法学研究

网络犯罪治理的刑行衔接:基本价值与运作模式

李怀胜

[摘　要]　在网络犯罪的深度社会化和产业链特征的双重加持下,网络犯罪成为严峻的社会挑战。在此背景下,网络犯罪案件的刑行衔接作为一种治理机制,契合对网络犯罪进行溯源治理、过程治理与协同治理的需求,反电信网络诈骗、个人信息保护、新业态的风险管控等网络治理课题也需要贯通性的责任处置策略。网络犯罪刑行衔接的两种模式包括刑事判决生效后的"刑-行关联罚"以及未能实现有效刑事判决后再反向衔接的"行-刑补罚",前者有助于实现法律责任的闭环而后者有助于司法解释中"多次行为入罪化"模式的实现。基于网络犯罪的产业链特征以及网络犯罪的协同治理需求,司法机关要对案件进行全链条审查,注重追究网络平台等犯罪案件"被害人"的行政责任。

[关键词]　网络犯罪;协同治理;刑行衔接;一体化责任

近年来,伴随着网络空间的深度社会化,网络犯罪呈现持续的高发态势,非接触性犯罪、跨网犯罪、网上网下联动犯罪等犯罪形态刷新了传统社会的犯罪治理难度,对其全链条治理、源头治理、综合治理的呼声日渐高涨,并成为相关立法的指导性理念。例如2022年9月2日,十三届全国人大常委会第三十六次会议表决通过的《中华人民共和国反电信网络诈骗法》(以下简称《反电信网络诈骗法》)就贯彻了网络犯罪协同治理的理念。①但"徒法不足以自行",治理方略的贯彻需要与之匹配的程序性机制和保障性制度,尤其是系统性的法律体制才可能克制系统性的网络犯罪,而行刑衔接作为一项横跨行政执法与刑事司法的综合性法律制度,其在网络犯罪治理中的作用应当得到重视。

2021年新修订的《行政处罚法》将行刑衔接作为修改的重要亮点,尤其是新《行政处罚法》第27条在传统的行政机关向刑事司法机关移送涉嫌犯罪案件之外,还加入了刑事司法机关向行政执法机关移送需要追究行政责任的案件的内容,即刑行衔接或者称为反向行刑衔接。②与学术界对行刑衔接制度的较为充分研究相比,对刑行衔接的研究才刚起步,③但反向行刑衔接的类似实践一直都存在。例如根据《最高人民法院关于适用〈中华人民共和国刑事诉讼法〉的解释》第303条的规定,判决生效

李怀胜,法学博士,中国政法大学刑事司法学院副教授(北京 100088)。本文系国家社科基金一般项目"人工智能时代算法安全的刑法保障研究"(22BFX048)的阶段性成果,同时受中国政法大学青年教师学术创新团队支持计划资助。

①李宁:《关于〈中华人民共和国反电信网络诈骗法(草案)〉的说明》,2022-09-02,http://www.npc.gov.cn/npc/c30834/202209/7019159f23fd4e93ab5617b0d98cdb68.shtml,2022-09-21。

②该条第1款规定:"违法行为涉嫌犯罪的,行政机关应当及时将案件移送司法机关,依法追究刑事责任。对依法不需要追究刑事责任或者免予刑事处罚,但应当给予行政处罚的,司法机关应当及时将案件移送有关行政机关。"

③目前可查的主要研究成果为练育强:《"刑事-行政"案件移送要件研究》,《国家检察官学院学报》2021年第4期;李奋飞:《涉案企业合规刑行衔接的初步研究》,《政法论坛》2022年第1期;周佑勇:《行政执法与刑事司法的双向衔接研究——以食品安全案件移送为视角》,《中国刑事法杂志》2022年第4期。

后，人民法院应当将判决送达被告人的所在单位。此外，对于原国家机关工作人员或者事业单位人员涉嫌犯罪被人民法院依法判处刑罚的，原单位的纪检监察部门可以依法依纪追加相应的行政处罚或者党纪处分。可见，刑行衔接有可能让当事人遭受综合性的法律制裁结果，这一点在当前的网络犯罪治理中尤其重要。笔者在本文中探讨网络犯罪治理中刑行衔接的理论基础、实践价值与基本模式。

一、网络犯罪治理中刑行衔接的理论基础与政策价值

笔者曾经就网络犯罪治理的行刑衔接专门撰文，[①]在笔者看来，网络犯罪行刑衔接的机制不畅等问题，同样存在于网络犯罪刑行衔接的情境。但刑行衔接绝非行刑衔接的逆用过程，而是具有独立的理论价值和实践性。

（一）刑行衔接的理论基础：网络犯罪协同治理中的一体化责任

需要指出的是，刑行衔接并非新《行政处罚法》的首创。早在2011年2月9日，中共中央办公厅和国务院办公厅发布的《关于加强行政执法与刑事司法衔接工作的意见》就规定："人民检察院对作出不起诉决定的案件、人民法院对作出无罪判决或者免予刑事处罚的案件，认为依法应当给予行政处罚的，应当提出检察建议或者司法建议，移送有关行政执法机关处理。"此外，1997年《刑法》第37条规定："对于犯罪情节轻微不需要判处刑罚的，可以免予刑事处罚，但是可以根据案件的不同情况，予以训诫或者责令具结悔过、赔礼道歉、赔偿损失，或者由主管部门予以行政处罚或者行政处分。"训诫和其他处罚的实现，需要借助刑行衔接，但其适用是以行为人构成犯罪且不必要判处刑罚为前提条件，也就是说，后续的民事责任和行政责任实际上是对行为人未实际承担刑事责任的补偿，起到了"补充处罚"功能。在部门规章层面，目前有《食品药品行政执法与刑事司法衔接工作办法》《安全生产行政执法与刑事司法衔接工作办法》等个别规范性文件规定了刑事司法机关向行政执法机关移送案件。在司法实践中，网络犯罪案件的实践摸索性色彩明显，缺乏深谋远虑的制度规划，但这不能否认刑行衔接在网络犯罪案件处置以及网络空间治理中的作用和价值。

刑行衔接的目的和后果，是追求责任的一体化处置，而违法和犯罪行为分属不同的执法主体，自然就需要多主体的协同治理，形成部门合力，因此网络犯罪的协同治理首先是执法主体的协同。互联网的分布式特性要求通过各种公共和私人行为体内部和相互之间的合作努力来解决网络空间的安全缺陷。[②] 网络信息内容监管领域一向以"九龙治水"式的多监管主体共生而著称，[③]网信监管执法体制历经多轮改革，目前已经确立了网信部门在互联网内容监管领域的统筹协调地位，但是"管理分散的局面并没有得到明显改善，各个分管的部门也没有放弃对其领域互联网信息内容的管理"，[④]越是如此，越要强调行政执法与刑事司法的衔接。

行刑衔接与刑行衔接涉及行政法与刑法的规制界限，同时也牵涉部门权力运作，行刑衔接与刑行衔接之所以在很大程度上被视为一个"中国式"问题，原因在于我国对行政违法与刑事犯罪实行"双轨执法体制"，[⑤]这种区分也一定程度上割裂了犯罪治理的内在协作力，[⑥]但双轨并不是脱轨，所

---

①李怀胜：《网络犯罪案件的行刑衔接机制研究——以反电信网络诈骗等网信监管为样本》，《中国刑事法杂志》2022年第4期。

②L. Huey, J. Nhan & R. Broll, "'Uppity civilians' and 'Cyber-vigilantes': The role of the general public in policing cybercrime", *Criminology & Criminal Justice*, Vol. 13, No. 1, 2013, pp. 81 - 97.

