**个人信息保护检察公益诉讼典型案例**

**目录**

1. 江苏省无锡市新吴区人民检察院督促保护服务场所消费者个人信息行政公益诉讼案

2. 湖南省长沙市望城区人民检察院督促保护个人生物识别信息行政公益诉讼案

3. 浙江省湖州市检察机关诉浙江G旅游发展有限公司侵害公民个人信息民事公益诉讼案

4. 江西省宜春市人民检察院督促保护医疗健康个人信息行政公益诉讼案

5. 宁夏回族自治区青铜峡市人民检察院诉张某某等人侵犯公民个人信息刑事附带民事公益诉讼案

6. 上海市浦东新区人民检察院诉张某侵犯公民个人信息刑事附带民事公益诉讼案

7. 广东省深圳市宝安区人民检察院诉付某等人侵犯公民个人信息刑事附带民事公益诉讼案

8. 辽宁省沈阳市大东区人民检察院督促规范政务公开个人信息保护行政公益诉讼案

**案例一：江苏省无锡市新吴区人民检察院督促保护服务场所消费者个人信息行政公益诉讼案**

【关键词】

行政公益诉讼诉前程序 服务场所 消费者敏感个人信息 数字技术

【要旨】

针对服务场所强制采集、非加密传输、违法存储、未定期删除消费者敏感个人信息，造成信息泄露安全隐患的行为，检察机关开展专项监督，制发诉前检察建议，督促职能部门依法履行监管职责，维护消费者个人信息安全。

【基本案情】

江苏省无锡市新吴区某健身房使用具有人脸识别、指纹识别等功能的信息管理系统，强制要求会员刷脸或录入指纹进入。由于该管理系统采用分级分层、前后端分离等技术，消费者在前端平台界面仅能看到被采集的个人身份信息，未被告知个人信息收集清单及权限。在部分会员明确拒绝人脸采集识别后，该健身房擅自将会员办卡时提供的照片录入系统作为刷脸进出凭证，且在会员要求删除照片等信息时，以无管理权限为由拒绝删除，其行为侵害众多消费者合法权益，损害社会公共利益。

【调查和督促履职】

2022年6月21日，“益心为公”检察云平台志愿者向江苏省无锡市新吴区人民检察院（以下简称新吴区院）反映，新吴区某健身房存在侵犯消费者敏感个人信息的情形。新吴区院运用公益损害风险防控平台，通过数据交叉比对、智能分析，排查易发生非法收集个人信息的服务场所，绘制风险防控“数字地图”，发现全市案件线索16件，其中涉及新吴区5件。经初步调查，新吴区院于2022年8月11日正式立案。

新吴区院引入专业技术机构协助调查取证，现场勘验涉案服务场所信息管理系统，出具专家意见，认为该系统在个人信息传输、存储等方面存在安全风险。针对涉案服务场所采集、存储个人信息的必要性和合理性，邀请公安、市场监管、第三方专业机构等召开论证会。新吴区院审查认为，根据《中华人民共和国个人信息保护法》第二十六条、第二十八条、第四十七条、《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》第一条第三款等规定，消费者的人脸、指纹等属于生物识别类敏感个人信息，涉案服务场所系公共场所，非维护公共安全必需且未取得消费者单独同意，强制采集、非加密传输、违法存储、未定期删除敏感个人信息的行为，损害了众多消费者合法权益。根据《中华人民共和国个人信息保护法》第六十条、第六十一条、《中华人民共和国消费者权益保护法》第二十九条、第三十二条第一款、第五十六条第一款第九项的规定，新吴区院于2022年8月12日向新吴区市场监督管理局制发行政公益诉讼诉前检察建议，督促对涉案服务场所依法处理，切实履行保护消费者合法权益的职责；开展行业规范整治，加大监管力度，建立长效机制，防范类似违法行为发生。

新吴区市场监督管理局收到检察建议后，对涉案5家服务场所进行集体谈话、责令改正，组织开展专项执法行动，并建立定期检查、约谈、通报等监管机制。涉案服务场所及时整改，改变进入场所方式，采取安全措施传输、定期删除个人信息，向监管部门报送个人信息管理情况。

