第38卷第4期 常州工学院学报(社科版) Vol. 38 No. 4
2020年8月 Journal of Changzhou Institute of Technology(Social Science Edition) Aug. 2020
doi: 10.3969/j.issn.1673-0887.2020.04.020

# 互联网黑色产业犯罪的现状考察及规制路径

杨阳,应文舒

(安徽大学法学院,安徽 合肥 230601)

摘要:随着网络技术的日益进步,互联网黑色产业犯罪日益猖獗。类型化、复杂化的黑色产业链对网络环境的负面影响不断扩大。跨区域化、平台化、网状化的特点给治理黑色产业犯罪增加了难题。面对司法机关调查取证难、犯罪手段多样化、无法实现精准打击以及刑法适用存在障碍的现状,为有效打击互联网黑色产业犯罪,必须转变应对思路,坚持联合治理,完善规范体系,创新治理机制,多层面、多角度、全方位地应对互联网黑色产业犯罪。

关键词:黑色产业犯罪;黑色产业链;现实状况;治理办法

中图分类号:D924.34 文献标志码:A 文章编号:1673-0887(2020)04-0100-07

## 一、互联网黑色产业犯罪概述

互联网黑色产业犯罪,俗称“黑产犯罪”。主要是指以各种信息技术为工具,以互联网为媒介,以获取非法经济利益为目的,以非法利益交换为连接形成的多环节分工、多阶层、市场化的犯罪活动[1]98。互联网黑色产业犯罪主要分为上中下三个模块,即:上游产业链,负责提供各种技术手段;中游产业链在上游的基础上整合各种资源信息,有效归类,销售信息;下游产业链利用购买的数据资源实施诈骗等犯罪行为。改革开放以来社会发展日新月异,伴随着第四次工业革命的到来,互联网技术得到显著提升,与之相联系共存的地下网络黑色产业群体也在自我进步,互联网黑色产业群体犯罪逐渐从传统的单项式演变成系统式、链条式、网状式的犯罪群体。更加趋向于系统化、复杂化、组织化的网络黑产行业亟须得到整治。

公安部第三研究所网络安全法律研究中心与百度联合发布的《2019年网络犯罪防范治理研究报告》(以下简称《报告》)显示,互联网黑色产业犯罪主要存在以下几种典型类型:电信诈骗、恶意程序、流量劫持、DDoS攻击、侵犯公民个人信息[2]。

(1)电信诈骗。是指犯罪分子通过购买而来的公民个人信息,编造虚假信息、拨打电话,实行全面撒网式的铺盖,进而获得被害人的信任,与被害人保持线上亲密关系,诱骗被害人给犯罪分子转账、汇款等,侵害其财产法益。其中的产业链条主要是由上游开发制作者研发木马病毒、钓鱼网站等,通过中游域名贩子、卡贩子进行数据信息收集,最后集中实施诈骗。各种垃圾短信、骚扰电话严重影响了人们的生活,也增加了一些人上当受骗的可能性。

(2)恶意程序。所谓的恶意程序就是不法分子为达到不正当目的,违背用户意愿或者未予授权的前提下,执行远程控制、恶意下载安装、信息窃取、恶意传播、系统破坏等行为的程序。这种程序以互联网、物联网为主要攻击对象,手段隐蔽难以被发现,并且有低成本高收益的优势,故成为众多不法分子的犯罪手段。上游产业为其制作恶意木马,如恶意盗号、窃取账号、流量劫持等,中游产业以手机为传播媒介,通过下载App、手机网页、电子邮箱等植入病毒,最后实施犯罪。

(3)流量劫持。我国第一例流量劫持案为付宣豪、黄子超DNS劫持案,最终上海市浦东新区人民法院以破坏计算机信息系统罪分别判处二人

收稿日期:2020-03-07

作者简介:杨阳(1996— ),男,安徽巢湖人,硕士研究生。

有期徒刑三年，缓刑三年。所谓的流量劫持就是通过各种恶意软件强制更改网络数据，使网络用户非自愿访问网站造成流量浪费的情形。即用户访问搜索引擎点击页面，页面强制跳转各类欺诈站点，赌博、卖淫、App 推广等不良网页，“黑产”从中获取流量，进行牟利。

