理论前沿

Web3.0 时代网络犯罪的代际特征及刑法应对

刘艳红

内容提要:网络犯罪与网络科技同步经历了 web1.0 到 web2.0 再到 web3.0 的迭代共生发展,并呈现出不同代际特征。不同于物理性的 web1.0 和 web2.0 时代,web3.0 时代的最大特征是智能性,个性化、互动性和精准应用服务的网络空间也成为犯罪空间,各种新型犯罪层出不穷,同时又兼有 1.0 与 2.0 时代网络犯罪的特征。如何界定复杂的侵害法益、追责对象以及定罪标准,是 web3.0 时代网络犯罪对刑法适用的挑战。与之相适应,刑法理论应确立实质损害标准来解决侵犯网络空间秩序行为是否构成犯罪,以具有法益侵害性结果为导向强化网络犯罪平台而非个人责任追究,以升维打击而非降维打击确立网络犯罪的定罪标准,从而有效解决 web3.0 时代网络犯罪及刑法规制问题。

关键词:网络犯罪　法益侵害　平台责任　定罪标准

刘艳红,东南大学法学院教授。

犯罪是一种社会现象,“不同的社会中犯罪行为的流行形式也是不同的;不同社会的犯罪控制机构也有明显的不同”。[1] 当下社会是科技时代,互联网成为生活的主要方式甚至等同于生活本身,网络改变了生活也改变了犯罪行为的形式。网络科技已历经 web1.0 到 web2.0 再到 web3.0[2]的发展变化,网络犯罪相应经历了不同代际的迭代升级。网络时代犯罪行为的形式区别于传统社会犯罪形式,其对刑法适用提出诸多新的挑战。为此,应将网络犯罪根植于网络科技的代际变化之中,总结出各代际网络犯罪的特点及变化,推动刑法理论因应“科技时代传统刑法理论与新问题之间的关系”问题,[3]促进网络犯罪研究的纵深化发展。

〔1〕 [美]迈克尔·戈特弗里德森、[美]特拉维斯·赫希著:《犯罪的一般理论》,吴宗宪、苏明月译,中国人民公安大学出版社 2009 年版,第 161 页。

〔2〕 Web(World Wide Web),全球广域网,又称万维网,是一种基于超文本和 HTTP 的、全球性的、动态交互的、跨平台的分布式图形信息系统。web1.0、web2.0、web3.0,也可称为互联网 1.0、互联网 2.0、互联网 3.0。科技界一般使用 web1.0/2.0/3.0 的简称,以此代表互联网迭代演进的三个不同时代。

〔3〕 参见刘艳红:《刑法理论因应时代发展需处理好五种关系》,《东方法学》2020 年第 2 期,第 6 页。

一　Web1.0/2.0 时代网络犯罪的代际特征:物理性

如同计算机犯罪的概念是伴随着计算机的出现而出现,网络犯罪的概念也是伴随着网络的出现而出现的。1969 年 10 月,美国“因特网之父”莱昂纳德·克莱因罗克首次把加利福尼亚大学洛杉矶分校的一台电脑和一家研究机构的一台电脑连接起来,并让它们“交谈”,成为互联网的雏形;1983 年 TCP/IP 协议成为全球互联网的标准协议时,计算机之间的连接(也即终端连接)才通行世界,全球性的终端连接真正开始。〔4〕 1991 年,我国建成第一条与国际互联网连接的专线;1994 年,我国实现与国际互联网的全功能连接,开启了真正意义上的中国互联网时代。在国际与中国互联网发展的三十年左右的时间里,瑞达网络公司的创始人诺瓦·斯皮瓦克(Nova Spivack)以 10 年为一个周期,将网络发展的第一个十年(1990 - 2000)作为“信息单向发布的 web1.0 时代”,第二个十年(2000 - 2010)视为“互动参与的 web2.0 时代”。〔5〕 与之相适应,这两个时代的网络犯罪也呈现出相应的代际特征,而它们共有的代际特征则是:物理性。

其一,web1.0 时代网络犯罪的代际特征是物理性,具体是犯罪对象与犯罪方法上的物理性。web1.0 时代,人与网络的关系是单向传播的,即网站编辑信息发布给网民,网民只是单纯地被动接受网站发布的信息,和网站没有任何互动。网站就好比公告牌,只不过它是数据海量的电子公告牌,而且会不断提供更新。〔6〕 网民用户与网络之间的关系类似于读报,用户是读者、接受者,电脑屏幕是“报纸”,上网不过是传统生活的网络延伸。在 web1.0 时代,网络是一种新事物,各大门户网站备受欢迎,新浪、搜狐、网易、腾讯等适时兴起,IE 浏览器也是浏览网页的主要工具。由于网络以计算机为媒介充当着“报纸”的作用,决定了此一阶段的网络犯罪只能是以网络或计算机作为损坏对象,犯罪方法也呈现物理性特征。web1.0 时代常见的物理性破坏是针对计算机的安全系统。计算机系统包括各个系统运转的电网,还包括防火墙以及计算机内部内容。透过防火墙连接外面的世界就要借助 TCP/IP 协议开发出来的因特(Inter),但是因特需要通过局域网系统往外突破。若要获得计算机内部的资料、重要机密文件等内容,则需打开数据库。为了用户信息安全和计算机自身安全,就必须要设置防火墙,防火墙是在“内部网与外部网之间实施安全防范”的系统,能够加强网络间访问控制,组织未授权的外部网信息传输,保护内部网的安全,免受非法用户侵入。〔7〕 而防火墙的防范并非万无一失,总有系统漏洞存在并被计算机犯罪高手所运用。系统安全漏洞,也叫系统脆弱性,广义而言是导致损害、威胁计算机信息系统的因素。“它是计算机系统在硬件、软件、协议的设计与实现过程中或系统安全

〔4〕 参见彭兰:《“连接”的引进——互联网进化的基本逻辑》,《国际新闻界》2013 年第 12 期,第 6 - 19 页。

〔5〕 刘琼、任树怀:《论 web3.0 下的信息共享空间》,《图书馆》2011 年第 2 期,第 83 页。

〔6〕 参见倪颖杰、王律科等:《基于高性能数据挖掘的网络海量信息处理平台》,《计算机工程与科学》2009 年第 A1 期,第 129 - 132 页。

〔7〕 参见罗明宇等:《计算机网络安全技术》,《计算机科学》2000 年第 10 期,第 63 - 65 页。

策略上存在的缺陷和不足;非法用户可利用系统安全漏洞获得计算机系统的额外权限,在未经授权的情况下访问或提高其访问权,破坏系统,危害计算机系统安全。"[8]因此,这一阶段网络犯罪刑法适用主要涉及两个罪名,即《刑法》第 285 条非法侵入计算机信息系统罪和第 286 条破坏计算机信息系统罪。总之,web1.0 时代的网络犯罪具有一些明显的犯罪特点:对象固化为物理性的介质即计算机和信息系统。此时的网络犯罪行为跟网络无关而是计算机犯罪。犯罪行为主要为物理性方法,即强行地破坏信息系统或称之为强行攻陷,而非通过软件数据的篡改进入,因此这一阶段的网络犯罪在技术侦查与取证方面相对较为容易,案件定性也比较简单。然而,与此同时,立法上滞后所导致的传统计算机犯罪罪名及处罚漏洞日益明显,口袋罪成为这个时代计算机犯罪适用的趋势。

