社会科学进展
2025 年 3 月第 7 卷第 3 期

大数据时代电信网络诈骗犯罪的治理困境及治理机制研究

张蓝羽

上海政法学院，上海

摘　要 | 大数据时代的到来加速了经济社会数字化的转型，以电信网络诈骗为代表的新型犯罪呈现高发态势。其特点包括犯罪主体的不确定性、作案手段的高隐蔽性、组织结伙性等。与此同时，个人信息隐私泄露与技术的滥用进一步提升了诈骗的精准性与危害性，严重威胁公民财产安全与社会稳定。当前，电信网络诈骗治理面临多重困境：诈骗技术快速迭代、跨境协作障碍突出、受害群体分散且财产追回困难等。对此，亟需构建多方联动的综合治理机制，从强化公众反诈意识、深化国际合作、完善技术防控体系等维度入手，形成全链条打击电信网络诈骗的闭环治理模式。

关键词 | 大数据；电信网络诈骗；个人信息泄露；跨境犯罪；协同治理

1　引言

随着大数据技术的广泛应用，电信网络诈骗犯罪呈现出智能化、跨境化、精准化的新特征，成为数字经济时代社会治理的顽疾。据公安部统计，五年来，全国公安机关共破获电信网络诈骗犯罪案件194.5万起，电信网络诈骗犯罪上升势头得到有效遏制，[1]其中AI换脸、虚拟货币洗钱等新型技术犯罪占比显著攀升，传统治理模式面临严峻挑战。当前学界对电信网络诈骗的研究多集中于单一维度：技术领域聚焦于数据加密与风险预警算法优化，法学领域侧重跨境司法协作的制度完善，社会学领域则强调公众防骗教育的普及。然而，现有研究对“技术迭代—犯罪升级—治理滞后”的动态矛盾缺乏系统解构，亦未充分整合技术防控、国际合作与公众参与的协同机制，导致理论建构与治理实践存在一定脱节。

本研究以“犯罪技术演进—治理机制失灵—体系化重构”为逻辑主线，揭示大数据时代电信网络诈骗犯罪的底层运行逻辑与治理效能瓶颈。理论层面，本研究通过解构“技术赋能犯罪—技术赋能治理”的双向关系，为网络犯罪治理理论提供新的分析范式；实践层面，所提出的协同治理路径可为公安机关、金融机构及国际组织提供可操作的政策工具箱，助力实现“事前预警—事中拦截—事后追损”的全链条闭环管理。在数字经济与犯罪技术深度耦合的当下，这一探索对维护公民财产安全、保障数字社会秩序具有紧迫的现实意义。

2　当前电信网络诈骗的特点

2.1　犯罪主体不确定性、高隐蔽性

大数据时代，互联网载体从传统电脑向智能手机、

作者简介：张蓝羽，上海政法学院研究生，研究方向：刑法学。
文章引用：张蓝羽. 大数据时代电信网络诈骗犯罪的治理困境及治理机制研究 [J]. 社会科学进展，2025，7（3）：208-212.
https://doi.org/10.35534/pss.0703036

平板等便携设备迁移，推动网络犯罪从“实体接触”转向“非接触式”模式。犯罪主体可借助虚拟身份隐匿真实信息藏匿于屏幕之外，其年龄、性别、职业等个人特征难以追溯，显著提升了侦查难度。值得注意的是，近年来电信网络诈骗的犯罪主体范围不断扩大，大量年轻人因技术误导或法律意识淡薄，沦为“帮助信息网络犯罪活动罪”（简称“帮信罪”）的涉案主体。据最高人民检察院统计，2022年上半年检察机关起诉帮信罪6.4万人，其中犯罪低龄化现象突出，涉案人员中30岁以下群体占比达64.8%，[2]反映出犯罪主体泛化与低龄化趋势。此外，诈骗团伙通过非实名电话卡、虚拟拨号软件、跨境服务器跳转等技术手段，进一步强化身份隐匿性，致使公安机关难以锁定犯罪源头，加大了侦破难度。