（4）DDos 攻击。其全名为“分布式拒绝服务攻击”（distrbitued denial-of-service attack），DDos 攻击是在 Dos 攻击的基础上进一步演变而来的一种新型攻击手段。即位于不同地方的两个以上的攻击者同时向某一特定机器发动“拒绝服务”式攻击，从而导致特定机器无法正常访问。最终会使网站服务器崩溃，无法正常提供服务。网络用户无法正常上网，浏览页面，导致网络运营商损失惨重。这种行为扰乱了网络秩序，破坏了网络环境。

（5）侵犯公民个人信息。随着后数字时代的到来，传统的身份信息类静态公民个人信息已无法满足不法分子的需求，他们更多地将目光转向个人活动类的动态信息。通过黑客侵入、撞库、网络爬虫等方法攻击数据库服务商，再通过中间商进行数据清洗以及验证，最后由非法数据利用者进行各种犯罪，从而逐步形成“源头—中间商—非法利用”的庞大地下网络黑色产业链。

## 二、互联网黑色产业犯罪现状考察

近年来，随着互联网的高速发展，网络犯罪逐渐呈现爆发态势，不仅数量在逐年增加，而且不断出现新型互联网犯罪，使司法部门疲于应对。时下，“黑产”正成为互联网犯罪中的关键词，“黑产”逐渐引起人们广泛关注，随着越来越多的“黑产”案件被警方侦破，互联网黑色产业也逐渐浮出水面。互联网黑产，不仅其隐蔽性给公安机关在办理案件时增加了难度，而且其复杂性也给司法机关在认定案件事实，正确适用罪名时制造了困难。面对法律的滞后性，如何正确运用法律规制不断恶化的互联网黑色产业，是当下法律必须要解决的问题。互联网黑色产业犯罪其特征表现如下：

### （一）存在严重的社会危害性

互联网黑色产业链的存在导致出现了各种新型网络犯罪，给公民的人身财产安全带来了巨大危害，互联网环境也遭到严重破坏。2017 年备受公众关注的徐玉玉电信诈骗案中，主犯陈文辉因犯诈骗罪与侵犯公民个人信息罪最终被判无期徒刑，追溯案件源头，还是离不开互联网黑色产业。“木马病毒—获取信息—实施诈骗”，一条完美的黑色产业链促使了此次悲剧的产生。根据最高人民法院发布的《司法大数据专题报告：网络犯罪特点和趋势》报告，从 2016 年到 2018 年底，全国各级法院一审审结的网络犯罪案件共计 4.8 万余件，在全国刑事案件总量中的占比为 1.54%，案件量和占比均呈逐年上升趋势。近些年不断出现的勒索病毒成为各大企业、银行、政府的心头之患。2019 年初全球较大的铝制品生产商 Norsk Hydro 遭到勒索病毒的攻击，不得不关停多条自动化生产线，使得世界范围内的铝制品交易价格受到影响，产生严重波动。据相关机构测算，截至 2017 年底我国黑色产业从业人员达到 130 万，形成高达千亿元级别的市场规模。此外根据有关报道，我国网络犯罪占据了总犯罪数的一半，并且每年的增长率惊人，达到的 30%。2016 年北京市发布的《2015 年第一季度网络犯罪数据研究报告》指出：2015 年第一季度北京网络安全反诈骗联盟共受理 4 920 件关于网络诈骗案件，涉案金额高达 1 772.3 万元，平均每人损失3 602 元。根据 2019 年发布的关于网络犯罪的报告，2018 年因网络犯罪导致全球经济每分钟损失 290 万美元，因网络钓鱼攻击导致全球经济每分钟损失高达 17 700 美元，每分钟泄露可标识数据记录 8 100条，头部企业每分钟因网络安全漏洞付出 25 美元的成本，因勒索软件攻击导致全球经济损失每分钟达 22 184 美元。

根据最高人民法院发布的《司法大数据专题报告：网络犯罪特点和趋势》，网络犯罪案件涉及多种罪名，其中诈骗罪排名第一，案件量占比高达 31.83%，其次为新型的开设赌场罪，占比为 10.45%[3]。将线下的犯罪活动转移到线上，通过网络平台展开业务活动，增加了犯罪行为的隐蔽性，加大了侦查难度。