其二,web2.0 时代网络犯罪的代际特征也是物理性,具体是犯罪工具上的物理性。web2.0 时代,人与网络的关系类似于开会,网民与网民,网站和网站之间可进行双向交流互动。[9] 网络不再是简单的信息发布者,而发展成为社交平台、人人网、维基网、天涯社区、博客、百合网等成为人与人之间沟通的重要平台,"就连一些垂直平台也融入了社交功能,淘宝的阿里旺旺就是一个很好的例证"。[10] 网民不再是单纯从网络接收信息,而是通过人与网络之间的互动,最终达到人与人之间的互动。所以 web2.0 时代在以往人和机器之间互动的基础上,发展出了人和人之间的具有即时性、便捷性的双向互动,类似于不同人在一个会场开会。人们上网,不再是简单地将传统生活延伸到网络,而是通过时时互动和交流,使传统生活在网络上发展为新的形态,如天涯社区、QQ 的个人空间等成为网民保留自己隐私的重要方式,从而取代传统社会隐私保留的方法。与 web2.0 时代相适应,此一阶段的网络犯罪,呈现出传统犯罪的网络异化,"网络替代计算机信息系统上升为犯罪工具,网络因素快速介入几乎所有的传统犯罪之中",[11]网络由此成为传统犯罪物理性的犯罪工具或者说媒介。也因此,web2.0 时代网络犯罪的代际特征也为物理性,只不过是以网络作为犯罪工具意义上的物理性。web2.0 早期阶段,"在即时通信和社区网络服务系统中还没有合适的方式或方法能够用来在好友或组成员间共享计算机或其他智能设备的 CPU、内存、磁盘、应用软件及其他资源或能力",[12]用户更多倾向于利用计算机现有资源或能力,在一定程度上缺少"他有我无"的这种共享机制。因此,在这一阶段,计算机系统仍然有受到网络攻击的威胁,并且威胁网络安全的原因来自多方面。计算机系统可能会受到非法入侵者的攻击,各类数据可能遭到泄露或者进行非法交易,"从内部网向共网传送的信息可能被他人窃听或篡改"等。[13] web2.0 时代不同于 1.0 时代由各门户网站平台主导内容生成,它是由用户主导内容生成的互联网产品模式,而这一模式主要是因为采用了 AJAX 应用技术,"借助 AJAX 可以将笨拙的 Web 界面转化成强交互性的

〔8〕 翟钰、张玉清等:《系统安全漏洞研究及数据库实现》,《计算机工程》2004 年第 8 期,第 68 页。
〔9〕 参见董慧、唐敏:《语义检索在 Web2.0 环境下的应用探讨》,《中国图书馆学报》2011 年第 3 期,第 115 - 116 页。
〔10〕 刘岩:《技术升级与传媒变革:Web1.0 到 Web3.0 之路》,《电视工程》2019 年第 1 期,第 45 页。
〔11〕 于志刚:《网络思维的演变与网络犯罪的制裁思路》,《中外法学》2014 年第 4 期,第 1049 页。
〔12〕 崔金红、王旭:《能力共享架构及其在 IM 和 SNS 中的应用研究》,《计算机科学》2008 年第 12 期,第 73 页。
〔13〕 参见金雷、谢立:《网络安全综述》,《计算机工程与设计》2003 年第 2 期,第 20 页。

AJAX 应用程序”。[14] 传统的网络应用采用同步交互过程,用户向 HTTP 服务器发出请求,服务器接收请求后向用户返回一个 HTML 页面。[15] 在这个过程中,用户等待时间较长,交互体验比较不理想。相比较而言,在 web2.0 时代,强调服务器与客户端的交互过程,服务器能够较为迅速地响应用户需求,并减少等待时间,糟糕的用户体验得到较大改变。此外,二者的核心区别在于从“外部应用”到“核心内容”的变化,用户从简单的浏览搜索获取信息发展成网络平台的交互行为,网络内容的建立者也由计算机专业人员转向全部用户。[16] web2.0 时代的网络平台特征,决定了这一时期的网络犯罪,基本上都是利用 web2.0 时代下交互的及时性,使用网络平台作为犯罪工具的。因此,此一时期各类利用网络作为物理性工具的犯罪飞速增加。[17]

其三,随着 web2.0 的快速发展,刑法中几乎所有的犯罪都出现了网络化,几乎所有的传统犯罪都可以利用网络实施,网络作为犯罪工具的物理属性被放大到极致。颜某凡盗窃案是 web2.0 时代利用网络作为犯罪工具的常见类型。[18] 该案被告人利用网络公司骗取被害人网络游戏账号安全码,非法进入被害人账号,窃取被害人在网络游戏中的虚拟装备并出售给他人获利。同一时期,类似案件大量发生。在这些案件中,作为 web1.0 时代网络犯罪对象物理性的主要特征退居其后,行为人犯罪的对象是游戏装备等虚拟财产,而不再是物理性的计算机及信息系统,作为物理性的客体而存在的计算机及信息系统仍然完好,被侵犯的只是虚拟性的财产。但是,行为人的作案工具却是真实存在的物理性网络,借助网络系统,行为人才得以登录他人账号并实施犯罪。在此,行为人实施的是传统盗窃犯罪,只不过利用了网络为犯罪工具,从而充分体现了 web2.0 时代的以网络作为犯罪工具的物理性代际特征。整个 web2.0 时代,网络犯罪主要都是以网络作为犯罪工具来实施传统犯罪。传统杀人、抢劫、绑架、盗窃、诈骗等犯罪经历了网络异化,涉财犯罪爆发性增长,帮助犯地位凸显。与之相适应,2000 年 12 月 28 日全国人大常委会通过《关于维护互联网安全的决定》,对这一时期将网络作为犯罪工具而实施犯罪的问题做了解释,从而使利用网络实施传统犯罪如何适用刑法问题得到了解决。web2.0 时代网络之所以成为实施传统犯罪的工具,出现传统犯罪的网络异化与大爆发,是因为“Web2.0 时代要求为用户提供的服务具备体验性(Experience)、沟通性(Communicate)、差异性(Variation)、创造性(Creativity)和关联性(Relation)”,[19] 而社交媒体的爆发和人们通过网络实现的人

〔14〕 吴吉义、平玲娣:《Web2.0 主流应用技术——AJAX 性能分析》,《计算机工程与设计》2008 年第 8 期,第 1913 页。AJAX 技术,是指“Asynchronous Javascript And XML”(异步 JavaScript 和 XML),它是一种创建交互式网页应用的网页开发技术。

〔15〕 参见吴吉义、平玲娣:《Web2.0 主流应用技术—AJAX 性能分析》,《计算机工程与设计》2008 年第 8 期,第 1914 页。

〔16〕 参见孙茜:《Web2.0 的含义、特征与应用研究》,《现代情报》2006 年第 2 期,第 69 - 70 页。

〔17〕 参见南京市雨花台区人民法院(2013)雨刑初字第 126 号刑事判决书、哈尔滨市宾县人民法院(2015)宾刑初字第 254 号刑事判决书;罗书臻:《最高法院公布利用网络侵害妇女未成年人犯罪案例》,《人民法院报》2014 年 10 月 22 日第 1 版。

〔18〕 参见广州市天河区人民法院(2005)天法刑初字第 1230 号刑事判决书、广东省广州市中级人民法院(2006)穗中法刑二终字第 68 号刑事裁定书。

〔19〕 李德仁、胡庆武:《基于可量测实景影像的空间信息服务》,《武汉大学学报(信息科学版)》2007 年第 5 期,第 377 页。

和人之间的时时互动,使得利用网络实施犯罪极为便捷,由此导致了利用 TCP/IP 协议为犯罪工具,亦即犯罪工具意义上的物理性,成为 web2.0 时代网络犯罪的主要代际特征。

总之,web1.0 时代网络犯罪是以计算机及其系统为物理性对象兼物理性方法而实施;web2.0 时代网络犯罪则是以网络作为物理性犯罪工具,并出现以涉财案件为主的传统犯罪的网络异化。无论是物理性对象还是物理性工具,web1.0 与 web2.0 时代,网络犯罪的共有特性都是物理性。该阶段的网络安全治理,主要是计算机及其系统的安全保护。

