

# 跨境电信网络诈骗挑战下个人信息保护的检察监督路径探索

王俊彦 陈威如 赵莹雪

北京市怀柔区人民检察院 北京市怀柔区 101400

**摘要:** 跨境电信网络诈骗犯罪与个人信息泄露密切相关,催生侵犯公民个人信息等关联犯罪,严重侵犯公民个人信息安全。检察机关在办理相关案件过程中,通过刑事追诉、法律监督、犯罪预防协同运作,形成个人信息保护“关联惩治—穿透治理—合筑防线”的“立体防御机制”。个人信息保护仍面临数据接口管理失范、去标识化未能落实到位等多种风险与挑战。检察机关应通过深化跨境司法协作构建跨境证据调取和审查运用体系、通过“四大检察”融合履职强化个人信息保护全方位治理、通过多部门协同联动技术赋能动态监测个人信息泄露风险,构建个人信息保护的动态协同治理体系,实现从静态、碎片化应对到动态、系统化治理的转变。

**关键词:** 跨境电信网络诈骗;个人信息保护;犯罪治理;检察实践

## 1. 引言:问题的提出

跨境电信网络诈骗犯罪与个人信息的泄露具有“共生关系”。当前,电信网络诈骗犯罪已呈现明显的跨境化、产业化、技术化特征,特别是以缅甸、柬埔寨等地为窝点,针对我国公民实施的跨境诈骗案件呈高发态势。在这类犯罪链条中,公民个人信息已成为关键“生产资料”,为诈骗分子实施“精准诈骗”提供信息支撑。调研中发现,类似超大跨境电信网络诈骗犯罪集团,大多采取公司化封闭管理,层级分明、分工明确,呈现“多行业支撑、产业化分布、集团化运作、精细化分工、跨境式布局”等跨国集团犯罪特征,“形成集个人信息获取、犯罪工具供给、互联网技术支持、引流推广、诈骗实施、钱款结算、资金跨境转移等为一体的完整产业链条”<sup>[1]</sup>;最高人民法院于 2024 年 2 月 7 日发布的跨境电信网络诈骗及其关联犯罪典型案例表明,“量身定制”的“精骗”模式催生了侵犯公民个人信息等关联犯罪,逐渐形成上游非法收集、中游代理商转手倒卖、下游诈骗犯罪非法利用的黑灰产业链,严重侵犯公民个人信息安全,甚至危

及公民生命财产安全。

跨境电信诈骗中的个人信息流转大体如下图所示:

在最高人民法院第 18 批指导性案例“张凯闯等 52 人电信网络诈骗案”中,诈骗集团在境外通过电信技术手段对境内居民的手机、座机电话进行群呼,散布“快递未签收”“护照签证过期”等与个人信息密切相关的虚假信息,诱使被害人接入冒充公安机关、检察机关办案人员的话务员并实施诈骗。该案中,由于诈骗分子掌握并明确提及被害人真实身份信息,使被害人误以为个人数据确实遭到泄露,进而落入资金转移陷阱,最终造成 75 名被害人损失 2300 余万元。

上述案例是跨境电诈案件的一个缩影,极具典型意义。由该案例可见,个人信息在跨境电诈案件中主要发挥的核心作用有:(1) 诈骗分子通过展示被害人准确的身份信息、消费记录等消除其戒备心理,构建被害人的信任;(2) 根据个人信息设计“量身定制”的诈骗话术;(3) 黑产市场对个人信息按价值分级(如金融资产、年龄、职业),诈骗集团据此锁定高价值目标。

表 1: 跨境电信网络诈骗犯罪中个人信息的功能与危害性分析

信息类型	诈骗场景应用	危害性表现	典型案例
身份信息	冒充司法人员要求“配合调查”	骗取大额资金,损害司法公信力	张凯闯等 52 人电信网络诈骗案
通讯信息	精准发送诈骗链接或钓鱼短信	诱导点击恶意程序,盗取账户资金	潘某平等 3 人侵犯公民个人信息案
财产信息	针对高净值人群设计投资骗局	涉案金额数千万,单案损失可达数百万,追赃困难	谢某浩、陈某旺诈骗、偷越国(边)境、林某掩饰、隐瞒犯罪所得案
行踪轨迹	虚构亲友事故要求紧急汇款	利用时空差阻断核实可能性	部分境外诈骗窝点使用位置生成器