### （二）黑色产业犯罪手段多变

十几年前，由于缺乏先进的科学技术支撑，科技数码产品的普及率也较低，尚无法形成大范围

组合式的数据截流。现如今,随着经济水平的不断提升,科学技术的高速发展,各种新型的黑色产业不断涌现,网络犯罪手段也多变,从传统的链条式逐步发展成为网状式的互联网黑色产业链,在技术手段、信息整合、资源利用、平台架构、流水线条、资金引流等方面越来越完备,使人们疲于应对。

2019 年广东湛江市公安局在开展的“净网 2019”专项活动中,侦查出 2 个“第四方支付平台”新型团伙,通过顺藤摸瓜发现了由“第四方支付平台—金融诈骗平台—诈骗团伙”组成的犯罪产业链条。警方发现,“第四方支付平台”主要通过与第三方支付平台或者银行合作,打通资金链条。他们通过中介寻找犯罪分子为其提供资金支持,事成之后从中抽取一定的手续费。不同于第三方支付平台取得了合法经营支付结算许可证,“第四方支付平台”属于违法网络支付途径,经常被用于赌博、洗钱等非法、违法活动,并呈现高隐蔽性、高复杂性、高危害性、高利润低成本、被害人数众多、分布广泛的特征。除此之外,广东警方还查处了一起新型网购平台代付刷单案件。由产业上游软件开发制作者研发出“0 元代付软件”,再通过中游销售渠道,下级软件销售者向实施刷单团伙售卖此产品。刷单团伙在互联网各大平台以高利润、高回报、低成本为诱饵售卖此软件,吸引涉世未深的年轻人,使他们上当受骗。这种新型网上刷单案件与传统刷单骗局的不同之处在于,它将传统的交付押金刷单变成以“0 元代付软件”为中介,犯罪分子将刷单者发送的代付页面金额修改为 0 元,使受害者在不知情的状态下完成原价付款,最终钱货两空。此外,警方还侦破了预装手机后门窃取验证码、散布虚假信息引流“吸金”、制售机器人服务网络赌博等其他新型网络犯罪手段。

其实互联网黑色产业链的违法犯罪手段远不止这些,其他如恶意注册账号、养号行为,薅羊毛行为,杀猪盘行为,劫持流量等行为在互联网上层出不穷。各式各样的互联网犯罪手法增加了犯罪的成功率,跨区域、产业链的犯罪模式加大了公安机关破案的难度,此外交叉性的网络犯罪也增加了司法机关查清案件事实、正确适用罪名的难度。

(三)黑色产业犯罪呈现跨区域化、平台化、网状化特点

由现实地域空间向网络虚拟空间犯罪的转变,使得黑色产业跨区域化更加方便。互联网技术所建构的虚拟空间拥有超越现实领土与自然国界的虚拟性,网络犯罪可能出现跨国性[4]。随着互联网技术的发展以及自身的特殊属性,传统的线下聊天交往方式比重逐渐减小,而匿名式的线上聊天逐渐成为当今社会的主流。各种 QQ 群、微信聊天群,以及各种网络论坛成为不法分子进行违法犯罪的主要地方。纵然相隔万里,也丝毫不影响不法分子准确顺利地实施犯罪。共同实施不法行为的犯罪分子可能都素未谋面,实施帮助行为的人与实行行为人可能都互不认识。上游产业商通常依靠“暗网”寻找下家,售卖各种技术产品,而购买犯罪工具的不法分子可能来自全国各地,当下游产业商在获取数据信息后,通过手机、电脑,以广撒网的方式,向不特定对象实施犯罪,最终实现异地销赃。从最高人民法院发布的数据可知,2016 年至 2018 年,在侦破的网络诈骗案件中,被告人利用的虚拟犯罪工具主要为微信、QQ、支付宝等,占比分别为 42.21%、35.23%和 15.28%。

当今黑色产业正逐步从个体、团体向平台发生衍变,利用平台,会成倍地提高非法活动效率、规模和破坏程度[5]。2018 年,思明警方在开展的“扫楼”行动中一举查获厦门朗誉网络科技有限公司、厦门然讯网络科技有限公司、厦门链家天下网络科技有限公司、茗皇芯(厦门)文化传播有限公司 4 家公司,捣毁了 5 个诈骗窝点,抓获犯罪嫌疑人 24 名[6]。4 家网络科技公司实行的平台化运作分工明确、精细,有高体系化、高组织化、高专业化等特点,不仅使违法犯罪的成功率大大提升,而且也提高了犯罪分子的存活率。相较于传统的简单的网络犯罪模式,“互联网 +”背景下的黑色产业中下游产业链在中上游产业链的基础上,违法成本大大降低。上中下三个产业链条相互依赖、相互生存,链条式、平台化架构,勾连不法分子,正一步步蚕食破坏网络环境,极大地危害大范围不特定的网络用户,甚至影响了社会稳定,危害到国家安全。要想全方位地解决互联网黑色产业犯罪问题,必须从源头治理、连根拔起,解决上游

