**分析网络安全案例**

2022年4月，我国国家安全机关破获了一起为境外刺探、非法提供高铁数据的重要案件。上海某科技公司为牟取利益，持续采集、传递数据给某境外公司。这起案件是《中华人民共和国数据安全法》实施以来，首例涉案数据被鉴定为情报的案件，也是我国首例涉及高铁运行安全的危害国家安全类案件。

据报道，如果不法分子利用数据故意干扰或恶意攻击，将会造成高铁通信无线信号中断，影响高铁运行秩序，对铁路的运营构成重大威胁。

事件起因是一家境外公司自称其客户从事铁路运输的技术支撑服务，为进入中国市场需要对中国的铁路网络进行调研，但是受新冠疫情的影响，境外公司人员来华比较困难，所以委托境内公司采集中国铁路信号数据，包括物联网、蜂窝和GSM-R，也就是轨道使用的频谱等数据。需要的器材设备普通易购，并非专用间谍器材，包括天线、SDR设备、电脑、移动硬盘。但利润却十分丰厚。

这家境外公司从事国际通信服务，但它长期合作的客户包括某西方大国间谍情报机关、国防军事单位以及多个政府部门。在数据时代，境外一些机构、组织和个人，针对我国重要领域敏感数据的情报窃密活动十分突出，给国家安全和经济社会发展造成了重大风险隐患。

随后双方约定了两个阶段的合作：第一阶段由上海这家公司按照对方要求购买、安装设备，在固定地点采集3G、4G、5G、WIFI和GSM-R信号数据；第二阶段则进行移动测试，由上海公司的工作人员背着设备到对方规定的北京、上海等16个城市及相应高铁线路上，进行移动测试和数据采集。在这个过程中将中国铁路信号数据等关键数据信息转移到境外，仅一个月采集的信号数据就已经达到了500个G。

对此，这个案件启示我们，我们要保护国家数据安全，保护数据不被境外势力窃取。相关数据中心要建立健全数据安全治理体系，包括数据分类、权限控制、备份恢复、审计监控等方面。国家基础信息、国家核心数据事关国家安全、国计民生和重大公共利益，是数据安全保护工作的重中之重。我们要进一步增加国家安全意识，坚持总体国家安全观，共同建立健全数据安全治理体系，提高数据安全保障能力，筑牢维护国家安全的钢铁长城。

这个案例同时启示我们在日常生活保护自身的数据安全也是十分重要的。保护个人信息不被盗取，我们可以采取以下办法：一、使用强密码，不要使用相同的密码，定期更改密码。二、不要随意丢弃含有个人信息的票据，如火车票、快递单、银行对账单等。三、注册各类应用、网站时尽量赋予最少的信息和权限。四、不要使用不正规的网站或软件。五、不要随意连接不明、不点击短信的不明链接和扫描未知二维码，不轻信电话、短信、QQ、微信中所谓退款、贷款验资、司法协查、商品退款、积分兑换、中奖退税等信息。

数据安全是一个国家的重要安全领域，也是企业和个人的重要安全领域。我们应该共同努力，建立健全数据安全治理体系，提高数据安全保障能力，筑牢维护国家安全的钢铁长城。