# **【举案说法】网上办事很方便 保密红线不能碰**

近年来，云南玉溪市保密局通过日常监督、专项检查、平台监管等多种方式，发现并查处了一批通过社交媒体平台、OA系统等存储、处理、传输国家秘密的违法违纪案件。本文选取3起典型案例进行分析。

典型案例

案例1：2022年8月23日，玉溪市某区街道副书记李某要求街道综治中心根据上级印发的涉密工作方案，制定街道相关文件。综治中心工作人员朱某到街道综合办领取文件后，交由综治中心人员杨某处理。为图工作方便，杨某向李某询问是否可以通过图文识别小程序将涉密文件转换为电子文档。经李某同意后，杨某使用手机对涉密文件拍照并使用图文识别小程序转换成电子文档，随后又在非涉密电脑上进行修改编辑，制作成该街道方案(未标密，引用了区级文件名及文件内容)，打印后在街道会议上研究讨论。案件发生后，该街道工作委员会给予杨某政务警告处分决定，同时责令李某作出深刻书面检查。

案例2：2023年1月8日，玉溪市某县委某部常务副部长李某拟修改完善两份涉密文件征求意见稿，并了解领导小组成员单位情况。因其外出工作，李某要求办公室主任海某把该涉密材料传送给他。海某当时提醒李某，涉密材料不能通过OA系统进行传递。但李某认为短暂传递一次，事后立即进行撤销，上级部门不会察觉，仍然要求海某进行传递。海某迫于李某压力，将涉密材料在OA系统上传递给李某，造成泄密。案件发生后，县纪委监委给予李某党内警告处分，县委某部给予海某批评教育处理。

案例3：2023年4月26日，玉溪市保密局收到上级移交的关于玉溪市某单位李某通过图文识别小程序扫描涉密文件的案件线索。经查，李某的图文识别小程序内存有涉密文件照片3张。该单位的公文交换系统不收发涉密文件，未建立涉密文件收发、传阅相关工作制度，李某表示已记不清涉密文件来源及事情经过。该案已移交上级进行查处。

案例分析

保密法第二十六条规定，禁止在互联网及其他公共信息网络或者未采取保密措施的有线和无线通信中传递国家秘密。随着信息技术的飞速发展，以QQ、微信为代表的社交媒体、OA系统及图文识别小程序也成为机关单位办公常用工具。机关单位人员切不可图方便而松了保密这根弦。通过网络通信工具传输信息，表面上是点对点、面对面传输，但所发信息并非直接到达对方，而是要经过众多网络、网络设备、平台服务器中转后才能被对方接收，并且在服务器中留有备份，无论是发送方还是接收方都无法对其彻底删除。同时，信息依托互联网进行非密网络传输时，存在被窃取、篡改的风险。

对策建议

提高政治站位。机关单位要坚决贯彻落实党管保密根本原则，深刻理解、高度认识保密工作对于国家安全和民族复兴的重大意义，严肃认真地做好保密工作。党政领导干部应当带头贯彻落实保密工作方针、政策，遵守党的保密纪律，履行保密工作领导责任。机关单位工作人员在工作中如果遇到领导作出违反保密法律法规的指令，可以先进行提醒，如果无效可以拒绝执行，切不可为了顺从领导，置法律法规不顾，最终只会害人害己，追悔莫及。

加强监督检查。面对部分干部职工保密意识淡薄，对待保密工作仍然存在轻视、侥幸、无所谓心理的情况，机关单位要加大保密违法违纪行为的查处和通报力度，充分阐释保密违法违纪行为造成的国家利益损失大、个人政治和经济成本高的后果，警示教育机关单位工作人员，形成不敢泄密、不能泄密、不想泄密的良好氛围。

强化宣传教育。机关单位要开展有针对性、形式多样、生动活泼的宣传教育，普及保密知识常识，确保保密意识入脑入心。要强化涉密人员敌情观念和保密意识，加强涉密人员日常监管教育和业务锻炼，组织签订保密承诺书，定期开展保密提醒，从主观上根除失泄密案件发生的土壤。

                                                                                                                   转载自《保密工作》2023年第12期