③李怀胜：《网络犯罪案件的行刑衔接机制研究——以反电信网络诈骗等网信监管为样本》。

④付士成、郭婧滢：《社交媒体治理视角下的互联网法律监管与行业自治》，《天津法学》2017年第3期。

⑤朱孝清：《企业合规中的若干疑难问题》，《法治研究》2021年第5期。

⑥高铭暄、陈冉：《刑事治理现代化背景下危害药品安全犯罪的治理转型》，《公安学研究》2022年第3期。

谓“分则两害,合则两利”,权力主体之间的协作是权力运行的内在要求,而行刑衔接与刑行衔接充当了双轨执法体制的黏合剂。行刑衔接和刑行衔接都是关乎权力分工、权力制约与权力配合的三位一体的执法体制。早期推动行刑衔接的主要动力是解决“有案不移”“以罚代刑”的问题,通过行刑衔接实现刑事司法对行政执法的有效监督。就刑行衔接而言,虽然其也有督促行政执法机关积极履职的意图,但更强调刑事司法机关与行政执法机关之间的配合,包括刑事司法机关内部的法、检、公的配合。刑行衔接的启动意味着刑事司法机关追究当事人刑事责任以失败告终,而不得不回退到行政执法流程中,此时案情已大白于天下,权力寻租的灰色空间被极大压缩,司法机关和行政执法机关均无隐匿案件的必要。

如果说公共行为者的强烈参与是公共利益治理的重要条件,[①]网络犯罪的协同治理也意味着法律责任的协同。法律责任的分配是由宪法、行政法律和刑事法律共同构建完成的,因而是立法者的专属性权力,行政权力与司法权力的边界划分是否合理,是立法者要考虑的问题。我们无法否认执法者、司法者对行政责任和刑事责任的分配具有现实的影响力,但行政责任和刑事责任的实际边际需要在现实的权力运作中逐步明晰。基于行为人危害性的大小而赋予其不同的法律责任,尤其是不能因为关注对“大鱼”的惩处而忽略了“虾米”,否则,有一天“虾米”也会变成“大鱼”。宽严相济刑事政策的“抓大放小”方针,“放小”是放弃追究刑事责任,而绝非放弃追究其他责任类型。

目前新的网络立法已经注意到运用综合性法律责任防治网络犯罪,《反电信网络诈骗法》第46条规定,“组织、策划、实施、参与电信网络诈骗活动或者为电信网络诈骗活动提供相关帮助的违法犯罪人员,除依法承担刑事责任、行政责任以外,造成他人损害的,依照《中华人民共和国民法典》等法律的规定承担民事责任”。也就是说,电信网络诈骗犯罪分子需要为其行为承担三位一体的法律责任,但这些责任各有其发动事由和判罚机关,司法机关可以对参与电信网络诈骗犯罪的人作出刑事责任判罚,但对犯罪分子可能承担的行政责任则需要通过刑行衔接措施交给有权行政机关作出判罚。

(二)刑行衔接的政策价值:推动网络犯罪的溯源治理

犯罪是严重背离社会主流意识形态的行为,它根植于特定历史时期的社会所赖以生存的物质生活条件,[②]因此犯罪是社会历史政治条件的产物。信息化时代孕育和催生信息化犯罪,网络犯罪与网络社会就如一个硬币的两个方面,网络犯罪随着网络时代的演变而不断“推陈出新”“同频共振”。网络犯罪是信息时代的产物,网络的超时空性、无限延展性等特性被犯罪分子充分利用,网络的安全问题愈发突出。在网络普及率和整体网民规模进入平台期的同时,[③]网络犯罪也进入高发期。2021年4月最高人民检察院披露的数据显示,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%。[④] 传统程式化的警察方式用于应对网络犯罪并不有效,[⑤]传统警察组织的结构性和文化性缺陷也导致网络世界的安全缺陷。[⑥]在此背景下,网络犯罪的“溯源治理”作为新的犯罪治理手段被正式提出来。

---

①J. van Erp, “New governance of corporate cybersecurity: A case study of the petrochemical industry in the port of Rotterdam”, *Crime, Law and Social Change*, Vol. 68, No. 1 – 2, 2017, pp. 75 – 93.

②刘文成:《犯罪学——犯罪现象·原因·对策》,北京:群众出版社,2001年,第29—30页。

③王思北:《“数字”点亮美好生活》,《新华每日电讯》2022年9月1日,第3版。

④戴佳:《检察机关去年起诉涉嫌网络犯罪14.2万人》,《检察日报》2021年4月8日,第1版。

⑤D. Walker, D. Brock & T. Stuart, “Faceless-oriented policing: Traditional policing theories are not adequate in a cyber world”, *The Police Journal*, Vol. 79, No. 2, 2006, pp. 169 – 176.

⑥J. Nhan & L. Huey, “Policing through nodes, clusters and bandwidth: The role of network relations in the prevention of and response to cyber-crimes”, in S. Leman-Langlois (ed.), *Technocrime: Technology, Crime and Social Control*, Portland, OR: Willan Publishing, 2008, pp. 66 – 87.

