最高检发布保护公民个人信息案例，揭示犯罪套路——

个人信息是怎么“失窃”的

人民日报记者 倪弋

境外“社工库”倒卖公民个人隐私，滥用GPS定位技术非法获取个人信息，窃取个人信息10亿余条并进行网络“开盒”……在《中华人民共和国个人信息保护法》实施5年之际，最高人民检察院发布一批依法保护公民个人信息典型案例，聚焦当前侵犯公民个人信息犯罪的新特点、新趋势，揭示犯罪套路和危害后果并进行警示提醒。

警惕“境内找买家—境外拿数据—境内加价倒卖”犯罪链条

2024年6月，王某、许某玲发现可以从境外网络“社工库”批量购买我国公民个人信息，便租赁场地、招募业务员、组建“工作室”。王某对接上游卖家，许某玲负责资金结算，业务员通过电话和网络寻找下游买家，形成“境内找买家—境外拿数据—境内加价倒卖”的犯罪链条，倒卖户籍、财产状况、行踪轨迹等信息，涉案198万余元。为逃避查处，团伙统一配工作手机和社交账号，用网络支付收款，再以虚拟货币向境外上游付款。

浙江省金华市婺城区人民检察院对电子数据作实质化审查，把信息源头、流转路径、资金结算一节节查明，依法认定犯罪事实和数额；引导侦查、监督立案，把上游供料人员、下游二次倒卖者一并抓获，实现全链条惩治。

侵犯公民个人信息犯罪日益呈现组织化、链条化、跨境化等特征，类似犯罪链条也藏在“公开信息”的二次加工里。刘某专门设立房产中介公司，招募人员从各类平台抓取“一手女房东”发布的房屋租售内容，再筛选出有一定经济实力的女性，把房产信息、联系方式等打包整理，向境外人员出售，共非法获取、出售信息2.4万余条，获利19万余元。

江苏省无锡市滨湖区人民检察院审查认为，已公开信息不是可任意倒卖的“公共资源”——刘某未经权利人同意，擅自改变信息公开目的与用途，定向加工后跨境提供，明显超出合理使用限度。检察机关以“情节特别严重”提起公诉，向行业主管部门制发检察建议进行风险提示，推动房源信息发布审核与中介行业源头治理。

犯罪手法从人工偷向技术窃转变，隐蔽性强、危害性大

2020年起，陈某丞、陆某鹏、马某力为博取网络影响力，使用脚本代码侵入某省事务平台系统，非法获取公民身份号码、电话号码等1600万余条；又编写程序窃取多个网络贴吧、云空间用户账号信息10亿余条。依托精准窃取的个人信息，犯罪分子对47名网友实施“开盒”、网暴、线下滋扰，致5名被害人因精神抑郁就医，多名未成年人、在校大学生产生厌学情绪。

审查起诉阶段，检察机关组织网络信息专家研判：陆某鹏侵入国家事务计算机信息系统并提供技术支持，构成非法侵入计算机信息系统罪与寻衅滋事罪，数罪并罚；陈某丞、马某力侵入系统获取信息，以侵犯公民个人信息罪论处，另因网暴行为构成寻衅滋事罪，数罪并罚。

在侵犯公民个人信息犯罪中，犯罪手法正越来越多地从传统的“人工偷”向“技术窃”转变。

2022年4月至2024年2月，王某某、林某某在互联网上运用“爬虫”程序，非法入侵某三甲肿瘤专科医院服务器，窃取患者个人信息、门诊医嘱数据、住院医嘱数据等共计385万余条，迁移至境外服务器存储达半年之久，并将部分医疗数据出售牟利。办案中，广东省广州市越秀区人民检察院破解医疗健康信息“可识别性”“关联性”认定难题，确认处方数据能精准追溯至特定患者，属于法律明确保护的医疗健康类敏感个人信息。刑事判决生效后，检察机关另行提起民事公益诉讼：虽然可查证获利仅1.08万元，但数据敏感度高、波及面广、修复成本大，且出境存储冲击公共卫生安全，据此酌定公益损害赔偿金150万元。

对老年人、名人等特定人群定制套路精准围猎

在一起典型案例中，潘某、范某发现，不少农村老人有激活医保电子凭证的实际需求，但手机操作不熟、防范意识不强。二人组建“村推”团伙，借“帮忙办业务”之名，在河南等6省500余个村庄挨家挨户“服务”，骗取2万余名老人的姓名、身份号码、人脸信息，批量实名认证支付宝账户后倒卖，非法获利180余万元。

河南省孟州市人民检察院精细审查电子数据，准确认定信息数量，对组织指挥者从严惩处；针对老人不知如何处置风险账号的难题，联合公安、基层组织入户排查，帮助注销本地涉案账号，同步开展普法宣传。

