来源：【交汇点新闻客户端】

本人人脸信息被窃取解封被冻结账号，账号被用作电信诈骗、发布虚假广告；进入无人值守停车场那一刻，你的停车信息已被转卖；点击“新闻链接”，身在何处被悄然获取……个人信息泄露已不是新鲜事，然而今年以来江苏政法机关打击处理的多起“首例”个人信息泄露案件，显示攻防博弈仍在升级。怎样才能打赢个人信息保卫战？记者进行了调查。

窃取个人信息已成黑色产业链一环

去年3月，常州一位刚有孩子的家长频繁收到影楼推销拍摄婴儿照电话，不堪其扰求助警方后，网安部门挖出一条完整的“黑客—代理—买家”犯罪产业链。警方查获犯罪嫌疑人窃取的信息有30余万条，涉及9省29市新生儿及家长，涉案资金400余万元。

传统低端的买卖身份信息、家庭住址等，如今早已“转型升级”。省公安厅网安总队案件科科长宋励介绍，当前信息泄露案例网络化、链条化特点非常明显，“盗取手段精细化，犯罪主体组织化，信息需求、盗取、交易形成一条完整的黑色链条，不法分子分工专业、配合高效，他们之前通过网络联系，彼此之间甚至不认识，隐蔽性很强”。

同时，更多种类的公民信息可能成为交易品，不法分子对个人信息侵犯程度正在加深。这些数据轻则被用于商业推销，重则成为黑产帮凶。如去年8月扬州警方侦办的一起泄露、贩卖快递面单信息案，查获200余万份全国快递面单照片，其上信息被倒卖给中间商后落入境外诈骗团伙之手，用于实施冒充客服退款等诈骗，警方已初步比中的相关现行案件就有260起。

窃取倒卖位置信息也成为黑色产业链一环。近日，南京市鼓楼法院审理的全国首例全链条打击侵犯公民停车信息案，揭开一条“非法寻车”黑色产业链：谢某与黄某、李某等系列案中13人围绕为上家“寻车”，分别负责联系上家、提供制作爬虫软件、非法数据查询、安装定位设备等，上下游之间环环相扣。包括本案，2020年以来鼓楼法院共受理41起侵犯公民个人信息案。该院刑庭庭长朱锡平分析发现，当下此类犯罪正从传统型向互联网犯罪迁移，侵犯公民行踪轨迹、财产信息等敏感个人信息的情形增多，且该类犯罪与电信网络诈骗等犯罪紧密关联，成为上游犯罪中重要一环，具有极大社会危害性。“过去，一些被告人利用工作便利泄露楼盘、快递等存储的公民个人信息，部分被用于拓宽业务渠道、定向推销，但现在情况明显复杂得多，犯罪分子拿到信息，进行GPS贴牌，就可以锁定车主的行踪轨迹，为关联犯罪留下隐患。”

最严重的位置泄露可能危及人身安全。2019到2022年，苏州市检察院立案监督挖出一起故意杀人案中侵犯公民个人信息案的“案中案”。该案中，犯罪嫌疑人通过某付费App获得其前女友个人位置信息后，追踪至苏州将其杀害。检察机关查明，通过付费使用这种软件，可发送伪装的新闻链接。接收者只要点开链接，其所处位置就会瞬间暴露。2021年12月，该App两名经营者涉嫌侵犯公民个人信息罪被移送至姑苏区检察院审查起诉。审查显示，该App已非法提供或出售公民个人行踪轨迹信息4572条。

近些年，随着人脸识别技术应用场景不断拓展，人脸信息泄露成为风险多发新领域。前不久，常州市法院宣判江苏首例“人脸解封”侵犯公民个人信息案。经审理查明，2021年8月至2022年2月间，郑某在被害人不知情的情况下，从他人处购得包含被害人姓名、身份证号码、身份证照片、视频动图等个人信息，随后在QQ、微信群联系客户接单，为涉嫌电信诈骗、网络赌博等违法犯罪被封的QQ号提供解封服务，共从中获利人民币2万余元。

“人脸识别等通过生物识别技术收集的信息一旦被泄露，受害人便无法通过更改信息加以防控和补救，容易导致人格尊严受到侵害或者人身、财产安全受到危害。”今年全国两会上，全国人大代表孙华芹专门提出建议，呼吁关注人脸识别技术违规滥用、管理缺失、数据泄露等问题。

