

品牌微聚焦

“春露”无声拂迷途

当两千年儒家教化智慧邂逅新时代未成年人检察工作使命，会碰撞出怎样的温暖回响？河北省景县检察院“春露”未检团队，以“春风化雨，润物无声”的坚守，交出了一份兼具法治力度与人文温度的检察答卷。

“春露”，寓意新生与希望，承载着无限可能与美好期许。这一品牌源自景县大儒董仲舒《春秋繁露》，深植“仁义礼智信”儒家内核与“教化成性”治理智慧，让传统文脉在检察办案中焕发鲜活生命力。


16岁的小雷（化名），便在这份温暖中重归正途。小雷自幼深陷成长困境：母亲患精神疾病，父亲眼睛失明，爷爷奶奶无力给予其正确引导，他渐渐沾染文身、酗酒恶习，混迹街头。2025年3月，醉酒后的他因干坏事“手脚麻利、头脑灵活、学技术又快又好”，那扇紧闭的心门才缓缓敞开，眼中重燃光亮。

此后，小雷主动疏远不良同伴，甚至劝说同伴迷途知返。六个月的帮教中，小雷表现优异，不仅将收入悉数上交养家，还写下厚厚一本帮教心得，字里行间满是蜕变与感恩。2025年12月，景县检察院依法对小雷作出不予起诉决定。


“春露”团队的实践，既填补了未成年人监护缺位的空白，更打破“犯罪即捕、即诉”的思维定式，将司法救助延伸至家庭修复、心理疏导与技能培育的方方面面，以精准帮教为迷途少年点亮归途。

不止于个案办理，“春露”团队还注重经验提炼与机制创新，将遏制未成年人流窜盗窃的办案实践，转化为跨区域协作机制与数字监督模型应用，办理的王某猥亵儿童案入选最高人民检察院《未成年人检察工作白皮书（2023）》，为全国未检工作提供了有益借鉴。

未成年人检察工作的重要意义在于拨开阴霾，洒落春露，帮助每一个偏航的孩子向阳而生。如今，“春露”团队已成为当地未成年人保护的闪亮名片。



扫码看视频



技术狂飙，如何为创新划定法治红线

——三地检察机关破解网络安全治理难题的探索实践

编者按

技术浪潮奔涌，法治守护同行。2026年1月1日实施的新修订的网络安全法，新增“加强人工智能安全监管”条款，清晰锚定国家支持AI关键技术研发与安全治理并重的发展航向。当生成式人工智能衍生虚假信息困扰、数据处理触碰个人隐私红线、解析软件不当截取网络流量等问题渐显，检察机关如何以法律监督为刃，划清技术创新与法治底线的边界？本期《先锋周刊》聚焦上海、江苏、浙江三地检察机关深耕网络安全领域的办案实践与创新探索，看检察蓝如何以专业担当，为数字时代筑牢法治屏障。

堵住AI生成中的管控漏洞

□讲述人：上海市徐汇区检察院公益诉讼检察室检察官助理 陈思琦

2025年8月25日依法立案调查。

立案后，我们第一时间通过可信时间戳固定生成图片的全过程证据，同步委托专业机构对图片违规性及潜在危害进行鉴定，明确了公益损害的事实。但办案很快陷入瓶颈：AI大模型的运行逻辑如同“黑盒”，如何精准界定技术缺陷与损害结果的因果关系？现有法律对AI生成违规内容的责任认定缺乏细化标准，监管边界如何划分？这些技术与法律交织的难题，成为案件推进的拦路虎。

幸运的是，立案前一个月，我院与徐汇区委网信办、区新型工业化办公室等8家单位会签的《关于加强人工智能协同治理的工作协议》，为破解办案难题提供了制度支撑。我们迅速启动协同机制，联合上海军事检察院开展军地协作，召开专题联席会议梳理办案难点，明确分工推进证据核查与问题溯源。同时，我们先后走访信息安全测评机构、科研机构及相关军事单位，邀请技术专家与军事专业