二 Web3.0 时代网络犯罪的代际特征:智能性

web3.0 是在 web2.0 的基础上发展起来的,它能够满足网民对于生命深度体验的心理需求,更好地体现网民的劳动价值,并且能够实现价值均衡分配。[20] 伦斯勒理工学院副教授吉姆·亨德勒(Jim Hendler)将 2008 年确定为 web3.0 时代的开端,[21] 同时,斯皮瓦克认为,web3.0 是"网络发展的第三个 10 年,即 2010 年至 2020 年",它"就是统计学、语言学、开放数据、计算机智能、集体智慧和用户在网上生成的内容全部集合到一起"。[22] 当我们有了移动终端的时候,就全面步入了万物互联时代,也就是 web3.0 时代。目前,中国的手机网民规模达 8.97 亿,网民中使用手机上网的比例由 2018 年底的 98.6% 提升至 2020 年 3 月的 99.3%,手机上网已成为网民最常用的上网渠道之一。[23] 这意味着,web3.0 是全方位互动的时代。3.0 时代的特征是个性化、互动性和精准的应用服务。用户的应用体验与分享,对网站流量和产品营销具有决定性作用。[24] 网民和网络之间在衣食住行等各个层面全方位紧密结合。以个人终端(手机)为中心点出发与整个网络世界进行信息互动。网络对用户了如指掌,替用户进行资源筛选、智能匹配,直接给用户答案。上网既不是 web1.0 时代传统生活在网络的简单延伸,也不是 web2.0 时代传统生活在网上的异化,而是在传统物理社会空间之外,多出一个网络社会空间,人们在网络空间中全方位量身定制想要的生活。web1.0 时代的"读报纸"到 web2.0 时代的"开会"终于发展到了 web3.0 时代"私人定制"。这个时代,不再是人找信息而是信息找人,[25] 智能性成为这个时代的典型特性。

一方面,web3.0 时代的网络是虚拟的社会空间,也是犯罪空间。万物互联的 3.0 时代,网络社会空间作为独立于物理空间的存在,也被犯罪人充分利用,言论犯罪、传播淫秽物品犯罪等以网络作为空间的犯罪盛行。还有非法经营罪等以网络为经营场所的罪名同样高发。传统犯罪场所从物理空间转移到了网络空间。比如,王某开设赌博网站案,王

〔20〕 参见刘畅:《网人合一·类像世界·体验经济——从 Web1.0 到 Web3.0 的启示》,《云南社会科学》2008 年第 2 期,第 83 页。

〔21〕 J. Hendler, W. Hall and N. Contractor, Web Science: Now More Than Ever, *Computer*, vol. 51, no. 6, 2018, pp. 12 – 17.

〔22〕 周易君编著:《web3.0 时代的服装网络营销:理论与营销》,经济日报出版社 2016 年版,第 3 页。

〔23〕 参见中国互联网络信息中心(CNNIC):《中国互联网络发展状况统计报告》2020 年 4 月,第 19 页。

〔24〕 参见崔婉秋、杜军平:《基于用户意图理解的社交网络跨媒体搜索与挖掘》,《智能系统学报》2017 年第 6 期,第 761 – 762 页。

〔25〕 参见殷慧霞:《web3.0 及其教育应用探究》,《信息技术与信息化》2018 年第 6 期,第 163 页。

某与他人合伙在网络上开设某互联网赌博网站,并雇用他人利用微信等移动通讯终端招揽众多赌徒向该网站投注,进行彩票网络投注赌博活动。[26] 本案中王某行为的发生地点即为网络空间而非物理世界的某个场馆。再如,最高人民法院第 20 批指导性案例 105 号洪某某、李某某等开设赌场案等,[27]这些案例都是利用网络空间而实施的犯罪行为。同时,作为独立空间的 web3.0 时代的网络空间,各种资源应有尽有,网民既是网络世界的受众,又是网络世界的主宰。网民对网络的参与重在体验对整个网络世界的生存、生长、生活的感觉。这也是为什么现在的很多软件都是免费的,电脑一开机,软件就会自动启动,依靠发布广告、做代理获得利润,这也是 web3.0 时代流量经济的产物。也因此,流量劫持、域名盗窃、深度链接等新型网络空间违法犯罪行为才会层出不穷。比如张某等人诈骗案。[28] 张某通过互联网购买一个网络游戏装备交易平台程序,并对该程序进行修改,再通过互联网向域名提供商和网站空间提供商分别购买域名使用权和网络空间使用权,将修改后的网络游戏装备交易平台程序上传到他人购买的网上虚拟空间运行发布,诱骗玩家到其网游交易平台网站中注册充值购买游戏装备,并通过第三方支付平台、网上银行转账等方式骗取钱财。由此可见,传统犯罪在 web3.0 时代,已经进入网络空间进行犯罪。传统犯罪既可以在物理世界实施,又可以在网络空间实施,现代社会正式步入双层社会时代。

另一方面,web3.0 时代的网络犯罪是以人工智能和大数据为特征的智能化网络科技犯罪。web3.0 的特征就是人工智能、关联数据和语义网的构建,[29]“智能时代是由大数据与人工智能等技术驱动发展的时代”,[30]通过搜索引擎对大数据的优化搜索,从而形成人和网络、人与人之间的沟通。人工智能则是通过人来训练机器、不断实现人的智慧,实现机器自己学习、迭代、发展。关联数据,是指数据网络上以结构化形式存在的数据集合体,它们能够被语义化网络所管理。语义网,是一种智能网络,它不但能够理解词语和概念,而且还能够理解它们之间的逻辑关系,可以使交流变得更有效率和价值。语义网的构建是通过人工智能识别数据实现人和人之间沟通的便利性。[31] 通过人工智能、关联数据和语义网,智能型平台海量收集大数据,并通过开发人工智能应用平台,使机器自动学习,帮助行为人精准实施犯罪,犯罪行为的实施已超脱人工阶段。在 web3.0 时代,“物联网依托多种信息获取技术,包括传感器、射频识别(Radio Frequency Identification,RFI)、二维码、多媒体采集技术等,其关键技术环节可以归纳为感知、传输、处理,数据处理和融合贯穿于物联网采集、控制、传输和上层应用的全过程”。[32] 比如全国首例 AI 犯罪中,以黄某

〔26〕 参见张小虾等:《开设网站供他人进行彩票投注该定何罪》,《检察日报》2019 年 6 月 2 日第 3 版。

〔27〕 参见赣州市章贡区人民法院(2016)赣 0702 刑初 367 号刑事判决书。

〔28〕 参见贵州省高级人民法院(2015)黔高刑二终字第 27 号刑事裁定书。

〔29〕 J. Hendler, Web 3.0 merging, *Computer*, vol. 42, no. 1, 2009, pp. 111 – 113.

〔30〕 周佑勇:《智能技术驱动下的诉讼服务问题及其应对之策》,《东方法学》2019 年第 5 期,第 14 页。

〔31〕 N. Shadbolt, W. Hall and T. Berners-Lee, The Semantic Web Revisited, *IEEE Intelligent Systems*, vol. 21, no. 3, 2006, pp. 96 – 101. 语义网(Semantic Web)由蒂姆·博纳斯一李(Tim Berners-Lee)1998 年提出,是 web3.0 时代的重要特征之一,意味着能使整个互联网成为一个通用的信息交换媒介。

〔32〕 王兴伟、李婕等:《面向“互联网 +”的网络技术发展现状与未来趋势》,《计算机研究与发展》2016 年第 4 期,第 733 页。

为首的团伙先非法获取网站后台用户数据,再将数据卖给下线。然后以吴某为代表的制作撞库软件团伙,通过“快啊”平台软件验证所盗来的账号密码是否匹配。该团伙将成功匹配的账号密码贩卖给其他网络诈骗团伙,对方再利用获取的账号实施各类网络诈骗和非法推广等违法活动。[33] 本案中,“快啊”具有深度学习的功能,效率和准确率远超过人工方式。基于“智能搜索、个人化空间和用户兴趣模型”的互联网 3.0 时代,具有“信息的聚合以及提供个性化的信息服务”功能,能够通过人工智能学习和数据挖掘等新技术手段,提炼出用户个性化的信息聚合,使得人机交互、人人交互更具有人类特征和个性特征。[34] 智能化的结果是,web3.0 时代的网络犯罪,在日益向网民提供个性化精准性应用服务的同时,网络平台的犯罪参与度也大为提高,网络犯罪的追责重点似乎发生了转移。

总之,与 web3.0 网络时代相适应,此一阶段的网络犯罪,主要是发生在网络空间领域,且是以人工智能和大数据为特征的智能化网络科技犯罪,同时各种新型犯罪层出不穷。如何对它们进行准确定性并精准地实现 web3.0 时代的刑法规制,在理论和实务中均面临着巨大挑战。