产业链，遏制其上下游的交流，从而有效打击中下游产业链。

## 三、互联网黑色产业犯罪治理困境

网络技术的发展为有效防护网络犯罪带来了全新的挑战。互联网黑色产业所呈现出来的链条化、平台化、组织化、跨区域化等一系列特点为有效治理黑色产业链增加了难度。网络虚拟空间不同于现实空间，其虚拟、快速等属性是治理黑色产业链的难点所在。网络黑产犯罪与传统犯罪的不同之处在于，受害者与不法分子之间没有现实接触，这为公安机关调查取证提出了难题。产业链条中各条线路之间交叉综合、关系复杂、内外勾结，往往使公安机关无法实现精准打击，并且相关法律法规在应对新生事物的时候具有一定的滞后性，这也使得治理黑色产业链困难重重、举步维艰。

### （一）司法机关调查存证取证困难

证据裁判是现代刑事诉讼的一项基本原则。互联网黑色产业犯罪通常以电脑、手机等电子产品为主要犯罪工具，因此其证据也多数以电子数据的形式表现出来。公安机关在侦破案件、查清案件事实时必须以大量的电子证据作为支撑，法院在法庭调查阶段需要检察机关提供电子证据作为定罪量刑的依据，故电子数据的重要性不言而喻。但互联网自身的特性，使电子数据也呈现出虚拟性、脆弱性、高速传播性、可复制性及可还原性等数字时代的特点，电子数据往往会被通过隐藏、加密、删除、破坏的方式保护，无法立即获取[7]。这给司法机关取证存证带来了许多挑战。电子数据的取证人员必须具备一定的计算机技术和法律知识，才能正确而合理高效地辨别筛选出哪些属于案件审理所需要的电子数据，进而合法客观地反映案件事实。但目前我国司法机关的取证技术手段相对落后，针对性人才较少，无法与现实需求相匹配，难以满足实践需要。

### （二）产业链条关系复杂无法精准打击

错综复杂的产业链条关系往往使得公安机关在处理时无从下手，并且常常有内、外部人员相互勾结，隐瞒真相，这大大增加了执法难度。如 2019 年 11 月江苏淮安警方打击的考拉征信案件，自 2015 年 3 月起考拉征信服务有限公司涉嫌非法缓存公民个人信息多达 1 亿多条，涉案人员多达 20 余人，警方通过不断摸排调查，竟然牵扯出一条庞大的贩卖公民个人信息产业链条（图 1），而考拉征信服务有限公司只是其中一环。他们通过上游购买接口，缓存大量公民个人信息，然后贩卖给下游产业，继续进行推销贷款、暴力催收等犯罪行为[8]。

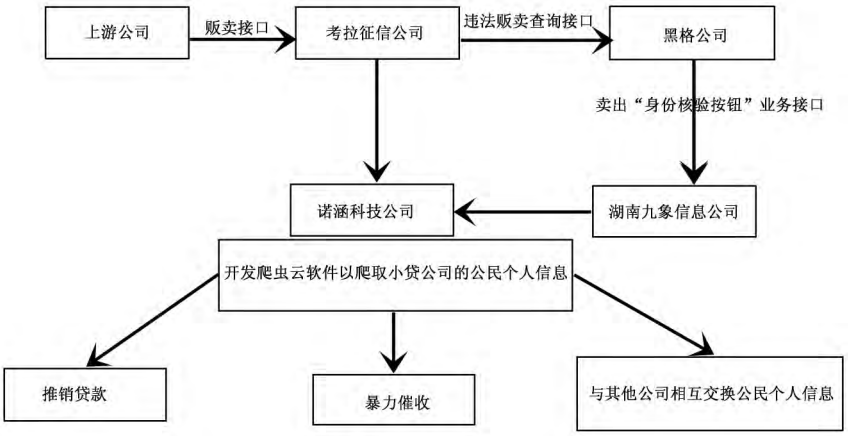


**图 1　考拉征信案黑色产业链条**

以“拖库—洗库—撞库”为主要犯罪模式的上游产业链条，与中下游产业链逐步形成一个闭环。除却纵向联合的犯罪模式，横向配合的模式也增加了整条犯罪链的复杂程度。仅仅解决单一环节的犯罪问题只是治标不治本，再加上各条产业链十分隐蔽，犯罪分子的反侦察意识又比较强，使得公安机关在侦破案件的过程中经常碰壁。