人员共同解码“黑盒”。

经多轮研判，专家团队最终锁定问题根源：该AI大模型的训练数据缺乏权威内容支撑，对军服规范、军人形象的认知存在偏差；关键词库更新滞后，无法精准识别相关提示词，且语义识别模型存在漏洞，难以拦截隐性违规指令。这一结论，为案件办理指明了方向，也暴露了行业内AI信息内容管控的共性短板。

厘清成因后，我们聚焦整改路径多方征询意见。相关军事单位建议，补充“央广军事”等官方平台发布的军服配套穿着图例、军人规范形象素材，优化模型训练数据；行业专家提出，需扩充关键词库，升级语义识别算法，通过对抗测试强化拦截能力，在严守安全底线的同时兼顾用户正常使用需求。现役军人及志愿者代表则呼吁，要强化企业主体责任，从源头上杜绝

AI生成不良内容。

基于查明的事实，我们依法向行政监管部门制发检察建议，督促其履行AI新技术信息内容监管职责，督导涉案企业完成全面整改。行政监管部门高度重视，第一时间约谈企业负责人，要求限期落实整改措施。涉案企业迅速行动，对存量违规图片全面进行源头清理，同步上线34条规范示例、28个正向形象提示词，优化关键词库与语义识别模型，构建起“权威数据赋能—语料清洗—内容审

核实时时拦截”的全流程管控体系。

2025年12月12日，军地检察机关联合军队人大代表、人工智能领域专家开展整改“回头看”。现场测试显示，输入相关不良提示词后，系统可立即识别并弹窗提示“请更换提示词后再试”，违规内容生成被有效阻断。为推动个案治理升级为行业规范，行政监管部门还对辖区备案的70余家AI大模型企业开展网络安全专项检查，全面排查同类安全隐患，筑牢行业监管防线。

从线索受理到案件办结，从源头整治到系统治理，作为公益诉讼检察官，我们深知，技术的进步不应成为突破公序良俗、损害国家利益的借口。我们要做的，就是在技术创新与安全守护之间架起坚实护栏，用精准监督回应群众期待，确保AI在法治轨道上向善而行，为网络强国建设注入检察力量。

（本报全媒体记者潘志凡 通讯员朱陆奇整理）

图①：2025年12月，上海市徐汇区检察院检察官开展案件线上“回头看”。

图②：2025年10月，江苏省昆山市检察院检察官在讨论应用侵犯公民个人信息安全法律监督模型。

图③：2026年1月，浙江省杭州市滨江区检察院检察官深入企业走访，帮助企业筑牢网络安全防线。

破解App注销难题

□讲述人：江苏省昆山市检察院公益诉讼检察部负责人 谢玲玲

2026年1月，我院数字检察应用中心大屏上，“侵犯公民个人信息安全法律监督模型”正实时排查手机App权限风险。“这个模型为我们精准揪出App侵权隐患提供了有力支撑。”我院数字检察办公室负责人介绍，该模型已入选《全国检察机关大数据法律监督模型汇编》，在全国400余家检察院落地应用，助力成案500余件。而这一切的起点，源于一条本地手机App违规收集信息的案件线索。

这条线索指向犯罪嫌疑人王某，他利用房产中介职务之便，非法出售多名业主信息，获利8万余元。办案过程中，被害人林某向检察官道出了心中的忧虑：“我是一名新手宝妈，这次经历让我格外警觉。我之前注册了不少母婴类App，有些根本无法注销账户，这些留在后台的信息会不会哪天也被泄露？”

“要是宝妈们常用的App都藏着这类风险，用户在数字空间的安全感从何谈起？”同事将卷宗递给我时说道，“刑事检察能惩处‘看得见’的犯罪者，但网络空间里不特定用户面临的‘看不见’的信息安全隐患，更需要我们主动关注、破解。”