犯罪分子对特定人群量身定制套路，进行精准围猎。

航空公司外包客服舒某屏热衷追星，利用系统权限查询明星待出行航班，100余架次航班信息经网络群组外流，引发跟拍、陪飞、“刷关”，不仅侵害个人隐私，更扰乱机场秩序、埋下公共安全隐患。北京市朝阳区人民检察院认定：待出行航班能锁定特定自然人未来时段所处位置，属行踪轨迹信息。检察机关以侵犯公民个人信息罪提起公诉，同步提起刑事附带民事公益诉讼。

检察机关提醒：任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人信息；广大群众要提高防范意识，刷脸授权前先问清用途，不购买来路不明的“定位查询”“背景调查”等服务，发现信息被泄露及时报警。

据2026年11月10日《人民日报》

AI时代，数据使用如何“知情同意”

新华社记者 舒畅

试想一下：一家服装公司，拥有你的姓名、交易记录以及长期消费行为数据。如今，这家公司决定开发生成式人工智能模型，并利用用户数据训练模型，提升商业竞争力。它需要重新征求你的同意吗？

在新加坡监管机构看来，答案是肯定的。

新加坡个人资料保护委员会发布了《生成式人工智能个人数据使用咨询指导原则》，这是其中一个案例。该指导原则基于新加坡《个人资料保护法令》，讨论机构在开发、部署生成式人工智能，以及系统投入使用后的不同阶段，如何透明、负责任地使用个人数据。

这一案例背后，是人工智能时代数据治理面对的一个难题：当数据用途不断扩展，用户如何获得真正有意义的知情同意？

新加坡数码发展及新闻部长杨莉明在新加坡数据节开幕式上发布该指导原则时表示，数据商业价值不断提升，可信赖的数据治理需要明确责任机制。如果个人数据被用于开发或改进生成式人工智能模型，机构应以清晰、直接的方式说明，而不能依赖宽泛笼统的描述。

不过，很多时候，问题并不是用户没有“同意”，而是不知道自己究竟同意了什么。

随后的论坛上，新加坡国立大学人工智能治理教授西蒙·切斯特曼做了一个现场互动：“过去一年里，如果你曾经点击过同意某些服务条款，允许对方使用你的数据，请举手。”

不少观众举起了手。

“如果你读完了所有这些条款，请继续举手。”

一些观众放下了手，现场响起笑声。

“你们有几位在撒谎。”切斯特曼说，即使是专家，通常也不会阅读那些冗长复杂的条款。

如何让用户充分知情？委员会提出，只使用“您的数据将用于新产品开发”这类笼统表述是不够的，机构应提供“人工智能专项通知”，明确说明数据使用目的、涉及的数据类型、使用方式，以及用户如何拒绝或撤回同意。指导原则建议，社交媒体平台如果希望利用用户数据开发生成式人工智能模型，可以同时更新隐私政策、制作专门说明页面、在平台内弹窗提醒，并通过邮件通知用户，同时提供拒绝的渠道。

委员会同时指出，即使个人数据已被用于生成式人工智能开发，用户仍有权要求查阅、更正自己的数据。但该机构也承认，实现这一要求并不容易。生成式人工智能模型通常依赖海量训练数据，这些数据并不一定以传统数据库形式保存，删除已经进入模型的信息，在技术上仍存在挑战。

切斯特曼说，互联网早期，人们面对的数据更多是“静态”的：用户搜索信息、获取内容。随着社交媒体兴起，数据开始记录用户与谁互动、个人偏好等更丰富的信息。未来，人工智能不仅收集数据，还可能基于数据进行推断，而这些推断可能超出个人主动提供、原本希望被使用的信息范围。数据治理正从单纯依赖用户同意的模式，转向加入更深层次的授权机制和问责要求。

新加坡星展银行首席数据与转型官尼潘利明也表示，过去企业主要关注数据集本身是否合法获取，但现在需要关注的是不断流动、不断变化的数据。

随着人工智能进一步发展为能够自主执行任务的智能体，知情同意将面临新的挑战。

美国谷歌公司政府事务与公共政策副总裁马卡姆·埃里克森说，智能体的发展带来一个悖论。一方面，用户希望智能体成为可信赖的助手，能够跨应用理解、整合信息，尽可能更高效地操作；另一方面，在涉及用户安全的关键时刻，又需要增加相关授权流程，让用户能够介入判断。

新加坡资讯通讯媒体发展局可信人工智能集群总监署长李婉诗提到，最近测试发现，如果给智能体设定一个目标，它可能会“尽一切可能实现目标”，并在过程中无意泄露敏感数据，这说明真实环境测试的重要性。面对人工智能快速发展带来的新问题，监管机构和企业需要共同探索下一步方向。 **据新华社**