# 【举案说法】不容侥幸！且看泄密事件的“墨菲定律”

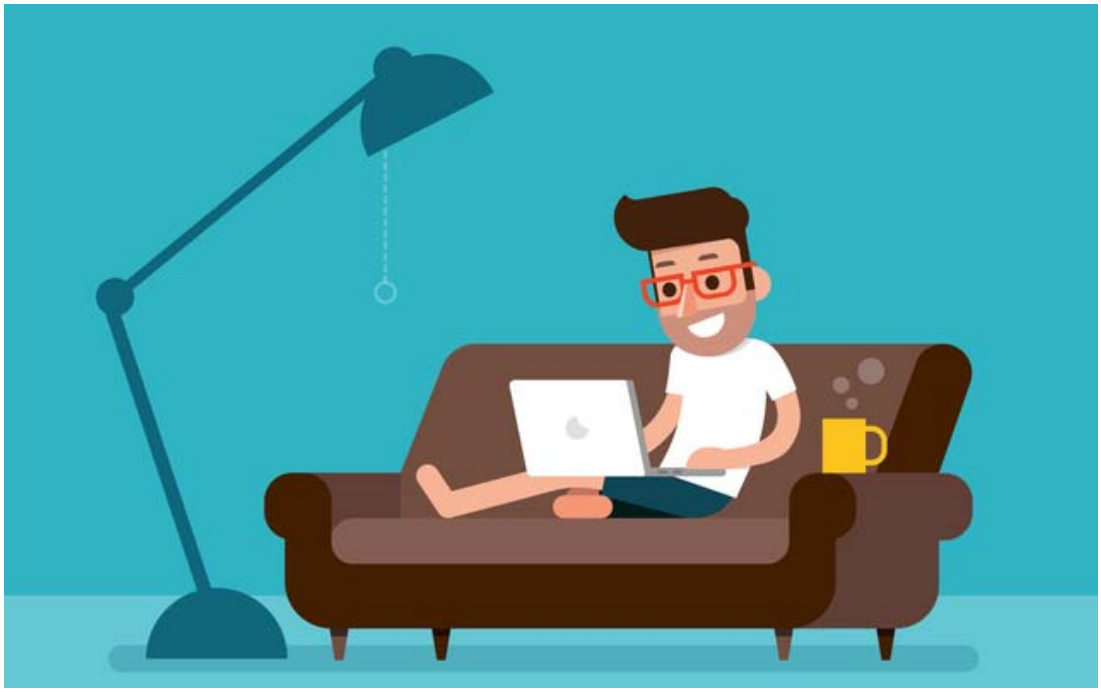
爱德华·A·墨菲是美国某空军基地的工程师。一次，他和同事在试验中，因仪器失灵发生事故。事后墨菲发现，原来是测量仪表被一名技术人员装反了。由此，他总结出规律：**凡事只要有可能出错，那就一定会出错**。这便是著名的“墨菲定律”。

而对于“非十分不可”的保密工作来说，“墨菲定律”格外适用。它揭示着：**如果存在违反保密规定的行为，即使此种行为造成泄密的可能性极小，也必然会导致泄密事件的发生**。我们不妨来看看以下 5 个案例。

# 典型案例

**案例 1：**2020 年 12 月，某单位负责人韩某参加培训，需撰写学习心得并将之发送至互联网邮箱。写作时，韩某认为学习心得不用于公开发表，便擅自引用了培训班发放的涉密学习资料内容。随后，他用微信将文件传给秘书包某，让包某代发至邮箱。2021 年 1 月韩某履新，接任者秘书张某需要撰写文稿，包某遂将微信中留存的韩某的学习心得提供给其参考。张某引用韩某文稿中的涉密内容写成一篇文章，并刊登在该单位网站上，造成严重泄密。

**案例 2：**2009 年，某单位工作人员赵某在承担涉密专项工作期间，因妻子身体不适需要照顾，将正在撰写的涉密文稿及资料拷至 U 盘，在家中未联网的计算机上进行处理。事后，赵某认为该计算机并不联网，有关资料尚属安全，故未及时清理。几年后，赵某的孩子需要上网学习，其妻将家中的计算机联网，造成该计算机被控制，存储在其中的涉密文件资料被窃。



**案例 3：**2009 年，某单位人员发现一涉密计算机存在故障，送单位信息中心修理。信息中心承办人宋某为该计算机更换硬盘，并将旧硬盘随手放置。几个月后，宋某在整理工作台时，忘记该硬盘来源，遂将硬盘连接在自己使用的互联网计算机上查看。由于该互联网计算机长期被控制，硬盘中的涉密文件资料被窃。

**案例 4：**2008 年，某单位驻外人员戴某在赴任途中，与老友李某见面，共同游览当地的风景名胜、感受风土人情，并拍摄了不少照片。离别前，李某提出将照片拷到戴某携带的涉密 U 盘上，遂将 U 盘连接至自己的互联网计算机。殊不知该计算机长期被控制，U 盘中的涉密信息被窃。

**案例 5：**2014 年的十一假期前夕，某单位涉密人员王某准备回乡探亲，但领导临时交办其一项重要涉密文稿任务。王某加班加点完成后，为方便修改稿件，将涉密文稿拷贝到自己使用的笔记本电脑中带回老家。随后，因弟弟学习需要使用电脑，王某将笔记本电脑留在家中，并提出让其弟通过电子邮件将上述涉密文稿发给自己，造成泄密。

## 深刻启示

通过 5 起案件，我们不难发现：只要违反保密规定，就在客观上存在泄密的风险；只要客观上存在泄密的风险，那么造成泄密就是迟早会发生的事。为有效克服墨菲定律的“魔咒”，各机关单位应当加强以下几个方面管理。

**1.增强涉密人员防范意识。**各机关单位要持之以恒进行保密教育，结合发生的典型案例，把规定讲透彻，把红线画清楚。要让涉密人员充分认识到，防范泄密，必须从最坏的可能性来设想和部署。必须严格执行各项保密规定，确保形成工作闭环。

**2.采取多种管理防控措施。**除了常规的物防、技防外，还要重视智能手段在保护国家秘密方面的作用，推动涉密信息系统和涉密载体智能化，推动智能监管、智能提醒等功能落地。

**3.全面彻底开展保密检查。**必须主动、及时清理死角、消除隐患，以降低泄密事件发生的概率，变事后管理为事前管理，变被动管理为主动管理。

**4.加大责任追究处罚力度。**对于涉密人员违反保密规定的行为，应当从严把握处理的标准和尺度，同时注意追究其直接领导和分管领导的责任，严格依规进行处理，在全单位形成克服松散心理、严格遵守规范的良好氛围。