溯源治理体现了一般预防的刑法思想。《黄帝内经》有曰:“上医治未病,中医治欲病,下医治已病。”高明的犯罪治理手段追求防患于未然,将犯罪扼杀于萌芽阶段。2021 年 2 月,中央全面深化改革委员会第十八次会议审议通过的《关于加强诉源治理推动矛盾纠纷源头化解的意见》强调:“法治建设既要抓末端、治已病,更要抓前端、治未病。要坚持和发展新时代‘枫桥经验’,把非诉讼纠纷解决机制挺在前面,推动更多法治力量向引导和疏导端用力,加强矛盾纠纷源头预防、前端化解、关口把控,完善预防性法律制度,从源头上减少诉讼增量。”①网络犯罪的溯源治理,就是要从终端的犯罪行为处罚,层层向上回溯,最终回到网络犯罪的源头,深层次剖析网络犯罪的发生机理、技术特性、行为表征,在犯罪治理过程中实现网络社会治理体系和治理能力的根本性提升。溯源治理不仅是网络犯罪的整体治理方略,更重要的是司法机关不能满足于具体个案中对犯罪分子的绳之以法,而是要通过刑行衔接等手段,彻底实现网络“小流域治理”,以个案推动网络社会治理创新。

“溯源治理”主要是由检察机关提出的,检察机关自然是溯源治理的鼓手和主要推动者。检察机关是社会公共利益的代表,负有监督法律实施以及推动维护社会公平正义的使命。近年来检察机关在个人信息保护公益诉讼领域进行探索。2022 年最高人民检察院印发《关于加强刑事检察与公益诉讼检察衔接协作严厉打击电信网络犯罪加强个人信息司法保护的通知》,强调在容易产生个人信息泄露风险的重点行业、重点领域,“在严厉打击刑事犯罪的同时,充分发挥公益诉讼检察职能,依法追究违法主体的民事责任”。这即是主张通过不同法律责任的绞合作用,达到对犯罪源的根本治理。2021 年 4 月,最高人民检察院发布 11 件全国检察机关个人信息保护公益诉讼电信案例,②为全国检察机关办理类似案例作出规范指引。检察机关借助反向行刑衔接推动着网络犯罪的上游回溯治理。

溯源治理是要扼杀网络犯罪的“七寸”,实践基础是网络犯罪的产业链特征。当然,产业链特征不是网络犯罪独有的,任何成熟的犯罪形态都会自发形成产业链;产业链特征也不是中国网络犯罪独有的,西方网络发达国家也大有犯罪产业链。③ 只是在信息技术的加持下,在经济利益的驱动下,在网络匿名性的掩护下,网络犯罪的产业链是最完备的,也是最复杂的。当前网络犯罪由点及线,由线及面,由国内及境外,黑灰产业群体正由链状结构向网状结构发展。④ 在这种情况下,对任何一个孤立的网络犯罪案件的惩处就网络犯罪整体格局而言,都不过是无关痛痒的小打小闹,在巨大的利益面前,很快就有新的犯罪势力填充旧的犯罪空间,进而呈现“野火烧不尽,春风吹又生”的景象。网络犯罪防护链条上的任何一处薄弱环节都具有“管涌”的风险。经历《刑法修正案(七)》《刑法修正案(九)》以及《刑法修正案(十一)》的多次修改,当前刑事立法层面基本实现了对网络犯罪的全流程覆盖,但如果从社会治理的角度看,我们也不能忽视对更加普遍的网络失范行为和网络违法行为的治理。每一个网络犯罪背后可能隐藏了海量的网络违法案件。国外的研究表明,每 6500 起网络犯罪中只有 1 起会向警方报告,其余的均为轻微欺诈犯罪。⑤ 在我国,在 2020 年上半年开展的“扫黄打非”专项行动中,全国“扫黄打非”办公室举报中心累计受理举报信息 14 万多件(条),举报数量较 2019 年同期上涨约 11%。⑥ 见微知著,网络空间其他领域的违法犯罪情况可见一斑。网络犯罪治理既要注重对已成势的犯罪的治理,也要注重对未成势的违法行为的治理,借此实

---

①《完整准确全面贯彻新发展理念 发挥改革在构建新发展格局中关键作用》,《人民日报》2021 年 2 月 20 日,第 1 版。

②闫晶晶:《斩断个人信息侵权与电信网络诈骗之间的利益链条》,《检察日报》2021 年 4 月 23 日,第 2 版。

③A. G. Fanno, “Multitaskeholder approach to internet governance: A collaborative effort”, *Suffolk Transnational Law Review*, Vol. 38, No. 1, 2015, pp. 69 – 91.

④刘为军:《电信网络诈骗治理须强化协同》,《法治日报》2022 年 6 月 29 日,第 5 版。

⑤D. Wall, “Policing cybercrimes: Situating the public police in networks of security within cyberspace”, *Police Practice and Research*, Vol. 8, No. 2, 2007, pp. 183 – 205.

⑥《上半年全国“扫黄打非”办受理举报 14 万件、发放举报奖金 103 万元》,2020 – 07 – 14, http://www.cac.gov.cn/2020 – 07/14/c_1596282375324305.htm, 2022 – 09 – 21。

现对犯罪的“层递式阻断。”[①]在网络黑灰产业链条中,不是所有环节都值得动用刑法手段,同一案件中也不是所有的犯罪嫌疑人都值得动用刑罚手段,在需要进行责任分流时,反向衔接的价值就体现出来了。司法机关对共同犯罪中应当追究刑事责任的人推进刑事司法流程,而对情节显著轻微不构成犯罪的人适用程序反转,进入反向行刑衔接流程中,由行政执法机关补充追究其行政责任,实现针对不同危害行为的差异化责任配置。

二、基于犯罪嫌疑人的网络犯罪刑行衔接的两种模式

常规的刑行衔接模式是对犯罪嫌疑人追究刑事责任失败后,再回退到行政处罚程序中,但网络法律领域越来越倾向于对当事人施加综合性的法律责任处置,由此形成了基于犯罪嫌疑人的网络犯罪刑行衔接的两种模式。

(一)“刑-行关联罚”:刑事判决生效后的刑行衔接

依照新《行政处罚法》第27条,刑行衔接仅指危害行为不需要追究刑事责任或者免除刑事处罚而另行给予行政处罚的情形,即后文所指的“刑-行补充处罚”,但在实际的刑行衔接运作中,即使对犯罪人已经判处刑罚的,依然存在刑行衔接的必要性。

1. 审判机关主导模式:刑事判决作出后追加犯罪人的资格罚

我国的刑罚依其类型可分为人身罚、财产罚与资格罚(剥夺政治权利、驱逐出境),行政法中的行政罚另有行为罚和申诫罚两类。我国的《行政许可法》要求公民、法人或者其他组织需要获得某种资格才能从事相应行为,这就是行政许可制度的由来。对这类行为资格的剥夺,就是资格罚,相应的,禁止当事人实施无须许可就可实施的行为,就是行为罚。行政法上资格罚的类型和适用范围大于刑法上的资格罚,因为它意味着主体的市场资格的丧失,一旦这种资格被剥夺,对于市场主体而言就属于灭顶之灾。充分发挥资格罚的功能和作用,能够强化网络犯罪治理的威慑性,避免某些较大的互联网公司“丢车保帅”或者将犯罪成本估算为公司的经营性成本。