2.2 组织结伙性与空间离散性并存

当前电信网络诈骗呈现高度组织化特征，犯罪团伙常以“金字塔式”层级结构运作：顶层人员负责策划与资金分配，中层人员实施话术设计、信息窃取等技术环节，底层人员执行转账洗钱等末端操作。以“杀猪盘”骗局为例，其团队通常分为“钓鱼组”（伪装身份建立信任）、“技术组”（伪造投资平台）、“洗钱组”（拆分转移赃款）三类分工，形成闭环犯罪链条。[3]值得注意的是，犯罪团伙虽以集团形式运作，但成员可依托网络实现跨地域协同。跨境电信诈骗团伙通常将话务员窝点设在东南亚国家，利用当地相对宽松的监管环境和较低的运营成本实施诈骗，将服务器架设在境外，以规避国内监管，资金流向中东虚拟货币平台进行洗钱操作。这种空间离散性导致公安机关难以全面锁定犯罪网络，仅能通过碎片化线索进行局部打击。

2.3 与个人隐私泄露问题粘性增强

大数据时代，个人信息的过度采集与非法交易为精准诈骗提供了“弹药库”。《2024年数据泄露风险态势报告》显示，2024年全年监测到37575起有效数据泄露事件，涉及金融、物流、航旅、电商、汽车等20余个行业，数据泄露风险态势依旧严峻。[4]网民每一次的“同意并授权”选择，都让渡了自己的一部分个人信息给网络平台。诈骗分子通过整合这些社交账号、消费记录、地理位置等碎片化数据，构建被害人的“数字画像”，进而量身定制诈骗脚本。例如，在河北山海关区的一起“冒充公检法”案件中，犯罪分子精确掌握被害人身份证号、家庭住址及近期行程，通过市公安局的“警官”的身份发放伪造“通缉令”制造恐慌，成功骗取80余万元。[5]此类“点对点”诈骗因信息高度匹配，迷惑性极强，已成为当前高发诈骗类型。可以说，个人隐私数据的泄露大大增加了诈骗的成功概率，个人数据隐私的泄露已经成为精准诈骗的重要前导性因素。[6]

2.4 技术快速迭代与社会热点捆绑

诈骗手段随技术革新不断升级，并与社会热点深度捆绑。2023年6月15日，国家反诈中心公布电信网络诈骗十大高发类案，并提到当前打击电信网络诈骗形势依然严峻。[7]近几年，随着群众防骗意识的觉醒和公安部深入推进打防管控的努力，传统单一的诈骗手段几近腰斩，但随之而来的是套路更加复杂的“骗中骗”。诈骗手段随技术革新不断升级，并与社会热点深度捆绑。校园防诈宣传中，不乏利用“花呗”平台个人学生认证影响征信、谎称海外代购骗取中间费等新型诈骗手段，而随着生成式人工智能的发展，利用AI进行换脸诈骗的新闻也频频爆出。瑞莱智慧数据指出，国内AI诈骗案件的涉案金额从2020年的0.2万元增长至2023年的1670万元，年复合增长率高达1928.8%。[8]借助ChatGPT等生成式AI工具，可自动化生成高仿真钓鱼邮件，极大降低犯罪成本。诈骗技术的加速迭代，诈骗团伙也会紧密追踪社会热点：2023年文娱市场复苏期间，“演唱会门票代购”骗局集中爆发，犯罪分子伪造票务平台链接，冒充客服诱导支付，许多“求票心切”的听众一掷千金，却最终陷入诈骗陷阱。

3 大数据时代电信网络诈骗的治理难点

3.1 诈骗技术快速迭代，防控滞后性显著

大数据技术的滥用使得诈骗手段不断升级，犯罪技术从“粗放式”转向“精准化”。以爬虫技术为例，网络爬虫是指按照一定规则自动获取网络信息的程序或脚本，[9]其本为合法数据采集工具，却被犯罪分子用于非法窃取个人信息。2023年，威胁猎人监测到的数据泄露事件中，公民个人信息泄露占比高达93.68%，其中“姓名+手机号+身份证号+银行卡号”等敏感信息组合频繁出现。在这些数据泄露事件中，爬虫技术是主要的攻击手段之一。[10]此类技术可在短时间内完成海量信息抓取，且操作痕迹易被清除，导致公安机关难以及时溯源。