新吴区院联合区市场监督管理局开展“回头看”，进行现场验收，确认涉案服务场所均整改到位。同时，新吴区院将其他11件案件线索移送无锡市人民检察院（以下简称无锡市院）。无锡市院开展服务场所公民个人信息保护专项监督活动，组织全市检察机关排查健身房、超市等服务场所126处，督促整改问题场所56处，删除违法采集信息9300余条，向经营者、消费者普法宣传3000多人次，有效保障公民个人信息安全。

【典型意义】

健身房、超市等公共服务场所采集的信息量大、面广、敏感度高，监管不到位，将严重危害众多消费者人身、财产安全。本案中，检察机关积极发挥公益诉讼检察职能，运用数字技术，通过“专业取证+专门论证+专家意见”等方式，破解公民个人信息保护领域线索发现、调查取证、损害认定等难题，制发诉前检察建议，开展专项监督，督促行政机关依法履职，推动服务场所规范收集、传输、存储、删除个人信息，加强数据安全管控，促进个人信息全链条保护。

**案例二：湖南省长沙市望城区人民检察院督促保护个人生物识别信息行政公益诉讼案**

【关键词】

行政公益诉讼诉前程序 个人生物识别信息 个人信息处理原则 公开听证

【要旨】

针对信息化建设对指纹和人脸识别等个人生物识别信息过度收集、未落实网络安全等级保护制度等问题，检察机关明确个人信息处理“合法、正当、必要和诚信原则”的内涵与外延，厘清各职能部门法定职责，督促其依法全面履职、协调联动，消除公民个人信息泄露风险，切实维护社会公共利益。

【基本案情】

湖南省长沙市望城区卫生健康局（以下简称区卫健局）为推进数字化门诊建设，自2019年7月12日起，要求长沙市望城区辖区内17家医疗卫生机构陆续使用电子签核系统推送疫苗接种知情告知书，疫苗受种者或监护人点击“同意”时系统自动采集指纹和人脸识别信息，收集电子数据的存储及主机均由各社区卫生服务中心管理。截至2022年3月11日，上述机构共收集83万余条涉及指纹、人脸识别等个人生物识别信息。

【调查和督促履职】

2022年2月11日，湖南省长沙市望城区人民检察院（以下简称望城区院）接到群众举报，反映自己和孩子的指纹和人脸等个人生物识别信息被医疗卫生机构过度收集，存在泄露风险。望城区院经初步调查确认属实，遂于2022年3月19日、5月16日分别对望城区卫健局、长沙市公安局望城分局（以下简称区公安分局）立案调查。

望城区院通过现场勘验、委托第三方单位对电子签核系统进行安全检测、调取相关书证与电子数据、询问相关人员、咨询专业人员等方式进行调查取证，查明：根据《中华人民共和国个人信息保护法》第五条、第六条、第二十八条至第三十条的规定，望城区17家医疗卫生机构违反个人信息处理的合法、正当、必要和诚信原则，过度收集服务对象指纹和人脸等个人生物识别信息，未按要求解决电子签核系统的弱口令、数据未加密等安全漏洞，未能防患未经授权的访问及个人信息泄露、篡改、丢失等高风险，未落实网络安全等级保护制度要求，对敏感个人信息保护的内部管理不到位。望城区卫健局和区公安分局对上述医疗卫生机构收集、处理敏感个人信息活动未尽到监管职责。

2022年5月11日、16日，望城区院分别向区卫健局、区公安分局送达行政公益诉讼诉前检察建议，建议区卫健局改进征求知情同意的方式，避免过度收集指纹或人脸识别信息等个人生物识别信息；完善技术和管理措施，防止未经授权的访问及个人信息泄露、篡改、丢失。建议区公安分局对17家医疗卫生机构未履行网络安全等级保护责任的行为依法处理。同时将上述检察建议抄送望城区网信部门。

望城区卫健局、区公安分局收到检察建议后高度重视，部署开展了专项行动。望城区卫健局认真进行调研，研究解决方案，并向长沙市卫生健康委员会（以下简称市卫健委）专题汇报，长沙市卫健委以望城整改方案为蓝本推进全市医疗卫生机制规范、合法处理个人信息。望城区公安分局召开专门网络安全会议，对全区医疗卫生机构进行网络安全检查。望城区卫健局、区公安分局召集医疗卫生机构、系统开发单位、网络安全检测公司、区数据中心等单位多次召开座谈会，望城区院和区委网信办受邀参会。截至2022年6月10日，全区23家单位均已完成电子签核系统升级，取消生物识别信息功能；21家单位已彻底删除既往数据，并按照保密文件要求将已收集个人生物识别信息交区疾控中心代为封存保管，疫苗有效期满后进行硬盘格式化删除；升级后的电子签核系统完善了内部信息安全管理制度、加强系统物理隔离、对数据传输和存储加密保护、新增限制授权访问等安全防护措施，信息安全等级保护经专家评定为1级，系统改为局域网内部运行，于2022年8月初在全区正式启用。