在网信监管执法领域,为了适应网络安全监管和业态治理的特点,网信监管执法主体开发了一些处罚手段,包括约谈、[②]暂停相关业务、停止传输、吊销许可证、下架应用程序、关闭网站等新型监管工具被广泛运用于网信内容监管领域。[③] 例如国务院《互联网信息服务管理办法》第23条规定,“违反本办法第16条规定的义务的,由省、自治区、直辖市电信管理机构责令改正;情节严重的,对经营性互联网信息服务提供者,并由发证机关吊销经营许可证,对非经营性互联网信息服务提供者,并由备案机关责令关闭网站。”审判机关在刑事判决生效之后,如认为有必要追加行政处罚的,则应当将案件线索移交给行政执法机关,由行政执法机关视情况追加行政处罚。但因审判机关没有强制性的要求行政机关作出行政处罚的权力,因此适合以司法建议的方式向行政机关反馈相关信息。

《反电信网络诈骗法》在刑行衔接方面有较大突破,即赋予了反向移送一定的强制性。《反电信网络诈骗法》第31条第2款规定,“对经设区的市级以上公安机关认定的实施前款行为的单位、个人和相关组织者,以及因从事电信网络诈骗活动或者关联犯罪受过刑事处罚的人员,可以按照国家有关规定记入信用记录,采取限制其有关卡、账户、账号等功能和停止非柜面业务、暂停新业务、限制入网等措施。”该法第36条第2款规定,“因从事电信网络诈骗活动受过刑事处罚的人员,设区的市级

①李奋飞:《涉案企业合规刑行衔接的初步研究》。
②周泽中:《行政约谈的规制功能及其法治约束》,《学习论坛》2019年第12期。
③崔俊杰:《互联网信息内容监管工具的实证分析与法治完善》,《中国行政管理》2020年第9期。

以上公安机关可以根据犯罪情况和预防再犯罪的需要，决定自处罚完毕之日起六个月至三年以内不准其出境，并通知移民管理机构执行。”信用惩戒以及限制再出境，是对受过刑事处罚的人的刑罚附随措施，通过对某项资格的禁止，在一定时间内剥夺犯罪人再犯罪的能力，进而实现刑罚的预防功能。这两项制度的推行，需要审判机关、公安机关、信用惩戒机构、移民管理机构等多部门的密切配合，尤其是审判机关作为刑行衔接的发动者，应具有推动刑行衔接的主动性。

那么，对犯罪人追加资格罚是否违背了一事不二罚原则？回答自然是否定的。国务院《行政执法机关移送涉嫌犯罪案件的规定》第11条规定：“行政执法机关对应当向公安机关移送的涉嫌犯罪案件，不得以行政处罚代替移送。行政执法机关向公安机关移送涉嫌犯罪案件前已经作出的警告，责令停产停业，暂扣或者吊销许可证、暂扣或者吊销执照的行政处罚决定，不停止执行。”按此规定，行政罚与刑事罚并行不悖，各自独立作出，追求行为人刑事罚的过程中并不影响行政罚的执行。我国《民法典》第187条规定，“民事主体因同一行为应当承担民事责任、行政责任和刑事责任的，承担行政责任或者刑事责任不影响承担民事责任；民事主体的财产不足以支付的，优先用于承担民事责任。”该条意味着同一行为可以同时引发刑事责任、行政责任与民事责任。反过来讲，如行政处罚没有来得及作出，亦不影响刑事判决的重新作出。我国的刑罚体系是以人身罚为主体的刑罚体系，而行政罚体系中有大量的资格罚。对于行政拘留以及罚款等人身罚和财产罚，刑法中有性质相同的刑罚类型，因而如果审判机关已经对行为人作出自由刑或者财产刑，则行政罚中行政拘留和罚款已被吸收进刑法而不能再次判罚。但对于行政法律赋予的特定资格、地位，刑事处罚并不能当然地吸收。在已经判处刑罚后，行政机关认为需要依法追究行为人特定行政责任的，可以再给予其相应的行政处罚。[①] 当然，作出刑事判决之后再对当事人追加行政罚，在法律责任上可能对当事人过于苛刻。欲解决这个问题，就需要从法秩序统一的原理出发，回归制度的初心，基于保障当事人正当权益和法律秩序稳定的需求，人民法院认为有必要对当事人追加行政罚前，可与行政机关事先沟通，在得到行政机关追加行政处罚的肯定答复后，再综合考量刑事处罚的力度。[②]

2. 检察机关主导模式：个人信息保护与反电信网络诈骗的行政公益诉讼

刑事判决生效后的刑行衔接的检察机关主导模式目前主要集中在个人信息保护与反电信网络诈骗领域的行政公益诉讼。在信息化时代，“数据就是石油”的理念已经深入人心，但个人信息的过度收集、不法转卖、违法使用等现象愈演愈烈。个人信息被视为隐私权在信息化时代的新维度，但同时个人信息的大规模泄露又进入公共安全范畴，[③]为此我国通过《个人信息保护法》《数据安全法》《民法典》《刑法》等法律规范建立了“私力救济 + 公法保护”的“双轮”保护模式，[④]但私力救济过高的维权成本以及受害者孱弱的举证能力让多数情况下的民事诉讼形同虚设，而公法保护重威慑惩罚轻安抚补偿的特性亦无法充分兼顾个体利益，行政公益诉讼开始作为私立救济和公法保护之外的第三种模式。2021年8月21日，最高人民检察院下发《关于贯彻执行个人信息保护法推进个人信息保护公益诉讼检察工作的通知》，提出“加强与行政机关协作配合，健全行政执法与公益诉讼检察衔接机制，加强与法院的沟通协调”。

最高人民检察院2021年4月公布的11起检察机关个人信息保护行政公益诉讼典型案例中，有多起案件属于刑事案件判决生效后，检察机关继续开展行政公益诉讼的案件。如在上海市宝山区人民检察院诉H科技有限公司、韩某某等人侵犯公民个人信息案中，H公司经理韩某将其在某天猫旗

①黄小伦、罗关洪：《区别情形处理行政处罚与刑事处罚竞合使用》，《检察日报》2017年6月26日，第3版。
②练育强：《行政执法与刑事司法衔接制度重构之理论基础》，《学术月刊》2015年第11期。
③梅夏英：《社会风险控制抑或个人权益保护——理解个人信息保护法的两个维度》，《环球法律评论》2022年第1期。
④范卫国：《证券公益诉讼：衍生逻辑、理论阐释与制度塑造》，《江西财经大学学报》2021年第6期。

