网络时代的刑法立法体系及其建构

李晓明*

内容提要　信息网络犯罪依据犯罪形态分为破坏信息网络安全的技术型犯罪、利用信息网络实施的传统犯罪及违反网络空间管理义务的犯罪，犯罪类型及特征不同，治理的侧重点也不同。我国刑法典一元模式难以适应网络时代发展，易造成网络犯罪的法网疏漏、刑罚结构的重刑化及刑法与前置法的衔接不畅。而三元立法模式能体现刑法规范体系维护价值的层次性与序位性，在适应犯罪类型化趋势及治理诉求差异上具有优势。其建构重点在于明确刑法典、单行刑法、附属刑法各自的立法原则，根据模式特点选择犯罪类型。其中，利用信息网络实施的传统犯罪以刑法典为主体，以单行刑法、附属刑法为补充；破坏信息网络安全的技术型犯罪以单行刑法为主体；违反网络空间管理义务的犯罪以附属刑法为主体。由此形成专门化、具有针对性和有效性的刑法科学体系，以适应网络时代治理犯罪之需。

关键词　网络犯罪　刑法典　刑法立法体系　三元立法模式

目　次

* 苏州大学王健法学院教授。本文系 2020 年度国家社科基金重大项目“网络时代的社会治理与刑法体系的理论创新”（项目批准号：20&ZD199）的阶段性成果。阮紫晴同学对本文亦有贡献，特此致谢。

网络时代犯罪治理的重要性不言而喻，但我国一元化的典籍立法模式难以适应当今的网络犯罪态势，检视、调整与完善现行刑法立法体系，以适应网络时代犯罪的风险迭变，是刑法立法面临的重大课题。本文运用类型化分析方法，系统梳理网络时代犯罪的特点，反思刑法典一家独大立法模式的不足，在借鉴域外立法经验的基础上，分析现行刑法立法体系存在的问题，对我国网络时代的未来刑法立法模式及其体系进行讨论，以期促进对信息网络犯罪的科学应对。

一、网络时代信息网络犯罪的类型化分析

随着网络技术的飞速发展，人类社会已进入网络和“大数据”时代，虚拟世界与现实社会的界限已发生叠变，相互间的互动愈加频繁，二者的边界亦日趋模糊，早有学者将网络虚拟空间称为刑事管辖的“第五空间”①，而且当今的网络确已成为人类生存的第二大空间。然而，网络技术在为社会发展注入新活力的同时，也使得网络犯罪风险呈现叠变性效应，给社会治理及刑法规制带来巨大冲击与挑战。互联网经历了 Web1.0、Web2.0 到 Web3.0 的发展变化，网络时代的犯罪必然区别于传统社会的犯罪。尤其随着网络技术在人们生活和工作中的渗透，犯罪手法也在不断翻新和隐蔽，其技术含量日新月异，辐射范围不断扩展，这决定了网络犯罪的广泛性及其与传统犯罪的交互性，故刑法在立法体系上应适时调整。

由于网络犯罪的广泛性及其与传统犯罪的交互性，运用抽象的概念思维应对网络犯罪或许存在局限。相比之下，类型化思维的多位性、动态性特征能为认识事物提供多元角度，②有助于在梳理和观察网络犯罪实践类型与特征的基础上，通过分析归纳将其上升至法学层面的规范类型，由此形成对网络犯罪有针对性的全面系统研究。网络犯罪通常有三种类型：一是以信息网络为对象的犯罪，也有学者将这类犯罪称为“纯粹的网络犯罪”或“狭义的网络犯罪”。二是以信息网络为工具的犯罪。这类犯罪侵害的仍是传统法益，只不过是以信息网络为犯罪工具，或称之为传统犯罪的网络化、虚拟化，如网络盗窃、网络诈骗等。三是随着 Web3.0 的发展和“网络空间”的独立，以网络为犯罪空间的犯罪，③如在网络空间寻衅滋事、开设赌场、侮辱、诽谤、传播淫秽物品等，甚至利用网络技术中元宇宙的沉浸式体验④进行性侵。2022 年最高人民法院、最高人民检察院、公安部发布的《关于办理信息网络犯罪案件适用刑事诉讼程序若干问题的意见》将拒不履行信息网络安全管理义务、非法利用信息网络、帮助信息网络犯罪活动等列为新的网络犯罪类型，由此强化了违反网络空间管理义务型犯罪。还有学者认为，应当以传统犯罪为

