用AI，这3件事千万别做！一不小心就违法

AI已成为提升效率的重要工具，写文案、做表格、查资料、做设计都更加便捷高效。但便利之下也隐藏着不容忽视的风险,如果使用不当，不仅可能惹上麻烦，还可能危害国家安全、触碰法律红线，严重的甚至会被追究刑事责任。下面一起来学习。

一、案例描述

小王是某单位工作人员，为提升工作效率，他尝试使用一款流行的开源AI工具分析一份标注“秘密”的内部报告。由于电脑系统默认开启公网访问，且未设置访问密码，小王上传文件后，该AI工具的后台服务端口直接暴露在公网。经查，该开源框架的默认配置存在安全缺陷，而单位未进行任何安全加固，也未对使用外部AI工具进行安全评估和审批。此次泄露导致内部涉密资料外流，损害了国家安全。该机关单位及直接负责的主管人员、直接责任人员小王等人依法受到处分。根据法律规定，如泄露内容经鉴定属于国家秘密且情节严重，相关责任人员可能构成过失泄露国家秘密罪，并依法追究**刑事责任**。

二、使用AI时有哪些红线不能碰

1.把涉密内容“喂给”AI。有人为了省事，把涉密文件、内部报告、国防科研数据、敏感政务信息直接输入AI，让其写报告、整理材料、润色文字；还有人把未公开的科研数据、技术参数、试验结果输入AI分析，甚至把涉及军事设施、敏感地理信息的照片发给AI识别。许多AI应用具有自动存储、云端上传、持续学习等功能，用户输入的文字和图片可能被后台记录。一旦被不法分子或境外机构获取，就可能造成国家秘密、工作秘密泄露。无论故意还是过失，只要情节严重，都可能被依法追责。

2.用AI非法抓取敏感数据。一些企业或个人为了训练模型，非法抓取人口、金融、能源、地理测绘等重要数据，甚至入侵政务网站、高校数据库、国企系统，窃取技术资料和行业敏感信息，用于训练AI或牟利。还有人收集公民个人信息、医疗健康数据并整合出售给境外机构。国家核心数据、重要数据和个人敏感信息，绝不能非法获

取、买卖或向境外提供。此类行为涉嫌非法获取计算机信息系统数据罪、侵犯公民个人信息罪等；若向境外提供，后果更严重。

3.**用 AI 造假传播虚假信息。**有人借助 AI 换脸、配音技术伪造官方通知、政策解读，或批量生成抹黑国家形象、煽动对立、制造恐慌的文章、海报、短视频。AI 生成内容成本低、传播快、迷惑性强，容易误导公众、扰乱秩序、损害国家公信力。特别是在重大节日、重要会议期间，危害更大。此类行为可能涉嫌编造、故意传播虚假信息罪，寻衅滋事罪，甚至危害国家安全类犯罪。

三、违法使用 AI，代价有多大

随意将涉密信息输入 AI，非法抓取数据，制作传播虚假信息，都会付出代价。轻则承担民事责任，如赔偿损失、删除内容、公开道歉；违反行政管理规定的，可能被罚款、行政拘留，公职人员还会面临降级、撤职直至开除处分。若严重危害国家安全和社会秩序，则可能触犯刑法，构成泄露国家秘密、非法获取数据、编造传播虚假信息等犯罪，面临有期徒刑甚至更重处罚。

四、用好 AI，记住 4 条准则

1.选择正规平台。在使用 AI 应用时，应优先选择国内正规平台提供的服务，避免通过社交媒体、陌生邮件、未知链接等非官方途径下载应用。对于声称提供“免费扫码试用”或“限时内测”的非官方来源应用程序，应保持警惕、注意甄别，确保数据安全。

2.审慎授予权限。在安装 AI 应用时，应仔细审查其权限请求，审慎授予访问通讯录、位置信息、相册、麦克风等涉及隐私的数据权限。定期检查已授权应用的权限状态，及时取消不必要的权限。

3.筑牢保密红线。严格遵守“涉密不上网，上网不涉密”的原则，严禁连接互联网使用 AI 应用处理国家秘密。工作中的机密文件、国家秘密、敏感政务数据，坚决不输入任何 AI 应用。

4.严守法律底线。不用 AI 偷数据、不搞违法研发，不造不传 AI 虚假信息。看到 AI 换脸、AI 造假的有害内容，不转发、不传播。疑似涉及国家安全的，及时拨打 12339 国家安全机关举报电话。

办公室 法制科