攻防博弈升级，打击难度攀升

当前，不仅窃取个人信息手段花样翻新，不法分子也越来越狡猾。梳理分析近年来苏州法院审理的239起侵犯公民个人信息犯罪案件，常熟法院刑庭审判员李浩然注意到，过半案件中，被告人在线上联络沟通、互相交换手中已有的数据后再贩卖获利，相关交易行为周期短、速度快，导致网络平台监管难以及时跟进，科技工具也为非法获取个人敏感信息提供了便利。

从受害者角度，李浩然分析，个人信息受侵害的公民范围广，被电话、短信广告等轻微骚扰后，寻求权利救济的公民人数较小，即使报案，公安机关也难以掌握犯罪线索，司法实践中一般靠市场监督管理局等职能部门进行突击检查或由同案人员检举。此外，侵犯公民个人信息的犯罪手段很隐蔽，办案过程中发现行为人会使用域外软件、虚拟货币进行交易结算，躲避公安机关侦查，导致证据固定困难。

困难不仅来自更狡猾的不法分子，也来自技术本身。“随着数字经济发展和全社会数字化程度的加深，特别是诸如人工智能加持下大数据的深度利用等，使得技术人员自己都无法预测，新技术运用和数据结合起来会发生什么。”长期致力信息安全领域法治研究的东南大学法学院副研究员徐珉川坦言，只要有数据、用数据，就有泄露风险，数字时代的系统性信息安全风险更为高涨，且几乎无法得到有效消除。

驻宁某高校信息安全专家李光（化名）也赞同泄露与利用间存在矛盾，“防止信息泄露难点在于数据可用性和安全性之间的权衡。”

以人脸识别应用这一新课题为例，刷脸开机、刷脸考勤、刷脸取款、刷脸购物、刷脸入小区，甚至刷脸倒垃圾，方便和风险并存。孙华芹分析，相关法律体系和标准规范虽持续完善，但涉及个人信息保护的规章制度均过于笼统，不利于法律落地，导致监管滞后，运转高效的安全监管体系尚未形成；监管职责分配上，网信、公安、市场、通管等部门都在积极履职，但地方由于职能交叉、手段受限等原因，尚无法全面监管到位；企业层面，人脸识别技术准入机制缺乏，生产企业鱼龙混杂，技术产品的安全防护能力参差不齐，一些企业缺乏系统性风险管控能力，对信息保护不够重视，从业人员个人信息保护教育缺失。另外，群众人脸信息保护意识也需提升。

近年来，在总体国家安全观指导下，信息安全保护日益受到重视。徐珉川告诉记者，我国相关领域立法思路清晰，在立法压力非常大的情况下，对现实的回应非常及时。“但系统性风险高企，使立法依然面临一定困难，主要体现在两方面：对实践中面临的系统性风险认识还不够全面及时，需要立法机关保持敏感性；二是制度的层次性、体系性已经彰显，但还有待于从宏观制度框架的讨论，向深度嵌入具体场景、具体实践的规则深化发展。”

既要全面打击，还要治理“生态”

近几年，江苏警方秉持“专业打职业”理念，常态化开展“净网”等专项行动，整治为侵犯信息安全提供技术支持的黑灰产，支持加大对利用新技术实施犯罪的研究和打击。宋励表示，警方还围绕打击网络犯罪过程中发现的突出的隐患，建立处置通报机制，既打且管，全面打击、生态治理。

如何进行生态治理？来看一起案件的处理。2016年5月至2018年6月，某机构负责预防保健工作人员李某某利用工作便利，非法获取母婴信息25124条，后通过网络将上述信息转售给儿童摄影店、儿童用品商家、奶粉专卖店等商家。按惯例，此类案件依程序提起公诉，李某某被判处刑罚便算了结。但公民信息被泄露屡禁不止，行政机关应有哪些作为？检察机关能否延伸职能，发挥司法惩罚和保护双重功效？基于此，办理该案的滨海县检察院围绕这起普通案件成立了专案组。

“专案组围绕被泄露信息是否属于健康生理信息、公共利益是否受到损害等关键问题进行重点研究，并对涉及所有信息条目逐一进行梳理归类、比对识别，找准侵害公民个人信息的关联点。”办案检察官告诉记者，经综合分析认定，李某某的行为侵犯了不特定多数人合法权益，可以列入公共利益范畴，于是向法院提起刑事附带民事公益诉讼。经审理，法院全部支持检察机关的诉讼请求，判决被告支付公益赔

