

网络犯罪的演变和刑事辩护新挑战

杨钺

河南首位律师事务所，河南 平顶山 467000

DOI:10.61369/SE.2025080038

摘 要： 网络犯罪随着技术发展逐步变化，从早期单一形态慢慢走向智能化、跨境化、产业化，法律规则虽慢慢完善，却还存在滞后问题。为应对其给刑事辩护造成的技术、证据、法律适用及审判程序等难题，本研究旨在找出有效的辩护办法。依靠提高律师专业能力、组建合作团队，改进证据质证工作，促进法律条款明确，适应审判新需求，来更好应对难题，保证辩护质量和司法公平。

关 键 词： 网络犯罪；技术更新；形态演变；刑事辩护；技术难题

The Evolution of Cybercrime and New Challenges in Criminal Defense

Yang Yue

Henan Shouwei Law Firm, Pingdingshan, Henan 467000

Abstract： With the development of technology, cybercrime has gradually evolved, transitioning from its early, singular form to become more intelligent, cross-border, and industrialized. Although legal regulations have been gradually refined, there remains a problem of lag. In response to the technical, evidentiary, legal application, and trial procedure challenges posed by cybercrime to criminal defense, this study aims to identify effective defense strategies. By enhancing the professional competence of lawyers, forming collaborative teams, improving the examination of evidence, promoting clarity in legal provisions, and adapting to new trial requirements, we can better address these challenges, ensuring the quality of defense and judicial fairness.

Keywords： cybercrime; technological updates; evolution of forms; criminal defense; technical challenges

引言

技术更新不断重塑网络空间生态，也让网络犯罪形态不断突破传统边界，从早期局部技术破坏逐步演变为全球化、产业化危害行为，对现有法律体系与司法实践构成冲击。刑事辩护是司法公正重要保障，应对新型网络犯罪时，需直面技术、证据、法律适用等多方面新难题。深入探究网络犯罪演变轨迹与刑事辩护挑战，不仅可给辩护工作提供理论指引，助力律师突破实务困境，更可推动司法资源合理配置，完善网络犯罪治理体系，维护数字时代社会秩序与公民合法权益。1 网络犯罪的演变历程

（一）早期网络犯罪形态

网络发展初期，受网络技术发展水平限制，网络未普及，仅在科研机构、高校及部分大型企业应用。当时网络犯罪主体多是掌握专业计算机技术的人员，普通民众因缺乏网络接入条件和技术认知，难以参与。犯罪行为主要聚焦对计算机系统攻击破坏，比如1998年肆虐的“CIH 病毒”，恶意修改计算机主板 BIOS 程序，造成全球数百万台计算机硬件受损。此外，非法入侵计算机系统窃取内部数据、盗用电子邮箱或网络游戏账号等行为也较常见。此类犯罪多为彰显技术能力或满足个人好奇心，未形成规模化盈利模式，且当时针对网络犯罪立法还不完善，打击力度有限。

（二）互联网 2.0 时代网络犯罪拓展

互联网 2.0 时代来临，网络从单向信息传播转向交互式参与，博客、论坛、社交平台兴起，用户生成内容成主流，网络用户规模迅猛增长。该变革推动网络犯罪从“技术破坏型”转向“利益驱动型”。网络诈骗、盗窃、赌博等盈利性犯罪大量出现，比如早期“钓鱼网站”模仿银行、电商界面，骗取用户账号密码和银行卡信息；“网络传销”借助社交平台传播，以高回报为诱饵发展下线骗钱。同时，网络侵犯知识产权犯罪增多，盗版音乐、电影、软件通过 P2P 下载平台广泛传播。犯罪组织形态也出现分工协作雏形，涵盖技术开发、资金流转、信息收集、话术培训等环节，且因互联网跨地域性，犯罪行为可跨地区实施，增加侦查溯源难度。该时期，我国立法逐步完善，对相关网络犯罪行为作出明确规制^[1]。

（三）移动互联网与智能时代新型网络犯罪

步入移动互联网与智能时代，智能手机、物联网设备普及，大数据、人工智能、区块链等新技术应用广泛，网络犯罪呈现智能化、跨境化、产业化、隐蔽化特征。人工智能遭滥用，比如利用“深度伪造”技术生成逼真视频、音频实施诈骗，或借助人工智能算法分析个人信息，实现精准诈骗；移动互联网与虚拟货币让犯罪突破地域国界限制，跨境电信网络诈骗频发，犯罪团伙在境外指挥，利用虚拟货币洗钱，资金流向难追踪；网络犯罪产业链成熟，以跨境电信网络诈骗为例，上下游分工精细，“帮助信息网络犯罪活动罪”激增，众多“低学历、低收入、低技术水平”人群受利益驱使为犯罪提供工具支持。