2022年8月8日，望城区院跟进监督发现，升级后的电子签核系统采用电子屏签字的方式确认接种告知并在局域网运行；收集的电子签字、疫苗接种等个人信息已加密；已收集的个人生物识别信息已在医疗卫生机构彻底删除。上述整改方式在全市范围内推广已显成效。同年8月11日，该院组织召开听证会，邀请人大代表、政协委员、“益心为公”志愿者及专家学者担任听证员，与会人员一致认为行政机关已采取积极有效措施全面履职，敏感个人信息被侵害的重大风险已消除。

【典型意义】

检察机关聚焦民生关切，依法能动履行公益诉讼检察职能，通过现场勘验和委托安全检测等智慧检察手段，发现公益事业单位个人信息保护安全风险，督促行政机关对过度收集的个人生物识别信息数据采取“备份封存+本地彻底删除+到期彻底删除”方式消除安全风险，并进行“电子签核系统升级改造+网络安全等级保护”技术整改，平衡好个人信息保护与公共事务管理中个人信息合理利用的关系，充分实现“互联网+”与公共卫生服务领域保障数据信息安全的良好结合，推动加强个人信息保护与公共卫生服务信息化建设的协同发展。通过办案将个人信息处理“合法、正当、必要和诚信原则”的内涵和外延予以具体化，落实网络安全等级保护制度，推动相关法律制度在司法办案中落地见效。

**案例三：浙江省湖州市检察机关诉浙江G旅游发展有限公司侵害公民个人信息民事公益诉讼案**

【关键词】

民事公益诉讼 游客个人信息 人脸识别 数据删除

【要旨】

检察机关针对景区违法采集游客人脸信息的情形，坚持上下联动、一体化推进，督促行政机关加强监管，促使景区运营企业合法合规收集、使用和存储人脸信息数据，开展人脸信息数据删除现场勘验，充分保障游客的知情权和选择权等合法权益，切实保护游客个人信息安全。

【基本案情】

A景区由浙江G旅游发展有限公司（以下简称G公司，其控股股东是某国有公司）负责实际运营。2020年7月，A景区通过招标委托浙江H科技有限公司（以下简称H公司）建设完成人脸识别系统，并投入运行。系统使用期间，A景区在采集游客人脸信息时未依法履行告知义务，存在强制要求购票游客录入人脸信息、“刷脸”入园的情形，且景区未对采集到的人脸信息定期予以删除，致使游客个人信息被侵害，损害了社会公共利益。

【调查和督促整改】

2021年10月，最高人民检察院（以下简称最高检）根据志愿者反映，将A景区要求游客“刷脸”入园、涉嫌侵害游客人脸信息的线索交由浙江省人民检察院（以下简称浙江省院）办理。2021年11月初，湖州市人民检察院（以下简称湖州市院）、湖州市南浔区人民检察院（以下简称南浔区院）联合成立专案组对该线索立案调查，对A景区人脸识别系统前端完成电子取证。经调查发现，A景区现场购票除要求游客提供身份证外，还要求游客进行“刷脸”认证，且未告知“刷脸”入园的必要性及后续如何处理刷脸信息，对游客人脸信息储存和使用缺乏具体制度规范。同年11月12日，浙江省院、湖州市院、南浔区院会同当地旅游度假区管委会、G公司等景区运营主体，同时邀请了浙江省消费者权益保护委员会相关工作人员和法律专家，围绕涉案人脸信息被侵害问题召开磋商会，就G公司删除景区前期采集储存的人脸信息数据，规范人脸信息的收集和使用等事项达成共识。同时，湖州市院与湖州市网信办开展磋商，网信部门对G公司提出整改要求。同年11月18日，湖州市院向G公司制发检察建议，督促G公司积极整改，确保依法运营。