三 Web3.0 时代网络犯罪刑法适用的挑战及解决路径

web3.0 时代并非隔绝 web1.0 和 2.0 时代而生,在科技断代上,前者是后者的延续。在犯罪断代上,前者是后者的迭代更新。因此,web3.0 时代的网络犯罪除了智能性之外,还具有复杂性,即基于 web1.0 和 2.0 时代网络犯罪残留的物理性以及 web3.0 时代的智能性混合而成的特性。为此,下文基于科技与犯罪的迭代共生性,结合新型网络失范行为,对兼容了 web1.0 和 2.0 时代的 web3.0 时代网络犯罪刑法适用的挑战与解决路径进行探讨。同时,这种挑战不是基于智能性的 web3.0 时代而去制造人工智能法学研究中的“假问题”,而是基于刑法教义学立场讨论其在刑法适用中的真问题。[35]

(一)网络空间秩序法益遭受实质损害方可定罪

复杂的 web3.0 时代的犯罪以网络作为犯罪空间,那么,是否侵犯网络空间秩序的行为就是犯罪?该问题涉及是否网络空间秩序法益受到侵害就能产生刑事可罚性的问题。对此,刑法理论的回应是,网络空间秩序法益受到侵害并不一定产生刑事可罚性,只有在法益侵害达到实质危害的程度时才能构成犯罪。

从 web3.0 时代开始,社会演变为双层社会空间,即现实的物理世界与虚拟的网络世界。犯罪一方面在现实社会空间发展,同时也在网络空间发生。而发生在网络空间的犯罪行为,侵犯的法益是网络秩序还是现实社会的公共秩序?有学者认为,网络秩序就是社会的公共秩序,网络空间也是刑法中的“公共场所”;社会公共秩序分为现实社会公共秩

〔33〕 参见王春:《绍兴警方侦破首例利用 AI 犯罪案》,《法制日报》2017 年 9 月 26 日第 8 版。
〔34〕 参见熊回香、陈姗等:《基于 Web3.0 的个性化信息聚合技术研究》,《情报理论与实践》2011 年第 8 期,第 96 页。
〔35〕 参见刘艳红:《人工智能法学研究中的反智化批判》,《东方法学》2019 年第 5 期,第 119、123 页。

序和网络虚拟社会公共秩序，侵犯了网络秩序的行为当然也就侵犯了社会的公共秩序。[36] 相关司法解释也肯定了这一观点。2010 年 8 月 31 日最高人民法院、最高人民检察院（下称“两高”）、公安部《关于办理网络赌博犯罪案件适用法律若干问题的意见》第 1 条规定，利用互联网、移动通讯终端等传输赌博视频、数据，组织赌博活动，构成开设赌场罪。2013 年 9 月 9 日“两高”《关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》第 5 条规定，“利用信息网络辱骂、恐吓他人，情节恶劣，破坏社会秩序的”；“编造虚假信息，或者明知是编造的虚假信息，在信息网络上散布，或者组织、指使人员在信息网络上散布，起哄闹事，造成公共秩序严重混乱的”，以寻衅滋事罪定罪处罚。毫无疑问，这两个司法解释肯定了网络作为犯罪空间的属性。无论是互联网网站、微博或是其他社交媒体工具如 QQ、微信等，网络空间都和现实物理空间一样具有公共场所属性，这在法理上并无问题。但是“刑法与法益保护的关系”并不是“在法益受到侵害的时候”就能“产生刑事可罚性”，[37] 侵犯网络空间秩序的行为不一定就是犯罪，只有法益侵害达到了应受处罚的程度，亦即具备值得处罚的法益侵害性程度 [38] 才能定罪处罚。与现实物理世界的犯罪一样，网络空间的犯罪行为也分为自然犯和法定犯。针对网络领域的自然犯与法定犯，如何判断行为是否达到了实质上值得处罚的程度则并不相同。

对于网络领域的自然犯，侵犯网络空间秩序这一虚拟法益不一定构成犯罪，应基于自然犯对公民人身健康、财产等实体法益的侵犯才能认定犯罪成立与否。一般而言，自然犯难以在虚拟的网络领域实施，比如故意杀人罪，虽然它们可以借助网络作为工具，比如通过网络约定见面时间与地点再实施杀人犯罪行为等，但这些犯罪属于利用网络作为手段或工具实施的犯罪，而不是侵犯网络空间秩序的犯罪，比如 2014 年 10 月 21 日，最高人民法院发布七起通过网络实施的侵犯妇女、未成年人等犯罪的典型案例均是如此。但是，自然犯中某些犯罪仍然可以产生对虚拟的网络空间秩序法益的侵犯。比如，《刑法》第 237 条第 1 款强制猥亵、侮辱罪以及第 3 款的猥亵儿童罪，《刑法》第 246 条的侮辱罪、诽谤罪，第 249条煽动民族仇恨、民族歧视罪，以及网络空间发生的财产犯罪等。侵犯网络空间秩序并不必然导致公民人身法益受到侵害，只有同时侵犯了物理世界公民的人身或财产等法益时，相关自然犯才能成立犯罪。实务中也有因在网络领域实施自然犯而被定罪的案例，但其定罪根据仍然在于侵犯了现实法益而非网络秩序法益。比如，骆某网络猥亵儿童案。[39] 猥亵儿童罪的法益是儿童的人身权利中的性权利与人格尊严，被告人将儿童裸照上传确实侵犯了儿童的人格尊严，尤其是当其以此要挟被害人见面意图猥亵对方时，其对儿童人身法益的侵害已达到应受刑罚处罚的程度。

网络领域法定犯的定罪标准不同于自然犯。法定犯本身侵犯的就是各类社会秩序，包括国家安全管理秩序、公共安全管理秩序、市场经济管理秩序、司法活动管理秩序，而所

〔36〕 参见于志刚：《网络思维的演变与网络犯罪的制裁思路》，《中外法学》2014 年第 4 期，第 1052 页。

〔37〕 ［德］克劳斯·罗克辛著：《德国刑法学总论》（第 1 卷），王世洲译，法律出版社 2005 年版，第 18 页。

〔38〕 参见刘艳红：《实质刑法观》（第二版），中国人民大学出版社 2019 年版，第 220 页。

〔39〕 参见最高人民检察院 2018 年 11 月 9 日发布的《关于印发最高人民检察院第十一批指导性案例的通知》（检例第 43 号）。

有这些秩序,其实就是广义的社会管理秩序。当其在网络空间实施时,自然都侵犯了网络空间的管理秩序。但是,只有在综合考量后确定侵犯网络空间秩序的行为具有现实危害性或者至少是紧迫的现实危害性时才能考虑构成犯罪。网络领域的法定犯可分为两种类型。一种是借助网络作为犯罪工具实施犯罪,体现的是 web2.0 时代的传统犯罪网络异化之特征,也是 web3.0 时代网络犯罪的复杂之处。比如网络毒品犯罪、恐怖犯罪,网络的发达使得这些犯罪的成本大为降低,支付手段更为便捷,组织犯罪在网络视频平台的帮助之下更为容易,但是这类犯罪侵犯的主要法益仍然是物理空间秩序,比如毒品管理秩序与社会公共安全,虽然也涉及对网络空间秩序的侵犯,但网络只是工具与手段,侵犯网络秩序不是目的。因此,对于这些犯罪的认定仍应秉承传统物理空间的危害性标准。另一种才是真正的侵犯网络空间秩序的犯罪,比如寻衅滋事罪、开设赌场罪、聚众淫乱罪等,它们才体现了前述 web3.0 时代的网络是虚拟社会空间因而也是犯罪空间之特性。对于这些法定犯而言,刑法要秉承谦抑主义,避免将侵犯网络空间秩序作为犯罪认定的主要标准,而要综合考量侵犯网络秩序的行为是否具有现实的危害性或者紧迫的现实危害性。基于法定犯存在“法益性欠缺”的先天不足,[40]对于侵犯网络空间秩序的法定犯,不宜仅仅因为对规范的不服从就认定为犯罪。近几年来,侵犯网络空间秩序行为被定罪的典型罪名是寻衅滋事罪,比如秦某寻衅滋事案、[41]张某甲寻衅滋事案[42]等。虽然司法机关认为,“网络空间并非法外之地,国家法律保护信息网络中正常的、合法的言论和信息交流活动,打击利用信息网络实施破坏社会公共秩序、市场经济秩序的犯罪行为”,[43]因而将这些在网络领域散发不当言论扰乱网络空间秩序的行为认定为犯罪。但是,仔细分析这些案例,案件中的被告人或是因为关注社会事件或是认为自己遭受不公或是因为对公共事务的处理不公等存在异议,且通过正当途径又得不到解决,因而通过网络发帖解决。如果仅仅为了保护网络空间的秩序,而将这些并未造成任何现实危害性或者紧迫的现实危害性的行为予以定罪,除了导致寻衅滋事罪急速地变为口袋罪之外,也使得网络空间秩序日益脆弱,公民的网络自由权日益逼仄。即便因为肯定论的司法解释具有有权解释的效力而不能不适用,在具体适用时,也应该秉承刑法谦抑性,尽量将侵犯网络空间秩序的行为通过现实的危害性或者紧迫的现实危害性这一处罚标准进行合理限定,体现出行为的实质可罚性并进而定罪。否则,肯定论及相关司法解释无论如何也难以避免遭受违背罪刑法定以及违宪的指责。当下司法实务中已有案例注意到了对网络秩序的侵害应该具有现实的社会危害性的问题,进而在网络空间的法益问题上起到了良好的方向指引作用。网络秩序是虚拟的也是虚无的,以侵犯网络秩序的行为是否具有现实危害性或者紧迫的现实危害性为定罪标准,可以为虚拟世界的刑事处罚确立真实的判断基准,以此使网络犯罪处理尽量恪守罪刑法定的实质侧面。