一、网络犯罪演变带来的刑事辩护新挑战

（一）技术专业挑战

随着网络犯罪向智能化发展，刑事辩护面临严峻技术专业挑战。传统刑事辩护中，律师主要围绕常规法律事实与法条适用开展工作，对技术知识要求较低。但当下网络犯罪涉及大数据、人工智能、区块链、加密通信等前沿复杂技术。例如区块链存证相关案件里，控方常以区块链数据不可篡改特性作为证据真实性依据。然而，律师若不深入了解区块链技术原理，难以察觉其中漏洞。实际上，区块链存证真实性不仅取决于上链后状态，上链前数据真实性以及上链过程是否合规同样关键，像联盟链、私有链存在节点被控制风险，数据可能经筛选后上链。如涉及 AI“深度伪造”技术案件，如何精准区分伪造与真实内容，以及明晰 AI 技术滥用和犯罪行为间因果联系，都需要律师具备深厚技术素养，否则难以在质证环节有效反驳控方观点，严重影响辩护成效^[2]。

（二）证据收集及认定挑战

网络犯罪隐蔽化和跨境化，使证据收集及认定成为刑事辩护棘手问题。电子数据作为网络犯罪案件核心证据，具有易失性和易篡改特点。侦查机关取证时，若未能及时依照法定程序固定证据，如未妥善扣押原始存储介质、未进行哈希值校验，极易导致电子数据完整性受损。而律师质证时，因电子数据技术复杂，难以自行核验其真实性，通常依赖专业技术鉴定。但鉴定机构资质、鉴定方法科学性等方面常存争议，进一步加大质证难度。因网络犯罪跨境化趋势显著，大量关键证据位于境外，像境外服务器数据、虚拟货币交易记录等，需通过跨境司法协助获取。但不同国家法律体系和证据标准差异巨大，部分境外证据可能因收集程序不符合我国法律规定，面临合法性质疑。同时，证据关联性认定也困难重重，例如境外服务器聊天记录，难以确凿证明与境内犯罪嫌疑人关联，侦查机关受跨境协作效率低、证据获取难等因素制约，无法提供充分关联证据，律师若不能有效指出这些问题，辩护工作将陷入被动。

（三）法律适用模糊性挑战

网络犯罪快速演变与法律滞后性矛盾突出，致使刑事辩护遭遇法律适用模糊困境。新型网络犯罪常涉及多个罪名交叉，如利用 AI 技术侵犯公民个人信息并实施诈骗，可能同时触犯侵犯公民个人信息罪、诈骗罪、非法利用信息网络罪等。不同罪名法定刑差异明显，可法律对罪名竞合适用规则规定不够清晰，实践中法

院裁判标准也不尽相同，律师辩护时难以精准选择对被告人有利的罪名适用路径。大数据、人工智能、区块链等新技术催生诸多新型概念，如公民个人信息范围、数据权益归属、区块链存证法律地位等，在法律中缺乏明确界定。以个人信息保护法为例，虽规定个人信息是与已识别或可识别自然人相关信息，但对于间接可识别信息认定存在争议。而区块链存证证据效力，法律仅有原则性规定，具体审查标准不明，导致法院采信率差异大，律师难以预判辩护方向^[3]。

（四）审判程序复杂性挑战

网络犯罪跨地域性和技术复杂性，给审判程序带来诸多难题，进而影响刑事辩护效果。依据我国刑事诉讼法及相关司法解释，网络犯罪案件管辖地包括犯罪行为发生地、犯罪结果发生地或被告人居住地。但因网络犯罪跨地域性，一个案件可能涉及多个犯罪地，不同地区法院可能均主张管辖权，导致管辖争议频发。不仅拖延案件审理进程，还可能因不同地区量刑标准差异，影响案件裁判结果，律师需耗费大量精力处理管辖异议，分散对核心辩护要点的关注。网络犯罪案件证据多为电子数据，且包含大量技术细节，如服务器日志、代码程序等。庭审质证阶段，控方需详细说明电子数据收集、保管、鉴定过程，辩方则要对证据合法性、真实性、关联性进行质证。但法官和陪审员可能因缺乏技术背景，难以理解质证要点，导致质证程序冗长低效。若案件涉及跨境证据或专业技术鉴定，境外证人出庭困难，技术专家证言专业性强，进一步增加质证复杂性，律师需花费更多时间准备质证意见，确保法官准确理解辩护观点。

二、应对网络犯罪刑事辩护挑战的策略

（一）提升辩护律师专业素养

知识学习层面，律师需主动系统掌握大数据、人工智能、区块链、加密通信等前沿技术基础原理，可报名司法行政部门或专业法律机构开设的网络犯罪辩护专项培训，如中国政法大学举办的“数字时代刑事辩护技术专题研修班”，掌握网络犯罪常见技术手段运作逻辑，比如理解区块链链上数据生成机制、虚拟货币交易链路追踪方法。同时定期阅读网络安全领域权威期刊与报告，如《中国信息安全》杂志发布的年度网络犯罪趋势分析，及时更新技术认知，缩小与网络犯罪技术发展的差距。团队协作层面，针对技术复杂的网络犯罪案件，律师需组建法律与技术协作团队。可与具备资质的电子数据取证公司、网络安全技术企业建

