刑事司法科学与治理
Criminal Justice Science & Governance
2025 年 第 6 卷 第 2 期

论我国信息网络犯罪的发展态势与相关刑事政策的完善

严宇飞　曾大庆

中南财经政法大学刑事司法学院，武汉

摘　要 | 在当前信息网络犯罪治理中，存在刑事政策与新型信息网络犯罪不匹配的问题，导致一些新型信息网络犯罪缺乏有效规制。相关数据显示，信息网络犯罪呈现出发案频繁、类型扩张的发展态势，亦存在较大的法益侵害性，还面临追诉难、量刑规则难把握的司法困境。本文通过整合信息网络犯罪的特征与发展态势，分析我国针对传统犯罪的刑事政策，提出应积极调整和优化现有刑事政策模式：在“宽严相济”基础上坚持“打早打小”，强调立法、司法与法教义学的协同优化，采取帮助行为正犯化、法益侵害认定的前置化及解释论优化等治理思路。此外，在信息网络犯罪治理中需体现刑法适用的去碎片化，加强和完善刑法相关前置法构建，形成综合治理体系与完整的犯罪预防生态。

关键词 | 信息网络犯罪；打早打小；前置法；刑事政策

一、引言

数字现代化建设正成为当前我国社会建设的重心和主要目标。近十年来，无论是公民的日常生活还是社会治理，都在不断融入信息网络技术，“互联网+”在各领域展现出技术优势，信息网络因而受到社会各领域的重视和应用。2023年2月，中共中央、国务院联合发布《数字中国建设整体布局规划》，这份文件不仅明确数字现代化建设将成为未来几年社会建设的核心任务，也指明了未来发展的方向与重点。紧随其后，10月25日，国家数据管理局的成立，无疑标志着我国数据管理体系的进一步完善，既体现了国家对大数据、人工智能等新兴技术的重视，也是构建数字社会蓝图的重要一步。“互联网+”已渗透到生活的各个方面，这些变化既提高了人们的生活质量，也推动了社会治理模式的革新。但当前技术赋能与社会治理的深度融合，导致了既有法律规制的响应速度与技术犯罪迭代速率之间的结构性失衡。

司法实践数据显示，近年来信息网络犯罪呈现爆发式增长与结构性异化的双重特征。随着信息网络犯罪的高发和多样化，社会治理模式在发生系统

性变革的同时，也面临技术风险和管理困境。[1]根据最高人民检察院的数据统计，2017年至2021年，全国各级法院一审审结的涉信息网络犯罪案件共计28.20万余件，案件量呈逐年上升趋势。其中，诈骗罪案件量占比最高，为36.53%，其次为帮助信息网络犯罪活动罪，案件量占比为23.76%。具体而言，2020年，全国检察机关起诉涉嫌网络犯罪（含利用网络和利用电信实施的犯罪及其上下游关联犯罪）14.2万人，同比上升47.9%。其中，利用网络实施的诈骗和赌博犯罪持续高发，占网络犯罪总数的64.4%。2021年，全国公安机关侦办侵犯公民个人信息等网络犯罪案件6.2万起，抓获犯罪嫌疑人10.3万名。2023年，检察机关起诉利用网络实施的犯罪32.3万人，其中电信网络诈骗犯罪5.1万人、帮助信息网络犯罪14.7万人、网络赌博犯罪1.9万人。[2]2023年检察机关起诉的电信网络诈骗犯罪中，主要方式包括刷单返利、虚假网络投资理财、虚假网络贷款、冒充电商物流客服、冒充公检法、虚假征信和虚假购物服务等。[3]此外，诈骗分子还通过视频电话联系受害人，进行身份冒充诈骗。

可见，信息网络犯罪的形态暴露出传统刑事政策的治理困境：其一，预备行为规制的滞后性，导致“犯罪阻断窗口期”错失；其二，虚拟空间的匿名性与跨国性，挑战传统侦查机制；其三，帮助行为正犯化等新型立法与教义学解释存在张力。在此背景下，亟需重新审视信息网络犯罪的特征、发展态势及其对刑事政策的需求，积极探索适应技术风险与社会治理模式变革的动态平衡路径。本文以信息网络犯罪的特征和发展态势为切入点，结合“宽严相济”刑事政策框架，提出立法、司法与法教义学的协同优化方案，以“打早打小”的预防性刑事政策为基础，完善前置法衔接机制，建立针对信息网络犯罪的综合治理生态。