我们随即开展初步调查，发现部分手机App存在明显违规问题：有的不公开隐私政策或个人信息收集使用规则，有的刻意不提供账户注销及信息删除渠道，甚至在用户未充分知情、明确同意的情况下，擅自抓取定位等敏感信息、关联其他App账户。进一步核查还发现，部分违规收集的数据流入运营者算法系统，被用于个性化推送，潜藏着多重信息安全风险。

这些行为不仅直接侵犯公民个人信息安全，更给大数据“杀熟”、精准诈骗等违法犯罪埋下隐患。为此，我们果断立案启动公益诉讼调查。可新的难题接踵而至：手机App数量庞大、版本迭代迅速，数据收集行为又相对隐蔽，传统“等案上门”或人工逐案筛查的模式，效率低下且难以实现全面覆盖，破解困局的突破口究竟在哪？

因局倒逼出新路，我们决定向技术借力，依托我院数字检察应用中心的专业力量，探索构建大数据法律监督模型。经过多轮论证、调试优化，“侵犯公民个人信息安全法律监督模型”最终落地，为精准排查手机App侵权隐患提供了硬核支撑。

该法律监督模型就像一名“数字侦探”，通过整合手机App安装包、开发运营企业信息等基础数

据，借助权限检测工具，可批量排查App申请的系统权限是否超出实际功能所需，快速锁定“越权”App。我们运用该模型，对辖区内互联网企业开发运营的App开展“扫描体检”，经人工复核确认，发现5款App未提供账户注销、个人信息删除功能，3款App未公开信息收集使用规则或隐私政策。

结合调查结果和行政部门职能归属，我们依法向相关单位制发检察建议，指出App信息收集模式存在的潜在安全隐患，建议其依法处置违法违规情形，加强日常监管，切实保障公民个人信息安全。检察建议发出后，相关部门迅速行动，责令涉案企业限期整改、下架问题App，明确整改到位后方可重新上架。

“检察官，我已经顺利注销了账户。没想到我的一个担心，真的推动了改变。”林某事后感慨道。

个案整改并非履职终点，如何实现长效治理、避免按下葫芦浮起瓢？关键就在于凝聚多方合力，形成齐抓共管格局。为此，我们针对手机App违法违规收集使用个人信息乱象，牵头公安机关等8部门召开公益诉讼联席会议。“手机App数量激增，给动态全覆盖监管带来不小压力。”“用户协议条目繁杂、专业性强，普通消费者难以读懂，线索识别难度大。”……会上，各部门坦诚交流监管难点。

我们顺势向与会代表展示了研发的法律监督模型，介绍其自动化扫描、快速生成风险App清单的功能，可为各部门排查线索提供支撑。这一思路得到各方普遍认同，各部门就强化线索移送、信息共享、联合普法等事项达成共识，明确各司其职、协同发力，立体式构建公民个人信息安全监管治理网络。

技术浪潮奔涌向前，应用场景日新月异，但检察机关守护公民合法权益的法治初心始终未变。通过办理这起案件，我们深刻认识到，面对数字时代的新挑战，唯有主动与时俱进、以数字技术赋能法律监督，才能精准破解监管难题，为公民个人信息安全筑起坚实法治屏障，让人民群众在数字空间的获得感、幸福感、安全感更加充实、更有保障、更可持续。

（本报全媒体记者管莹 通讯员葛梦桐整理）

清除盗用流量“寄生虫”

□讲述人：浙江省杭州市滨江区检察院刑事检察部检察官 朱昊

2026年1月，新修订的网络安全法正式施行，对我们一线检察官来说，最直接的感受就是办理新型网络犯罪有了更明确的指引。手头一起“姆大厂流量羊毛”案正在推进后续治理，其办理思路恰好契合新法精神，这不由得让我想起，当我把这起案件的17册卷宗从手推车上搬到办公桌，翻开第一本案卷时，心底涌现出的强烈直觉：这绝非一起普通案件。