此外，“嗅探+撞库”组合技术成为新型威胁：犯罪分子通过嗅探设备截取手机信号，获取短信验证码后登录被害人账户，再利用“撞库”（即利用泄露的账号密码尝试登录其他平台）扩大攻击范围。此类技术具有高度隐蔽性，公众难以察觉，监管部门亦难以及时预警，只能在大量案件发生后才能有针对性地进行技术干预，技术防控的滞后性成为治理核心难点。

3.2 境外犯罪据点扩张，国际协作阻力突出

在国内严厉打击电信网络诈骗犯罪的背景下，犯罪分子的“生存环境”变得严峻，为规避国内高压打击，电信诈骗团伙开始加速向境外转移。[11]据公安部统计，2023年约65%的诈骗窝点集中于东南亚地区，其中缅北、柬埔寨西哈努克港成为电信网络诈骗犯罪的高发区域。[12]犯罪分子以“高薪务工”为诱饵招募人员，形成跨境产业链。2024年12月，演员王某因看到泰国拍

https://doi.org/10.35534/pss.0703036

戏的虚假招聘信息，被诱骗至缅甸妙瓦底的电诈园区。王某从失联后到被成功解救的整个过程，引发社会广泛关注。该事件凸显了东南亚地区电信诈骗和人口贩卖问题的严重性，同时也反映了跨境犯罪打击的复杂性。当前，跨境打击面临三重障碍：第一是程序繁琐，跨境取证通常需要通过国际刑警组织等国际执法合作机制进行协调，这使得案件协查周期较长，平均长达6个月；二是法律冲突，部分国家将电信诈骗定性为“经济纠纷”，拒绝引渡主犯，限制了国际社会共同防范和打击的积极性；三是治理缺位，缅北等地长期存在地方武装庇护犯罪集团的现象，导致电信网络诈骗犯罪“打而不绝”。上述问题致使境外追逃与打击效率低下，抓捕犯罪嫌疑人的战线被无限拉长。

3.3 受害规模庞大，跨地域特征显著

在当前大数据互联网快速发展的背景下，电信网络诈骗依托分工协作模式，呈现“一对多”的规模化特征。这导致了一个治理困境——受害规模庞大且跨地域特征显著。分工协作的诈骗团伙，在一个诈骗周期内，可以持续对成百上千名被害人实施诈骗。同时，这种诈骗方式不再受地域限制，诈骗话务员可通过虚拟定位软件伪装在被害人所在地，利用“伪基站”发送本地化诈骗信息。其结果是被害人数量的海量化，以及被害人空间分布的分散化。2023年最高检发布《检察机关打击治理电信网络诈骗及其关联犯罪工作情况（2023年）》显示，诈骗犯罪已突破地域限制，全国各地均有被害人，被害人年龄、职业、经历、地域等特征已不再是决定诈骗能否成功的重要标准。[13] 受害人的分散性使得案件管辖混乱，多地警方协调成本激增。

3.4 涉案资金转移迅速，追赃挽损难度高

近年来，电信网络诈骗案件数量呈现出惊人的增长速度。随着互联网技术的不断发展，电信网络诈骗的手段也在不断迭代升级，如“杀猪盘”、淘宝刷单、直播诈骗、木马链接等。目前，在电信网络诈骗犯罪中流行的手段为GOIP技术。通过GOIP设备远程操控，赃款可在30分钟内经数百个账户层层分流，快速拆分，从而实施诈骗行为。在获取到诈骗赃款后，黑产团伙利用“跑分平台”将赃款拆解为小额交易，以规避银行风控系统。犯罪分子同时利用虚拟货币交易平台将境内资金转换为加密货币，再转至境外兑换为外币。[14] 电信诈骗资金流转呈现“快、隐、跨”的特征，使得资金转移迅速且难以追踪，给警方调查取证带来极大困难。