(三)网络帮助行为认定困难

当下刑法在应对新型黑色产业犯罪时存在一定的缺陷。最主要的是对于帮助行为的认定,理论界与实务界都存在一定的争议。互联网黑色产业犯罪主要可以分为 3 种类型:第一种为计算机信息系统的犯罪,是针对上游产业制作木马病毒、恶意程序、网络爬虫等侵入计算机系统的行为;第二种为破坏网络业务活动、妨害网络秩序的犯罪,主要是中间商进行数据销售的行为;第三种为利用计算机网络实施传统犯罪,主要是下游产业团伙以互联网为媒介,实施诈骗、盗窃、诽谤等传统犯罪[9]。我国刑法修正案(九)新增罪名之一"帮助信息网络犯罪活动罪"标志着网络犯罪概念的正式使用[10]。此罪也是中立帮助行为正犯化的典型表现。帮助信息网络犯罪活动的帮助者必须"明知"他人进行犯罪活动而予以帮助,但是在产业链的各个环节中,他们相互素未谋面、互不相识,如何判断"明知"成为难题。在传统的犯罪理论认知中,帮助行为的社会危害性在一定程度上要弱于实行行为。但是黑色产业链下的帮助行为的危害性丝毫不亚于实行行为。因为帮助信息网络犯罪活动罪的特征之一就是帮助对象的不确定性,再加上互联网传播信息的散发性、匿名性等特点,想要正确判断更是难上加难。

黑色产业以社会工程学和社会工程学数据库为基础,采取数据挖掘、网络渗透等手段,非法获取公民的个人身份信息、账号信息、上网轨迹、浏览内容等信息形成社会工程数据库,在"暗网"平台频繁交易、反复清洗,成为黑色产业链的源头之一[1]99。互联网黑色产业犯罪上游产业以侵害网络系统、网络数据及网络信息安全为主。在正确界定上游产业行为对于中游产业行为、中上游产业行为对于下游产业行为的帮助界限以及各环节横向帮助行为等问题上也存在界限模糊的问题。上文提到的徐玉玉案件的源头在于考生信息的泄露,杜某作为陈某购买信息的上家是整条产业链的上游关键环节,杜某的辩护人称"陈某诈骗行为与本案无关联性,恶劣社会影响的后果不应由杜某承担责任",但是法院最终不予采纳此辩护意见,法院认为杜某虽不明确知晓陈某购买其所窃取的考生个人信息的目的,但其供认自己对陈某购买考生个人信息系用于非法活动已有所怀疑,且其出售的考生个人信息客观上确被陈某用于犯罪。杜某依法应对其出售他人信息行为所造成的恶劣社会影响承担相应的责任(山东省临沂市罗庄区人民法院,2017 鲁 1311 刑初 332 号)。由中立帮助行为转为帮助行为的关键点在于"明知",但是网络是一个虚拟的、散发性的社会空间,如何准确判断"明知"还有待商议。

## 四、互联网黑色产业犯罪治理对策

在网络技术时代,治理黑色产业问题需要消除刑法万能主义的思维,多角度、全方位地有效结合各部门法,实行联合治理。网络的技术架构与规则架构是目前互联网赖以维系的两个支柱[11]。应以技术应对技术,通过大数据建设,调查分析黑色产业动态,从而实现有效打击。网络平台、运营商、网络用户也是打击黑色产业的主力军。必须完善相关法律法规,加强网络治理能力,净化网络环境。