舰店获得的个人信息售卖，被检察院提起公诉，该天猫旗舰店所在地的检察机关审查线索后以行政公益诉讼立案，并与负有监督管理职责的行政机关进行磋商。行政机关认定“某公司天猫旗舰店”的经营公司在执行网络安全信息制度的防范措施上存在明显漏洞，遂对该公司立案调查。① 当然，借助公益诉讼还可以进行“刑民”衔接。2019 年 12 月，徐某等合谋在浙江省杭州市、湖州市、绍兴市等地非法从事手机卡“养卡”活动。这些卡被用于电信网络诈骗犯罪活动。某区检察院向法院提起刑事附带民事公益诉讼。2021 年 12 月 31 日，法院以侵犯公民个人信息罪判处徐某等人有期徒刑三年至有期徒刑七个月不等刑期，判令被告人连带赔偿人民币 14 万元，并在国家级新闻媒体上进行公开赔礼道歉。②《反电信网络诈骗法》第 47 条规定：“人民检察院在履行反电信网络诈骗职责中，对于侵害国家利益和社会公共利益的行为，可以依法向人民法院提起公益诉讼。”本条规定也是这部法律的亮点之一。借助公益诉讼模式推动刑行衔接，具有方式灵活等特点。个人信息法律治理中，行政治理的作用是民事手段无法替代的，通过公益诉讼督促行政机关积极履职不失为一条积极路径。

（二）“刑－行补充处罚”：刑事程序终止后的刑行衔接

刑事程序终止，是指未获得生效法律判决前的程序停止状态。根据《刑事诉讼法》第 163 条规定，公安机关侦查过程中，发现不应对犯罪嫌疑人追究刑事责任撤销案件的，或者根据《刑事诉讼法》第 177 条的规定，人民检察院决定不起诉的，都会导致刑事程序终止的效果，不过本文所称的刑事程序终止仅限后者。

1. “刑－行补充处罚”中刑行衔接的具体适用

就刑罚和行政罚的关系而言，刑事程序终止后的刑行衔接，具有“刑－行补充处罚”的性质，即在刑事责任无法实现的情况下，基于行为人行为体现的整体的危害性，有必要追加相应的行政处罚，此时就有必要启动刑行衔接机制，它也可以理解为无法追究刑事责任的“回退”机制。“刑－行补充处罚”中的刑行衔接在网络犯罪适用的必然性在于，网络新兴业态中的违法与犯罪界限尚处在司法摸索中。网络的普及带来了大量的新兴业态创新，但正因为是“新兴”业态，其业态发展往往超前于法律规定，在新兴业态与既有法律规则相冲突时，究竟是对新兴业态“扶上马送一程”，在“良性违法”的容忍限度内评估其对社会整体利益的价值，还是直接出示红牌，叫停其发展节奏，非常考验监管者的智慧，同时又充斥着不同利益主体复杂的博弈。③ 对新兴业态的认识差异，不仅影响到行政监管的尺度，也影响着网络新型犯罪的边界。对于以网络新兴业态为名的网络犯罪的认定，其前置的行政规范可能分属于不同的网络监管执法主体，且也涉及复杂的技术性、专业性问题，其违法和犯罪的界限并非泾渭分明甚至一团模糊，由此造成大量的“同案不同判”现象。2022 年 8 月，杭州互联网法院在其成立五周年之际，发布了“网络不正当竞争”十大典型案例，这十大典型案例包括流量劫持、商业诋毁、算法自动抢红包、刷机案等等，这些在此法院被认定为不正当竞争的案例，在彼法院则完全可能作为犯罪处理。就目前不算陌生的网络爬虫案件而言，既有认定为不正当竞争的案例，④又有认定为非法获取计算机信息系统数据罪，⑤或者侵犯公民个人信息罪的案例。⑥ 为充分保障数字经济的

①《上海市宝山区人民检察院诉 H 科技有限公司、韩某某等人侵犯公民个人信息刑事附带公益诉讼案》，2021－04－22，https://www.spp.gov.cn/spp/jcgysljgrxxbh/202104/t20210422_527823.shtml，2022－09－22。

②高志华、李帅：《劳务人员个人信息保护刑事附带民事公益诉讼办案思考》，《中国检察官》2022 年第 14 期。

③马长山：《智慧社会建设中的“众创”式制度变革——基于“网约车”合法化进程的法理学分析》，《中国社会科学》2019 年第 4 期。

④广东省深圳市中级人民法院（2017）粤 03 民初 822 号民事判决书。

⑤北京市海淀区人民法院（2017）京 0108 刑初 2384 号刑事判决书。

⑥浙江省杭州市西湖区人民法院（2020）浙 0106 刑初 437 号刑事判决书。

生命力和活力，又为防范新型业态可能造成的安全风险，我国提出了“包容审慎”的监管原则。2020年1月1日起施行的《优化营商环境条例》在第55条中规定，“政府及其有关部门应当按照鼓励创新的原则，对新技术、新产业、新业态、新模式等实行包容审慎监管。”包容审慎监管旨在追求效率与安全的动态平衡，[①]包容审慎不应当仅是网络新型业态的监管原则，也应当成为网络新型业态安全风险的司法原则。2018年《反不正当竞争法》增加了第12条不正当竞争条款，为经济法介入网络新型业态治理扫清了法律障碍，客观上也为刑法治理起到了分流作用。《反不正当竞争法》第24条规定，违反本法第12条行为的，可以由监督检查部门责令停止违法行为，并处以罚款。刑行衔接可以在此充当刑事程序的容错机制，对于进入到刑事司法流程的新型业态案件，应客观理性审视其存在的安全风险以及对社会公共利益造成的损害，没有必要作为犯罪处罚的，也不能放任自流，“包容审慎”不是放任，值得追究行政责任的必须追究行政责任。

法律责任的一体化是近年来网络犯罪治理的新动向。《反电信网络诈骗法》第38条规定，组织、策划、实施、参与电信网络诈骗活动或者为电信网络诈骗活动提供帮助，构成犯罪的，依法追究刑事责任。尚不构成犯罪的，由公安机关处十日以上十五日以下拘留，没收违法所得，并处以相应罚款。这是《反电信网络诈骗法（草案三审稿）》新增加的内容。它强调，即使在少捕慎诉慎押模式下放弃追究部分共同犯罪人刑事责任，也并不能免除其行政责任，这是严密法网的重要举措，而该条款的落实，自然也有赖于司法程序中的刑行衔接。

刑行衔接适用的另一个领域是检察机关主导的企业合规改革。[②] 最高人民检察院2022年7月21日《关于印发涉案企业合规典型案例（第三批）的通知》中的第一个案例是网络平台的刑事合规案件。上海Z公司通过爬虫程序爬取某外卖平台的数据，造成外卖平台流量成本增加，直接经济损失4万元。检察机关对Z公司相关责任人员作出不起诉决定，制发《合规检察建议书》，并邀请网信办、知名互联网安全企业、产业促进社会组织等的专家成员参与合规整改。[③] 在本案中，检察机关邀请行政机关以及第三方组织参与合规整改，但在决定对涉案企业不起诉后，并没有要求行政机关对涉案企业作出行政处罚。行政处罚可否成为网络犯罪案件刑事合规的一个前提条件，还有待进一步的理论探索。