① 参见屈学武：《因特网上的犯罪及其遏制》，载《法学研究》2000 年第 4 期，第 83 页。传统刑事管辖理论将“四空间说”解释为领陆、领水、领空和“拟制领土”（如船舶、飞机、国际列车和驻外使领馆等）。

② 参见杜宇：《类型思维与刑法方法》，北京大学出版社 2021 年版，第 23-38 页。

③ 参见于冲：《网络刑法的体系构建》，中国法制出版社 2016 年版，第 31 页。

④ 参见赵国栋、易欢欢、徐远重：《元宇宙》，中译出版社 2021 年版，第 13-14、23-26 页。

参照，将网络犯罪划分为“与传统犯罪本质无异的网络犯罪”“较传统犯罪呈危害‘量变’的网络犯罪”及“较传统犯罪呈危害‘质变’的网络犯罪”。[⑤] 也有学者依据侵害法益的不同，将网络犯罪划分为侵害公法益的网络犯罪与侵害私法益的网络犯罪。[⑥]

本文旨在探讨网络时代刑法立法体系建构的方向与原则问题，这需对网络时代背景下的犯罪形态予以全面把握。因此网络犯罪指向广义说，具体分为破坏信息网络安全的技术型犯罪、利用信息网络实施的传统型犯罪和违反网络空间管理义务型犯罪三种。

（一）破坏信息网络安全的技术型犯罪

欧洲理事会 2001 年主导签署的《网络犯罪公约》将网络犯罪定义为：“针对计算机系统、网络及计算机数据的保密性、完整性及可用性，以及对上述系统、网络和数据滥用的行为。”[⑦] 美国司法部界定的网络犯罪有三种类型：（1）以计算机或服务器本身为犯罪对象；（2）以计算机为犯罪物理场所或独特形式的资产损失的源头；（3）利用计算机实施传统犯罪。日本常见的网络犯罪类型有：（1）滥用电脑实施的犯罪；（2）加害于电脑的犯罪；（3）窃取电脑信息的犯罪。[⑧] 可见，各国对计算机及网络犯罪的类型划分大致有共同思路：一是以计算机及网络为对象的犯罪，二是以计算机及网络为工具的犯罪。

国内有广义说与狭义说，广义说是指以计算机及网络为犯罪工具和犯罪对象的总称，即纯正计算机及网络犯罪和不纯正计算机及网络犯罪。[⑨] 狭义说是指依靠计算机及网络技术对计算机及网络实施的技术型破坏、侵入和控制的犯罪。我国《刑法》第 285 条非法侵入计算机信息系统罪，第 286 条破坏计算机信息系统罪，以及《刑法修正案（七）》增设的《刑法》第 285 条第 2、3 款非法获取计算机信息系统数据、非法控制计算机信息系统罪和提供侵入、非法控制计算机信息系统程序、工具罪等，均是指“狭义说”。

显然，上述罪名把数据视作计算机信息系统的部分内容，关于数据保护的两个罪名的保护对象被限定为计算机信息系统内部，为计算机信息系统的功能实现而存储、处理和传输的内部数据。[⑩] 随着数据时代的到来，网络数据大量汇聚，尤其是云存储、云计算技术的普及，使得数据与计算机信息系统在技术层面逐渐分离，数据自身的价值不断突出，数据梳理、分析、挖掘、处理和应用技术也迅猛发展。这虽然促进了数字经济的繁荣，但同时也带来了数据的安全风险，甚至危及个人隐私、财产安全、企业安全、社会秩序与国家安全等。为加强数据安全的独立保护，有学者建议参照德国对 CIA（Confidentiality 即数据保密性、Integrity 即数据完整性、Availability 即数据可用性）犯罪的界定，围绕数据的保密性、完整性与可用性在我国刑法中确立数据安全法益，并增设以数据为犯罪