(一)转变应对思路

刑法作为治理社会的最后一道防线,应该少用慎用,要打破刑法工具主义、万能主义的旧思维,树立正确的刑法理念。要从源头抓起、从源头治理,以解决上游技术产业链为目标进行刑事手段的设计。正所谓打蛇打七寸,上游黑色产业链作为整条产业链的龙头,以提供各种黑色科技手段、贩卖各类技术软件为特征,为下游犯罪做技术支撑,是下游犯罪的源头。应对各类黑色产业犯罪应当做好类别分析,分门别类,不能一刀切,要一切从严、从早。了解黑色产业犯罪模式是进行有效治理的前提。应对黑色产业类型的多元化,需要积极联合各部门,打造开放共治共享理念,发挥各部门法的作用,从被动治理向积极主动预防转变。要充分发挥网络平台、运营商的关键作用,加大监管力度,提高技术手段,净化平台环境,将黑色产业犯罪扼杀在摇篮里。应加大网络运营商的责任,让网络运营商不再做黑色产业的保护伞。各个网络服务商的不作为使得黑色产业屡禁不止,网络服务商作为整个链条的核心点,掌握并流通互联网所有的数据,必须严格关注流量的细节与内容,承担起数据信息安全的监管责任。要打

通各个部门之间的信息闭塞点，加强信息流通，提高运营商与网信部门的沟通交流。要发挥政府有关部门的监管作用，继续坚持网络安全法所提倡的重监管理念，提高政府治理能力、治理水平，严厉查处相关部门及有关人员滥用职权、徇私舞弊，监管不到位、执法不及时等问题。

（二）完善规范体系

针对黑色产业链犯罪的跨区域、平台化、网状式的犯罪特点，在刑事规范层面需要进一步完善现有刑事实体法与程序法关于互联网黑色产业犯罪的规定。针对司法机关调查取证难的问题，需要完善电子数据的收集方法，大力培养复合型人才，提高应对技术难题的水平，提高证据获取提取能力。由于黑色产业犯罪链分工明确，侵害对象范围广、人数多，单起案件可能涉案金额较小，无法达到犯罪构成要件的标准，无法给予刑事打击。为此需要加强非刑事法律法规的建设，以弥补单个部门法的不足。应加快“个人信息保护法”的制定脚步，将碎片化的保护方式整合起来，实现全面系统的规范保护。规范个人信息使用，压制黑色产业链生存空间，要继续完善《网络安全法》，贯彻网络实名制，增加黑色产业犯罪成本。网络注册实名制既增加了网络服务商的监管义务，也提高了不法分子的违法难度。但是对于个人违反网络实名制是否应该受到惩罚，目前的《网络安全法》尚未予以规定。我们认为应该在一定范围内适当地增加网络用户义务，进一步细化关于实名制的相关规定，为国家治理网络犯罪降低难度。网络虚拟空间的隐蔽性使得个人更加容易实施犯罪行为，逐步细化网络实名制的好处在于，将市民熟人社会转换到网络虚拟社会，增加网络空间的现实性，能为公安机关查处犯罪行为提供线索，提高破案率，为司法机关定罪量刑提供依据。但是，网络实名制也容易造成个人信息的泄露，为此必须加强对网络服务提供者的监管力度，完善网络实名制平台管理制度。此外，不能忽视行政执法在治理黑色产业中所起到的作用，因为行政执法可以有效弥补刑事手段在相关方面的不足。行政执法是法治的基本要素，缺乏执法，立法的调控社会关系的目的无从实现[12]。相关行政部门的执法能力不足，在相关治理活动中缺乏内在动力也是导致黑色产业泛滥的原因之一。因此，相关行政主管部门必须发挥带头作用，及时出台相关规范性文件，明确有关黑色产业的类型、特征及主要防治办法和应对措施。当网络运营商出现履行义务不到位、不及时等问题时，要及时予以告诫，并视情节严重情况予以处罚。应构建以网络安全法、个人信息保护法、电子商务法、互联网信息服务法以及电信法为核心的网络犯罪治理规范体系，为依法治理黑色产业犯罪提供法律依据[13]。