2.“刑－行补充处罚”后刑行衔接的价值：违法行为向犯罪的二次转化

刑行衔接的另外一个价值，是便于行政违法行为向犯罪的二次转化，为第二次追究行为人的刑事责任铺平道路。理解这一点，就要谈到中国刑法特有的“多次行为”现象。多次行为是指中国刑法以及司法解释中大量存在的多次实施同一类型的违法行为而累积构成犯罪或者加重处罚的现象。如《刑法》第153条第1款关于走私普通货物、物品罪的规定，“走私货物、物品偷逃应缴税额较大或者一年内曾因走私被给予二次行政处罚后又走私的，处三年以下有期徒刑或者拘役，并处偷逃应缴税额一倍以上五倍以下罚金”，即基于前次行为已经受过行政处罚的事实，而导致后行为被作为犯罪处理，但如果没有前次受到行政处罚的行为，后行为只需追究行政责任即可。近年来我国新制定或修订的司法解释广泛采用了多次行为的立法模式。多次行为是否是良善的法律模式，理论上争议颇多，[④]不过本文想说明的是，既然刑法和司法解释存在大量多次行为入罪化的事例，则刑行衔接就成为落实多次行为入罪化的重要保障性机制。

---

①刘权：《数字经济视域下包容审慎监管的法治逻辑》，《法学研究》2022年第4期。

②李奋飞：《涉案企业合规刑行衔接的初步研究》。

③李海洋：《最高检发布第三批涉案企业合规典型案例》，《中国商报》2022年8月23日，第3版。

④李怀胜：《多次行为入罪化的立法价值与体系性反思》，《政治与法律》2020年第7期；张明楷：《简评近年来的刑事司法解释》，《清华法学》2014年第1期。

例如，为遏制电信网络诈骗犯罪的势头，司法机关针对出租与买卖信用卡、电话卡的行为也就是俗称的“两卡犯罪”进行严厉打击，但这样做的直接后果就是非法利用信息网络罪的适用率飙升。最高人民检察院2022年工作报告显示：2021年“协同推进‘断卡’行动，起诉非法买卖电话卡和银行卡、帮助提款转账等犯罪12.9万人，是2020年的9.5倍。”①实践中发现，部分非法交易“两卡”的行为人因涉案卡数较少、初犯偶犯、主观明知及情节严重难认定等原因被做出不起诉决定，但后又再实施“两卡”违法行为。尽管2019年《最高人民法院、最高人民检察院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》（以下简称《帮助信息网络犯罪活动等罪解释》）第12条将“二年内曾因非法利用信息网络、帮助信息网络犯罪活动、危害计算机信息系统安全受过行政处罚，又帮助信息网络犯罪活动罪的”作为帮助信息网络犯罪活动罪“情节严重”的情形，②但由于仍在前案取保候审期间，前案未能作做出行政处罚等，现案中无法适用上述司法解释的“情节严重”，从而再次取保候审或者不起诉，犯罪嫌疑人的屡犯、再犯并未得到任何实质性、终局性处罚。北京市东城区人民检察院在办理一起涉“两卡”犯罪案件中，对代办企业对公账户的王某作出相对不起诉决定，同时向案件的侦查机关制发检察意见书，建议对王某依照《网络安全法》依法作出行政处罚，这是在电信网络诈骗犯罪案件中运用刑行衔接机制的典型实例。③ 检察机关对涉“两卡”犯罪作出不起诉的嫌疑人向公安机关移送线索，由公安机关依据《网络安全法》进行行政处罚，可以有效防止嫌疑人反复作案又无从打击的司法困境。当然，目前《反电信网络诈骗法》已经生效实施，公安机关可直接依据本法第31条对涉“两卡”违法人作出行政处罚。

三、犯罪相关人：网络犯罪案件刑行衔接中的第三方责任

在网络空间中，基于网络犯罪的产业链特征以及网络犯罪的协同治理需求，一个犯罪案件带出来的所有违法与犯罪的节点，都要成为刑行衔接的对象。网络犯罪的产业链特征意味着所有的网络环节都可能被犯罪所利用，例如一个完整的电信网络诈骗犯罪可能包括侵犯公民个人信息、互联网接入、服务器托管、网络存储、通讯传输、广告推广、支付结算等各个环节。为遏制网络犯罪，需要网络空间的全链条、全主体履行相应的法律责任和义务，任何一处监管疏漏和不足都可能被犯罪分子所利用，从而造成网络犯罪防范的“管涌”效应。因此，笔者以平台责任为例，探讨非犯罪嫌疑人的刑事案件当事人以及其他案件关联人作为刑行衔接的责任追究对象的正当性与必要性。

（一）第三方责任的基础：平台的权力属性与犯罪防控责任

信息技术所形塑的，不仅仅是传统社会结构，还有网络社会的组织模式。在技术引发的商业变革中，网络平台异军突起。网络平台的主体责任与网络平台在信息化时代内生的权力属性密不可分。以安德鲁·夏皮罗（Andrew Shapiro）为代表的网络理论家将互联网的本质定性为“社会控制工具”，网络的本质是“信息独裁”。④ 网络在结构上的最大影响是分权，人和事都不再依赖一个中心点彼此连接。⑤ 在此情况下，“国家过滤机制黯然失色……复制、折射、反映、描述社会和历史的权力确实已经弥散化、去中心化，国家对复制社会的权力垄断已经被打破了”。⑥ 在智能互联网社会，互联网

①张军：《最高人民检察院工作报告》，《人民日报》2022年3月16日，第2版。
②该司法解释对非法利用信息网络罪也作出了相同的规定。
③张玮、汪珮琳：《被不起诉后，还要受行政处罚》，《检察日报》2022年5月31日，第6版。
④蔡文之：《国外网络社会研究的新突破——观点评述及对中国的借鉴》，《社会科学》2007年第11期。
⑤[美]埃瑟·戴森：《2.0版数字化时代的生活设计》，胡泳、范海燕译，海口：海南出版社，1998年，第19页。
⑥刘建军、沈逸：《网络政治形态：国际比较与中国意义》，《晋阳学刊》2013年第4期。

平台、数据公司等新兴商业组织塑造着全新的经济业态、商业模式和交易规则，成为日益重要的新型法律关系主体，它具有此前法律关系主体所不可想象的“准立法权”“准行政权”和“准司法权”。[①] 大型互联网公司甚至可以订立交易规则，为“交易立法”。

