

廉 政 警 示

第 83 期

北京中医药大学纪委办公室（监督检查室、监察处） 2024 年 8 月 15 日

无视党纪法规，这些泄密案例发人深省

党和国家事业的蓬勃发展，须臾离不开保密工作的有力保障。自觉遵守保密纪律是党员干部的义务，也是党纪国法的要求。

《中国共产党纪律处分条例》规定，泄露、扩散或者打探、窃取党组织关于干部选拔任用、纪律审查、巡视巡察等尚未公开事项或者其他应当保密的内容的，视情节给予警告直至开除党籍处分。

每一名党员干部都必须履行“严守党的纪律，保守党的秘密”的庄重承诺，严格遵守党和国家各项保密制度规定，以实际行动诠释对党忠诚。

违纪托人走后门 考察资格被取消

某市市委决定选拔一名县委书记，市卫计委主任迟某是组织考察对象之一。市委组织部干部一处副处长宋某是经办人。迟某为及时掌握“组织动态”，托人找到宋某，希望得到帮助。宋某将组织考察情况以及其他考察对象等有关情况透露给迟某，并为其出谋划策。经组织调查，迟某

被取消考察资格，并给予严厉处分；宋某泄露、扩散党组织秘密，被给予相应处分。

偷拍密件传亲属 违规违纪遭处分

某市司法机关工作人员茅某在机要秘书蔚某处看到1份关于某重点案件处理意见的机密级文件。茅某的姐姐正是该案的当事人之一，为让姐姐早日吃上“定心丸”，茅某趁蔚某不备时，用手机偷拍了文件首页，微信发给了姐姐，姐姐又将图片发到该案当事人的微信群中，导致大范围泄密。事件发生后，有关单位给予茅某党内警告和行政记过处分，给予其姐姐党内严重警告和行政记大过处分。

泄露举报人身份 干预办案被判刑

某镇纪委书记吴某接到一封中央扫黑除恶督导组以秘密级别转办的实名举报信，主要反映该镇副镇长宁某涉黑涉恶问题线索。吴某随后把举报信复印给宁某。之后，宁某在吃饭时故意将举报信拿出给同席者阅看、拍照，导致该实名举报信在社会上流传。举报人身份被曝光后，遭到具有黑社会背景的被举报人家属的警告质问，造成恶劣的社会影响。事件发后，22名公职人员受到党纪政务处分，2人移送司法起诉。

案例警示

党纪法规不容破坏。保密纪律是重要的政治纪律和政治规矩，党员干部要时刻绷紧保密纪律这根弦，切实增强保密意识，严守保密工作规定，时刻保持清醒的头脑和高度的警惕性与责任感，筑牢保密安全防线，绝不做违反党纪国法的事情。

严格遵守工作纪律。对正在办理、尚未公开的干部选拔任用情况、信访举报内容、巡视巡察事项等应保密的内容，不得打探、扩散、泄露。

确保不该说的不说、不该传的不传。

警惕防范泄密风险。要经常性地排查、警惕日常工作中存在的泄密风险点，自觉抵制金钱物质诱惑和江湖义气“绞杀”，防止违纪提供“情况”、疏通“关系”等现象。要严守保密底线，做到公事家事内外有别，切忌以私犯公，犯下大错。

多名年轻干部泄密被查！

年轻干部是党和国家事业发展的希望。从近年来失泄密案件分析中发现，保密意识淡薄、保密常识欠缺、保密制度执行不严是导致年轻干部发生失泄密问题的主要原因，值得反思与警醒。

案例一 遮挡密标，掩耳盗铃

2022年8月，某市直单位新选调干部孙某在周末值班期间接收到上级部门的涉密会议通知。孙某将密级标识遮挡后拍照，通过微信发送给梁某。梁某收到后及时发现问题，立即通知孙某删除，并向单位领导汇报。案发后，孙某被给予党纪政务处分，其所在部门负责人被给予批评教育处理。

案例二 无知无畏，自欺欺人

2021年12月底，某省直机关业务骨干赵某起草工作总结等多个综合类文稿。恰逢元旦假期，赵某擅自将多份涉密材料刻录，并通过单位互联网计算机上传至个人微信文件传输助手，以便回家使用。该涉密材料自动备份至计算机微信客户端文件夹中，在保密检查中被发现。案发后，赵某被给予党纪政务处分。

案例三 疏于管理，麻痹大意

2020年6月，某县委办公室秘书股股长小张在整理蒋某移交的涉密文件时，被领导临时安排外出，他随手将涉密文件放在了窗台上。回来后他忙于处理工作，将此事置之脑后，几日后才想起。最终，涉密文件未能找回。案发后，小张被给予党纪政务处分，调离工作岗位，相关责任人受到通报批评等处理。

案例四 主观臆断，投机取巧

2021年，某市直机关吴某收到一份上级印发的标注“内部”字样的工作方案，为方便起草落实方案，吴某使用手机拍摄文件，通过“传图识字”微信小程序扫描识别为电子文档。吴某后将起草的初稿发送至单位微信工作群征求意见，被同事张某、廖某等多次转发，导致文件知悉范围扩大，给相关工作造成被动。案发后，吴某被给予党纪政务处分，张某、廖某等被给予通报批评、责令检查等处理。