总之,web3.0 时代网络犯罪的治理,必须在网络权益保护与公民网络自由之间寻找

〔40〕 刘艳红:《“法益性的欠缺”与法定犯的出罪》,《比较法研究》2019 年第 1 期,第 86 页。

〔41〕 参见北京市朝阳区人民法院(2013)朝刑初字第 2584 号刑事判决书。

〔42〕 参见榆林市吴堡县人民法院(2016)陕 0829 刑初 27 号刑事判决书。

〔43〕 参见昆明市五华区人民法院(2014)五法刑二初字第 91 号刑事判决书。

到合适的平衡点,否则就难以遏制实务中因打击网络犯罪之需而不断造成刑法罪名成为口袋罪的趋势。刑法对网络空间秩序的保护不能过于虚空,不能仅因侵犯网络空间秩序就对行为入罪,而必须具体化为实质危害的法益侵害标准。

(二)网络犯罪的追责重点应该由个人转向平台

面对 web3.0 时代智能性行为主要由平台发动之特点,刑法对网络犯罪的传统惩罚对象提出了挑战,即网络犯罪的治理对象是个人还是平台?结合 web3.0 时代平台与网民智能互动和人性化、精准化的应用服务特征,以及平台在网络违法犯罪中作用日益显著这一趋势,网络犯罪追责重点应该由个人责任转向平台责任。

在 web2.0 时代,网络平台治理是轻度规制与有限责任。平台是建筑学结构用语,在网络时代,被用来比喻网络空间提供给用户交流的场所。在 web2.0 时代,诸如新浪、QQ 等都是这样的场所,"代码权和上传信息的权利仍属于用户",平台是"技术中立的法律地位",平台的"本质是用户获得网络服务的'工具'"。[44] 1998 年 10 月 28 日美国颁布的《千禧年数字版权法》(DMCA)第 512 条是"网上内容责任限制"的有关规定,其中规定了避风港原则,即对仅提供空间服务的网络服务提供者,如果其网络平台相关内容涉嫌侵权,在能够证明其无恶意且及时删除的情况下,无需承担责任。[45] 2006 年 5 月 18 日国务院修改后的《信息网络传播权保护条例》第 14 - 17 条、第 20 - 23 条设立了避风港原则。自此,在 web2.0 时代,网络平台的规制是"轻度规制"与"有限责任"[46]的理念。亦即在不过多限制而是在鼓励互联网发展的前提下,引入了避风港原则以及由该原则确立的网络平台规制的间接责任同时也是有限责任原则。2009 年 12 月 26 日我国通过的《侵权责任法》第 36 条以立法的形式确立了避风港原则的法律地位,相关条文在 2020 年 5 月 28 日通过的《民法典》第 1194 条和第 1195 条继续得以体现。按照这些规定,"网络平台因为并不提供内容,只要没有对特定侵权行为故意视而不见,并在接到权利人的通知后及时采取了处理侵权信息的措施",[47] 就可以不承担侵权责任。然而,随着 web3.0 时代的到来,网络平台进一步深化发展为集工作、生活和服务一体的综合平台,庞大的网络群体以及体量巨大的网络经济都需要安全的网络环境。[48] 同时,网络平台的功能也发生了变化,平台快速迭代发展,从最初的提供简单链接发展到全面参与社会资源配置,功能越来越强。功能的强化,也意味着平台应当承担更多责任。[49] 在治理策略上,已由轻度规制发展到重度规制,间接有限责任发展到直接全面责任,"强化网站主体责任"[50]成为网络

〔44〕 张凌寒:《互联网新闻治理中社交媒体的平台责任》,载李林、支振锋主编《中国网络法治发展报告(2018)》,社会科学文献出版社 2018 年版,第 97 页。

〔45〕 M. E. Asp, Section 512 of the Digital Millennium Copyright Act: User Experience and User Frustration, *Iowa Law Review*, vol. 103, no. 2, 2018, pp. 752 - 753.

〔46〕 参见周汉华:《正确认识平台法律责任》,《学习时报》2019 年 8 月 7 日第 4 版。

〔47〕 张凌寒:《互联网新闻治理中社交媒体的平台责任》,载李林、支振锋主编《中国网络法治发展报告(2018)》,社会科学文献出版社 2018 年版,第 97 页。

〔48〕 参见游涛、杨茜:《应对网络新型犯罪:做足功课 拿出对策》,《人民法院报》2017 年 3 月 5 日第 3 版。

〔49〕 参见张凌寒:《互联网新闻治理中社交媒体的平台责任》,载李林、支振锋主编《中国网络法治发展报告(2018)》,社会科学文献出版社 2018 年版,第 97 页。

〔50〕 参见王一彪:《新时代呼唤构建良好网络舆论生态》,《人民日报》2018 年 4 月 19 日第 7 版。

平台责任的主要方向。我国 2017 年 6 月 1 日实施的《网络安全法》第 57 条至第 75 条，对网络平台从设立到运营、从内容制造到信息提供等进行了全过程的法律规制，网络平台不再是遵循避风港原则即可免责的法外之地，而是必须全面接受政府强制监管，“政府设定标准，平台承担普遍性监控义务”，〔51〕平台成为网络时代重要的责任主体，web3.0 时代网络犯罪的追责重点由个人转向平台，“刑法增设拒不履行信息网络安全管理义务罪倒逼网络平台配合政府履行网络安全监管义务”，〔52〕正式宣告了网络时代单纯个人责任的终结与平台责任的兴起。