二、信息网络犯罪的含义与特征

（一）信息网络犯罪的含义

一般认为我国的信息时代起始于1984年，即我国已步入信息时代近40年，并经历了网络1.0时代、2.0时代及网络“空间化”时代的三重变迁。[4]近年来，拥有高速、泛在、低时延、万物互联等优势的5G时代来临，也引起了网络风险的社会化，不可避免地滋生了新型网络犯罪，信息网络犯罪的定义也随着技术的发展和对这一现象理解的深入而不断演化。

最初，信息网络犯罪主要指针对计算机信息系统的犯罪行为，如病毒制作、黑客攻击等，这些行为直接危害了计算机系统和网络安全。基于信息网络犯罪的多样化特征，现可将其区分为纯正网络犯罪和不纯正网络犯罪。在大数据时代，网络不仅是犯罪对象，也成为犯罪发生的场所，人工智能和大数据技术的应用，使得网络犯罪手段更加复杂和隐蔽。《人民检察院办理网络犯罪案件规定》中将网络犯罪分为三类：一是针对信息网络实施的犯罪，即直接侵害网络系统安全的犯罪；二是利用信息网络实施的犯罪，即使用网络作为工具实施的犯罪，如网络诈骗、网络赌博等；三是其他上下游关联犯罪，即与网络犯罪相关的辅助性犯罪，如提供技术支持、资金结算等。在司法实践中，对网络犯罪的打击范围通常将互联网上、下游相关联的犯罪作为线索，以实现对网络犯罪的全方位打击。

信息网络犯罪定义的演变，体现了对网络空间犯罪现象认识的深化，同时也反映了法律适应技术发展和社会需求的过程。随着网络技术的不断进步，信息网络犯罪的类型和手段也在不断演变，对法律体系和司法实践提出了新的挑战。

（二）信息网络犯罪的特征

纵观几十年来的网络犯罪治理过程，能发现网络犯罪存在从“技术型”到“精准数据型”的转变趋势。在早期，网络只能起到联结作用，用户获取

---

［1］刘艳红．网络时代社会治理迭代升级与犯罪控制协同化的刑事政策［J］．社会科学文摘，2024（6）：110–112.

［2］最高人民检察院．最高检披露2020年国内网络犯罪大数据［EB/OL］．安全内参，2020.

［3］国家反诈中心．国家反诈中心推《2023版防范电信网络诈骗宣传手册》［EB/OL］．荆楚网–湖北日报网，2023.

［4］王志祥，徐嘉崎．论前端防范视域下网络犯罪的交叉合作治理模式［J］．北京警察学院学报，2023（1）：1–16.

信息少，无法实现交互功能。因此第一阶段的网络犯罪多为针对计算机本身的犯罪，但此类犯罪通常体现为“技术型”犯罪，大多数人群在此阶段难以接触到相关专业知识，因此此类犯罪并不显著。随着数字时代的发展，互联网时代、“空间网络”时代已经完全来临。计算机逐渐被移动设备取代，网络犯罪所依托的基本数字技术已经成熟化、大众化。网络犯罪的低成本与低要求，导致案件数量不断增长，也导致许多传统犯罪类型开始转向“网络化”，如诈骗罪、盗窃罪、猥亵罪等，开始频繁出现于网络空间。依托大数据技术开展的网络犯罪，是最新型的犯罪模式。新型网络犯罪起始于盗窃个人信息，再利用大数据分析和人工智能技术实施具体诈骗，这决定了数字时代下的网络犯罪需要不同层级的配合，而并不过分依靠个人的技术能力，直接导致缺乏技术能力的普通人也能成为此类犯罪的参与者。我国严厉打击的跨境电信诈骗、网络赌博、转移非法资金等犯罪行为，多基于以上模式实施。

三、信息网络犯罪的发展态势

（一）传统犯罪向新型犯罪的范式转移

在我国法制现代化的建设过程中，通过制定合理的刑事政策、建立体系化的传统刑事法律规范、完善刑事司法流程等多种手段联合治理，已经形成了治安形势转好的良好趋势。近年来，我国发生的杀人、爆炸、抢劫等严重暴力犯罪及非正常上访和群体性事件，呈逐年下降趋势，社会公众的安全感始终高于90%。2015年，我国每10万人中发生杀人案件0.67起，是世界上杀人案件发生率最低的国家之一。[1]除以上严重暴力犯罪率下降外，传统的信息网络犯罪也在不断减少，如在信息网络发展初期高发的破坏计算机信息系统罪、非法侵入计算机信息系统罪，当前计算机病毒制作、传播和黑客行为等犯罪行为虽仍然存在，但相较于新型的信息网络犯罪已然式微。网络犯罪典型形态（如破坏计算机信息系统罪、非法侵入计算机信息系统罪）的发案率已从2015年占比12.3%，下降至2022年的4.1%，反映出传统信息网络犯罪治理的有效性。