在此背景下,个人信息保护不应局限于私法领域的人格权保护。一方面,我国《刑法》第 253 条之一所保护的法益并非个人信息自决权,而是信息利用所影响的公共秩序和公共安全利益;<sup>[2]</sup>另一方面,在诈骗犯罪治理中需强化个人信息保护的源头阻断功能。这种复合性保护需求与检察机关的职能不谋而合:既要通过追诉犯罪切断个人信息非法流转渠道,又要通过法律监督推动前端防护机制建设。

## 2. 跨境电信网络诈骗治理下检察机关个人信息保护“立体防御机制”

在办理跨境电信网络诈骗案件过程中,检察机关通过刑事追诉、法律监督、犯罪预防协同运作,形成个人信息保护“关联惩治—穿透治理—合筑防线”的“立体防御机制”。

### 2.1 依法严厉惩治跨境电信网络诈骗犯罪及其关联犯罪

近年来,我国对电信网络诈骗犯罪打击和治理力度持续加大。2015 年《刑法修正案(九)》增设“帮助信息网络犯罪活动罪”以来,司法实践中很长时间都没有该类案件的判决,直到 2019 年“两高”通过《关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》以后,加之电信网络诈骗案件激增,该罪才得以激活。<sup>[3]</sup>根据最高人民检察院 2024 年工作报告显示,全国检察机关共起诉电信网络诈骗犯罪 7.8 万人,同比上升 53.9%;起诉利用网络实施的侵犯公民个人信息犯罪 2458 人,办理公益诉讼 5061 件,保护个人隐私和信息安全。一方面,检察机关为高质效办好跨境电信网络诈骗案件,在证据审查运用的困境方面给出了“检察方案”,通过强化对境外证据的调取、构建跨境电诈犯罪类案印证体系、及时查证嫌疑人辩解合理性三方面构建跨境电信网络诈骗案件证据体系<sup>[4]</sup>。另一方面,注重对关联犯罪案件尤其是侵犯公民个人信息案件的办理。例如,最高检发布的检察机关依法惩治侵犯公民个人信息犯罪典型案例鲍某等人侵犯公民个人信息案反映出,“吸粉”引流是电信网络诈骗犯罪的上游关键环节,已形成黑灰产业链。成立公司、招募人员,形成较稳定“引流”团队,非法获取客户微信号并提供给上线,既为诈骗犯罪提供了帮助,又侵害了公民个人信息安全,同时触犯多个罪名的,应当择一重,依法从严惩处,从源头斩断电信网络诈骗犯罪黑灰产业链条。

### 2.2 对侵害个人信息行为的“穿透式”治理

在惩治跨境电信网络诈骗犯罪及其关联犯罪的同时,

检察机关亦应对侵害个人信息行为采取“穿透式”治理模式,即在对相关犯罪进行追诉的同时,强化刑事检察与公益诉讼检察衔接协作,通过及时发现并移送相关线索,启动公益诉讼程序、制发检察建议等,彻底封堵个人信息泄露源头。

例如王某某等人诈骗、侵犯公民个人信息案,检察机关对涉及不特定多数人个人信息泄露案件提起附带民事诉讼,并制发检察建议,督促相关企业完善公民个人信息保护措施,以能动履职提升检察综合治理效能。

又如江苏省南通市人民检察院督促规范固话批量申请业务防范电信网络诈骗行政公益诉讼案,该案系南通市院一下级检察机关刑事检察部门在办理唐某等 3 人帮助信息网络犯罪活动案中发现案件线索,即境外诈骗分子指挥境内不法人员注册“空壳公司”申办批量固定电话,实施电信网络诈骗。电信业务经营者应当落实《反电信网络诈骗法》,强化固话开户审核。检察机关在依法刑事打击的同时,对未落实上述反诈义务的经营者,可以发挥公益诉讼检察职能,监督其依法整改。