网络平台的数据优势和技术优势已然形成，强行消解将损害国家整体的网络竞争能力，因而国家与网络平台合作就成为必然。为了适应网络“平台化”的现实，监管部门开始强化“平台责任”，将平台作为网络用户与网络监管者的中介，并且事实上构建了监管者－平台－用户的阶层式结构。在平台的各类义务中，犯罪的防范与治理义务占有重要比重。在数字世界中，人们普遍认为，安全利益相关者必须共同努力，检测和响应感知到的在线信息威胁。[②] 网络平台的犯罪防范义务，包括对网络平台的安全保障义务，平台内违法有害信息的处置义务，以及必要的信息收集和留存义务，[③]这是基于犯罪防控需要的一般性的犯罪控制义务，此外，在具体的犯罪行为发生后，网络平台还要对司法机关履行证据提供特定性的义务内容。[④] 既然有明确的义务内容，自然也要有明确的责任后果。

（二）网络平台的多重身份：刑事被害人与行政违法人

网络平台在犯罪防控与治理中负担了多种义务，在犯罪治理过程中，网络平台基于法律责任的转换，可能同时出现多种身份属性。网络平台身份的多元性，是对网络平台进行刑行衔接的基础。

例如，《网络安全法》第21条建立了网络安全等级保护制度。事实证明，许多网络安全事件以及网络犯罪的发生，均是相关网络运营者没有履行网络安全等级保护制度或者履行不到位所致。例如，2019年3月，泰州某事业单位集中监控系统遭黑客攻击破坏。经查，该单位网络安全意识淡薄，曾因存在安全隐患、不落实网络安全等级保护制度被责令整改。整改期满后，未采取有效管理措施、技术防护措施。[⑤] 因此，提升网络运营者的网络保障义务，对于防范网络犯罪具有标本兼治的作用。网络平台如因未履行网络安全登记保护制度的相关要求致使网站被黑客攻破，网站内储存的数据和公民个人信息被泄露，网络平台在黑客攻击事件中是以被害人的身份出现的。黑客攻击事件的发生与网络平台未履行网络安全登记保护制度的相关义务具有密切联系，网络平台行政违法在先，依然要依据《网络安全法》第59条进行行政处罚。同时，因数据和公民个人信息泄露造成用户人身、财产损失的，网络平台还要依据《民法典》承担相应的民事侵权责任。可见，在一起黑客攻击事件中，网络平台具有双重身份。一方面网络平台是刑事案件的被害人，刑事司法机关追究黑客的刑事责任是为维护网络平台的合法权益；另一方面，网络平台未履行网络安全等级保护义务导致黑客攻击事件发生的，网络平台同时违反了《网络安全法》的相关规定，因此是行政违法案件的违法人，甚至还有可能是民事侵权案件的连带侵权人。重大网络安全事件发生后，公安机关往往将精力放在刑事案件的侦办上，并在对网络平台的“同情”心理下，有意无意忽视对网络平台的处罚。故此，审判机关在对破坏计算机信息系统等案件审理过程中，要注意查明网络平台在犯罪发生中的作用，重点审查网络平台是否怠于行使相关的网络安全保障义务，以及公安机关是否已经对网络平台处以相应的行政处罚。如有，则要向公安机关反向移送案件，要求公安机关追加处罚。

---

①马长山：《智能互联网时代的法律变革》，《法学研究》2018年第4期。

②B. Dupont，“Security in the age of networks”，*Policing & Society*，Vol. 14，No. 1，2004，pp. 76－91.

③裴炜：《针对用户个人信息的网络服务提供者协作执法义务边界》，《网络信息法学研究》2018年第1期。

④例如《反电信网络诈骗法》第26条第1款规定：“公安机关办理电信网络诈骗案件依法调取证据的，互联网服务提供者应当及时提供技术支持和协助。”

⑤《8个等级保护违规处罚典型案例解析》，2019－12－26，https://www.bj3gweb.com/link2019122601.html，2022－09－22。

再如，在刑事诉讼流程中网络平台负有信息收集存储义务、信息审查监控义务和信息披露报告义务，[①]如《反恐怖主义法》第19条规定了电信业务经营者、互联网服务提供含有恐怖主义、极端主义内容的信息的防范传播义务、停止传输义务、记录保存义务、主动报告义务。另根据《刑事诉讼法》第54条第1款的规定，“人民法院、人民检察院和公安机关有权向有关单位和个人收集、调取证据。有关单位和个人应当如实提供证据。”如果公检法机关向网络平台调取数据时，网络平台却未履行相应的数据存储义务，导致出现严重后果，就要对网络平台进行刑行移送，追究其行政责任。

在防治电信网络诈骗犯罪中，公安机关已经充分重视到一些网络经营者在网络犯罪中的“被动参与者”角色。《最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》第3条第8项规定：“金融机构、网络服务提供者、电信业务经营者等在经营活动中，违反国家有关规定，被电信网络诈骗犯罪分子利用，使他人遭受财产损失的，依法承担相应责任。”另外，《人民检察院检察建议工作规定》第11条规定，“人民检察院在办理案件中发现社会治理工作存在下列情形之一的，可以向有关单位和部门提出改进工作、完善治理的检察建议：（一）涉案单位在预防违法犯罪方面制度不健全、不落实，管理不完善，存在违法犯罪隐患，需要及时消除的；（二）一定时期某类违法犯罪案件多发、频发，或者已发生的案件暴露出明显的管理监督漏洞，需要督促行业主管部门加强和改进管理监督工作的。”司法机关在办理网络犯罪案件中，应当树立“全景扫描”的意识，建立“小病也要全身体检”的理念，在每一起网络犯罪案件中，实现“惩治”“预防”“服务”三种观念，[②]犯罪产业链要往上游回溯，法律责任要往行政责任甚至民事责任倒推，执法链条要向两端（执法端与司法端）扩展，在个案正义的完全实现中推动网络犯罪态势的根本改观。

（三）刑行衔接中强化网络平台第三方责任的价值

网络平台是“网络社会重要的组织力量，对维护网络信息安全负有重要社会责任”。[③] 当前网络犯罪仍然处于高位高发态势，预防和惩治网络犯罪的被动局面没有得到明显改善。网络平台的网络犯罪防控义务的落实，是网络犯罪协同治理机制的重要一环。网络平台不但是网络犯罪治理的“利益攸关方”，也是“责任攸关方”，其对网络犯罪的防控水平对网络犯罪防控走势的影响是毋庸置疑的。网络平台在提供服务过程中，收集了大量的公民个人信息。为保障个人信息安全，《网络安全法》《数据安全法》以及《个人信息保护法》都明确了信息收集者的各种信息保护义务。保障用户个人信息安全，是网络平台的法律义务，也是道德义务。网络平台怠于行使网络安全登记保护制度的义务要求或者个人信息保护的相关要求，导致公民个人信息泄露，表面上看网络平台是犯罪的被害者，但这里所谓的“被害”之于网络平台而言可能只是商业信誉的受损，如果信息泄露事件未被宣扬出去，则网络平台实际上毫发无损。国外的研究表明，企业报告的网络攻击事件只占很小部分，因为企业并不愿意宣扬这类事件。[④] 而履行平台的安全保障义务则要投入大量的精力，一些网络平台对应当承担的行政义务干脆置若罔闻，这就相当于将企业责任风险转嫁给社会。网络平台和网络监管者立场和价值取向是不同的，网络平台更注重业务的可持续运营和商业利益。而任何信息泄露事件的发生都会给信息被泄露的用户个人造成人身损害和财产损失，我们甚至可以说网络平台是名义上的被害人，而用户个人才是真正的被害人。通过刑行衔接督促网络平台履行信息保障义务，正是为了保障广大网络用户的切身利益。