⑤ 参见刘宪权：《网络犯罪的刑法应对新理念》，载《政治与法律》2016 年第 9 期，第 6-7 页。

⑥ 参见苏青：《认识网络犯罪：基于类型思维的二元视角》，载《法学评论》2022 年第 2 期，第 88 页。

⑦ 前注 ⑥，苏青文，第 81 页。

⑧ 参见刘艳红：《网络犯罪的法教义学研究》，中国人民大学出版社 2021 年版，第 105-107 页。

⑨ 参见赵廷光、朱华池、皮勇：《计算机犯罪的定罪与量刑》，人民法院出版社 2000 年版，第 33 页。

⑩ 参见李源粒：《大数据时代数据犯罪的制裁思路》，载《中国社会科学》2014 年第 10 期，第 103 页。

对象的专有犯罪。[11]数据是信息的载体，信息是数据的内容，二者间具有天然的密切联系，数据犯罪与信息犯罪必然有交叉或重合。有些数据与特定信息间并不存在直接、明确的指向，如经过去识别化、脱敏处理的数据与价值密度低的数据，不过这些数据经特殊技术处理（数据汇聚、整合及挖掘）后仍可能存在侵犯国家秘密、商业秘密、个人信息等风险，故应增设独立的数据罪名，并强调相关罪名对数据保护的特殊性，以严密刑事法网。

问题在于，如果将数据安全独立于计算机及网络安全的保护，那么新增设的数据犯罪是否应被纳入破坏信息网络安全的技术型犯罪的范畴呢？首先，数据犯罪中的数据是大数据时代下依托某种存储技术存在于信息网络空间内的二进制代码，数据犯罪的发生往往无法脱离信息网络。其次，借鉴他国经验，如欧盟《网络犯罪公约》及美国《电脑欺诈与滥用法》均将数据犯罪与计算机系统犯罪相并列，将二者纳入网络犯罪规制的范畴。我国未来的刑法立法也可以考虑将数据犯罪与计算机及网络犯罪并列为新型纯正意义上的信息网络犯罪，并将其纳入破坏信息网络安全的技术型犯罪范畴。

综上，破坏信息网络安全的技术型犯罪实际上囊括了侵害计算机信息系统安全的犯罪、侵害信息网络秩序的犯罪与侵害数据安全的犯罪。这些犯罪的共同特点是：（1）以计算机和信息网络技术为核心手段，具有高度技术性与专业性；（2）犯罪空间的虚拟化、隐蔽性与跨时空的互动性导致犯罪危害结果的弥散化，以及秩序侵害种类的多重性和不确定性；（3）基于技术的迅速发展，犯罪手段与行为类型不断更新、变化和丰富，使犯罪呈现多样化趋势。

（二）利用信息网络实施的传统型犯罪

伴随着信息技术的发展与互联网的普及，信息网络使得人们的生活、工作与交往发生翻天覆地的变化。与此同时，信息网络技术被滥用的风险也在增大，传统犯罪从现实社会转入虚拟空间，呈现出传统犯罪网络化、网络犯罪常态化的趋势。尤其在网络时代，网络替代计算机信息系统成为犯罪工具是不争的事实，也使得网络几乎介入所有的传统犯罪之中。当然，由于我国刑法对犯罪场所、对象、行为方式及危害后果未作明确限定，故通过扩张解释仍能应对传统犯罪的网络化现象，且在教义学原理上可适用于利用信息网络实施的传统犯罪，[12]但网络时代仍对传统犯罪的不法构造形成巨大冲击，甚至扩大了犯罪圈。表现在：

一是行为方式的多元化。信息化技术的高速发展为传统犯罪行为方式的多样化提供了载体与空间。以非法吸收公众存款罪为例，其规制以不法或变相提高利率等方式吸纳公众存款的行为，还发展为包括网络借贷和网络众筹。2022 年《最高人民法院关于审理非法集资刑事案件具体应用法律若干问题的解释》规定“变相吸收”时，明确纳入以网络借贷、投资入股、虚拟货币交易等方式非法吸收资金的行为。尤其近年来区块链技术与金融结合生成多种新型网络金融产品，以 ICO（Initial Coin Offering，即“首次代币

[11] 参见杨志琼：《我国数据犯罪的司法困境与出路：以数据安全法益为中心》，载《环球法律评论》2019 年第 6 期，第 159 页。

[12] 参见皮勇：《论中国网络空间犯罪立法的本土化与国际化》，载《比较法研究》2020 年第 1 期，第 142 页。

发行”）为典型。2017 年中国人民银行等七部门印发《关于防范代币发行融资风险的公告》，明确指出代币发行融资属非法融资。但实践中 ICO 在融资方式上又呈现多样性，目前主流的 ICO 融资模式就包括功能类、债权类、股权类三种。[13] 非法吸收公众存款罪需具备非法性、社会性、公开性、利诱性等特征，且成立的前提是吸收“资金”，而 ICO 是否具有“利诱性”及募集数字货币是否属“资金”范畴存在较大争议，不仅需结合 ICO 融资的行为方式加以判断，更需要结合网络行为进行研究，可见其行为方式的复杂性。