2021年11月24日，G公司回复检察机关称，已委托H公司通过远程操作，将景区违规收集储存的人脸信息数据进行删除。为确保删除工作符合规范，切实维护公民信息安全，浙江省院组织技术力量会同办案人员赴现场开展技术勘验，湖州市院邀请人大代表、人民监督员进行现场见证。在相关人员的监督下，A景区前期采集、储存游客人脸信息共计120万余条完全删除。同时，G公司已建立起人脸信息采集和使用的制度规范。目前，景区门口和购票处已设置告知牌，告知游客“刷脸”入园的相关事项，征求游客意愿，游客可以自由选择人脸识别、购买纸质门票、网络购票等多种方式进入景区。对于采用人脸识别进入景区的游客，景区会根据游客入园的需要合理设置人脸数据删除的期限，并在游客游玩结束后自动删除人脸信息，确保游客人脸信息安全。

【典型意义】

人脸信息属于敏感个人信息，一旦被泄露或者非法使用，容易导致人格尊严受到侵害或者人身、财产安全受到危害。本案中，景区违法采集游客人脸信息，严重侵害了游客个人信息安全，检察机关充分发挥一体化办案优势，坚持依法办案与服务营商环境、个人信息保护与景区智能化建设有机结合，融合社会公众力量共同参与监督，督促行政机关加强监管，促使信息处理者依法整改，建立合规体系，在提升景区管理智能化水平的同时，推动形成个人信息保护合力，实现办案效果最优化。

**案例四：江西省宜春市人民检察院督促保护医疗健康个人信息行政公益诉讼案**

【关键词】

行政公益诉讼诉前程序 医疗健康个人信息 保险营销 行业治理

【要旨】

针对医疗机构非法向保险代理机构提供患者医疗健康信息进行保险营销的行为，检察机关可以通过诉前检察建议督促行政机关依法履职，消除个人信息泄露隐患，推动行业规范治理，切实保护公民个人信息安全。

【基本案情】

2021年以来，部分保险代理机构与江西省宜春市中心城区5家大型医院达成协议，由保险代理机构在合作医院推销相关保险产品。部分保险代理机构业务人员在推销保险产品过程中，为精准销售“手术意外险”等险种，通过合作医院违法获取大量患者的姓名、手术类型、联系电话等医疗健康信息，对相关患者进行保险推销，患者不堪其扰。该行为严重侵害患者的合法权益，损害了社会公共利益。

【调查和督促履职】

2022年2月，江西省宜春市人民检察院（以下简称宜春市院）收到群众举报，称其家属办完住院手续后，有保险代理机构业务人员向其推销“手术意外险”。宜春市院立案办理并进行全面摸排核实，一是查明医疗健康信息泄露源头。通过走访宜春市中心城区各大医院，了解医院与保险代理机构签订合作协议情况，并初步核实保险代理机构业务人员通过医院手术科室护士站查询病人纸质病历或登录病历管理系统违法获取大量患者医疗健康信息（包括病人姓名、身份证号、联系方式、手术类型等）的情况。二是通过大数据比对分析，发现保险代理机构业务人员手机通话记录与患者办理住院手续时间点相吻合，手机通话的先后顺序反映患者在办理住院手续后不久即会接到保险代理机构业务人员电话，进一步印证了患者个人信息泄露的事实。

宜春市院审查认为，根据《中华人民共和国个人信息保护法》《医疗机构病历管理规定》等法律法规，医疗健康等信息属于敏感个人信息，未经公民本人同意，或未具备具有法律授权等个人信息保护法规定的理由，医院向保险代理机构提供患者医疗健康信息，改变了公民公开个人信息的范围、目的和用途，不属于法律规定的合理处理；保险从业人员收集、使用获取的医疗健康信息从事保险营销违反国家规定，侵害了不特定多数患者个人信息权利。卫生健康部门对侵害医疗患者个人信息的行为负有监管职责。

2022年7月8日，宜春市院向宜春市卫生健康委员会（以下简称宜春市卫健委）制发行政公益诉讼诉前检察建议，要求其依法处理相关医院，采取有效整改措施，及时堵塞患者个人信息保护漏洞；加强日常监管，对本辖区范围内所有医疗机构开展全面清查；加强个人信息保护宣传教育，切实增强医护人员关于患者个人信息的保护意识。