偿款3.32万元。检察院还同财政部门研究出台管理办法，建立公益赔偿款财政专用账户托管机制，并就赔偿金后续使用问题达成合意，让公益赔偿款服务公益事业。

不仅如此，滨海县检察院还依法向相关主管部门制发检察建议，督促加强对医疗卫生机构的监管力度，完善公民个人信息保护机制。收到建议后，主管部门立即召开警示教育大会，签订信息安全责任状，约谈涉案部门负责人，建立相关信息专人保管制度。从去年起，该县主管部门对生育信息监管情况进行年度全面检查，并专门向检察机关通报检查结果。

针对近年来江苏多起关于母婴生育信息、停车信息、行车轨迹、个人居住地址等个人信息被违法违规收集、泄露案件，江苏检察机关积极履行公益诉讼职能，对侵犯公民个人信息的行为进行监督。对通过法治方式督促有关各方各负其责、携手共抓的做法，徐珉川十分赞同：“安全无法独立实现。法治要起到勾连、润滑的作用，营造运营者、技术提供者、消费者等共同追求信息安全的生态，让制度维护者有能力有意识进行监督，让消费者有能力认识风险、规避风险，让受害者遇到风险积极维权，共同形成有效运作的良好生态。”

建立维护个人信息安全共同体

建立维护个人信息安全的良好生态，需要企业、个人及监管部门各方面的携手努力。

数据的使用者和拥有者都要肩负起主体责任。宋励提醒，个人要绷紧信息安全这根弦，做到快递单、收据等重要信息不要乱扔，下载软件要认真阅读隐私条款，日常生活中不访问未知网站、不点击未知链接、邮件，在社会网站上尽量不暴露个人信息，分级设置密码，等等。承办停车数据泄露案件的南京市鼓楼区检察院检察官李海波还从技术角度提醒，如具备条件，尽量按照有关平台提示进行认证，确保自身信息得到更高级别防护。“像停车平台采用数据保护措施时为了兼顾用户使用便利与数据安全，往往对认证用户与未认证用户采取不同的数据保护方案，这就提醒公民个人在使用停车平台的时候，要提高自身的数据安全保护意识。”

企业疏于防范往往造成比个人疏于防范严重得多的后果。李海波说，无论是停车平台还是其他相关企业，都要加强研发投入与制度建设，并制定合规和符合自身实际的规章制度，加强内部员工警示教育，防止内外勾结泄露数据。李光认为，技术研发上要更重高效，例如数据匿名、差分隐私等，在保证数据可用性的前提下保护用户隐私；还要实现有效的追溯机制，方便发现泄露的途径和源头，从而进行弥补和追责。

在提交全国人大的建议中，孙华芹专门提出，要构建针对企业的全流程风险防控体

系。即事前要引导企业主动开展安全影响评估，积极履行合规义务，构建安全管理制度、应急响应管理制度；事中要对开展人脸识别应用的企业场所，定期开展安全评估、合规审计等；事后要落实追责制度，并建立投诉举报机制加大监管力度，“构建以事前预防为中心、事中监管为常态、事后救济为保障的全方位数据信息安全防护网。”

为适应变化剧烈的个人信息安全保护新形势，制度设计还需更新理念。徐珉川感到，当前本领域立法主要遵循“自上而下”思路，对实践反馈有滞后。“要大兴调查研究，立法机关与一线实践强化有效沟通，还要鼓励各地区各行业根据实践及时出台制度、完善标准，以自下而上的反思性、回应性的制度，来推动顶层设计的落地、充实和完善，避免风险不断积累。”他还提醒，立法要“软硬兼施”。“我国信息安全立法目前更倾向于关注软件应用、数据信息等‘软’的一面，而关键信息基础设施、算力资源等‘硬’的一面，作为信息安全大厦的基座，需要对相关的电信法等规范能否适应新形势、衔接新要求、配合新任务作出进一步思考，构建传统和前沿规范制度之间有传承、能衔接、可协调的体系化治理机制。”

新华日报·交汇点记者 陈月飞 顾敏 卢晓琳 胡兰兰

编辑: 林元沁

本文来自【交汇点新闻客户端】，仅代表作者观点。全国党媒信息公共平台提供信息发布传播服务。

ID：jrtt