盗卖信息、定向“开盒” 这些案件都判了

通过“开盒”网暴，非法获取公民个人信息数据9亿余条；利用担任铁路车站客运员的职务便利，通过铁路车票系统查询他人搭乘高铁的具体信息，并以每条10元至60元不等的价格出售……近日，最高人民法院发布侵犯公民个人信息犯罪及关联犯罪典型案例。

保护账户密码安全

妥善处理纸质信息

警惕网络“诱饵陷阱”

遏制信息泄露风险

图片来源：公安部网安局

帮助他人定向“开盒”

网络“开盒”作为新型网络暴力违法犯罪，在网络上公开发布煽动网民针对特定人员攻击谩骂，或者提供有偿查询、帮助他人定向“开盒”，给被害人及其家人的身心健康和人身安全造成极大伤害。

2023年至2025年间，被告人林某某、王某某非法获取公民个人信息数据，后以虚拟货币收款等方式出售牟利。经查，林某某非法获取公民个人信息数据6亿余条，王某某非法获取公民个人信息数据3亿余条。二人利用加密通信工具设立群组，担任群组管理员，在群组中发布针对他人侵犯隐私、侮辱谩骂等违法犯罪信息。

最终，法院综合本案事实、情节、后果等，对被告人林某某以侵犯公民个人信息罪判处有期徒刑六年六个月，并处罚金人民币六万元；以非法利用信息网络罪判处有期徒刑一年，并处罚金人民币一万元，决定执行有期徒刑七年，并处罚金人民币七万元。对被告人王某某以侵犯公民个人信息罪判处有期徒刑五年六个月，并处罚金人民币五万元。

最高人民法院刑三庭二级高级法官王珂认为，此案例提示公众，一定不能非法获取、提供、出售公民个人信息，更不能为了宣泄情绪或者牟利而将他人的隐私信息在网络上“开盒”发布。

行业“内鬼”泄露个人信息

“内鬼泄露”指的是利用职务便利非法泄露公民个人信息，如运营商、快递、汽车4S店、房地产等企事业单位内部工作人员泄露公民个人信息。

2019年1月，被告人陈某某利用担任铁路车站客运员的职务便利，通过铁路车票系统查询他人搭乘高铁的具体信息，并以每条10元至60元不等的价格出售。上述非法获取的公民个人信息部分被出售给被告人林某某等人，用于有偿查询演艺人员等的行程信息。截至2021年9月，陈某某违法所得共计约19万元。

法院对被告人陈某某等人以侵犯公民个人信息罪判处有期徒刑三年八个月至有期徒刑九个月，缓刑一年六个月不等，并处罚金人民币二十万元至一万四千元不等。对于检察机关提起的附带民事公益诉讼，判决责令陈某某等人分别支付公益损害赔偿金二十万元至一万余元不等，删除所有非法获取的公民个人信息，并在国家级媒体上公开赔礼道歉。

最高人民法院刑三庭二级高级法官王珂认为，公民个人信息是网络犯罪黑灰产业链条中最核心的一个要素，从源头上防范和杜绝个人信息的泄露，是依法惩治此类犯罪的根本。

如何保护个人信息安全？

一、从账户密码安全着手

避免使用生日、手机号码、“123456”等简单组合作为密码。建议采用“场景化密码”策略，如“买菜App=Mc@2025#”（即买菜拼音首字母+年份+特殊符号）。

审慎注册信息提供，防止过度信息披露。在非必要场景下，建议使用“临时信息”替代真实信息。例如，快递收件信息可设置为“代收点+昵称”（如“幸福区小A收”）。

二、洞察线下场景隐蔽风险

妥善处理纸质信息，确保信息彻底销毁。对于快递单、车票、水电费单等纸质文件，在销毁前需使用油性笔涂抹覆盖姓名、地址、电话等关键信息。

身份证复印件应注明用途，如“仅用于2025年5月办理XX业务”，并确保字迹横跨证件主要区域。对于废弃手机、电脑等电子设备，在恢复出厂设置后，建议使用专业数据擦除软件（如“数据粉碎”工具）进一步清除存储数据。

明确社交信息边界，防范信息泄露风险。在社交媒体使用过程中，应谨慎发布个人生活信息。朋友圈定位避免精确到“家楼下”，晒娃时避免露出孩子正面及姓名，旅游照片注意避开家门、车牌等敏感细节。

三、遵循线上活动安全准则

警惕网络“诱饵陷阱”，避免陷入钓鱼风险。对于短信中包含的链接，切勿随意点击。如收到“您的快递已签收”“积分即将过期”等短信，应先通过官方APP或网站进行核实。正规银行及平台不会通过短信要求用户输入密码。

在连接WiFi时，应谨慎选择公共网络，商场中无密码的WiFi可能为黑客搭建的钓鱼网络，建议优先使用手机热点或向店员确认官方WiFi名称。对于网页弹窗信息，需保持冷静，仔细核实网址是否为正规域名。

定期维护设备安全，强化电子设备防护。手机和电脑应开启“自动更新”功能，及时安装系统补丁以修复最新安全漏洞，避免因嫌重启麻烦而关闭更新。

四、建立“应急响应机制”

及时采取行动，遏制信息泄露风险。一旦发现账号异常，应立即修改密码，开启登录保护功能，并检查“最近登录设备”，删除陌生终端设备。

如收到诈骗电话或短信，需详细记录对方掌握的个人信息（如“对方知晓我上周购买快递的信息”），并拨打110报警电话或通过“12321网络不良与垃圾信息举报受理中心”进行投诉。

养成信息审计习惯，持续监测个人信息安全。建议每年通过“中国人民银行征信中心”官网查询个人信用报告，确认是否存在陌生贷款或信用卡开户记录。

定期梳理手机APP，卸载三个月以上未使用的软件，尤其关注曾授权通讯录、定位等敏感权限的工具类APP。

来源：新华社