宜春市卫健委收到检察建议后，组织召开加强患者诊疗信息安全管理工作部署会，督促5家涉案医院限期整改，制定出台《第三方保险业务关于患者医疗健康信息的保密规定》，明确规定保险代理机构业务人员接触患方时间、不得私自提前与患方联系等，并规范患者诊疗信息查询程序，堵塞信息泄露漏洞。同时，宜春市卫健委在全市439家医疗机构部署开展为期一个月的患者诊疗信息安全专项整顿活动，共发现并整改重大信息安全隐患37个，推动建立风险防范机制256项，组织12994名医务人员分期分批参加患者诊疗信息安全培训，进一步增强医疗健康信息保护意识，筑牢公民个人信息安全防护网。

【典型意义】

医疗健康信息属于可能影响公民人身、财产安全的敏感个人信息。本案中，医疗机构违反法律规定的合法、正当、必要和诚信的原则，未经患者同意向保险代理机构提供相关个人信息，严重侵害公民个人信息安全和合法权益，扰乱了社会公共秩序。检察机关运用大数据比对等方式全面调查取证，依法发出检察建议，督促行政机关查处医疗机构违法违规行为，并通过开展专项整顿、安全培训等方式，堵塞医疗健康信息安全漏洞，推动医疗机构、医疗从业人员增强风险防范意识，强化行业自律，健全医疗健康信息保护长效机制。

**案例五：宁夏回族自治区青铜峡市人民检察院诉张某某等人侵犯公民个人信息刑事附带民事公益诉讼案**

【关键词】

刑事附带民事公益诉讼 股民个人信息 电信网络诈骗 公益损害赔偿金 二审改判

【要旨】

针对非法利用信息网络侵害众多公民个人信息违法行为，检察机关可以提起刑事附带民事公益诉讼，依法追究行为人的刑事与民事双重责任，对侵犯公民个人信息违法犯罪行为起到有效震慑作用，有力维护法律权威尊严、社会公平正义和社会公共利益。

【基本案情】

张某某非法获取股民电话号码、相关证券公司信息及创建虚假股票投资微信群码，提供给吴某“吸粉引流”话务团伙用于电信网络诈骗。2020年11月至2021年5月，吴某组织“吸粉引流”话务团伙10余人先后在宁夏青铜峡、湖北武汉、湖北鄂州租住房屋，冒充相关证券公司客服拨打客户电话5万余次，为200多个涉电信网络诈骗群“吸粉引流”14130人。每拉1人进群视为做成一单，每单获利10元不等。吴某自组织“吸粉引流”话务以来，收到上线张某某扣除每单获利后转账资金703142.7元，其在扣除每单获利后按照下线做成单数将款层层转至下线人员。公安机关以张某某等人非法利用信息网络罪移送检察机关审查起诉。

【调查和诉讼】

2021年9月10日，宁夏回族自治区青铜峡市人民检察院（以下简称青铜峡市院）在办理张某某等人非法利用信息网络罪一案过程中，发现该案存在侵犯众多公民个人信息行为，可能损害社会公共利益。2021年10月8日，青铜峡市院依法以刑事附带民事公益诉讼立案。检察机关经审查认为：违法所得是行为人实施违法犯罪活动而获取的不法财物，依法应予追缴；公益损害赔偿是行为人因实施民事侵权行为对社会公共利益造成损害应承担的民事赔偿责任。追缴违法所得与公益损害赔偿的责任性质、侵害主体均不同，追缴违法所得和承担公益损害赔偿可以同时适用。2021年11月29日，青铜峡市院向青铜峡市人民法院提起刑事附带民事公益诉讼，请求依法判令各被告删除所有非法获取的公民个人信息，解散、删除创建的微信群，消除潜在的公民信息泄露风险，依据违法所得数额支付公益损害赔偿金，并在国家级媒体上向社会公众赔礼道歉。

开庭审理时，一审法院结合公安机关补充侦查结果，认定被告张某某等16人为实施电信诈骗等违法犯罪发布信息，违法所得数额为739581.08元，其行为构成非法利用信息网络罪，应依法判处有期徒刑，没收违法所得并处罚金。刑事没收违法所得与民事公益损害赔偿金属于双罚，同时适用加重了对被告的惩罚，仅支持在国家级媒体公开道歉、删除信息和解散微信群的诉讼请求。一审宣判后，被告人朱某、王某某对刑事判决不服提出上诉。青铜峡市院认为一审判决对公益损害赔偿金不予支持，混淆了刑事责任与民事责任的界线，属适用法律错误，经请示吴忠市人民检察院同意，于2022年2月21日依法提出上诉。