尽管国家反诈中心已经建立了基于大数据分析的涉诈预警提示机制，并通过层层联动的方式，将预警信息传递到基层民警，以开展反诈宣传，但要想在诈骗分子通过层层账户嵌套将资金转移之前及时止付并追回受害者的损失，仍然面临极大的困难。多数案件中，被害人报案时资金已被转移，致使追赃工作陷入僵局，“反诈”工作难以取得实质性进展。

4 当前电信网络诈骗犯罪的预防与治理机制展望

4.1 提升公众信息免疫力

在应对电信网络诈骗的治理挑战时，需构建多维度、全链条的协同防控体系。首先，提升公众的“信息免疫力”是阻断诈骗犯罪的关键环节。电信诈骗犯是利用“信息不对称”进行交流并犯罪的典型犯罪类型，犯罪分子为了能够顺利得手，在前期针对潜在被害人一定要做的就是“心理操控”，并成功“控制”被害人并将钱财转移到手。从防范的角度来看，阻断虚假信息的接受过程比阻断虚假信息的输入过程要重要得多。因为接受过程是潜在被害人的主动过程，普通被害人的接受过程被阻断，也就意味着财产权益没有受到侵害。而要阻断虚假信息的接受过程，就需要提高公众的“信息免疫力”，助力其及时识破骗局。针对不同群体的认知差异，应采取分层化、场景化的反诈宣传策略。例如，面向老年群体可通过社区讲座、情景剧还原“保健品诈骗”“冒充亲属急救”等常见套路；针对学生群体，可利用短视频平台推出“反诈剧本杀”互动内容，让公众成为自身财产安全的第一责任人。

此外，除了传统的宣传教育方式外，技术预警与人工干预结合的多层次反诈防护工具也不可或缺。公安部会同工信部、中国人民银行联合推出的“反诈神器”国家反诈中心App自上线以来，累计受理群众举报线索2323万条，向群众预警3.1亿次，也在防范诈骗工作中发挥了重要作用。[15] 其内置的“诈骗信息实时弹窗提醒”功能，会通过弹窗提醒用户，智能识别诈骗信息并及时预警，从而降低用户受骗的可能性。凸显技术工具在强化公众主动防御中的重要作用。

4.2 构建跨区域跨境国际合作机制，削减管辖权限制

由于新时代下网络电信诈骗的跨地域性特点，跨境治理的协助困境已成为阻碍我国打击网络电信诈骗的最大障碍之一。跨境治理的合作壁垒需通过国际合作网络破解。例如我国提倡签订的《上海合作组织成员国保障国际信息安全政府间合作协定》，在打击跨国网络犯罪方面发挥着重要作用。2019年12月，联合国通过了中国、俄罗斯等47国共同提出的《打击为犯罪目的使用信息通信技术》决议，正式开启谈判制定打击网络犯罪全球性公约的进程。[16] 我国打击网络犯罪的国际合作取得了一定成效，但还存在一定漏洞。比如，和我国签订双边引渡条约的国家有60个，其中亚洲国家20个、欧洲国家14个，[17] 虽然数量上看具有一定优势，但其中并不包含欧美大部分发达国家，也不包括大量电信诈骗团伙聚集的缅甸。双边司法引渡条约的存在能够有效加快电信

网络诈骗犯罪的打击步伐，比如和我国签订双边条约的柬埔寨、老挝、菲律宾等东南亚国家，因为有引渡条约的存在，诈骗团伙在此地发展频频受阻。同时我们也在逐步收紧打击电诈的包围圈，“反诈”行动取得有效进展。反观缅甸，因为没有和我国有签订双边引渡条约，现在的缅北已经成为名副其实的“电诈天堂”。

