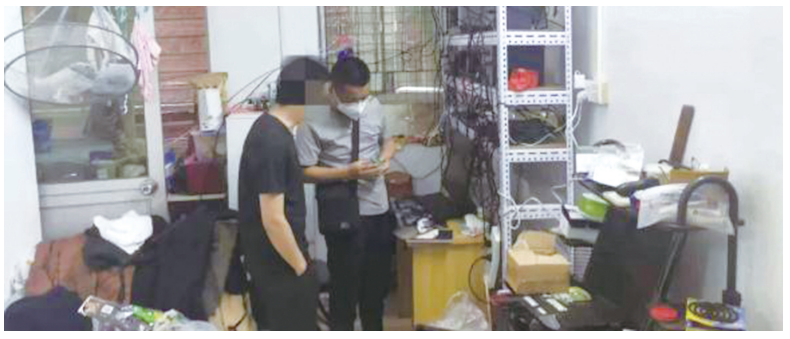
用ChatGPT编假新闻 警方出手了

ChatGPT浪潮澎湃，但背后暴露出的人工智能法律风险、围绕ChatGPT展开的无序商业行为等亦汹涌来袭，如何应对成为关注焦点

N法治日报 新甘肃客户端 IT时报 财联社

今年，由美国人工智能研究室OpenAI开发的全新“聊天机器人”ChatGPT火了。作为一款人工智能语言模型，它不仅能和人展开互动，还可以写文章、制定方案、创作诗歌，甚至编写代码、检查漏洞样样精通，上线仅两个月全球活跃用户破亿。

ChatGPT的问世掀起了新一轮人工智能浪潮，但其使用过程中可能涉及的法律问题不容忽视。目前，已有安全团队发现，网络攻击者开始使用ChatGPT创建恶意软件、暗网站点和其他实施网络攻击的工具，甚至已有诈骗团伙用ChatGPT生成“剧本”，进行更有针对性的精准诈骗。



民警在嫌疑人住处对其使用的电脑及百家号进行取证（图片来源于新甘肃客户端）

编假新闻赚流量牟利，甘肃一男子落网

近日，甘肃平凉市公安局网安大队侦破一起利用AI人工智能技术炮制虚假不实信息的案件。这也是自1月10日《互联网信息服务深度合成管理规定》颁布实施后，甘肃省侦办的首例案件。

4月25日，平凉市公安局崆峒分局网安大队在日常网络巡查中发现，某百度账号出现一篇标题为“今晨甘肃一火车撞上修路工人致9人死亡”的文章，初步判断为信息虚假不实。网安民警随即开展工作，发现共计21个百度账号均在同一时间段发布该文章，文章内容地点除平凉市崆峒区外还涉及兰州、陇南、定西、庆阳等地，文章点击量已达1.5万余次。经查，涉案百度账号均为广东深圳某自媒体公司所有，公司法人代表洪某弟有重大作案嫌疑。

5月5日，专案民警在广东东莞嫌疑人住处对其使用的电脑及百家号进行取证。经审讯，犯罪嫌疑人洪某弟通过微信好友获知网络赚取流量变现方法，并购买大量“百家号”。同时使用“易撰”网页版，在全网搜索近几年社会热点新闻，为规避百家号查重功能，洪某弟通过近期火爆的ChatGPT人工智能软件将搜集到的新闻要素修改编辑后，使用“海豹科技”软件上传至其购买的百家号上非法获利。

洪某弟利用现代科技手段编造虚假信息，并散布在互联网上，被大量传播浏览，其行为已涉嫌寻衅滋事罪。

目前，崆峒公安分局对犯罪嫌疑人洪某弟采取刑事强制措施，案件正在进一步侦办之中。

门槛消失，ChatGPT版“诈骗剧本”已上线

伴随着ChatGPT的横空出世，同时被降低的，还有“诈骗的门槛”。腾讯安全策略发展中心的安全团队观察到，已经有诈骗分子开始利用ChatGPT编写“钓鱼剧本”，这大大提高了骗子实施精准诈骗的效率。

在网络安全领域，有一个专用名词叫“社攻”，也即利用社交关系攻击的方式。诈骗分子通过与被害者聊天，诱导其点击恶意链接，或者下载一些恶意软件，从而在电脑里“种好木马”，常见的话术有：“你孩子在学校生病了”“你被法院起诉了”“你获得一笔退款”等等。

