天马行空

由于创建智能体十分便捷,那么这些智能体背后,创建者的真实身份,就显得令人疑惑了。记者发现,每个智能体的名称下方,有浅色小字标注着创建者的用户名。点击用户名,还能进入创建者的个人主页。不过,在用户的个人主页下,除了其发布的作品、创建的智能体列表等,并没有任何个人信息的显示,也没有路径可以与该用户取得联系。

记者随机使用一些机构、单位的名称,以及一些明星的姓名进行搜索,出现的智能体数不胜数。例如顶着某位女明星姓名的智能体,在列表中连续下拉几个屏幕,都滑不到底。排在前几名的,已经有几万甚至十几万人“聊过”。记者点击进入该智能体对话页面,发现“她”不但使用了该明星的大幅照片作为背景,“说话”声音也极为相似。这些智能体的创建者,显然都不是该明星本人。

除了有侵权之嫌,这些被创建出来的智能体,如何与人沟通呢?记者以自己创建的智能体为例尝试发现,“诞生”的智能体,不需要任何后续操作,直接就可以向其发送信息进行对话,且会迅速给出回答。但这些回答仍来自大模型原本的数据库,并不是记者的答复,也无法对答案进行修改。

有时,相关答案并不一定靠谱。例如记者向“某日报新闻助手”咨询,请提供该日报的文化新闻。智能体马上显示,“以下是当天该日报的一些文化新闻——2025年2月19日,北京惠民文化消费季正式启动……”然而记者翻遍该日报当天消息,并没有相关内容。

事实上,北京惠民文化消费季已举办12届,每年均在夏秋季启动,持续数月。今年1月24日,第十二届北京惠民文化消费季刚刚收官,距新一届启动为时尚远。如果有用户将记者创建的智能体当成真正的“某日报”来询问,很可能会得到一条假消息。

呼吁配套监管 警惕潜在风险

相较AI图像、视频等产品,AI智能体创建,目前处于起步阶段。记者查看多款当下热门大模型APP,发现该功能仅在数款APP中搭载,暂未普遍推广开。新奇之余,相关“配套”约束显得没有那么面面俱到。

“为您定制个性化的家庭财务规划前,请您提供详细信息,包括收入情况、支出情况、资产状况……”记者向一个名为“理财规划师”的智能体发问,收到这样的回复。但以现有系统来看,用户无法查询智能体创建者的真实身份,以及所提供个人信息的去处与处置方式。

此外,记者在大模型APP中,也查询不到在线客服的联系方式,基本均需要翻阅文档、查看指南等寻找资料。在某APP的隐私政策文档中,记者找到一个400电话,拨打后工作人员称,这是相关实体教育产品的客服电话,想要咨询大模型问题,可以通过网站来反馈。记者点开工作人员发来的网址,页面上提供的在线客服仍为智能助手,无法解答智能体相关的疑问。

大模型APP中的智能体创作,用意为何?在知名数字经济学者、工业和信息化部信息通信经济专家委员会委员刘兴亮看来,智能体,即Agent,可以将其视作“智能AI时代的APP”,是对传统APP的升级,一种让人工智能更好融入日常生活的途径。除了实现智能问答,其主要优势在于可以自主执行任务,解决复杂问题,比如制作PPT、解决法律问题等。

大模型中的智能体,或可视作功能细分的雏形。目前,各智能体尚不支持创建者自行回答问题,“我们使用AI都是会收到实时答复,如果由创建用户来回答的话,现在肯定是做不到的”。不过有观点认为,后续不排除部分大模型会支持智能体创建者“自行创作”,在原有大模型基础上,进行个性化数据训练、开发等。

由于智能体创作刚开始发展,刘兴亮认为应给予一些时间空间来进行观望,同时勿忽视对可能存在隐患状况的监测。“假使有人创建了和我同名的智能体,甚至头像也用了我的照片,那我肯定是不愿意的。后续应该会像互联网社交平台一样,推出一些审核相关的功能。”与此同时,也应提醒公众,对于AI智能体等新生事物,好奇之余要多一分警惕心理,不要对其名称、头像、声音等过于轻信,防范因来路不明的智能体导致的隐私泄露等潜在风险。 (《北京晚报》)