### 2.3 延伸检察触角防范化解风险

此外,检察机关还应与相关部门协同联动,凝聚多方力量共同形成防范个人信息泄露、预防电信网络诈骗的治理合力。

在王某某涉嫌掩饰、隐瞒犯罪所得案中,行为人系电信网络诈骗下游实施非法买卖、出租、出借银行卡行为的“卡农”,且因犯罪情节轻微被作不起诉处理。同时,检察机关应当根据《反电信网络诈骗法》第 44 条的规定,及时制发检察意见书,将案件移送公安机关作出行政处罚,并对涉案财产处置提出意见,持续跟踪督促落实,确保行为人受到应有法律惩处,同时达到进一步预防犯罪的效果。

在贵州省贵阳市南明区人民检察院督促规范涉诈企业营业执照监管行政公益诉讼案中,检察机关与法院、公安、行政主管部门、金融机构协同联动,一方面,畅通信息共享渠道,常态化开展涉诈企业营业执照、对公账户监管;另一方面,加强法治宣传,将反诈宣传充分融入各部门日常履职工作,开展新设市场主体涉电信网络诈骗违法犯罪警示教育。

## 3. 跨境电信网络诈骗治理下个人信息保护动态协同治理体系构建的检察方案

目前,检察机关在惩治跨境电信网络诈骗犯罪及其关联犯罪的过程中已然形成个人信息保护“关联惩治—穿透治

理—合筑防线”的“立体防御机制”，但依然面临许多新的风险和挑战。对此，在跨境电信网络诈骗犯罪治理的大背景下，应进一步探索构建个人信息保护动态协同治理体系。

### 3.1 个人信息保护面临的新挑战

随着技术手段的迭代更新和犯罪模式的复杂化，个人信息保护在跨境电信网络诈骗治理中面临诸多新挑战。

(1) 数据接口管理失范。相关民生服务系统未对合作企业数据调用权限进行分级管控、加密工作不到位，导致教育、医疗等敏感信息被过度采集，甚至被黑客窃取。如在浙江某妇产医院因第三方签到软件违规上传孕周、预产期等数据，最终导致大量产妇医疗信息流入黑产市场。因省级医疗信息共享平台接口未做好加密工作而遭黑客攻破，四川省某精神卫生中心 2.7 万份患者档案被盗。

(2) 去标识化未能落实到位。虽然我国《个人信息保护法》第 51 条明确要求处理个人信息时应采取加密、去标识化等安全技术措施，但实践中仍存在未采取相应措施即将个人信息进行公开的情况。如十堰市张湾区检察院发现辖区内几个社区在公示大量公民个人信息中未隐去居民的姓名、完整身份证号码、家庭住址、手机号码等敏感信息。周口市郸城县检察院发现，某镇公示耕地补贴名单时虽隐去身份证号中间八位，但通过姓名、村组、完整银行卡号仍可精准定位个人。

### 3.2 个人信息保护的动态协同治理体系构建

面对跨境电信网络诈骗犯罪及其关联犯罪的复杂性和系统性，单一治理手段已难以有效应对。检察机关需要在坚持已形成个人信息保护“关联惩治—穿透治理—合筑防线”的“立体防御机制”的基础上，进一步推动建立多主体协同、多机制联动、多资源整合的治理体系，实现从静态、碎片化应对到动态、系统化治理的转变。

#### 3.2.1 关联惩治——深化跨境司法协作，构建跨境证据调取和审查运用体系

在数字检察战略实施中实现个人信息安全并规制潜在风险，需要构建多层级、立体式的个人信息检察保护体系，规范检察机关收集、处理公民个人信息等行为是实现公民个人信息安全的重中之重。<sup>[5]</sup>在此基础上，优化跨境证据司法协助取证制度。针对跨境取证效率低、周期长等问题，需进一步优化跨境证据司法协助取证制度。在遵守被请求国法律法规的情况下，适当简化刑事司法协助流程，探索“点对点”的文书手续送达传递，精简司法协作文书内容。<sup>[6]</sup>构建跨境