实际上，这是一起直指数据安全新型网络犯罪案件——不法分子施某等人借“姆大厂流量羊毛”牟利，其编写的云解析软件，能够绕过安全防护屏障，在未经授权的情况下，将第三方视频内容私自上传至多家互联网企业服务器。用户每一次点击观看产生的存储、带宽与流量费用，全被悄然转嫁给毫不知情的互联网“大厂”。2023年6月，一家大型互联网公司察觉服务器数据异常，流量费用较往常激增数倍，这条隐蔽的黑产业链条终于浮出水面。

经查，施某等人正是借助这款解析软件“搭便车”转嫁成本，将视频内容上传至各大互联网企业服务器，再把真实访问地址嵌入自己运营的网站供用户点击，从而实现“背靠大树好乘凉”的非法牟利模式。他们专挑流量规模大的知名企业下手，直至案发，已通过售卖软件非法获利171万余元，给被害企业造成的实际经济损失与潜在安全威胁，更是难以估量。

面对对象虚拟化、行为隐蔽化、获益间接化的办案难点，我们果断依法介入引导公安机关委托专业鉴定机构，对涉案程序源代码、数据传输路径、存储方式及解析逻辑开展全面技术鉴定。同时，我们与公安民警、技术鉴定人员、审计人员建立常态化沟通机制，逐条厘清软件运行原理，精准界定其对计算机信息系统的控制程度，最终从海量电子数据中梳理出犯罪行为与危害结果之间环环相扣的完整证据链。

在充分审查案件事实与证据的基础上，办案团队围绕盗窃罪与非法控制计算机信息系统罪两个罪名进行论证，通过类案检索、理论研讨、检察官联席会议等多重方式，细分犯罪行为模式，精准适用法律条文，最终将该案定性为非法控制计算机信息系统罪，并依法提起公诉。

2025年5月，随着法槌落下，施某、郭某、王某等3名被告人分别被判处有期徒刑四年至一年六个月不等，各并处罚金。至此，这起新型网络犯罪案件暂告一段落。

但案件的办结，并未让我们停下思考的脚步。流量就是资源，数字经济时代，盗用流量的现象并非个例。我们在开展追赃挽损工作时发现，由于非法控制行为消耗的算力资源价值、硬件设施损耗及电力成本等都难以精准量化，被害企业的经济损失难以量化。

为此，我们双管齐下推进后续治理：一方面，多次与被告人及其辩护律师沟通，通过耐心释法说理，推动公安机关、法院促成被告人主动退赔，最大限度为被害企业挽回经济损失；另一方面，通过深入企业实地走

访、召开座谈会等形式，提醒企业强化服务器异常流量监测、未授权访问拦截等技术防护能力，助力企业筑牢网络安全防线。

回首这起案件，它恰似一面棱镜，折射出数据要素化时代的新型安全挑战：网络犯罪的形态正从直接窃取信息，悄然演变为对数字基础资源的隐秘“寄生”——流量、存储与算力，这些支撑人工智能研发与运行的“数字基建”，已成为黑灰产业觊觎和滥用的目标。

此类犯罪不仅作案手法更隐蔽、追溯难度更大，还可能从源头污染数据池、侵蚀算力根基。这已不仅是网络空间治理的重要命题，更是一项关乎智能时代发展根基的战略课题。

我院所在的杭州高新区（滨江），是“中国数谷”试点示范核心区。立足区域定位，我们也正致力于构建惩治与治理并重的数字安全防护体系，精准打击犯罪形成震慑，同时以前瞻思维推动制度创新，探索构建“三数一链”数据可信流通基础设施，主动融入区域发展大局，参与数据要素“改革沙盒”等创新探索，秉持包容审慎监管原则，引导技术力量服务创新发展，让法治为技术创新保驾护航。

这一切努力，都是为了将技术纳入法治轨道，把数据置于安全基座，为数字经济与新质生产力蓬勃发展培育活力与可靠性兼具的沃土。我坚信，一个可信、安全的数字未来，正在不远处等着我们。

（本报全媒体记者龚婵媛 通讯员冷美霞整理）