随着Web3.0时代的到来，传统的刑事政策在遏制信息网络犯罪中愈发显现颓势。犯罪形态发生根本性转变：犯罪载体从物理空间向虚拟空间迁移，犯罪手段从技术攻击向数据操控演变，犯罪对象从系统安全转向数字资产与个人隐私，形成对传统犯罪的“数字替代”效应。帮助信息网络犯罪活动、电信网络诈骗、侵犯公民个人信息等新型信息、网络犯罪，以及网络侮辱诽谤、网络盗窃、基于信息网络的“隔空猥亵”等案件层出不穷，并逐步动摇了传统犯罪的“稳固地位”。

（二）新型网络犯罪的演进特征

一是技术驱动性犯罪爆发增长。互联网的匿名性、便捷性给犯罪分子带来了便利，以区块链、元宇宙、生成式AI为技术基底的新型犯罪激增，其中以网络为主要手段的犯罪数量较上年同期增长了63.5%。[2]与信息网络相关的具体犯罪行为，包括提供技术支持、资金转移、售卖个人信息等。此外，犯罪呈现“技术代差”特征，上游依托智能合约开发犯罪工具，中游利用深度伪造实施精准诈骗，下游完成资金洗白，形成完整的技术链。

二是黑灰产业的转型与升级。伴随着元宇宙和区块链等新兴科技的兴起，新型网络犯罪层出不穷，虚拟货币已成为滋生网络犯罪的“土壤”，而“黑灰”产业链条也在不断扩展、升级，支撑着网络犯罪。利用区块链新技术实施的网络犯罪支撑服务逐步增加，促成了黑灰产业的服务转型，如提供犯罪功能模块、数据交易平台化、犯罪服务订阅化。黑灰产业的专业化、系统化，使犯罪分子拥有了更具隐蔽性、高效率的作案方式。

三是传统犯罪的数字化范式转移。传统的犯罪，如赌博、盗窃、传销等，都已转入网络领域，利用互联网的隐蔽性、便利性，呈现出日益复杂化的态势。传统以赌博、传销、盗窃为主要特征的犯罪行为，依托于互联网，转为以网络化为主要形式的犯罪行为。传统赌博行为通过网络化表现为利用直播平台和虚拟货币结算，传统传销行为转为依托社交电商模式裂变，传统盗窃行为转向涉资钱包破解与交易数据窃取等。

---

［1］喻海松．网络犯罪的态势与刑事对策的调整［J］．法治现代化研究，2018（1）：141–147.

［2］漆世钱．网络犯罪侦查的发展现状与对策［J］．网络安全技术与应用，2019（3）：98–99.

四是犯罪主体呈现出“三低三跨”的趋势，即低年龄、低认知、低门槛和跨地域、跨业态、跨平台。在犯罪群体方面，犯罪主体从特定群体逐渐向多样化发展，涵盖不同年龄、文化程度、职业的人员。实践中，未成年人涉案占比上升，犯罪工具购买成本下降，犯罪主体无需掌握技术原理仅按教程操作，整体呈现要求降低的特征。案件涉及境外服务器明显多于境内，合法互联网服务被恶意利用从事非法行业的占比增高，单案平均涉及的应用平台也在增加，呈现犯罪覆盖面扩大的特点。“三低三跨”的趋势，对年龄分层治理、技术反制措施和跨境办案协作都提出了新的挑战。

五是信息网络犯罪生态圈层化演进。当前信息网络犯罪形成了“三圈层”的生态系统，核心圈层是实施网络诈骗、数据勒索等犯罪，支撑圈层是非法技术开发、数据供给和资金通道等黑灰产业，最外层是衍生出的洗钱、销赃等下游产业。在信息网络犯罪中，“产业链”正逐步形成，从核心犯罪一直延伸至犯罪支撑和下游犯罪，正是这样的产业链，导致了网络犯罪的专业化和规模化。同时，随着新兴互联网技术的发展，互联网犯罪市场不断扩张，而传统犯罪也在不断地渗透。