立长期合作，邀请电子数据分析师、网络安全工程师担任技术顾问参与案件辩护。具体案件中，技术顾问可协助律师梳理案件技术脉络，如绘制跨境电信诈骗资金流转技术链路图，解读服务器日志、代码程序等技术证据中关键信息，帮助律师识别控方证据中技术漏洞，比如指出区块链存证中节点控制导致的数据筛选问题。

（二）优化证据收集及质证策略

证据固定层面，律师应在案件侦查阶段尽早介入，引导当事人留存与案件相关电子数据证据，如聊天记录、资金转账凭证、操作日志等，并协助当事人用合规方式固定证据，比如通过公证机构对电子数据存证，确保证据完整性与合法性。同时律师可向侦查机关申请查阅电子数据取证笔录，监督侦查机关取证程序合规性，若发现侦查机关未扣押原始存储介质、未做哈希值校验等问题，及时提出书面异议，要求侦查机关补正或作出合理解释，避免因取证程序违法导致证据无效。质证方法方面，针对电子数据证据，律师应构建技术与法律双重质证框架。技术层面借助技术顾问支持，审查电子数据生成、存储、提取过程，如核验区块链存证上链数据是否与原始数据一致，判断境外服务器数据提取是否符合技术规范；法律层面依据《刑事诉讼法》《电子数据规定》等法律法规，审查取证主体资质、取证程序合法情况，如质疑无资质机构出具的电子数据鉴定报告效力，指出跨境证据未履行法定司法协助程序问题^[4]。

（三）推动法律适用明确化

理论研究层面，律师可结合办理的网络犯罪案件，开展法律适用问题研究，撰写学术论文或案例分析报告，比如针对 AI “深度伪造” 诈骗案件中罪名竞合问题，分析不同罪名构成要件差异，提出 “从一重罪处罚” 适用建议。同时参与高校、科研机构组织的网络犯罪法律适用研讨会，与法学专家、法官、检察官共同探讨新型网络犯罪法律定性问题，比如研讨区块链存证的证据效力认定标准，推动形成理论共识。案例参考层面，律师应系统梳理最高人民法院、最高人民检察院发布的网络犯罪指导性案例

与典型案例，如 “李某非法利用信息网络案” “张某帮信案” 等，总结案例中关于罪名认定、兜底条款适用、电子数据证据审查的裁判规则。

（四）适应审判程序新要求

面对审判程序复杂挑战，需从管辖应对、庭审准备、程序沟通三方面适应审判程序新要求。管辖应对层面，律师应在案件受理阶段及时审查管辖合法情况。若发现案件有多个可能管辖法院，且不同法院对同类案件量刑差异较大，可依照当事人利益最大化原则，提出管辖权异议。如在跨境电信诈骗案件中，若犯罪行为发生地涉及多个省份，而当事人居住地法院对同类案件量刑较轻，可收集当事人居住地与案件关联证据，如当事人在居住地接收诈骗资金、与上家在居住地沟通等，向法院主张由当事人居住地法院管辖，并提交管辖权异议申请书及相关证据材料，争取有利的审判管辖法院。庭审准备层面，针对电子数据证据多、技术细节复杂特点，律师应提前制作庭审质证提纲与技术说明材料。把电子数据证据按类型分类整理，如服务器日志、虚拟货币交易记录、聊天记录等，针对每类证据列出质证要点，包括证据来源合法情况、完整性、关联性等；制作技术术语解释手册，把区块链、哈希值、VPN 等专业术语转化为通俗表述，帮助法官与陪审员理解。同时模拟庭审质证场景，和技术顾问一起演练，预测控方可能提出的质证反驳观点，提前准备应对方案，确保庭审中能清晰、准确阐述质证意见^[5]。

三、结束语

总而言之，网络犯罪随着技术发展逐步演变，给刑事辩护造成技术、证据、法律适用及审判程序多方面新挑战。要应对诸多挑战，得靠提升辩护律师专业素养、优化证据收集及质证策略、推动法律适用明确化、适应审判程序新要求多管齐下。构建技术与法律融合辩护体系，进而有效突破实务困境，保障辩护质量，维护司法公正，为数字时代网络犯罪治理提供有力支撑。

参考文献

- [1] 温朝鑫. 大数据背景下电信诈骗犯罪的特点及对策 [J]. 法制博览, 2024(18): 7-10.
- [2] 张涵. 帮助信息网络犯罪活动罪的行为类型与治理研究 [J]. 法制博览, 2024, (27): 30-32.
- [3] 张文东, 朱珊珊, 张淑平. 海峡两岸跨境电信网络诈骗犯罪刑事管辖权冲突的调适 [J]. 台湾研究, 2023(6): 89-96.
- [4] 苏畅, 葛也驰, 李雅静. 未成年网络性侵害的刑法规制现状和完善途径 [J]. 法学 (汉斯), 2024, 12(8): 5420-5437.
- [5] 韩斌, 高宏, 钱娜. 侵害英雄烈士名誉, 荣誉罪治理机制研究 —— 以 “某小球” 网络侮辱英烈案为视角 [J]. 法制博览, 2023(28): 94-96.