2022年6月7日，吴忠市中级人民法院经开庭审理后，对朱某、王某某当庭提出的撤诉请求，裁定准许撤诉，并作出二审判决，认为检察机关起诉要求民事赔偿，符合法律规定。原判追缴各被上诉人违法所得与附带民事公益诉讼起诉人要求承担民事赔偿责任并不矛盾，各被上诉人被追缴违法所得，再行承担民事赔偿责任，不属于重复赔偿，一审判决适用法律错误，应予纠正。同时认定张某某等16人犯非法利用信息网络罪事实清楚，证据确实、充分，定罪准确，量刑适当，维持原判。以犯非法利用信息网络罪判处张某某等16人七个月至一年六个月有期徒刑不等，没收违法所得，并处3千元至6千元罚金不等；依法支持检察机关公益诉讼损害赔偿金诉请，判决各被告按照没收的违法所得金额承担民事赔偿责任，共计赔偿损失739581.08元。目前，案件已进入执行程序。

【典型意义】

侵犯公民个人信息犯罪严重危害公民个人信息安全，易引发电信网络诈骗等衍生犯罪，社会危害性较大。本案中，检察机关充分发挥刑事、公益诉讼检察职能联动优势，依法对非法利用信息网络犯罪提起刑事附带民事公益诉讼，追究违法行为人的刑事与民事双重责任，追缴违法所得并承担民事公益损害赔偿金，对非法获取、使用公民个人信息的行为形成惩治震慑，实现了“三个效果”的有机统一。

**案例六：上海市浦东新区人民检察院诉张某侵犯公民个人信息刑事附带民事公益诉讼案**

【关键词】

刑事附带民事公益诉讼 客户订单个人信息 公益损害赔偿金 调解

【要旨】

检察机关在办理涉网络的侵犯公民个人信息刑事案件时，对侵害众多个人信息权益的，可依法提起刑事附带民事公益诉讼，诉请被告承担停止侵害、消除危险、赔偿损失等民事责任。相关公益损失难以直接计算的，按照侵权人通过网络交易获得的利益确定赔偿金额。

【基本案情】

2021年7月下旬，张某通过网络技术手段非法侵入某软件公司计算机信息系统，获取该公司系统内客户订单信息6万余条。客户订单信息中包含消费者姓名、手机、住址、交易记录等信息。之后，张某将上述个人信息出售给他人，并在暗网获利人民币38760元。因客户交易信息泄露，某软件公司被第三方交易平台索赔，部分客户接到诈骗电话，众多消费者面临诈骗风险，公共利益处于持续受损状态。

【调查和诉讼】

上海市浦东新区人民检察院（以下简称浦东区院）通过上海市检察机关“公益诉讼全息办案智能辅助系统”发现张某侵犯公民个人信息线索。2021年12月8日，浦东区院以张某侵犯公民个人信息刑事附带民事公益诉讼立案。检察机关统筹发挥刑事检察与公益诉讼检察职能作用，引导公安机关调取某软件公司被索赔、消费者接到诈骗电话及张某通过网络交易获利等证据，证明张某实施违法侵权行为、社会公共利益受损及二者存在因果关系。

2022年1月24日，浦东区院以张某犯侵犯公民个人信息罪向浦东新区人民法院提起刑事附带民事公益诉讼，诉请判令张某在国家级新闻媒体上对其侵犯公民个人信息的行为公开赔礼道歉，删除保存在阿里云等存储介质内的公民个人信息数据，并按其侵犯公民个人信息的获利赔偿人民币38760元。

2022年3月2日，浦东新区人民法院公开开庭审理本案。围绕公益损害与私益损害的区别及违法所得的庭审焦点，浦东区院认为，张某窃取及转卖行为导致众多消费者人身财产损失风险及个人信息保护秩序的破坏，无法通过张某与技术公司赔偿等私益赔偿得以实现。通过提起公益损害赔偿可以更好的修复受损公益，起到惩罚及预防违法行为的作用。根据《中华人民共和国民法典》第一千一百八十二条规定，赔偿数额按照被侵权人因此受到的损失或者侵权人因此获得的利益予以确定。据此检察机关认定张某应赔偿数额为通过网络获利的金额人民币38760元。在浦东新区人民法院主持下，张某认可检察机关附带民事公益诉讼提出的诉讼请求，双方达成调解。

