内部发行
注意保存

警钟长鸣

2022年第5期（总第141期）

中共和平区纪委　　2022年5月29日

保密这根“弦”须臾不能松

---解析《保密法》12种严重违规行为（一）

编者按：保守党和国家秘密是保护国家政治安全，经济持续发展、社

会长期稳定的重要基础。自觉遵守保密纪律更是党员干部和国家公职人员应尽的义务。当前，保密工作和网络信息安全形势日益严峻，保密违纪违法案件高发多发，给国家安全和利益带来较大风险。为进一步提高全区各级党员干部和涉密人员的保密意识，自本期《警钟长鸣》开始，将对《保密法》规定的12种常见、最典型的严重违规行为进行案例解析。希望广大党员干部能够认真汲取教训，引以为戒，切实提高政治站位，持续做好保密各项工作。

一、非法获取、持有国家秘密载体：不属于国家秘密知悉范围内的人员，通过窃取、骗取、抢夺、购买等非正当途径和手段，获取并留存涉密载体；知悉范围内的人员，未经批准留存涉密载体，经提醒、督促拒不上交；知悉范围内的人员离职离岗后，未按照有关规定及时清退涉密载体等。

【典型案例】北京市最高人民法院民一庭助理审判员王林清非法获取国家秘密案。2018年6月至8月，王林清在他人的唆使下先后采用借阅、骗取案卷材料后偷拍等方式，非法获取凯奇莱公司案件的大量卷宗材料，

并通过手机微信或者电子邮件等方式将所拍摄材料提供给赵发琦。经国家保密局鉴定，王林清伙同赵发琦非法获取的材料中有5份属机密级国家秘密。2022年5月7日，北京市第二中级人民法院一审公开宣判被告人王林清受贿、非法获取国家秘密案，对被告人王林清以受贿罪判处有期徒刑十年，并处罚金人民币一百万元，以非法获取国家秘密罪判处有期徒刑五年，决定执行有期徒刑十四年，并处罚金人民币一百万元；对其受贿所得财物及其孳息依法予以追缴，上缴国库。

【案例启示】王林清身为国家工作人员，利用职务上的便利，以非法方式获取国家秘密，走上违纪违法道路，警示我们:在现实工作中，部分党员干部、公职人员或被经济利益诱惑，或是法制观念淡薄，在侥幸心理的驱使下，不惜违反保密纪律，做出失密泄密行为，断送了自身大好前程，也给国家造成不可挽回的损失。广大党员干部在本职工作中，应自觉牢固树立国家安全意识和保密观念，时刻保持头脑清醒，增强在保密工作中“明辨是非”的能力，切实把好保密关。

二、买卖、转送或者私自销毁国家秘密载体：国家秘密载体属于国家所有，应当按照国家有关规定配发或装备，任何组织和个人不得私自买卖、转送。机关、单位应当按照国家有关规定和标准销毁国家秘密载体，任何组织或者个人不得私自销毁。

【典型案例】某国企人力资源部职员张某未按照国家有关规定和标准销毁涉密文件资料问题。2018 年 3 月，某国企人力资源部职员张某，在处理部门文件过程中，由于刚刚入职，对业务工作不熟悉，未遵守涉密文件资料销毁有关规定，将 2 本涉密图书夹

杂在其他文件资料中交由保洁人员处理。随后，保洁人员将上述文件出售给废品收购站点。事后，该单位给予张某通报批评，调离现岗位，对其他责任人分别给予相应处理。

【案例启示】本案中该国企新入职人员张某将国家秘密载体作为废品处理，暴露出两个问题：一是单位不重视涉密文件管理，在涉密载体的收发、传递、使用、保存、送销等环节未形成闭环；二是清理、管控涉密载体的工作人员警惕性不强，单位内部对涉密人员的保密常识培训不到位。各级机关、企事业单位要对保密工作真重视、多强调、

常提醒，涉密人员要知纪律、守规矩、绷紧弦，只有层层履职尽责，才能真正守牢保密防线。

三、非法复制、记录、存储国家秘密：未经批准、擅自复制、摘抄涉密文件资料；擅自对涉密谈话、会议和活动等内容进行文字记载或录音、录像；私自留存、存储国家秘密信息或者国家秘密载体。

【典型案例】某直属单位技术保障处干部王某擅自扫描涉密文件留存问题。2018年3月，某部委在开展保密检查时发现，某直属单位技术保障处干部王某擅自扫描涉密文件存储在

涉密计算机中。经查，王某出于留存参考目的，未履行审批手续，擅自扫描机密级文件1份、秘密级文件4份，存储在涉密计算机中。事件发生后，该部委给予王某行政警告处分，延长其预备党员预备期8个月，责令其作出深刻检查；对负有领导责任的处长陈某进行通报批评，取消其2018年评优资格，责令其作出书面检查。