严守保密纪律是年轻干部的责任义务 年轻干部要从以下方面做起 真正成为堪当大任的栋梁之才

有定力，筑牢理想信念之基。

保密工作事关党和国家发展全局，年轻干部要不断提高政治站位，深刻认识到做好保密工作对国家安全和利益的重要意义，牢记肩上的保密责任。同时，在日常工作中要提高分辨是非的能力，严格按照保密规定行文办事，坚决杜绝失泄密事件发生。

善学习，主动学习丰富阅历。

年轻干部要将保密知识和保密能力作为一项业务基本功，积极参加保密业务培训及保密宣传教育活动，主动学习保密知识，不断增强保密意识，熟练掌握保密工作的方针政策和法规纪律要求，全面掌握岗位所必需的保密知识和技能，确保自身保密工作能力始终适应形势和任务发展需要。

知敬畏，严格遵规守纪。

年轻干部要心有所畏，敬畏法纪、敬畏工作，非涉密场所不谈论涉密事项，在从事涉及国家秘密的工作事项时，时刻保持如临深渊、如履薄冰的自觉与谨慎，始终把保密纪律和规矩挺在前面，将保密要求内化于心、外化于行。在日常工作中，年轻干部从一开始就要养成良好的保密习惯，坚决防止违反保密规定的“第一次”行为出现。

警惕！这些办公“黑科技”可能有失泄密风险！

科技蓬勃发展的数字时代，网上办公以其时效性和便捷性成为当今社会一种流行的工作方式。诸多线上平台汇集了强大的即时交流、格式转化、文件快传、群组讨论等兼顾社会交流和办公工具属性的“黑科技”功能，成为广大上班族处理日常事务的首选。然而，近年来因使用网上办公程序而导致的失泄密案件屡屡发生，暴露出一系列风险隐患。

——云助手泄露涉密文档。“文件传输助手”能够实现文件云端存储，在不同设备终端均可下载使用。一些上班族为图工作便利，将涉密文件违规传输至“传输助手”，方便下班后使用个人手机或电脑下载处理。殊

不知涉密文件上传网络后，电脑和手机设备自动同步与存储的过程大大增加了境外间谍情报机关通过木马病毒获取相关文件的风险。此外，传输软件公司后台也能轻易获取涉密文件，且无法有效控制知悉范围，极易造成失泄密。

——**图文识别小程序泄露密件原件。**OCR 识别技术的成熟给办公工作带来了十足的便利，种类繁多的图文识别小程序能够轻松抓取图片信息中的文字并一键转换文本。部分涉密岗位工作人员为导入密件文字内容，违规将密件使用线上小程序进行拍摄识别。尽管有意遮盖了密件的红头标志和密级，但密件原件的图片上传网络平台后，境外间谍情报机关通过技术手段能够轻松获取软件后台数据，窃取国家秘密。

——**AI 写作泄露涉密内容。**近年来，AI 写作蓬勃发展，逐渐成为许多办公人士的“笔杆子”，用户只需要输入具体需求，就能一键生成文章。部分涉密人员在起草涉密材料时，为节省工作时间，违规将涉密素材和涉密文件内容输入 AI 写作小程序生成文章，并认为只是截取文件片段，不至造成泄密。殊不知，AI 小程序会自动收集用户输入的信息内容以供自主学习，相关数据易被境外间谍情报机关窃取，造成国家秘密泄露。

——**工作群组泄露涉密信息。**许多单位为方便沟通，组建了许多用来通报交流工作事项的“工作群”。部分单位违规在“工作群”中通知、讨论涉密工作事项，甚至将涉及国家秘密和工作秘密的内容以图片、文件等形式在群聊内发布。这些群聊中的涉密信息极易被群成员转载甚至对外公开，无法控制知悉范围。境外间谍情报机关还能通过网络攻击获取重点工作群组的聊天记录，存在极大失泄密隐患。

国家安全一切为了人民，一切依靠人民。我们在享受科技给日常工

作、生活带来便利的同时，也要坚决绷紧保密防范之弦，警惕境外间谍情报机关利用网络窃取我国家秘密的阴谋诡计。

——网上办公勿涉密。严禁通过互联网处理涉密信息，使用办公软件时禁止在线上发布、传播涉密信息，不能以方便工作为由将涉密文件线上存储。

——小程序使用莫大意。严禁将涉密文件拍摄、摘录后上传互联网，使用文字识别、AI 写作等功能时应杜绝输入涉密文件，防止方便了工作却泄露了秘密。

——个人设备常自查。从事涉密岗位、有机会接触到涉密内容的工作人员应定期对手机、电脑等私人电子设备开展自查，杜绝用互联网设备处理涉密信息，同时也要及时对涉密计算机开展病毒自检，防止境外间谍情报机关植入病毒窃取数据。

——企事业单位重教育。涉密企事业单位要定期开展国家安全宣传与保密警示教育，对内部“工作群”加强监督检查，履行涉密材料处理的日常监督责任，抓好涉密人员日常管理。

【来源：共产党员微信公众号、国家安全部等】