2022年6月1日，浦东新区人民法院在互联网上公告调解协议，公告期满后未收到任何意见或建议。2022年7月1日，浦东新区人民法院作出调解书。张某已按照调解书内容履行全部诉讼请求。2022年8月12日，浦东新区人民法院判决被告人张某犯侵犯公民个人信息罪，判处有期徒刑三年、缓刑四年，并处罚金。

【典型意义】

通过非法入侵计算机系统的方式获取大量公民个人信息并通过网络出售牟利，是侵害众多公民个人信息权益的一种表现形式。本案中，检察机关在依法追究其刑事责任的同时，通过公益诉讼追究侵权人应承担的民事责任，体现保护公益、全面追责的独特价值。检察机关在提起附带民事公益诉讼时，可提出停止侵害、删除数据、赔偿损失等诉请。公益诉讼损害赔偿是建立在维护个人信息安全秩序基础上对受损公益提出的补偿。针对网络侵害的特点，相关公益损失难以直接计算的，可以按照侵权人通过网络交易获得的利益确定公益损害赔偿金额，对于办理同类案件具有一定的借鉴意义。

**案例七：广东省深圳市宝安区人民检察院诉付某等人侵犯公民个人信息刑事附带民事公益诉讼案**

【关键词】

刑事附带民事公益诉讼 快递面单个人信息 数据采集工具 企业数据合规

【要旨】

对于快递行业龙头企业内部员工利用工作便利泄露信息，因快递业数据采集工具“巴枪”管理不善导致大量公民个人信息受到侵害的情形，检察机关以刑事附带民事公益诉讼追究违法者民事责任，通过制发社会治理类检察建议督促企业依法规范寄递用户信息采集管理，全面维护用户个人信息安全。

【基本案情】

2020年10月以来，某快递公司营业点主管以及仓库管理员付某等8人，利用职务便利通过营业点主管账户查询指定手机号码对应的快递单号，再通过手机拍照将快递单号发至购买方，购买方通过“巴枪”（快递业数据采集工具）获取快递单号在某快递公司的所有信息，包括寄收方姓名、联系方式、收寄货地址、物品信息等，严重侵犯公民个人信息安全，损害了社会公共利益。

【调查和诉讼】

广东省深圳市宝安区人民检察院（以下简称宝安区院）通过该院综合指挥中心案件集中评估平台，在刑事案件中发现付某等8人侵犯公民个人信息民事公益诉讼案件线索。公益诉讼检察部门发挥一体化办案优势，全程参与刑事案件调查，厘清证据链条，全面掌握付某等8人违法事实和社会公共利益受损情况，并多次走访某快递公司了解其日常监管模式及操作流程。

2021年8月，宝安区院依法提起刑事附带民事公益诉讼，诉请判令付某等8人支付其侵犯公民个人信息赔偿金240183.08元。人民法院经审理于2022年5月作出判决，支持宝安区院全部诉讼请求，以侵犯公民个人信息罪判处付某等8人有期徒刑十个月至三年不等并处罚金；判决付某等8人支付公益诉讼赔偿金共计240183.08元。目前，付某等8人已全额支付公益诉讼赔偿金。

案件办理过程中，宝安区院发现快递行业普遍存在快递查单系统权限设置过大、查单系统账号和密码安保级别低、“巴枪”管理不到位等问题。某快递公司作为快递行业龙头企业，虽然已采取多种安全保障措施，但在硬件设置和管理流程风控上仍然存在改进空间。2022年10月9日，宝安区院向某快递公司发出检察建议，建议其针对涉案个人信息的管理漏洞整改治理，依法规范个人信息收集、管理措施。

某快递公司收到检察建议后积极开展整改，聘请专业机构针对个人信息泄露风险点进行全流程梳理。一是优化用户个人信息保密制度，落实保密内容、细化保密环节及明确保密责任。严格设置不同级别员工的查询、访问权限，实行“账号负责制”；二是根据服务范围或服务对象分配内部人员的最小所需数据访问权限，快递员仅可查询其服务客户相关地址信息，通过一键拨号功能隐藏客户真实手机号；三是严控账号安全风险，采用CAS框架对应用进行统一的用户登陆管理；四是另行开发APP逐步取代“巴枪”，同步加强对现有“巴枪”的管理，宝安区院及时跟进监督，邀请人大代表走访某快递公司营业点，现场抽查管理人员登陆系统、“巴枪”查询权限等整改情况，经组织整改验收确认相关公益损害风险已消除。