我国要努力加强跨境侦查协作的力度，积极争取同他国刑事司法部门的合作，继续简化跨境犯罪的侦办和移送程序。为此，可依托《联合国打击网络犯罪全球公约》框架，推动电子取证标准化与协查流程简化。在区域性层面，东盟“反诈情报共享中心”已初显成效；2024年中柬联合行动中，柬警方捣毁了多个位于西哈努克市的赌诈窝点，抓获了一大批中国籍违法犯罪嫌疑人，我国警方将130名中国籍涉赌诈违法犯罪嫌疑人押解回国。[18]对缅甸等“司法洼地”，需通过外交施压与经济合作双轨并进，迫使其加入国际反诈体系，同时与欧美共建“诈骗账户黑名单数据库”，实时拦截跨境资金异动。除了积极同其他国家进行引渡条约的合作之外，我们还可以利用“一带一路”倡议，凝聚起“一带一路”沿线国家的打击网络电信诈骗的共识，利用现有合作平台，积极拓宽国际司法合作新道路，共同打击网络电信诈骗。

4.3 畅通反诈侦查路径，完善各方协同机制

技术协同是打通治理链条的核心支撑。网络电信诈骗作为一种新型犯罪，犯罪过程的前、中、后期均涉及多方社会基础设施部门，如网络、金融、通信等。因此，电信网络诈骗治理需依托跨部门技术协同，形成“多位一体”的治理模式，有效打通协同合作侦查机制。

首先是通信端的防控。犯罪分子主要通过网络通信或手机通话来与潜在被害人进行交流，因此电信运营商在网络电信诈骗的孕育期扮演着关键阻拦角色。公安机关和电信运营商应建立实时合作机制，电信运营商针对高度疑似诈骗账号进行上报，公安机关针对上报的疑似账号进行监控，同时做到社区派出所民警及时响应，上门劝阻，做到及时将“转账汇款”行为扼杀在摇篮中。

其次是金融端的拦截。犯罪分子在进行诈骗后迅速将账户内的钱财进行转移，并层层分发到其他洗钱账户，防止公安机关直接通过账户追查到犯罪团伙。因此金融机构需对电信诈骗黑名单账户实施控制，对系统预警的电信诈骗账户及时中止汇款交易，通过区块链技术追溯资金流向，并向客户提示风险。打造“监测–拦截–溯源”全链条防线，助力形成打击治理电信网络新型违法犯罪的强大合力。

最后是数据端的共享。公安部门需与通信、金融等领域深化数据共享。打通公安、通信、金融三方数据接口，构建“涉诈黑名单库”，实现高危账号全网同步封禁。

此外，针对AI换脸、虚拟货币洗钱等新型犯罪手段，需强化技术反制能力：训练深度学习模型识别伪造音视频，在关键领域推广量子加密通信技术，并与国际机构搭建“数据沙盒”，模拟攻防演练以预判犯罪技术迭代趋势。

5 结语

大数据时代的到来，为经济社会注入活力的同时，也为电信网络诈骗犯罪提供了技术温床。此类犯罪呈现出主体隐蔽性强、组织结伙性高、技术迭代迅速等特点，并与个人信息泄露深度绑定，形成精准化、跨域化的犯罪生态。治理过程中，技术防控滞后、跨境协作障碍、受害人分散及资金追损困难等问题凸显，亟需构建多维度协同治理体系。

未来的治理路径需以“技术反制技术”为核心，通过AI识别、区块链追踪等手段破解犯罪工具；以“共治替代单治”为方向，深化跨国司法协作与数据共享，压缩犯罪分子的境外生存空间；以“预防优于惩治”为理念，通过分层教育提升公众信息免疫力，从源头阻断诈骗信息传播链。唯有技术、制度与公众意识三方协同，方能构筑起电信网络诈骗治理的立体防线，为数字社会的安全发展提供坚实保障。