网络犯罪追责由个人责任到平台责任的转向，并不意味着所有的平台违法行为都是犯罪，还需要合理界定平台刑事责任。因为，平台责任显然不同于平台治理，前者侧重于事后追责，是一种结果责任；后者侧重于事前与事中的责任履行，是一种过程责任。〔53〕合理运用事后责任对技术风险进行评价，通过司法裁判威慑风险行为，从而达到有效规制违法犯罪的目的。〔54〕尤其是，对平台刑事责任的追究更应该对后果的危害性予以考量，即根据危害原则判断平台犯罪成立与否。基于实质危害的“危害原则所体现的法治精神、限制刑罚权、保护公民自由、追问国家强制干预的合法性等理念”，〔55〕也是有效区分平台民事、行政与刑事责任的根本性标准。拒不履行信息网络安全管理义务罪的合理解释，以准确理解“网络服务者提供者不履行法律、行政法规规定的信息网络安全管理义务”和“经监管部门责令采取改正措施而拒不改正”两个要件为重要前提。其一，网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务的认定。平台犯罪是平台违反国家网络监管义务超出合理注意义务而导致的犯罪。平台犯罪首先是违反前置法的行为。《刑法》第 286 条之一规定的“网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务”，是追究平台责任的前提条件。这里的“法律、行政法规”亦即拒不履行信息网络安全管理义务罪的前置法，范围广种类多，比如《网络安全法》《电子商务法》《计算机信息系统国际联网保密管理规定》《互联网信息服务管理办法》，等等。这些前置法中最重要的是《网络安全法》，该法要求平台开展经营和服务活动必须遵守法律、行政法规，履行网络安全保护义务，接受政府和社会的监督。根据该法第 59 – 75 条的规定，网络运营者、网络产品或者服务的提供者违反相关法律规定，情节严重的，即可能构成拒不履行信息网络安全管理义务罪。根据前置法的规定，违背国家网络安全保护义务，不接受政府监管超出合理注意义务的行为，就会构成平台犯罪。随着平台的发展和细分，各类平台义务来源都有所不同，每种平台的义务来源都须根据前置法的规定。义务来源无法判断，平台责任也就无法追究。比如李某等人“摩范出行”平台共享汽车事故案中，〔56〕“摩范出行”

〔51〕 张凌寒：《互联网新闻治理中社交媒体的平台责任》，载李林、支振锋主编《中国网络法治发展报告（2018）》，社会科学文献出版社 2018 年版，第 98 页。

〔52〕 于冲：《网络平台刑事合规的基础、功能与路径》，《中国刑事法杂志》2019 年第 6 期，第 94 页。

〔53〕 参见周汉华：《正确认识平台法律责任》，《学习时报》2019 年 8 月 7 日第 4 版。

〔54〕 参见周佑勇：《论智能时代的技术逻辑与法律变革》，《东南大学学报（哲学社会科学版）》2019 年第 5 期，第 75 页。

〔55〕 姜敏：《危害原则与法益保护原则比较研究》，《比较法研究》2019 年第 6 期，第 164 页。

〔56〕 参见韩丹东、姜珊：《共享汽车平台须尽提醒审查义务 情侣被撞身亡引思考》，《法制日报》2019 年 9 月 23 日第 8 版。

平台没有汽车租赁资质,其租车行为属于违规操作。从义务来源分析,其已具备“不履行法律、行政法规规定的信息网络安全管理义务”的构罪要件,而这种不履行义务的行为是否构成犯罪,则还要看行为与结果之间的因果关系以及其他构成要件是否具备。至于“网络服务提供者”,根据 2019 年 11 月 1 日“两高”《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》(下称“《网络犯罪解释》”)第 1 条规定,“网络服务提供者”包括三类人:一是网络接入、域名注册解析等服务的网络服务提供商,即 NSP(Net Service Provider);二是信息发布、搜索引擎、即时通等服务的网络内容服务提供者,即 ICP(Internet Content Provider);三是利用信息网络提供的电子政务、通信、能源、交通等公共服务的网络应用服务提供商,即 ASP(Application Service Provider)。司法解释的上述规定,实际上是对网络服务提供者作了扩大解释,据此,网络接入服务商、网络内容服务商以及网络应用服务商都属于网络服务提供者,从而使刑法中网络平台犯罪的主体大大超过了以往法律中网络服务提供者的范围,《网络犯罪解释》对网络服务提供者的扩大解释恰恰体现了 web3.0 时代强化平台追责之趋势。其二,经监管部门责令采取改正措施而拒不改正。根据《刑法》第 286 条之一规定,“经监管部门责令采取改正措施而拒不改正”是依法追究平台刑事责任的前提条件。根据《网络犯罪解释》第 2 条规定,认定“经监管部门责令采取改正措施而拒不改正”,应当根据法律、行政法规的规定,充分考虑网络服务提供者是否有能力履行改正措施,合理确定改正措施及期限。然而,不以“文书形式”责令整改是否能认定为“经监管部门责令采取改正措施而拒不改正”?实务中,有的是以文书形式责令整改,还有的是以非文书形式责令整改。比如,胡某拒不履行信息网络安全管理义务罪一案中,被告人胡某通过租用的服务器和技术手段,为他人非法提供境外互联网接入服务。当地公安局分局先后两次约谈被告人胡某,要求其停止联网服务,并对其做出警告、罚款和没收违法所得的处罚。事后,胡某拒不改正继续出租翻墙软件,违法所得共计人民币 20 余万元。法院审理认为,胡某未经许可提供国际联网代理服务,同时监管部门通过约谈责令其采取改正措施后仍然拒不改正,属于情节严重,已经构成拒不履行信息网络安全管理义务罪。〔57〕 可见,监管部门责令整改并非必须以文书形式做出。司法解释要求以文书形式做出,意在强调文书具有明确性的效果。但是,如果现场约谈而没有下达具体文书,只要依法明确要求责令改正的,当然应认定为“经监管部门责令采取改正措施”。总之,在认定“经监管部门责令采取改正措施而拒不改正”要件时,不能僵化地理解只有以文书形式责令改正的才行,对此必须采取实质解释,如果采取的是与文书有同样效果的责令改正要求,同样属于“经监管部门责令采取改正措施”。此外,拒不履行信息网络安全管理义务罪的主观罪过为故意,应当对行为人遵守法律规范的态度和能力进行把握,即只有在行为人有能力实施犯罪以外的行为时,才能够予以追责。〔58〕 网络服务提供者只有对不履行法律法规有认识且不遵照执行,才有追究平台责任的可能性,出于过失的行为不应承担刑事责任。

〔57〕 参见上海市浦东新区人民法院(2018)沪 0115 刑初 2974 号刑事判决书。

〔58〕 参见张明楷:《责任论的基本问题》,《比较法研究》2018 年第 3 期,第 11 页。

总之,根据 web3.0 时代网络平台在违法犯罪行为中的高参与度,应将刑法对网络犯罪的追责重点由个人转向平台,加强对平台责任的监管与规制;对网络犯罪的治理应从强化个人责任转向强化平台责任。与此同时,对平台刑事责任的追究应立足于构成要件的实质解释,以具有法益侵害性的结果为导向落实平台犯罪的刑事责任。

(三)网络犯罪的定罪标准宜升维而非降维打击

复杂的 web3.0 时代网络犯罪频发,较之线下犯罪,网络犯罪应该升维治理还是降维打击抑或同维打击?面对这一新的挑战,刑法理论应根据网络犯罪的特点,对网络犯罪进行升维打击而非同维或降维打击。web3.0 时代网络空间作为以人工智能与大数据为核心的智能化时代,网络成为所有网民开放共享的自由空间,网民与网络的智能互动使得网络全方位地重新塑造着人们的生活。便捷性、快速性、开放性、智能性等特性,使得网络信息传播快速且普遍,智能性的 web3.0 时代网络的集聚效应决定了网络违法犯罪行为的雪球效应显著。如此一来,如何界定具有复杂性的 web3.0 时代网络犯罪的认定标准,成为当下网络犯罪刑法适用面临的重要挑战。面对 web3.0 时代层出不穷的网络犯罪,刑法的认定标准应该降维或升维抑或保持与传统犯罪同样标准?

