内部发行
注意保存

警钟长鸣

2022年第6期（总第142期）

中共和平区纪委　　2022年6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（二）

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，本期《警钟长鸣》将继续对《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，切实引以为戒，持续做好保密各项工作。

一、在未采取防护措施的情况下，在涉密信息系统与互联网及其他公共信息网络之间进行信息交换，容易被植入“木马”等窃密程序，使涉密信息系统受到远程控制，导致国家秘密被窃取。

【典型案例】出于“省事”心理违规上传涉密内容，造成失泄密后果。某市教育局体育艺术卫生保健站网站站长陈某、网站维护和信息发布人员邢某参加了某涉密会议。会后，邢某将1份与会议相关的机密级领导讲话录入个人使用的计算机中。此后，为方便学习，他在未向站长陈某请示、

未履行审查手续的情况下，将上述机密级文件上传至网站，造成泄密。事件发生后，有关部门给予陈某行政警告处分、邢某行政记过处分。

【案例启示】麻痹心理、省事心理直接导致了本案例中邢某违反保密法律法规，置国家秘密安全于不顾。这些心理的背后，是保密意识的淡薄和敌情观念的弱化，是对新时期保密工作面临形势的严峻性和复杂性的估计不足，是对自己行为可能造成严重危害的估计不足。各级机关和广大公职人员要引以为鉴，提防两种心理，时刻将“国家利益高于一切，保密责

任重于泰山”根植心中。

二、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的；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】将网盘当作“涉密硬盘”，违规存储涉密文件资料。某市经济和信息化局办公室借调人员孙某为撰写材料方便，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】网盘是放在互联网上的“大硬盘”，因其具有多终端登录、容量大、速度快等特点，受到一些机关单位工作人员亲睐，随之而来，也屡屡造成不少失泄密事件。本案中的孙某为一己之便，没有仔细查看拟上传的文件资料中是否含有涉密内容，便将涉密文件资料混同其他文件资料一并存储在网盘中，严重违反了保密法律法规。我们要深刻汲取教训，以案为鉴，在日常工作中切实加强数字化网络化条件下的保密管理工作，

严防此类失泄密案件的发生。

三、擅自卸载、修改涉密信息系统的安全技术程序、管理程序的；安全技术程序、管理程序，是指为确保涉密信息系统的运行安全、信息安全而安装在涉密信息系统中，对系统进行安全保密防护的应用程序。擅自卸载、修改，将造成涉密信息系统技术防护和管控能力下降或丧失，大大增加泄密风险。

【典型案例】违规升级软件，造成泄密风险问题。2020年9月，有关部门在工作中发现，某县级单位1台涉密计算机多次发生违规外联。经查，该计算机为办公室工作人员孙某使

用，孙某在使用过程中，看到某软件发生故障，就多次按照软件提示，尝试连接互联网进行自动修复，造成违规行为发生。

【案例启示】本案例中孙某保密意识淡薄，明知计算机的涉密属性，还连接互联网进行软件修复，这种行为极易造成涉密信息系统技术防护能力下降或丧失，大大增加泄密风险。广大机关单位是国家秘密产生的源头，机关单位公职人员是国家秘密载体制作、使用和管理职责的主要承担者，我们要在工作实践中，时刻绷紧保密这根弦，从严抓好保密法纪执行和保密措施落实，严防

泄密事件发生，确保党和国家秘密安全。

四、将未经安全技术处理的退出使用的涉密计算机、涉密存储设备赠送、出售、丢弃或者改作其他用途，其中存储的国家秘密信息即使删除仍可以通过技术手段回复，存在严重泄密隐患。

【典型案例】违规送修涉密计算机，造成涉密文件失控。某单位综合处处长魏某为图工作方便，违规安排工勤人员将1台涉密计算机送外维修，致使维修人员将该计算机连接互联网，并在该机上交叉使用两个非涉密U盘，造成相关涉密文件失控。有关部

门给予魏某党内警告处分。

【案例启示】此泄密典型案例，暴露了少数机关、单位没有严格落实涉密人员包括编外、借调、临聘人员保密管理要求，存在着保密意识薄弱、保密知识缺乏、保密管理松懈等问题。各级单位要充分认清当前保密工作的重要性，教育引导相关工作人员提高保密意识和对保密工作的责任心，纠正部分人员“无密可保、有密难保”的错误认识，筑牢保密思想和保密安全防线。

五、邮寄、托运国家秘密载体出境，或者未经有关主管部门批准，携带、传

递国家秘密载体出境的；向境外传递涉密载体，应当按照国家有关规定办理。外交信使能够到达的地方，须由外交信使携运；境外目的地不通，外交信使或者信使难以携运，且却因工作需要自行携运出境的，应当向有批准的保密行政管理部门或机构申请办理批准手续。

【典型案例】未经有关主管部门批准，携带、传递国家秘密载体出境问题。某市市委副秘书长马某在筹备年底全市经济工作会议期间被安排因公出国。为不影响所负责会议材料的审改，马某擅自将6份秘密级会议材料和有关内部资料随身携带，准备出

国，在机场海关检查时被海关人员发现，当场扣留。事件发生后，马某被责令向市委保密委作深刻检查，取消其当年市委办公室工作实绩考核评优资格，一年内不允许因公出境。

【案例启示】与境内的安全保密环境相比，国家秘密载体在境外携带、使用、保管各环节面临的不可控因素多，泄密风险大，一旦泄露很难采取补救措施。保密法禁止邮寄、托运国家秘密载体出境，或者未经有关主管部门批准，携带、传递国家秘密载体出境。广大机关、单位在能够满足工作需要的前提下，应尽量避免国家秘密载体出境，特

殊情况确需传递国家秘密信息出境的，应当按照国家有关规定办理。

六、通过普通邮政、快递等无保密措施的渠道传递国家秘密载体的；普通邮政、快递、物流不具备安全保密保障条件，通过这些方式传递涉密载体，将造成涉密载体管理失控，极易泄密，应当严格禁止。

【典型案例】违规使用快递等方式传递涉密载体问题。某涉密单位产品部员工李某擅自通过韵达快递将某密品发送到其他涉密单位。经鉴定，该密品属于秘密级国家秘密。事件发生后，有关部门给予李某行政记过处

分，调离涉密岗位，扣发1年保密补贴，经济处罚2万元；给予负有领导责任的部门支部书记欧某行政警告处分，经济处罚1万元；对党委书记李某等3人进行通报批评，经济处罚5000元。

【案例启示】普通邮政、快递、物流等不具备安全保密保障条件，通过这些方式传递涉密载体，缺乏安全管控措施，可靠性差，有可能造成涉密载体丢失。保密法严禁通过普通邮政、快递等无保密措施的渠道传递国家秘密载体。在工作中，各机关、单位应严格执行保密规定，在国内传递

涉密载体应通过机要通信、机要交通或者指派专人传递；在市内传递机密级、秘密级涉密载体，应通过机要交换站进行。