AI需构筑安全防线 暴露数据隐私

独居老人陈爷爷，通过子女赠送的智能音箱，找到了新乐趣。“小智不仅能陪我听戏、聊天，还会在我忘记吃药时主动提醒，它居然还记住了我所有孙辈的生日。”

29岁的小王原本是文案策划，因擅长与AI“对话”，现已成功转型为提示词工程师。

当前，AI大模型加速赋能千行百业，推动人们生活日新月异，这位能干又贴心的“数字伙伴”正加速融入我们日常生活。然而，每一次技术跃迁必然伴随着新的挑战，当AI的触角延伸越广、嵌入越深，随之而来也暴露出数据隐私、算法偏见等潜在风险，亟须我们构筑安全防线，助推这场深刻的智能变革，安全赋能美好未来。

资料照片

高速发展背后的“暗礁”

数据隐私与安全边界模糊。个别单位因直接使用开源框架建立联网大模型，导致攻击者未经授权即可自由访问内部网络，从而引发数据泄露和安全风险。据公开案例显示，某单位工作人员在处理内部文件时，违规使用开源AI工具，由于电脑系统默认开启公网访问且未设密码，导致敏感资料被境外IP非法访问和下载。

技术滥用与虚假信息产生。利用AI的深度学习算法进行自动化的数据处理，实现图片、音频及视频的智能模拟和伪造，这种技术被称为深度伪造（Deepfake）。一旦该技术被滥用或恶意使用，将给个人合法权益、社会稳定甚至国家安全带来诸多风险和挑战。国家安全机关工作发现，某境外反华敌对势力通过深度伪造技术生成虚假视频，并企图向境内传播，以误导舆论、制造恐慌，对我国家安全构成威胁。

算法偏见与决策“黑箱”。AI的判断源于其所学习的资料，若训练数据本身存在社会偏见或代表性不足等问题，大模型便可能放大歧视。测试显示，某些AI会系统性偏向西方视角。当研究人员用中英文向某同一个AI提问历史问题时，发现英文回复会刻意回避、淡化某些史实，甚至会给出包含错误历史信息的内容，引发重大歧误，而中文回复则相对客观。

安全守则：给“数字伙伴”的三条守则

守则一：划定“活动范围”。做到“权限最小化”，联网AI不处理涉密数据、语音AI不收集环境语音、智能助手不保存支付密码，关闭“数据共享”“云空间”等不必要的访问权限。

守则二：检查“数字足迹”。养成定期清理AI聊天记录、修改AI工具密码、更新防病毒软件、查看账号登录设备等习惯。同时避免随意下载使用来源不明的大模型程序，对提供身份证、银行账户或其他敏感信息的要求保持警惕。

守则三：优化“人机协作”。向AI提问时，在提示词中明确禁止AI过度推演，并要求AI显示来源或思考过程，对重要信息进行跨平台验证，合理辨别AI生成结果，特别是涉及政治、历史、意识形态等话题时，要具备独立思考意识，辩证看待AI的回答，避免陷入“AI幻觉”。

国家安全机关提示

安全是发展的前提，发展是安全的保障。只有懂科技、安全使用科技，才能让AI大模型这一新兴科技成为推动社会进步的正能量。广大用户应当提高安全意识，审慎授权大模型软件权限。如发现AI大模型存在窃取个人信息，向境外传输敏感数据等危害网络安全的问题线索，可通过12339国家安全机关举报受理电话、网络举报平台（www.12339.gov.cn）、国家安全部微信公众号举报受理渠道或者直接向当地国家安全机关进行举报。

人生新起点，切勿大意疏忽

通过个人努力顺利考公“上岸”，是人生的崭新开始。然而，由于社会经验相对不足、身份转变尚在适应期，个别人员的保密意识尚未完全筑牢，初入职场的公职人员易被境外间谍情报机关视为目标对象，以各种卑劣手段拉拢策反，危害我国家安全。

密件当“论文”随意传

境外间谍情报机关常假借学术研究、行业调研等名义套取内部文件。部分新入职公职人员仍带有校园知识共享思维，不熟悉工作流程且对涉密载体的保管处置缺乏了解。公开案例显示，某从事文件收发工作的青年公职人员，于入职当年先后多次将涉密文件带回家中，违规上传至境外网站，严重违反保密规定，最终因故意泄露国家秘密罪被依法判刑。

间谍当“朋友”热络谈

境外间谍情报机关人员通过伪造身份、打造虚假“人设”账号，在社交平台精准锁定新入职公职人员群体，并利用其正处于社会身份转变的心理调适期等特点，在交往中营造“知心朋友”“人生导师”等形象，通过长期情感陪伴逐步建立信任关系，借此套取工作中的敏感信息乃至国家秘密。公开案例显示，某单位从事装配工作的青年公职人员，通过交友软件结识一名实为境外间谍情报机关工作人员的“女网友”。在对方长期的情感攻势下，该公职人员逐步放松警惕，多次向其提供国家秘密并非法获利。

窃密当“兼职”大意做

境外间谍情报机关将窃密活动包装成所谓的兼职岗位，利用报酬丰厚、工作轻松的噱头吸引刚入职的公职人员。公开案例显示，某研究生毕业后进入某党政机关下属研究所工作，下班途中被一名外籍间谍主动搭讪，对方以“学术合作”为名提出兼职邀请，要求其搜集单位内部行业数据及分析报告。该青年被高额报酬吸引，持续非法提供核心涉密资料，最终因危害国家安全受到法律严惩。

国家安全机关提示

思想防线要筑牢

新入职人员应系统学习保密法律法规，吃透禁止性规定的行为边界，夯实保密意识与履职能力。尤其要警惕“想当然”“无所谓”等侥幸心理，要将“可为与不可为”的准绳内化为思维自觉，从根源上规避因认知缺位引发的泄密风险。

纪律红线不能碰

新入职人员应培养健康良好的兴趣爱好，牢固树立正确的金钱观和价值观，始终保持清醒头脑，自觉抵御不良诱惑，坚决摒弃“以密谋财”的错误观念，深刻认识到任何对涉密信息的牟利企图，都将付出沉重代价，既断送个人前程，更会损害国家利益。广大公民应增强国家安全意识，如发现可疑线索请及时通过国家安全机关举报受理电话、网络举报平台（www.12339.gov.cn）、国家安全部微信公众号举报受理渠道举报或者直接向当地国家安全机关进行举报，共同筑就维护国家安全的钢铁长城。

（均来源于国家安全部微信公号）

责任编辑/王睿卿 E-mail:fzbfyzk@126.com