电子数据证据审查运用体系。要立足跨境电信网络诈骗犯罪案件的证据特点，确保境外证据的“三性”，在查清境外电信网络诈骗犯罪团伙、集团运作模式的基础上，充分挖掘在案证据的证明力，查证排除辩解的合理性与证据之间的矛盾。通过依法惩治跨境电信网络诈骗关联犯罪，彻底斩断个人信息黑色交易流转链条。

#### 3.2.2 穿透治理——深化“四大检察”融合履职，强化个人信息保护的全方位系统治理

充分发挥检察机关“四大检察”融合履职效能。畅通跨部门线索移送渠道，探索组建“刑事+公益诉讼+技术”办案团队，集中办理涉及侵犯公民个人信息的电信网络诈骗案件，推动全链条打击。探索特定条件下检察机关不经公告直接提起反电信网络诈骗或个人信息保护民事公益诉讼，创新适用于网络空间治理，倡导科技向善的公益损害替代修复方式；检察机关在个人信息保护公益诉讼中应当更加具有主动性和扩张性，应当享有调查核实权，其目的是为了还原国家利益、公共利益受损的过程<sup>[7]</sup>；还可探索检察机关直接向相关企业制发民事公益诉讼检察建议，督促企业履行个人信息保护职责。<sup>[8]</sup>

#### 3.2.3 合筑防线——多部门协同联动，技术赋能动态监测个人信息泄露风险

加强与公安机关以及金融、教育、医疗等相关行业和相关行政部门的数据共享，构建数据库，建立沟通协调机制，实现各部门数据的互联互通。同时进行技术赋能，运用大数据、人工智能等技术，实时动态检测平台个人信息流转情况，发现异常及时通知公安机关开展核查。大数据技术应用方面，可通过采集海量数据，深入挖掘各类数据相关性，监测电诈犯罪热点，对犯罪走势进行预测；还可对诈骗风险进行动态监测、关键字识别，总结犯罪规律和特征，做到风险预警。人工智能技术应用方面，基于自然语言模型技术、知识图谱的应用，一方面识别诈骗行为、预防犯罪，另一方面溯源个人信息泄露源头，为检察机关及时采取个人信息保护治理措施提供线索和依据。

### 4. 结语

在数字时代，检察机关应成为个人信息安全的法治守护者与网络空间正义的规则引领者。通过强化“关联惩治—穿透治理—合筑防线”的“立体防御机制”，构建个人信息保护的动态协同治理体系，在打击犯罪与保障权利间寻求动

态平衡,这不仅关乎个体权益的保障,更关系到国家治理体系在数字时代的现代化转型。跨境电信网络诈骗犯罪下个人信息保护的检察实践仍需不断探索,为营造清朗网络空间、切实维护人民群众生命财产安全贡献检察力量。

#### 参考文献:

- [1] 翁音韵,刘洋.跨境电信网络诈骗犯罪的刑事规制困境与纾解[J].人民检察,2023,(22):25.
- [2] 杨凯.以公法法益观理解侵犯公民个人信息罪[N].检察日报,2021-12-10(003).
- [3] 张启飞,虞纯纯.论电信网络诈骗犯罪的刑法规制[J].法律适用,2023,(08):75.
- [4] 陈禹潼.刑事一体化视野中的跨境电信网络诈骗犯罪疑难问题研究[J].法律适用,2024,(10):120.
- [5] 陈在上,任逸飞.数字检察视域下个人信息保护的风险及其规制[J].河北科技大学学报(社会科学版),2025,25(04):82.
- [6] 徐恺东,张茂,邵淑琼.跨境电信网络诈骗犯罪的预防策略[J].人民检察,2025,(11):63.
- [7] 华鑫.检察机关提起个人信息保护公益诉讼司法探讨[J].天中学刊,2025,40(05):27.
- [8] 邱景辉.提升反电信网络诈骗检察公益诉讼治理效能[J].人民检察,2022,(16):43.

**作者简介:** 王俊彦(1998.02-),男,汉族,安徽明光人,硕士研究生,四级检察官助理,研究方向:诉讼法学、刑法学。

陈威如(1996.07-),男,满族,辽宁义县人,硕士研究生,四级检察官助理,研究方向:诉讼法学、刑法学。