四、现有刑事政策的困境

上述网络犯罪形态的深层变革，实质上构成了对传统刑事治理体系的系统性挑战。当犯罪场域完成从物理空间向数据空间的迁移、犯罪生态演化为三圈层产业链协同、犯罪主体呈现“三低三跨”新特征时，建立在传统犯罪治理框架下的刑事政策在Web3.0时代的犯罪治理场域中，逐渐暴露出结构性不适配的问题。传统以物理空间为治理场域、以实行行为为规制对象、以线性犯罪过程为打击重点的治理逻辑，难以应对虚拟空间内即时扩散、全链协同、技术代际迭代的新型犯罪生态。正是这种犯罪形态与治理工具之间的代际落差，导致当前刑事政策在网络犯罪治理中面临着四重困境。

（一）对实行行为与预备行为的偏重不同

传统刑事政策主要对实行行为加以规制。从法益侵害的角度考虑，传统犯罪多为结果犯，基于其预备形态、未遂形态的法益侵害性和社会危害性较小，一般不将其作为规制重点。除法益侵害性和社会危害性外，传统犯罪的刑事政策还主要考虑了传统犯罪的侦查实践。传统犯罪结构相对简单，对于处于犯罪未遂，甚至预备阶段的轻罪和轻微罪案件，传统刑事政策一般并不重视，也很少纳入刑事规制的范围。这主要是因为传统犯罪的结构相对简单，侦查工作主要集中在犯罪实行阶段，特别是已经完成的犯罪行为，因为这些案件更容易取证和定罪。由于司法资源有限，传统刑事政策倾向于优先处理对社会秩序和公民权益造成直接影响的既遂犯罪。因此，传统罪刑规范的设置，导致传统刑事政策很少关注预备行为。

然而，面对现代信息网络犯罪，这种以实行行为为中心的刑事政策不再适应，传统刑事政策的以上特征与现代信息网络犯罪的处置很难匹配。现代信息网络犯罪一旦进入实行阶段，其法益侵害性往往难以避免，侦查难度也极大，往往伴随着难以挽回的法益侵害和社会危害性。因此当前提出了“打早打小”的网络犯罪刑事政策，对于高科技信息网络犯罪，最好的规制方法是将其遏制于未发之时，以此将犯罪分子对人民群众的损害降到最低。

（二）对涉案财物的关注度不同

传统刑事政策往往将重点放在犯罪行为的实施和完成上，而对犯罪既遂后的赃物处理和其他后续行为关注不多，这种情况与传统犯罪的纵向链条较短有直接关系。在传统犯罪中，一旦犯罪行为完成，犯罪分子通常已经达到了其目的，赃物的处置相对简单，如直接变卖或转移，而且这些行为往往不构成新的犯罪，因此被视为事后不可罚行为。

然而，随着信息网络犯罪的兴起，犯罪既遂后的赃物处理和其他后续行为变得更加复杂，涉及的技术手段和法律问题也更多样。网络犯罪的赃物可能是数字货币、虚拟商品或其他不易追踪的资产，其转移和洗钱方式可能涉及复杂的金融操作和跨国流动。这就要求刑事政策不仅要关注犯罪行为的实施，还要对赃物的追踪、定位和处置给予更多关注。为了适应这种变化，刑事政策需要进行相应的调整和完善。

（三）犯罪场域的虚拟化转型

犯罪场域主要强调犯罪的空间对犯罪形态和侦

查方式带来的影响。犯罪场域从物理空间向虚拟空间的迁移，不仅改变了犯罪行为的实施方式，更动摇了传统刑事治理的底层逻辑。当犯罪行为的物理痕迹被数据流取代、犯罪现场从街巷延伸至云端时，以物理空间为基石的侦查手段和治理框架面临着一定压力。传统的犯罪对策往往建立在物理空间的犯罪行为基础上，而网络犯罪则具有虚拟性、匿名性与跨国性等特点，这些特点使得传统对策在应对网络犯罪时显得力不从心。