“为了赢得被骗人的信任，诈骗分子通常有多套沟通剧本，分别扮演警察、老师、客服等角色，原本这些剧本需人工编写，且必须具备一定的专业知识。比如扮演HR，你要深入了解对方的工作；扮演保险公司业务员，要对保险业务有比较清晰的了解……”腾讯安全团队告诉记者，通过ChatGPT，编写剧本不再需要有“专业能力”的骗子，而且“剧本”几乎瞬间生成，大大提升了行骗的效率，因此，未来“剧本”里很可能会出现更多样化的角色、诱骗手段，形成新的钓鱼攻击方式。

因无法核实信源，存在泄露信息、提供虚假信息等隐患

除了被用于网络诈骗，ChatGPT存在的信息泄露、知识产权等法律风险也愈发受到关注。

公开资料显示，ChatGPT可以总结研究论文、回答问题、生成可用的计算机代码，甚至快速通过美国医学执照考试、沃顿商学院的MBA期末考试、司法考试。一些医学论文预印本和已发表的文章甚至正式赋予了ChatGPT作者身份。

但在受访的法律人士看来，ChatGPT的强大功能也隐含着不少法律风险。

“ChatGPT对信息、数据来源无法进行事实核查，可能存在个人数据与商业秘密泄露和提供虚假信息两大隐患。”北京盈科（上海）律师事务所互联网法律事务部主任谢连杰说。

谢连杰分析说，ChatGPT依托海量数据库信息存在，其中包括大量的互联网用户自行输入的信息，因此当用户输入个人数据或商业秘密等信息时，ChatGPT可能将其纳入自身的语料库而产生泄露的风险。虽然ChatGPT承诺删除所有个人身份信息，但未说明删除方式，在其不能对信息与数据来源进行事实核查的情况下，这类信息仍然具有泄露风险。

其次，人工智能生成的信息并不总是准确的，ChatGPT常常出现“一本正经地胡说八道”的情况，需要一定的专业知识才能辨别真伪；也可能有不法分子恶意“训练”人工智能，使其提供诈骗信息、钓鱼网站等内容，损害公民人身财产安全。

此外，ChatGPT在建立语料库、生成文本时，如果使用并非公开的开源代码、使用开源代码商用未办理许可证或者未按照许可证的要求实施的，可能会导致侵权。

借势贩卖租赁账号 “搭便车”山寨频出

ChatGPT走红后，由于服务端对中国大陆的IP有限制，无法注册使用，其账号一时在国内多个网购平台、社交平台上销售火热。在某电商平台上售卖成品账号的店铺，一天之内多达万人付款，价格最低1.68元。

近日，多个电商平台对ChatGPT账号销售行为进行了查禁，相关关键词被屏蔽。然而，记者在社交平台上搜索“ChatGPT账号”等关键词发现，仍有不少网友在提供代注册、有偿账号分享服务，围绕ChatGPT账号展开的买卖行为仍在野蛮生长。

泰和泰（重庆）律师事务所高级合伙人朱杰认为，这种买卖行为可能构成非法经营等违法行为。ChatGPT的正版服务由境外机构提供，而未经我国相关部门批准利用VPN跨境提供经营活动是被明确禁止的，所以国内这些代问、代注册的商家以营利为目的，搭建或使用VPN进行注册账号，未办理国家相关行政许可，擅自经营买卖国外账号，可能会受到行政处罚甚至刑事处罚。

ChatGPT账号价值被炒作成商品以外，借其名称热度“搭便车”的牟利行为也大量出现。近日，记者查询发现，以“ChatGPT”“智能问答”等字眼做名称的小程序、公众号数量激增，不少小程序都显示有“1000+人最近使用”。

记者使用其中一些小程序后发现，这些产品不仅和ChatGPT毫无关系，而且大多以免费试用为噱头，吸引用户注册使用后，再推出收费服务，最终目的是诱人充值以牟利。例如，一个名为“××超级AI”的公众号中提到，可以为用户提供ChatGPT中文版的服务。

可当记者点击进入“AI情感问题”一栏，还未进行任何操作，对话框就显示记者“已经用完今天的免费次数”，后续体验需要购买VIP，分别为19.9元的一天会员、199元的月度会员与999元的年度会员。

朱杰说，“山寨”软件打着正版软件的旗号进行宣传，欺骗消费者进行下载，可能构成虚假广告；同时，“山寨”软件使用的名称及标志如与正版软件相同或相似，引导他人误认为与正版存在特定联系，可能构成反不正当竞争法中规定的商业混淆行为，将受到行政处罚。