【典型意义】

物流行业掌握大量公民个人生活信息，通过大数据分析后可精准画出用户购物习惯、消费水平、生活轨迹的图谱，极易滋生诈骗、不正当竞争等违法行为。本案中，检察机关通过刑事附带民事公益诉讼加大侵权成本、震慑违法犯罪，同时通过制发社会治理检察建议，着力实现“后端惩治”到“全流程风控”转化，引导快递行业龙头企业良性运行，建立快递企业个人信息安全保护通用标准，实现“由点到线，由线到面”的辐射效应。

**案例八：辽宁省沈阳市大东区人民检察院督促规范政务公开个人信息保护行政公益诉讼案**

【关键词】

行政公益诉讼诉前程序 保障性住房个人信息 政务公开 去标识化处理

【要旨】

检察机关针对政府行政部门在政务公开过程中出现的未能对公民个人信息进行有效保护的问题，通过履行公益诉讼监督职责，实现对公民个人信息保护的同时，为行政部门的政务公开工作提供了法律支持并推动形成信息公开的标准化方案。

【基本案情】

“沈阳市住房保障网”公示了2013年至2022年期间多个公租房项目申请公租房保障人员的摇号结果、配租结果等信息，公开的各类名单包含有公民个人的姓名、身份证号、户籍所在地、申请住房门牌号、申请家庭人口情况、人均居住建筑面积、人均可支配月收入等信息，共计87000余条。上述公民个人敏感信息未进行任何去标识化、匿名化处理，存在严重安全隐患，社会公共利益持续受到侵害。

【调查和督促履职】

2022年5月12日，辽宁省沈阳市大东区人民检察院（以下简称大东区院）接到群众举报反映上述问题线索。经沈阳市人民检察院指定管辖，大东区院于同年5月18日立案调查。经查，沈阳市保障房行政主管部门在政务公开过程中，对足以确定公民身份的个人敏感信息未依法进行去标识化、匿名化处理，致使87000余条个人信息存在严重安全隐患。2022年5月31日，大东区院向沈阳市保障房行政主管部门发出行政公益诉讼诉前检察建议，建议其加强对已发布的政府公开信息审查力度，对本案涉及的个人信息及时进行去标识化处理，防止个人信息泄露。

该部门收到检察建议后高度重视，第一时间派员与大东区院座谈会商并达成整改共识。随后，该部门就双方共商的整改方案向上级部门及审计部门请示批准后，对“沈阳市住房保障网”相关信息进行梳理排查，组织对各工作网站开展全面排查，并对涉公民个人敏感信息采取点对点的去标识及隐匿化举措。对已超过公示期限的信息，立即从互联网上撤除。对后续要进行公示的信息，通过办公软件程序设计，将信息上传网络之前先按照既定整改方案进行处理：两字姓名中的第二个字用符号替代；三字姓名中间的字用符号替代；身份证号码第7-14位数字用符号替代；公租房申请人公示信息中，家庭住址公示至区县街道，不再具体到楼号门牌号；电脑派位结果公示中“电脑派位房间号”公示至街路名，具体小区及楼号门牌号用符号替代；低收入住房困难家庭公示信息中，不再公示申请人身份证号码、家庭所在社区、家庭成员关系、家庭人口数、困难具体情况等。

2022年8月，大东区院进行跟进监督，登录相关网站查询，发现网站公示的所有涉及公民个人的信息，均已对身份证号码和姓名实现了去标识化处理，对非必要公示项目不再进行公示，公示内容均按照整改后标准执行，公益损害风险已消除。

【典型意义】

公民个人信息保护问题在诸多政府部门的政务公开过程中普遍存在，基于保障房信息必须公开公示的要求，往往忽略了对个人敏感信息的保护。本案中，检察机关就政务公开活动和公民个人信息保护之间如何兼顾、平衡的问题进行了有益探索，并没有“就案办案”，而是与行政机关共商解决方案，通过检察建议督促其主动作为，既保证行政机关全面展示其工作程序的公平公正公开，又兼顾其中的公民个人信息安全，体现了双赢多赢共赢的办案司法理念，取得了良好的法律效果和社会效果。

信息来源：<https://www.spp.gov.cn/spp/xwfbh/wsfbt/202303/t20230330_609756.shtml#2>