首先，网络犯罪的虚拟性，使得犯罪行为可以在没有实际物理接触的情况下完成，这给犯罪侦查和证据收集带来了巨大挑战。在网络空间，犯罪分子可以轻易地隐藏自己的真实身份和位置，而受害者和证据往往分散于不同的服务器和地理位置，难以追踪和固定。其次，网络犯罪的匿名性，为犯罪分子提供了一层天然的保护。通过使用加密技术、代理服务器、虚拟私人网络（VPN）等手段，犯罪分子可以在不暴露真实身份的情况下进行非法活动，这大大增加了执法机关的侦查难度。再次，网络犯罪的跨国性，意味着犯罪行为和受害者可能分布在世界各地。这不仅涉及不同国家和地区的法律体系和司法管辖问题，还需要跨国执法合作和信息共享，而这些在实际操作中往往面临诸多障碍和限制。最后，网络技术的快速发展，也为网络犯罪提供了新的作案手段和平台。例如，区块链技术的出现，为洗钱等金融犯罪提供了新的渠道；人工智能和机器学习技术的发展，则可能被用于自动化的网络攻击和诈骗行为。

由此可见，网络这一犯罪场域已突破传统刑事治理的物理基础，这种犯罪场域的范式转换，使得刑事政策亟待构建以网络数据为核心的治理模式。具体而言，需通过统一技术标准、确立数据主权、完善国际司法协作机制的三维治理架构，重塑适应网络犯罪动态演变的常态化治理体系，从而实现侦查模式与制度框架的协同变革。

（四）犯罪分工和犯罪中承担的角色不同

张明楷教授认为：刑法分则就单独犯罪的规定，实际上是关于正犯的规定。[1]由此也可以推断，传统犯罪的刑事规范和刑事政策一般是以正犯为中心的。如以正犯为中心确定帮助犯，以主犯的量刑为根据确定从犯的量刑等，可以说，在传统犯罪中个人犯罪为一般，共同犯罪为例外。但在当前的信息网络犯罪中，不能直接沿用这一分类和处理方式，在现代信息网络犯罪中往往有明确的组织架构和犯罪系统。在互联网环境中，“一般是共同犯罪，个别犯罪是例外”。与以往的“孤军作战”不同，互联网犯罪已逐步告别了“单兵作战”的格局，呈现出“共犯”的形态突出、数量大的特点。人民法院的数据显示，在一起网络犯罪中，平均有2.73人参与其中，超四成是共犯。根据统计资料，参与有组织或较大有组织犯罪的犯罪嫌疑人，在全部案件中占比达83%。[2]

此外，在基于互联网的犯罪中，犯罪活动被细分成了基于网络平台的多个环节，每一个环节都有明确的分工合作，各取所需，每个人都有自己的利益诉求，从准备工具到组织人员、寻找目标作案、获取利润、销赃分赃，形成了一个完整的犯罪利益链。

可见，信息技术的融合为犯罪活动带来了“革命性”的变化，特别是在共同犯罪领域。首先，技术手段的引入，使得犯罪行为的分工更为细致和专业化，这种分工不仅极大地提高了犯罪活动的效率，而且通过分散犯罪环节，有效降低了被侦破的风险。在网络时代，这种共同犯罪因其高效和隐蔽的特性，成了犯罪分子的新选择。其次，信息技术的参与，也使得网络犯罪的实施更依赖外部资源和协作。由于网络犯罪的复杂性，单独的个体很难掌握所有必要的技能和资源来独立完成犯罪，因此，犯罪分子往往需要依赖一个由不同专业技能者组成的网络来共同完成犯罪行为。这种依赖性不仅体现在技术层面，还可能涉及资金、信息、物流等多个方面。综合来看，信息技术的发展为网络犯罪带来了新的机会和挑战。它不仅促进了犯罪活动的分工和专业化，也使得犯罪分子在实施犯罪时更加依赖于团队合作和外部资源。这种趋势要求在制定此类犯罪的刑事政策时，不仅要关注犯罪行为本身，还要深入分析犯罪背后的分工网络和协作机制，以便更有效地预防和打击犯罪

[1] 张明楷. 刑法学（第5版）（上）[M]. 北京：法律出版社，2016：389.

[2] 检察日报. 2020年检察机关起诉涉嫌网络犯罪人数上升近五成[N]. 检察日报，2021-04-08（4）.

