机关、单位工作人员：当心，图文识别有风险

近年来，个别机关、单位工作人员保密意识淡薄，为图省事使用图文识别小程序处理公务，造成涉密资料及内部敏感数据外流。下面一起来学习。

一、典型案例

1.某次重大活动服务保障期间，某单位副职领导王某在落实上级机关下发的机密级安保工作方案时，要求第三方服务人员李某，把该方案通过技术手段转化为方便编辑的 Word 格式文档。李某不会操作，便请同为第三方服务人员的同事袁某帮忙。袁某用手机拍摄该方案后，用图文识别小程序进行转化并通过文件传输助手传输，造成泄密。事后，王某被给予行政警告处分，李某、袁某被解除劳动合同。

2.2020 年 6 月，某涉密单位办公室主任孙某接到上级下发的一份机密级文件，为图工作方便，使用手机将该文件拍照并通过图文识别小程序转换成电子文档。令他没想到的是，其上传的涉密文件已经留在小程序开发公司的服务器中，该公司一名员工发现服务器中存有涉密文件，便将文件导出后售卖，最终被抓获并移送司法机关追究刑事责任，孙某也因此受到严厉的纪律处分。

3.2022 年 9 月 13 日、14 日，某市广播电视台所属广播中心机要员顾某接到该台总编室电话通知，按惯例到该台摘抄有关需要传达落实的涉密文件（机密级 1 份、秘密级 1 份）。顾某贪图方便，使用手机对两份涉密文件拍照并使用图文识别小程序转换成电子文档，随后利用无线网络通过文件传输助手发送到携带的互联网笔记本电脑中。调查中，顾某最初矢口否认实施过上述行为，经深入技术核查，又发现其于 2022 年 7 月至 8 月间，以相同方式违规上传其他 6 份涉密敏感文件。案发后，顾某及负有领导责任的广播中心主任、副主任等均受到纪律处分和组织处理。

二、原因分析

图文识别小程序看似简易便捷，却暗藏多重泄密风险，主要体现在以下3个方面。

数据流转管控失范。市面上图文识别小程序多为市场化运营，数据存储服务器归属第三方企业。数据上传后在平台、合作服务商之间无序流转，传输链路不透明、流向不可追溯，数据风控机制缺失。

协议条款暗设陷阱。一些图文识别小程序服务协议暗藏数据采集条款，用户上传的文字、图片、表格等资料将被平台自动归集并长期留存，用于算法迭代与模型训练，存在数据被违规调取、囤积甚至违规出售隐患。

安全防护能力薄弱。部分图文识别小程序研发成本低、安全架构简陋，缺乏专业加密防护设施，易遭受爬虫抓取、黑客入侵，进一步放大泄密风险。

三、温馨提示

机关、单位工作人员必须牢固树立总体国家安全观，摒弃侥幸松懈心理，精准识别图文识别小程序安全风险，以严谨规范的办公行为，筑牢保密防线。

强化人员思想防范。常态化开展保密警示教育，破除侥幸心理，明确“小”工具亦存在重大安全隐患，杜绝随意使用图文识别小程序处理办公资料。涉密文件、内部纪要、未公开业务数据、专项会议资料、敏感工作台账，一律禁止上传至任何图文识别小程序。

规范信息处理防范。办公资料严禁随意拆分、脱敏后上传图文识别小程序，严禁依靠人工遮挡、字符替换规避风险，涉密资料应全程采用涉密信息系统处理。

健全日常监管防范。严格落实保密自查制度，定期排查图文识别小程序使用情况，建立违规使用台账，做到早发现、早提醒、早整改。

办公室 法制科