参考文献

[1] 公安部. 全国公安机关5年来打击整治电信网络诈骗犯罪取得显著成效[J]. 中国防伪报道，2024（6）：7–8.
[2] 最高人民检察院网上发布厅. 2022年上半年检察机关起诉帮信罪6.4万人[EB/OL]. （2022–07–22）[2025–03–05]. https://www.spp.gov.cn/spp/xwfbh/wsfbt/202207/t20220722_566409.shtml#1.
[3] 方映红. “杀猪盘”电信网络诈骗犯罪侦防研究[J]. 中国人民警察大学学报，2022，38（7）：78–83，91.
[4] 威胁猎人. 2024年上半年数据泄露风险态势报告[EB/OL]. （2024–07–04）[2025–03–05]. https://mp.weixin.qq.com/s?__biz=MzI3NDY3NDUxNg==&mid=2247497450&idx=1&sn=a5f755af70a3adeadd04a35ddb73a8f7.
[5] 网信山海关. “冒充公检法”诈骗套路升级 山海关一女子被骗80余万元[EB/OL]. （2023–05–05）[2025–03–05]. https://www.thepaper.cn/newsDetail_forward_22972474.
[6] 张扬，邓志源. 电信网络诈骗犯罪态势分析与体系化应对[J]. 湖北警官学院学报，2021（6）：80–88.
[7] 袁猛. 公安部公布十大高发电信网络诈骗类型

https://doi.org/10.35534/pss.0703036

［N］. 人民公安报，2023–06–16（2）.
［8］定焦One. AI换脸，该抵制吗？［EB/OL］.（2024–08–28）［2024–12–24］. https://baijiahao.baidu.com/s?id=1808592771198980634&wfr=spider&for=pc.
［9］张佳华. 大数据时代新型网络犯罪的惩治困境及进路［J］. 学习与实践，2022（5）：85–95.
［10］威胁猎人.《2023年数据泄露风险年度报告》［EB/OL］.（2024–01–22）［2025–02–05］. https://mp.weixin.qq.com/s/gwafJTo–ic2W2YGycopkwA.
［11］刁珂. 电信网络诈骗犯罪的解构与对策展望［J］. 产业与科技论坛，2023，22（17）：40–42.
［12］张月恒，陈纹洁，郭媛丹. 打击跨国电诈，每一个“妙瓦底”都不放过［N］. 环球时报，2025–02–22（5）.
［13］最高人民检察院网上发布厅. 最高检发布《检察机关打击治理电信网络诈骗及其关联犯罪工作情况（2023年）》［EB/OL］.（2023–11–30）［2025–02–05］. https://www.spp.gov.cn/spp/xwfbh/wsfbt/202311/t20231130_635181.shtml#1.
［14］王爱迪. 地下钱庄非法跨境汇兑犯罪防控对策研究［J］. 河北公安警察职业学院学报，2021，21（3）：41–44，50.
［15］董凡超. “七大反诈利器”有效防范电信网络诈骗［N］. 法治日报，2023–06–21（2）.
［16］孟念，丁华宇. 网络诈骗犯罪的治理困境与对策分析［J］. 陕西行政学院学报，2023（4）：72–76.
［17］吴琼. 中国对外缔结引渡条约30年来成绩斐然［N］. 法治日报，2023–09–04（5）.
［18］张天培. 中柬警方执法安全合作取得新战果［N］. 人民日报，2024–04–15.

Governance Dilemma of Telecommunication Network Fraud Crime and Governance Mechanisms in the Era of Big Data

Zhang Lanyu

Shanghai University of Political Science and Law, Shanghai

Abstract: The arrival of the big data era has accelerated the digital transformation of the economy and society, and new types of crime represented by telecommunication network fraud have shown a high incidence of crime, whose characteristics include the uncertainty of the subject of the crime, the high degree of concealment of the means of operation, and the organization of gangs. At the same time, the leakage of personal information privacy and the abuse of technology further enhance the accuracy and harmfulness of fraud, seriously threatening the safety of citizens' property and social stability. Currently, the governance of telecom network fraud is facing multiple difficulties: rapid iteration of fraudulent technology, outstanding obstacles to cross-border collaboration, dispersed victim groups and difficulties in property recovery. In this regard, there is an urgent need to build a multi-party comprehensive governance mechanism, starting from strengthening public awareness of anti-fraud, deepening international cooperation, improving the technical prevention and control system and other dimensions, to form a closed-loop governance model for the whole chain to combat telecom network fraud.

Key words: Big data; Telecommunications network fraud; Leakage of personal information; Cross-border crime; Collaborative governance