活动。

五、信息网络犯罪的刑事对策

（一）法益侵害认定的前置化

法益侵害认定的前置化，是指通过提前介入，以预防性保护的方式，阻止犯罪行为对法益造成损害。这种立法思维在现代社会风险不断升级的信息网络犯罪背景下显得尤为重要，它通过降低入罪门槛、设立新罪名或调整既有罪名，来实现对某些法益的加强保护，如刑法修正案（十一）设立的高空抛物罪、非法植入基因编辑、克隆胚胎罪等。

与以上罪名相似，在信息网络犯罪中，一旦信息网络犯罪进入实行阶段或完成犯罪后，对法益的侵害巨大，且常常难以在此类案件中运用“恢复性司法”，因此提前保护信息网络犯罪所保护的部分法益意义重大，最典型的案例就是电信诈骗后资金往往流入国外，难以追回。

非法利用信息网络罪，是将保护法益前置，通过将“利用信息网络设立用于实施诈骗、传授犯罪方法”等预备行为正犯化，做到将原本的预备行为单独成罪。从形式上看，此种规定亦符合实质预备犯对行为的类型性、定型性要求。[1]也有学者从“积量构罪”的角度对这一法益保护前置的教义学解释予以支持，认为非法利用信息网络罪是一种积极的犯罪形态，其特点是行为的累积效应。[2]在这一罪名下，不同的行为根据其对法益的威胁程度和与下游犯罪行为的接近程度，其危害性也会有所不同。具体来说，那些更接近于实际犯罪行为的网络活动，因其可能直接促成犯罪结果的发生，其法益侵害程度自然更高。

将“积量构罪”的理论应用于信息网络犯罪，将进一步优化相关刑事政策。例如，在评估信息网络犯罪的危害性时，法律会综合考虑行为的性质、频率、影响范围及与实际犯罪的关联程度等因素。这样的立法设计，旨在早期识别并干预那些可能逐步升级为严重犯罪的网络行为，从而有效预防和减少网络犯罪的发生。

但需要注意，这一做法在实践中容易导致立法的泛滥，违背“消极性预防的刑事政策”这一观点，特别是对于刑法总则关于预备犯的一般规定，过多地在分则中将预备犯实行化，会使总则的相应部分形同虚设。但本研究认为，从信息网络的发展态势和管理信息网络犯罪的功利性视角来看，将信息网络犯罪中的部分预备行为实行化并无问题，也体现了刑事政策“宽严相济”的基本要求，立法上罪名的“严”，可以通过司法中认定和量刑的“宽”予以调和，达到理想的刑事政策运行状态。

（二）帮助行为的正犯化

与法益侵害认定的前置化相似，帮助行为的正犯化同样是指通过提前介入，以预防性保护的方式，阻止犯罪行为对法益造成损害。在信息网络犯罪中，现有的一些罪名已经实现了这一功能，最典型的是“帮助信息网络犯罪活动罪”。刑法修正案（九）新增这一罪名，主要是针对网络犯罪的共犯行为进行规制，是预防网络犯罪蔓延的特殊预防方法。与法益的保护前置化相似，帮助行为的正犯化同样存在着立法泛滥等问题，如刘艳红教授批判了帮助行为正犯化的做法，认为这一做法存在立法的严谨性问题，帮助信息网络犯罪活动罪的设立，在一定程度上表明我国刑法立法的严谨性有待强化，需要进一步探讨刑法作为国家强制手段对个人的处罚范围和力度。同时对帮助行为正犯化进行了检讨，认为帮助行为正犯化可能带来诸多理论争议，如间接帮助行为的延伸问题，以及对不特定对象提供帮助行为的可罚性问题。刘艳红教授指出，面对信息网络化时代犯罪形式的变化，立法者需要采取相应措施，但也需要保持刑法立法的严谨性，避免过度扩大处罚范围。[3]

（三）解释论的优化

对此，张明楷教授提出通过解释论方法解决这些问题，他认为解决新型的网络犯罪有一元模式和二元模式两种形式：一元模式是在现有法条中增加新的行为类型和对象，二元模式是增加新的法条来专门规制新型犯罪。毫无疑问，一元模式更具有

---

［1］阎二鹏．预备行为实行化的教义学审视与重构——基于《中华人民共和国刑法修正案（九）》的思考［J］．法商研究，2016（5）：62.

［2］皮勇．论新型网络犯罪立法及其适用［J］．中国社会科学，2018（10）：138.

［3］刘艳红．网络犯罪帮助行为正犯化之批判［J］．法商研究，2016（3）：22.