降维是一个科幻名词,最早出现在小说《三体》中,“攻击者首先改造自己,把自己改造成低维生命,比如由四维生命改造成三维生命,当然也可以由三维改造成二维,当整个文明进入低维后,就向敌人发起维度打击”。[59] 在此,降维就是将攻击目标所在的空间维度降低,使其无法在该空间内生存,然后予以打击。正如短信技术嗅探犯罪,为截取到他人的账户资料等信号,不法分子会使用伪基站强制干扰 3G 或 4G 信号,强制用户降维到 2G 网络状态,因为 2G 通道下短信和通话信息是明文传输方式,对犯罪分子而言在 2G 状态下可以截取到他人的完整信息。[60] 降维打击所蕴含的降低维度予以打击之意,后衍生为降低标准予以打击。网络犯罪与网络科技的发展迭代共生,web3.0 时代网络犯罪日益智能化和多样化,刑法理论和实务中为了及时打击网络犯罪,出现了降维打击的趋势,即较之于物理世界的犯罪,将网络犯罪的认定标准予以降低。刑法对网络犯罪的降维打击表现在立法与司法两个层面。立法上,基于“‘打早打小’,坚决依法严厉惩处利用信息网络实施的”犯罪,“有效维护网络安全和经济、社会生活秩序”[61] 的刑事政策,扩大网络犯罪的打击面,并采取了比线下犯罪更为低的定罪标准。通过《刑法》第 286 条之一拒不履行信息网络安全管理义务罪和第 287 条之二帮助信息网络犯罪活动罪这两个罪名,刑法“实际上是在作为和不作为两个方向围堵了网络中立帮助行为的出罪空间”,并使得网络中立帮助行为“走上了全面可罚化的道路”。[62] 尤其是,帮助信息网络犯罪活动罪,通过将中立网络帮助行为正犯化,大大扩大了刑罚处罚范围。[63] 刑法对于网络犯罪的帮助行

〔59〕 刘慈欣著:《三体(III·死神永生)》,重庆出版社 2016 年版,第 515 页。

〔60〕 参见颜之宏等:《可怕!一觉醒来“存款蒸发”警惕!短信嗅探“隔空刷卡”》,《济南日报》2018 年 10 月 19 日第 A6 版。

〔61〕 最高人民法院、最高人民检察院、公安部、司法部《关于办理利用信息网络实施黑恶势力犯罪刑事案件若干问题的意见》第 1 条第 1 款。

〔62〕 参见刘艳红:《网络中立帮助行为可罚性的流变及批判》,《法学评论》2016 年第 5 期,第 49 页。

〔63〕 参见刘艳红:《网络犯罪帮助行为正犯化之批判》,《法商研究》2016 年第 3 期,第 21 页。

为也进行了全面打击。《刑法》第 287 条之一非法利用信息网络罪,仅仅设立非法网站或发布有关违法信息等行为,并不意味着会产生危害网络秩序的结果,本罪“规定的实质是将部分犯罪的预备行为提升为实行行为,完成了预备行为就视为犯罪既遂”。[64] 如此降低犯罪构成的标准,将预备行为等同为实行行为予以打击,固然使得网络领域的失范行为难以存在,然而却也极大地影响了互联网技术的发展。司法中,面对 web3.0 时代网络新型违法犯罪行为,为了应对网络安全治理的诉求,司法实践在“口袋罪”思维指引下通过刑法客观解释,对网络犯罪罪名进行扩大化与入罪化,并成为网络违法犯罪行为治理的方向。[65] 比如,将网游公司员工利用网络游戏软件运营的工作便利行为扩大解释为“侵入”,并以非法获取计算机信息系统数据罪定罪;[66]将虚拟财产扩大解释为财产并将侵犯网络虚拟财产的行为定为财产犯罪;对非法利用信息网络罪中的“违法犯罪”进行扩大解释,将通过网络购买仿真枪、买卖驾照分数以及利用信息网络实施仅违反治安管理处罚规定的行为也作犯罪处理,[67]《网络犯罪解释》第 7 条[68]也肯定了这种观点,从而导致线下违法行为一旦线上实施就构成了犯罪。

面对立法与司法实践中对网络犯罪降维打击的趋势和做法,结合 web3.0 时代网络犯罪的特点,网络犯罪的刑事治理应该升维,而不应该同维,更不应该降维。同维打击看似线下线上犯罪定罪标准相同,但因为网络犯罪的前述特点,这种形式的平等实则是不平等的。网络犯罪的便捷性与弥散性决定了网络犯罪定罪标准应该升维而不是降维或者同维,采取较之线下犯罪更高的定罪标准。网络空间除了具有前述所说的“场所”特性,它还具有“产品”与“媒介”两个特性,[69]这决定了网络犯罪容易实施且传播性强。如果不根据网络的特点,将网络犯罪的标准采用低于或者与线下犯罪相同的定罪标准,则违背了 web3.0 时代网络犯罪的特性。比如《刑法》第 217 条侵犯著作权罪以“违法所得数额较大或者有其他严重情节”为入罪标准,2004 年 12 月 4 日“两高”《关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释》第 5 条规定了针对线下侵犯著作权罪的入罪标准。在网络环境下,行为人以营利为目的,未经权利人许可而向他人传播音乐、电影、录音录像制品和其他作品的行为,在网络空间几乎处于失控状态,因为数字化产品的复制和传播过于容易。通过将作品上传到网络上的复制,为了使作品被他人访问而由网络服务器做出的自我复制,以及访问者阅读作品时自己计算机作出的暂时复制,这三类有别于传统复制权的复制,[70]加之鼠标点击所轻松完成的传播,辅之以深度链接、网络快照等各种新型传播形式,使得网络侵权作品的复制和传播不

〔64〕 张明楷著:《刑法学(下)》(第五版),法律出版社 2016 年版,第 1051 页。

〔65〕 参见刘艳红:《网络时代刑法客观解释新塑造:“主观的客观解释论”》,《法律科学》2017 年第 3 期,第 95 页。

〔66〕 参见北京市石景山区人民法院(2017)京 0107 刑初 96 号刑事判决书。

〔67〕 参见缑杰、吴峤滨:《〈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〉重点难点问题解读》,《检察日报》2019 年 10 月 27 日第 3 版。

〔68〕 该解释第 7 条规定:“刑法第二百八十七条之一规定的‘违法犯罪’,包括犯罪行为和属于刑法分则规定的行为类型但尚未构成犯罪的违法行为。”

〔69〕 参见刘艳红:《网络犯罪的刑法空间解释向度》,《中国法学》2019 年第 6 期,第 217 - 218 页。

〔70〕 参见杨彩霞著:《网络环境下中国著作权刑事保护研究》,中国社会科学出版社 2016 年版,第 13 页。

但较之线下更为容易而且传播面更广,违法所得和营利数额也都更大,因此,对于通过信息网络传播侵权作品行为的入罪标准,应该高于线下传播侵权作品行为的入罪标准。然而,2011 年 1 月 7 日“两高”、公安部、司法部《关于办理侵犯知识产权刑事案件适用法律若干问题的意见》第 13 条“关于通过信息网络传播侵权作品行为的定罪处罚标准问题”,对网络传播侵权复制品行为的入罪标准明确采取了与线下犯罪一样的标准。相较于线下犯罪,“在网络空间,数据可以摆脱有效的国家管控而在全球范围内迅速、充分地传播。因此,经由电子通信和网络匿名,儿童色情信息的传播变得相当容易。通过互联网进行恐怖主义或极端主义招募与宣传,实施跨国赌博,以及非法出售商品,也会遭遇类似的问题”。[71] 这意味着,侵犯著作权行为一旦在网络领域实施,其复制与传播数额的起点必然惊人,远远超出线下侵权行为的数额。这些都表明了网络犯罪的特殊性,可能的话,有建立网络犯罪独立定罪标准的必要性。将线下犯罪入罪标准生搬硬套到网络领域的做法,既忽视了线上与线下传播侵权行为的本质差异性,也是对网络传播侵权作品行为的降维打击,是极不合理的。

网络犯罪数据或数额的虚拟性,决定了网络犯罪定罪标准应该升维而非降维或者同维。网络犯罪如果侵犯的是虚拟财产,虽然虚拟财产“虚而有价”,但其价值性根据什么来体现,本身争议极大。虚拟财产的价值性与实体财产相比,也无法相提并论。在刑法对虚拟财产的财产属性没有明确规定且司法实务中对虚拟财产性质本身就不统一的情况下,应根据有利于被告人原则,将侵犯虚拟财产犯罪的入罪标准设置为数倍于线下侵犯实体财产犯罪的入罪标准。目前我国刑法对虚拟财产犯罪的入罪标准采用的是和侵犯实体财产同一的标准,比如盗窃犯罪,线上和线下犯罪适用的都是“两高”2013 年 4 月 2 日《关于办理盗窃刑事案件适用法律若干问题的解释》的标准。司法实践中,采用与线下盗窃相同数额标准作为线上盗窃虚拟财产犯罪的入罪标准,就属于降维打击。因为虚拟财产的价值难以认定,根据该解释第 4 条,盗窃的数额根据价格证明、交易价格、水电等仪表显示的数据、电信等用户支付的数额等。实务中对虚拟财产的数额认定主要就是沿用该条司法解释的规定,竭力寻找虚拟财产背后的价格证明,包括销售数额、购进价格、为虚拟财产的保存所支付的托管费用、服务器运营商虚拟财产支付的成本或维护费用等,在无法证明有效价格的情况下,委托价格鉴定的做法也非常普遍。但是,无论是有效价格证明证据的寻找或是委托价格鉴定,虚拟财产数额的认定资料相对模糊,收益不明,销赃数额因个人喜好程度差异极大,购进价也缺乏市场衡量标准等。虚拟财产的数额认定还要通过一定技术手段才能合理确定虚拟财产的数额,[72] 而技术的运用都具有相对性。诸如此类,决定了侵犯网络虚拟财产的犯罪数额难以得到准确认定。只有区分虚拟与实体财产的不同属性,将侵犯虚拟财产的定罪标准提高到数倍于侵犯实体财产的定罪标准,才能实现线上犯罪治理与线下犯罪治理之间的罪刑均衡。目前刑事立法没有针对侵犯网络虚拟财产

