收集涉密文件资料泄密案件启示

一、典型案例

案例 1：闫某系某政法大学刑事侦查专业硕士研究生，研究方向为物证技术。2015 年 9 月至 2016 年 3 月，为撰写硕士论文收集资料，闫某从学校图书馆借阅了《刑事科技导论》《XX 市公安局 2010—2013 年刑事案件汇编》等书籍资料，部分标注“秘密”或“内部资料 严禁外传”，又从其所属的刑事司法学院资料室借阅了《2009 年 XX 省公安机关政内保典型案例》《刑事勘验与现场绘图指南》等书刊，其中有 1 份标注“机密”。经查，闫某都办理了普通的借阅手续，学校图书馆虽制定了关于涉密书刊资料外借和复制的规章制度，但没有得到严格执行，学院资料室仅在固定资产管理规定中提及涉密资料应当专人管理，但没有真正落实。闫某对借阅书刊资料进行拍照（部分使用文字识别软件转换为电子文档），保存在个人笔记本电脑中，在向其导师、校外导师报送稿件以及向 7 家杂志社投递稿件时，使用互联网邮箱传递了 1 份涉密资料。核查中还发现，闫某有使用互联网云盘备份资料的习惯，在其云盘上存储了大量专业资料，部分属于公安机关警务工作秘密信息。事件发生后，学校上级主管部门组织对互联网上的涉密及内部信息进行清理，该政法大学重新制定了涉密书刊资料使用管理细则并指定各级管理责任人，同时依纪给

予闫某记过处分，对其作出硕士论文内审不合格及延期毕业处理。

应当说，高校学生并非涉密人员管理的重点关注对象，但少部分学生尤其是研究生基于其专业领域和研究方向，可能会接触到少量国家秘密信息。这些学生因论文写作、课题研究的需要，往往会大量收集各类资料，而他们基本上都没有接受过系统的保密基础知识和技能培训，在一定程度上存在着管理真空。

案例 2： 2018 年 7 月，某市保密局在工作中发现，该市科技局办公室副主任孙某使用的非涉密计算机中存储、处理涉密文件资料。经查，孙某原为某军区通信部门干部，后调至后勤部门，在服役期间，孙某收集了大量与其职务相关的文件资料（经鉴定其中 1 份属于军事秘密），将其数字化后存储于个人的笔记本电脑。2012 年孙某转业到某市发改委信息中心，继续收集与业务有关的文件资料，至 2017 年调至该市科技局前，共收集了包括 1 份机密级、7 份秘密级在内的 1100 多份发改领域文件资料。孙某将所有收集到的文件资料分门别类，集中存储于个人笔记本电脑。2018 年 2 月，为撰写相关文稿作参考，孙某使用移动硬盘将部分数据导出至其在科技局的办公电脑，直至案发。事件发生后，该市纪委监委依纪给予孙某政务处分，同时责令其作出深刻检查，并在全市范围内通报。

很多机关单位工作人员因业务需要，有收集与其具体从事工作有关资料的习惯，少数人甚至把收集范围扩大到与己无关的业

务。其中一些人在办理退休、调动、辞职、解聘、退役等离职手续时，往往只对有形的国家秘密载体和涉密信息设备进行清退，而将其收集的电子文件资料复制到个人的信息设备内，为日后的工作、学习作参考，造成很大的泄密隐患。

案例 3： 2017 年 12 月，有关部门发现，博客“老兵 123”违规发布 1 份有关军队转业干部安置工作的文件，经鉴定属于秘密级国家秘密。经查，当事人郭某于 1993 年从部队退伍，被安置在县农业局工作。因对安置待遇不满，郭某长期向市、县有关部门信访。为对其诉求提供依据，其通过多种渠道收集关于军人转业、退伍安置及优抚方面的政策和规定，同时在互联网上搜索相关内容，并陆续发布到自己注册的博客中，供自己和战友使用。2012 年至 2014 年，郭某共在其博客“老兵 123”上发布文章 31 篇，除两篇为本人手机拍照后上传，其余的都是从其他网站或论坛转发，来源文件均未标注国家秘密标识。

互联网网站、论坛、博客经常相互转发文章，多次转发的现象也极为普遍，其中也可能会包含涉密文件资料，而这些涉密文件资料在被转发时往往会被删除国家秘密标识并转换格式，从文章外部特征上已经很难判断出其国家秘密属性。在网络上不加区分地收集、转发文件资料，特别是收集、转发一些较为敏感领域的文件资料，客观上可能会导致涉密文件资料的进一步扩散。

二、案例警示与防范措施

出于工作、研究等目的，需要收集文件资料的机关单位及其人员，应当时刻绷紧保密这根弦，注意在以下 4 个方面做好防范工作。

1. 岗位职责范围。应当严格按照实际工作需求收集，具体到机关单位工作人员而言，就是必须基于岗位职责要求，和本人从事的具体工作内容相关。案件查处实践中发现，少数机关单位工作人员有“资料控”的倾向，无差别、尽可能地网罗一切其可以接触到的文件资料，虽然其动机一般都是大量占有资料为今后工作、学习参考，但这种超范围收集资料的行为本身也有可能构成保密违规行为。

2. 资料合法来源。文件资料应当从正常渠道收集，确保其合法性和正确性，同时也确保了涉密文件资料的知悉范围符合保密规定。互联网上既有官方正式公布或授权指定媒体公布的文件，也有其他网站或者自媒体转载的来源不明的信息，在收集、使用时需要甄别其性质和来源，原则上非官方媒体正式公布的文件资料不得作为开展相关工作、研究的正式依据。

3. 文件资料管控。对已经收集到的涉密文件资料，应当按照其不同密级和保密期限分级分类管理，对于经过批准复制、下载、汇编、摘抄的涉密文件资料按照原件管理。需要注意的是，收集、使用涉密文件资料的机关单位必须为实际工作中确有必要知悉且具备相应保密条件，坚决杜绝向无直接业务关系或无隶属关系的机关单位发送、索要涉密文件资料。

4. 移交清退销毁。相关人员在发生岗位变动、部门调整、退休转业等离职离岗情形时，应当将其保管的文件资料全部移交或清退，并办理相关手续。收集的涉密文件资料使用完毕后，除按规定留存或存档外，应当及时送交销毁工作机构或承销单位销毁。鉴于收集工作客观上会产生较多的复印件和电子文件，在移交清退销毁时，需要注意仔细检查，防止遗漏。

（转载自国家保密局
http://www.gjbmj.gov.cn/n1/2019/1115/c420077-31458076.html）