“性价比”。[1]此外，刑事立法应坚持法益保护主义，即只有严重侵害法益或侵害重要法益的行为，才应被规定为犯罪。但对于信息网络犯罪需要特殊对待，信息网络犯罪侵犯了新型法益，一些以前未被刑法保护或未被认为是利益的新型法益，如数据安全、个人信息保护等，现在需要由刑法来保护。例如，电子文书的信用等，在网络时代受到新的侵害，需要通过刑事立法来加强保护。又如财产、名誉等一些传统法益，在网络时代增加了新的内容或形式，需要刑法通过解释或修改来适应新的保护需求。

（四）坚持“打早打小”的刑事政策

在网络犯罪领域坚持“打早打小”的刑事政策，要求执法和立法机关在刑法的限度内，采取更加积极主动的措施来预防和打击犯罪行为，包括通过教育提高公众的警觉性，利用技术手段加强网络监控，以及通过立法创新来应对网络犯罪的新形式和手段。跨部门和跨国界的合作也至关重要，以实现情报共享和资源协同，有效打击网络犯罪。此外，需要采取早期干预措施，对可疑行为进行警告和监管，同时鼓励开发和使用先进的技术防范手段。法律教育的强化，司法程序的优化，以及为受害者提供支持和保护，都是这一政策的重要组成部分。政策的成功实施，还需要持续的评估和改进，以适应网络犯罪的不断演变。

在网络犯罪领域坚持“打早打小”的刑事政策，意味着需要构建一个综合性的防御体系，这个体系从提高公众意识开始，通过教育和宣传让每一个网络用户都成为潜在的防线。同时，加强技术的研发和应用，利用先进的监控和分析工具，提前识别和防范犯罪行为。立法和司法机关要迅速响应，不断更新法律以适应网络犯罪的新趋势，同时提高司法程序的效率，确保犯罪行为能够被快速识别和惩处。

国际间的合作也至关重要，因为网络犯罪往往不受国界限制。通过跨国界的信息共享和协作，可以更有效地打击网络犯罪。此外，通过建立一个全社会参与的监督和举报机制，可以动员公众参与网络空间的治理。

在这一过程中，保护个人数据和隐私，防止信息泄露和滥用，也是减少网络犯罪潜在危害的关键。法律的适应性不仅要跟上当前的犯罪手段，还要能够预见未来可能出现的新型犯罪方式。通过持续的法律教育和公众宣传，提高整个社会的法律意识和网络安全意识，形成一种人人都知道如何安全行事，以及在遇到可疑行为时如何采取行动的文化。

整体而言，这种刑事政策的实施是一项系统性社会工程，需要政府、企业、教育机构和每个公民的共同努力和参与，以形成一个强大、多层次的网络安全防护网。

（五）完善综合治理体系

1. 信息网络犯罪刑法适用的“去碎片化”

完善针对信息网络犯罪的综合治理体系，在刑事司法层面需要“去碎片化”，对信息网络犯罪的整体体系进行刑事规制。传统犯罪中，帮助行为的危害性源于对正犯行为的加速作用，危害程度也低于正犯行为。然而，在网络犯罪的背景下，帮助行为的角色和影响力发生了根本性的变化。网络犯罪的帮助行为不仅可能为正犯行为提供必要的技术支持或资源，而且在某些情况下，其危害性甚至可能超过正犯行为，因为它们可能直接影响到更广泛的受害者群体，造成更大规模的损害。

因此，治理网络犯罪的关键，在于打破犯罪分子的利益链条，特别是针对网络犯罪背后的黑色产业链进行严厉打击。[2]这种产业链往往涉及多个环节，包括但不限于技术支持、资金流转、信息传播等，它们共同构成了网络犯罪的生态基础。通过有效打击这一产业链，可以从根本上降低网络犯罪的实施能力和持续发展的可能性。[3]

为了应对网络犯罪刑法适用中出现的横向碎片化问题，需要采取一种更为系统和全面的方法。这不仅包括对单一犯罪行为的打击，更涉及对整个犯罪网络的深入分析和精确打击。通过识别和切断犯罪分子之间的联系，可以更有效地预防和减少网络

---

［1］张明楷．网络时代的刑事立法［J］．法律科学，2017（3）：72.

［2］王华伟．我国网络犯罪立法的体系性评价与反思［J］．法学杂志，2019（10）：128-140.

［3］喻海松．网络犯罪形态的碎片化与刑事治理的体系化［J］．法律科学，2022（3）：67.