---

①裴炜：《数字正当程序：网络时代的刑事诉讼》，北京：中国法制出版社，2021年，第37页。
②刘为军：《论侦查、预防、服务三元一体的侦查理念》，《中国人民公安大学学报》（社会科学版）2020年第2期。
③李源粒：《网络安全与平台服务商的刑事责任》，《法学论坛》2014年第6期。
④J. van Erp，“New governance of corporate cybersecurity：A case study of the petrochemical industry in the port of Rotterdam”.

公安机关在办理网络犯罪案件中，可以根据案情对作为刑事案件被害人的网络平台直接予以行政处罚，但最理想的做法依然是等待刑事案件尘埃落定再决定是否对网络平台追加处罚。刑事诉讼流程较之行政处罚程序的差异在于，它能够更充分保障各方当事人的合法权益，当事人享有充分的诉讼权利和辩护权利，在此基础上得到的犯罪事实更接近“客观真实”。刑事案件的判决书发生效力之后，公安机关可以基于刑事判决书认定的事实更充分和全面地评估网络平台导致犯罪发生的作用和责任，进而作出更适当的行政处罚。司法机关在完成判决后，认为应当对网络平台追加行政处罚的，应当通过司法建议或者检察建议的方式，督促公安机关积极履职。

《刑法修正案（九）》新增的拒不履行信息网络安全管理义务罪为双向行刑衔接铺平道路。本罪出台之初，刑法学者一度担心本罪会过度扩张网络平台的刑事责任，为此提出了各种限定其刑事责任的方式，[①]但一直到今天适用本罪的案件数量非常有限，其主要原因在于本罪将行政违法要素作为前置性的入罪条件，只有“经监管部门责令采取改正措施而拒不改正”，并导致危害后果发生的，才可能构成犯罪。反向行刑衔接的落实，实际上有助于倒逼网络平台真正落实其网络主体责任。而根据两高《帮助信息网络犯罪活动等罪解释》第6条，网络主体具备“对绝大多数用户日志未留存或者未落实真实身份信息认证义务的”以及“二年内经多次责令改正拒不改正的”情形的，即认定为构成拒不履行信息网络安全管理义务罪的“严重情节”，进而构成犯罪。该条规定的合理性姑且不论，它的存在再次提醒司法者，要注重通过行刑衔接和刑行衔接来强化网络平台的主体责任的落实，通过刑事责任的“慑压”，来保证网络平台的犯罪预防与犯罪控制义务的实现。[②]

四、结　语

当前网络犯罪对传统社会的“侵入性”越来越明显，网络犯罪危害性的辐射效应在传统空间落地生根，同时传统犯罪又对网络犯罪具有“反哺”效应，网上网下“虚实”联动更进一步加剧了网络犯罪的治理难度。传统的“头疼医头，脚疼医脚”式的应对犯罪策略，在网络犯罪浪潮面前近乎失效。各国立法者和司法者都在思索信息化时代更为可行的犯罪治理策略，例如近年来国际社会兴起了针对网络犯罪的“多利益攸关方”（multitaskeholeder）的治理模式，[③]强调执法者、网络用户与互联网公司对网络犯罪的协同治理。在我国也有观点提出，面对网络社会新矛盾类型，司法也应积极探索多元主体协同合作化解模式。[④] 针对网络犯罪的特点与发展趋势，我们需要提出涵括刑事实体和刑事程序的一揽子防控策略，并将其作为网络社会治理创新的重要内容。网络社会中时间和空间都无法阻挡矛盾的快速释放，这要求法律快速回应网络社会治理的现实需求。行刑衔接和刑行衔接（即反向行刑衔接），契合了网络犯罪协同治理的现实需求，是实现对网络犯罪多元共治的配套性法律制度，通过这套机制的黏合作用，真正起到调动刑事司法机关、行政执法机关以及各类网络主体“相互交往、互惠合作”的作用，推动建立“网络空间命运共同体”。

（**责任编辑：**吴　欢）

---

①涂龙科：《网络内容管理义务与网络服务提供者的刑事责任》，《法学评论》2016年第3期。

②由反向行刑衔接推而广之，还可将刑事责任与党纪责任衔接起来。2017年《党委（党组）网络安全工作责任制实施办法》第8条规定，存在发生严重网络安全事件的，各级党委（党组）应当逐级倒查，追究当事人、网络安全负责人直至主要负责人责任。协调监管不力的，还应当追究综合协调或监管部门负责人责任。

③A. G. Fanno，“Multitaskeholder approach to internet governance：A collaborative effort”.

④李占国：《网络社会司法治理的实践探索与前景展望》，《中国法学》2020年第6期。

The Convergence of Criminal and Administrative Law Enforcement in Cybercrime Governance: Basic Value and Operation Pattern

LI Huaisheng

Abstract: Under dual effect of the deep socialization of cybercrime and its characteristic of industrial chain, cybercrime governance has become a severe social challenge. The difficulty in dealing with this challenge exceeds that of traditional crime. In this context, a reversed coherence mechanism of administrative and criminal law enforcement in policing cybercrime meets the needs of source governance, process governance and collaborative governance towards cybercrime. Issues for cyberspace governance like anti-telecom and online fraud, personal information protection, and risk management of new industry require a coherent strategy for determining legal responsibility as well. Two modes of reversing the coherence in administrative and criminal law enforcement are giving "related penalty" after the criminal judgment coming into force, and giving "supplementary penalty" after reversing the coherence due to the failure of conducting criminal sanction. The former is helpful to realize the closed loop of legal responsibility while the latter is conducive to realizing the mode of "criminalization of repeated acts" in judicial interpretation. Based on the characteristic of the industrial chain of cybercrime and the demand for collaborative governance of cybercrime, the judiciary should review the whole chain of cases and focus on the administrative responsibility of the "victims" of crimes such as the network platforms.

Keywords: cybercrime; collaborative governance; convergence of criminal and administrative law enforcement; integrated responsibility

About the authors: LI Huaisheng, PhD in Law, is Associate Professor at School of China University of Political Science and Law (Beijing 100088).