〔71〕 [德]乌尔里希·齐白:《信息社会中的刑法》,周遵友译,载赵秉志主编《走向科学的刑事法学》,法律出版社 2015 年版,第 31 页。

〔72〕 参见刘品新、张艺贞:《虚拟财产的价值证明:从传统机制到电子数据鉴定机制》,《国家检察官学院学报》2017 年第 5 期,第 79 页。

犯罪规定高于线下犯罪入罪标准，为了纠正对虚拟财产犯罪降维打击可能带来的罪刑失衡及不利于被告人的后果，应在司法实务中提倡对侵犯虚拟财产犯罪的数额认定严格把关，尽量以有效价格证明为依据认定虚拟财产犯罪的数额；避免在有有效价格证明的基础之上，人为抬高虚拟财产的数额。通过实务认定的严格把关，矫正刑事立法和司法解释对虚拟财产犯罪采取线上线下相同入罪标准这一实乃降维打击的做法所带来的罪刑失衡。比如李某盗窃虚拟财产案件中，〔73〕被告人通过销售虚拟财产取得了实体财产的对价，法院认定被告人盗窃虚拟财产的数额为 16000 元，而没有采纳价格认证中心脱离实际交易价格的虚高认定，无疑是严格防止对虚拟财产犯罪降维打击的最好例证。实务部门的理性做法值得肯定，同时也说明对虚拟财产犯罪不应采用与实体财产犯罪一样标准的立论具有合理性。

网络犯罪证据难以查证确实，这也决定了网络犯罪入罪标准应该升维。不同于线下犯罪，网络犯罪基本上是非接触式，以网络电信诈骗为例，犯罪人充分利用网络科技精心设计骗局，根本不与被骗人接触，得手后迅速转移赃款，要查明犯罪人的具体诈骗数额往往存在诸多困难，甚至不少电信诈骗案件的被害人都无法联系上，这些都对案件侦破，特别是具体犯罪事实和数额的认定带来了极大困难。〔74〕在网络犯罪证据难以达到线下犯罪证据的证明力时，数额无法准确认定，犯罪情节难以量化证明，不宜采取与线下犯罪一样的入罪标准，而是应该相应提高网络犯罪入罪标准，以此实现疑罪从无的法治理念。这种做法在相关司法解释中也得到了体现和运用。《网络犯罪解释》第 12 条规定，帮助信息网络犯罪活动罪的定罪标准，“确因客观条件限制无法查证被帮助对象是否达到犯罪的程度，但相关数额总计达到前款第二项至第四项规定标准五倍以上”。〔75〕这一做法其实就是为了避免降维打击所带来的网络犯罪治理不彰。

特别需要说明的是，对于刑法设立的计算机与网络犯罪专有罪名，如非法侵入计算机信息系统罪、破坏计算机系统罪、非法利用信息网络罪、帮助信息网络犯罪活动罪等罪名，由于不存在对应的线下犯罪罪名，因此也不存在与线下犯罪相比所带来的降维或升维打击问题。

总之，在信息网络技术快速发展的时代背景下，传统的犯罪定量标准体系日渐滞后，难以适应网络犯罪科学治理的需要，也根本无法对不断增长和变形的网络犯罪作出科学、合理的定量评价。〔76〕在针对网络犯罪建立独立的定罪量刑标准之前，刑法理论与司法实践不宜采取比线下犯罪更低或者同样的定罪标准，否则就是对网络犯罪进行降维打击，从而过于扩大网络犯罪的打击面，并不利于网络的健康发展。

---

〔73〕 李某窃得他人账号及该账号名下的游戏虚拟装备并以人民币 16000 元的价格转让给他人牟利。检察机关办案过程中请当地价格认证中心出具价格鉴定报告，认定盗窃数额为人民币 29800 元。法院审理认为，“根据本案已查明的事实和确认的证据，依照现行法律，对本案盗窃数额认定人民币 16000 元为妥。公诉机关指控被告人李某盗窃数额巨大不当，本院予以纠正”。参见慈溪市人民法院（2012）甬慈刑初字第 1402 号刑事判决书。

〔74〕 参见喻海松著：《网络犯罪二十讲》，法律出版社 2018 年版，第 266 页。

〔75〕 比如，该条第二项至第四项规定的“为三个以上对象提供帮助的”可以构成犯罪，如果被帮助人的行为是否构成犯罪难以查清，则须为 15 个以上的对象提供帮助的才能构成犯罪。

〔76〕 参见于志刚、郭旨龙：《信息时代犯罪定量标准的体系化构建》，《法律科学》2014 年第 3 期，第 127 页。

结 语

基于科技与犯罪的迭代共生,对兼容了 web1.0 和 web2.0 时代的 web3.0 时代网络犯罪进行刑法规制,必须准确界定复杂 web3.0 时代网络犯罪的侵害法益、网络犯罪的追责对象与网络犯罪的定罪标准等问题。为此,刑法理论应确立实质损害标准解决侵犯网络空间秩序行为是否构成犯罪,以具有法益侵害性结果为导向强化网络犯罪平台而非个人责任追究,以升维打击而非降维打击确立网络犯罪的定罪标准,从而有效解决 web3.0 时代网络犯罪认定与处罚的难题。在我国民法典刚刚通过并正式开启了公民权利保障的法治化新时代,必须切实"贯彻实施民法典提高国家治理现代化水平",〔77〕为此,打击网络犯罪的同时必须重视对公民个人权利的保护,反对 web3.0 时代网络犯罪治理中的泛刑化做法,以避免造成网络治理领域公民权利保护的寒蝉效应,妥善推进国家网络治理能力的现代化。

[本文为作者参与的东南大学人民法院司法大数据团队负责的2018 年度国家重点研发计划项目"面向诉讼全流程的一体化便民服务技术及装备研究"(2018YFC0830200)的研究成果。]

[**Abstract**] Through the symbiotic development from Web 1.0 to Web 2.0, and to Web 3.0, cybercrime and network technology show distinctive intergenerational features. Different from the physical Web 1.0 and Web 2.0 era, the most significant feature of Web 3.0 era is intelligence, and the cyberspace of personalized, interactive and precise application services has also become a crime space, with all kinds of new crimes that also have the characteristics of cybercrime in Web 1.0 and Web 2.0 era emerging endlessly one after another. A great challenge in the application of criminal law to cybercrimes in the era of Web 3.0 is to identify complicated legal interests infringed upon by such crimes, the subjects of criminal responsibility, and the standard of conviction. Correspondingly, criminal theory should apply the substantive injury criterion to decide whether an act of disruption of cyberspace order constitutes a crime, take the possession of infringement of legal interest as the orientation to strengthen the investigation of the responsibility of platforms, rather than individuals, and establish the standard of conviction of cybercrimes by raising, rather than lowering, the dimension of the fight against such crimes, so as to solve the problems of cybercrimes and t he criminal law regulation in the Web 3.0 era.

(责任编辑:王雪梅)

〔77〕 周佑勇:《贯彻实施民法典 提高国家治理现代化水平》,《学习时报》2020 年 6 月 19 日第 1 版。