犯罪的发生。同时，这也要求执法机关加强合作，共享情报，形成打击网络犯罪的合力。

此外，随着网络技术的不断进步，网络犯罪的手段和形式也在不断演变。因此，法律制度和刑事政策也需要不断更新，以适应新的挑战。这可能包括制定新的法律规定，加强对网络服务提供者的监管，提高公众的网络安全意识，以及通过技术手段提升网络犯罪的侦测和防范能力。

总之，有效应对网络犯罪不仅需要对帮助行为的危害性有清晰的认识，更需要对整个网络犯罪生态系统进行全面的分析和打击。通过斩断利益链，强化法律制度，提高技术防范能力，以及加强国际合作，可以更有效地应对网络犯罪带来的挑战。

2. 完善刑法的相关前置法

在信息网络犯罪领域，前置法是那些在犯罪行为实际发生前，就对可能引发犯罪的行为进行规制的法律规范，能起到较好的预防效果，也减少了刑法的使用成本，如《网络安全法》《个人信息保护法》《反不正当竞争法》《电子商务法》《计算机信息系统安全保护条例》《数据安全法》等。在信息网络犯罪领域，刑法的前置法通过提前介入和降低入罪门槛，实现了对潜在犯罪行为的有效预防和干预。[1]它扩大了法益保护的范围，将个人信息和数据安全等新型网络相关法益纳入保护，同时强化了法律的威慑力，使犯罪分子在预备阶段就可能受到法律制裁。前置法还促进了社会治理现代化，引导和规范网络行为，提高网络环境的安全性。

随着信息技术的发展，前置法能够及时应对新出现的网络犯罪手段，填补法律空白，并通过国际合作增强打击跨国网络犯罪的能力。此外，它还提高了公众的法律意识，使人们更加了解如何安全地使用网络，以及如何防范网络犯罪。前置法的实施有助于优化司法资源的配置，通过减少严重犯罪案件的发生来提高司法效率，并适应社会发展对网络安全和秩序的不断增长的需求。通过这些方式，刑法的前置法成了维护网络安全和秩序、应对信息网络犯罪的重要工具。

六、结语

信息网络犯罪呈现从“技术型”向“精准数据型”跃迁的态势，传统刑事政策需基于“宽严相济”的刑事政策框架，通过“打早打小”策略实现犯罪阻断的前移，从结果本位转向风险预防。具体路径上，需构建法益侵害前置化、帮助行为正犯化的立法技术，强化基于大数据技术的防御手段，并通过国际协作破解跨国犯罪治理难题。实践表明，唯有以“去碎片化”思维整合立法、司法与技术治理资源，形成完善的信息网络犯罪生态治理闭环，才能有效应对网络犯罪的蔓延。这一刑事政策的完善，既是适应数字社会的必然选择，又是构建信息网络安全的核心命题。

（责任编辑：王梦华）

［1］阎二鹏．我国网络犯罪立法前置化：规范构造、体系检讨与路径选择［J］．法治研究，2020（6）：80–93.

On the Development Trend of Information Network Crime in China and the Improvement of Related Criminal Policies

Yan Yufei Zeng Daqing

School of Criminal Justice, Zhongnan University of Economics and Law, Wuhan

Abstract: In the governance of information network crimes, there exists a mismatch between existing criminal policies and new types of information network crimes, resulting in the lack of effective regulation for some current new types of information network crimes. Relevant data, indicate that information network crimes show a trend of frequent occurrence and type expansion, with significant infringement on legal interests, as well as judicial difficulties in prosecution and the application of sentencing rules. By integrating the characteristics and development trends of information network crimes and analyzing China's criminal policies against traditional crimes, this paper proposes that the existing criminal policy model should be actively adjusted and optimized. Based on the principle of "combining leniency with severity", we should adhere to the principle of "cracking down early and on a small scale", emphasize the joint optimization of legislation, judicature and legal doctrine, and adopt such governance approaches as the principalization of assisting acts, the pre-positioning of the identification of legal interest infringement, and the optimization of interpretive theory. In addition, it is necessary to reflect the de-fragmentation of the application of criminal law in the governance of information network crimes, strengthen and improve the construction of relevant pre-laws of criminal law, and form a comprehensive governance system and a complete crime prevention ecology.

Key words: Information network crime; Cracking down early and on a small scale; Pre-law; Criminal policy