【案例启示】王某擅自扫描涉密文件存储在涉密计算机中，并非出于工作必需，且事先没有经过领导审批，是个人违规行为，虽然并未造成实际泄密后果，但是存在严重的泄密隐患，

这种行为必须严令禁止。涉密单位要经常性开展保密监督检查，以涉密人员、涉密信息设备、涉密载体管理为重点，仔细查、严格查、反复查，压实保密管理主体责任，把日常保密监管融入工作方方面面，不断查漏补缺，确保及时消除风险隐患。

四、在私人交往和通信中涉及国家秘密：在私人交往、通信中涉及国家秘密，会导致国家秘密知悉范围的扩大，造成国家秘密失控，必须严格禁止。

【典型案例】广西南丹县疾控中心办公室主任熊朝盛、工作人员区俊祥泄露疫情防控工作材料问题。2020

年1月26日，熊朝盛在未经审批的情况下，擅自将该县新型冠状病毒感染的肺炎防控有关工作材料通过QQ发送到本单位QQ工作群。区俊祥发现这一信息后，随即将原文转发到其个人微信群，并被其他群内成员转发扩散，在社会上造成不良影响。2020年2月3日，南丹县监委决定对熊朝盛、区俊祥进行立案调查。

【案例启示】近年来，机关单位工作人员违规通过微信等移动应用发布、传输、处理涉密文件材料的泄密行为多发易发。本案中熊朝盛、区俊祥作为疾控中心工作人员，应知泄露

疫情防控工作材料会引发的后果，却仍然将涉密文件转发到其个人QQ、微信群，究其根源，主要还是由于机关单位保密制度执行不严、保密管理不到位，工作人员保密意识、保密常识欠缺。全面加强微信使用的保密管理，规范工作人员特别是日常工作中接触、知悉国家秘密人员的移动办公行为，已刻不容缓。

五、在互联网及其他公共信息网络或者未采取保措施的有线和无线通信中传递国家秘密：互联网、固定电话网、移动通信网、广播电视网等公共信息网络，以及没有保密措施的有线和无线通

信，都无法确保信息传递的安全，不能用来传递国家秘密。

【典型案例】某市经济和信息化局办公室人员孙某将秘密级文件资料违规上传到网盘问题。2020 年 12 月，为撰写材料方便，某市经济和信息化局办公室人员孙某在未经保密审查的情况下，擅自将计算机中存储的有关文件、资料上传到某网盘，其中包括 6 份秘密级国家秘密，被给予党内警告处分。

【案例启示】有的机关、单位工作人员知保密、懂保密，也能够预见违

规使用网盘存储、传递、分享涉密文件、资料可能造成泄密，但仍缺乏应有的警惕，为了所谓的“方便工作”，犯了不该犯的错。我们必须认识到，互联网具有高度的开放性，甚至部分服务器还在境外运行，通过网盘存储、传递、分享国家秘密，网盘服务运维人员能随时查看其中的内容，存在国家秘密接触范围失控问题，应当绝对禁止。

六、使用非涉密计算机、非涉密存储设备存储、处理国家秘密信息：使用非涉密计算机、非涉密存储设备存储、处理国家秘密信息，将使国家秘密失去

有效控制和保护，极易造成泄密。

【典型案例】某市委研究室副主任张某使用非涉密计算机处理涉密文件问题。2018年6月，某省保密局在保密检查中发现，该市市委研究室副主任张某，违规在连接互联网的非涉密计算机中存储、处理1份标注“秘密”的文件（经核实，此件为该市市委办公室2015年正式印发的涉密文件）。经查，2017年12月，张某作为单位公认的“笔杆子”，承担了某次涉密会议的会议材料起草工作。期间，其因所用涉密计算机无法正常启动，向信息部门报修，技术人员查看后表

示，此为硬件故障，短时间内无法修复，建议其换一台计算机临时使用。为了抓紧完成文稿起草任务，张某在技术人员帮助下，用光盘将存储在故障涉密计算机中的部分文件夹，刻录拷贝到另一台连接互联网的非涉密计算机处理。在文件拷贝过程中，其未认真查看文件夹内详细情况，误将标密文件一并存储到连接互联网的非涉密计算机中，直至在保密检查中被发现。事件发生后，张某深刻认识到自己的错误行为，主动配合组织进行调查，作出深刻检讨。

【案例启示】部分单位使用非涉

密计算机存储、处理涉密信息的情况时有发生，一方面是工作人员保密意识、风险意识不强，对保密法律法规缺乏学习；另一方面是对涉密计算机及移动存储介质和涉密配套设备管理不到位，未能采取强制分类管控措施。要防范互联网计算机泄密事件的发生：一要加强保密技能学习，提高防范窃密泄密的实际能力。二是要系统落实保密人防、物防、技防措施，切实加强计算机及网络保密管理，坚决做到“上网不涉密、涉密不上网”。