（三）创新治理机制

提高犯罪治理的智能化水平是大数据时代背景下治理黑色产业犯罪的有效手段之一。以技术手段应对技术犯罪是创新治理黑色产业犯罪机制的核心所在。为此，必须构建黑色产业犯罪数据平台，时刻监管黑色产业犯罪状态和趋势，打造国家级重点治理中心，以应对跨区域、大范围的黑色产业犯罪。充分利用人工智能、区块链等先进技术手段进行提前防控，为保障全社会应对黑色产业犯罪提供技术支持。通过技术手段检测各平台数据异常表现，搭建自动识别平台，感知数据异常时主动发布预警信息的系统指令。要充分发挥企业大数据优势，协助警方进行数据分析、数据调查、数据匹配和线索固定，实现预防黑色产业犯罪前置化，由消极应对转变为积极预防。治理黑色产业也需要发挥“组合拳”的作用，充分要吸纳社会力量，形成各方参与治理的新态势，实现社会共同治理。治理黑色产业犯罪已逐步成为广大人民群众共同的任务，网络安全是保障国家安全的重要组成部分，需要联合政府部门、科研人员、企业以及广大人民群众的力量。各大科研院所需积极培养复合型人才，为应对技术犯罪添砖加瓦，为彻底解决黑色产业犯罪储备相关人才；相关企业要积极主动配合公安机关，实现“企业 + 公安”的双元治理体系；要提高公民的法律素养，增强公民网络安全意识。目前由于社会群众包括相关企业对网络安全以及个人信息保护意识较薄弱，给不法分子实施网络黑色产业犯罪创造了机会，使不法分子提高了犯罪成功率，政府、电商、网络平台应肩负起文明上网的宣传义务，时刻提醒人们文明上网，禁止浏览黄色网站、禁止发布不良言论、禁止下载攻击软件等。网络黑色产业犯罪中的被告

大多为十八九岁的年轻人,他们存在一定的认知缺陷,容易走上违法犯罪道路,因此应提前予以应对。此外还要加强与世界接轨,网络世界就是虚拟的地球村,应联合世界各国共同应对黑色产业犯罪,实现资源共享、人才交流等,及时准确地掌握国际黑色产业犯罪动态,实现联合治理。

## 五、结语

互联网黑色产业犯罪是一个动态的、类型化的新型网络犯罪模式。刑法在应对新鲜事物时既要掌握限度也要敢于突破。治理黑色产业犯罪并不是一蹴而就的,而是一个长期的治理过程,也不是单靠某一方力量就能解决问题,需要发挥社会整体力量,遵循共享共治的新模式,要抓住产业犯罪的源头,遏制上游产业链条,逐个击破。为有效应对变化莫测的新型黑色产业犯罪,我们必须转变传统治理思路,坚持联合治理理念,完善规范体系,从技术层面与规范层面共同打击黑色产业犯罪。

## 参考文献


[1] 袁丽欣,顾益军,次仁罗布. 互联网黑色产业现状分析与对策研究[J]. 北京警察学院学报,2018(6):98-102.

[2] 公安三所网络安全法律研究中心. 2019 年网络犯罪防范治理研究报告[R/OL]. [2020-02-15]. https://www.secrss.com/articles/16003.

[3] 司法大数据专题报告:网络犯罪特点和趋势[EB/OL]. [2020-02-13]. https://www.sohu.com/a/354923998_100002800.

[4] 刘艳红. 论刑法的网络空间效力[J]. 中国法学,2018(3):89-109.

[5] 赵丽莉,马可,马民虎. 网络黑色产业链负外部影响及其治理研究[J]. 情报杂志,2019(10):96-103,118.

[6] 林利萍. 思明警方百余警力"扫楼"捣毁 5 个诈骗窝点刑拘 24 人[EB/OL]. (2018-12-31) [2020-02-15]. http://www.taihainet.com/news/xmnews/gqbd/2018-12-31/2219905.html.

[7] 陈利明,高瑛,任艳丽. 网络犯罪案件办理中的取证困境与对策:以"一元木马"系列网络诈骗案为例[J]. 人民检察,2018(6):22-25.

[8] 涉嫌泄露亿条公民信息 考拉征信被查[EB/OL]. (2019-11-21) [2020-02-15]. http://finance.ce.cn/bank12/scroll/201911/21/t20191121_33663168.shtml.

[9] 陈兴良. 互联网帐号恶意注册黑色产业的刑法思考[J]. 清华法学,2019(6):13-25.

[10] 刘艳红. 网络犯罪的刑法解释空间向度研究[J]. 中国法学,2019(6):202-223.

[11] 刘宪权. 网络犯罪的刑法应对新理念[J]. 政治与法律,2016(9):2-12.

[12] 张新宝,葛鑫. 基于个人信息保护的电信诈骗综合治理研究[J]. 中共中央党校学报,2016(5):42-49.

[13] 赵秉志. 构建新型网络犯罪防治体系[N]. 人民日报,2017-11-13(07).


责任编辑:庄亚华