二是行为对象的虚拟化。传统犯罪网络化过程中，行为对象不再限于现实空间的人、物及秩序，而开始向虚拟空间的数据信息、虚拟财产或网络空间及秩序延伸。以网络虚拟财产为例，从过去网络平台的虚拟币、游戏装备、道具，到现在以比特币为代表的各类区块链虚拟币，再到最近元宇宙中的数字资产如 NFT（Non-Fungible Token，即“非同质化代币”）藏品、数字化身、数字土地等，虚拟财产对现有的“财产”概念形成巨大冲击。饱受争议的是，上述虚拟财产是否属于盗窃罪的侵害对象？肯定说认为，我国刑法中的财物包括有体物、无体物和财产性利益，而虚拟财产具有数字性、价值性、专属性、流通性、相对稀缺性，故虚拟财产属于刑法上的财物。[14] 否定说认为，虚拟财产不属于盗窃罪所能侵害的“财物”，刑法保护虚拟财产的唯一路径是通过对数据的直接保护来实现。[15] 最高人民法院研究室《关于利用计算机窃取他人游戏币非法销售获利如何定性问题的研究意见》认为，“虚拟财产不是财物，本质上是电磁记录，是电子数据……这种电磁记录、电子数据在刑法上的法律属性是计算机信息系统数据”[16]。此后，将游戏代币、虚拟货币等虚拟财产作为财物进而认定为侵犯财产犯罪的判例较少，但仍有部分法院将虚拟财产认定为财物。[17] 可见，犯罪行为对象的虚拟化及在此过程中衍生出的各种新行为对象，为传统刑法规范的适用带来了不少理论与实践上的障碍。

三是侵害程度的严重化。与现实社会的犯罪比，网络犯罪侵害的程度明显增大。首先，在物理空间，行为人往往需要事先选择犯罪场地、准备犯罪工具，而网络空间的虚拟性、无形性、隐蔽性为犯罪实施提供了优渥的条件。[18] 其次，网络具有开放性和扩散性，决定了网络信息传输的即时性、瞬间性和弥散性，故传统犯罪的网络化易使受害人由特定个人转向不特定多数人，造成犯罪结果的不可控性。最后，网络空间的犯罪可能涉及人身财产、公共秩序、国家安全等各个领域，侵害的覆盖面会更为广泛，危害程度也更甚。

四是共犯归责的复杂化。传统犯罪具有清晰的行为参与结构，即以实行犯为中心要

---

⑬ 参见陈毅坚、陈海劲：《私人数字货币发行的刑法规制研究》，载《湖南社会科学》2022 年第 3 期，第 80 页。

⑭ 参见张明楷：《非法获取虚拟财产的行为性质》，载《法学》2015 年第 3 期，第 15-23 页；陈兴良：《虚拟财产的刑法属性及其保护路径》，载《中国法学》2017 年第 2 期，第 165-171 页。

⑮ 参见刘明祥：《窃取网络虚拟财产行为定性探究》，载《法学》2016 年第 1 期，第 156 页；欧阳本祺：《论虚拟财产的刑法保护》，载《政治与法律》2019 年第 9 期，第 50 页。

⑯ 喻海松：《网络犯罪的刑事对策与审判疑难问题解析》，载《人民司法》2018 年第 23 期，第 55-56 页。

⑰ 参见广东省佛山市中级人民法院（2016）粤 06 刑终 1152 号刑事判决书；吉林省敦化市人民法院（2019）吉 2403 刑初 13 号刑事判决书。

⑱ 参见杜磊：《网络犯罪的特征与刑法规制路径》，载《河北法学》2017 年第 7 期，第 94 页。

求意思联络和行为共同的阶层结构，而网络空间彻底改变了传统的犯罪形态，导致犯罪参与行为的结构发生了根本性变化。表现为：（1）网络犯罪几乎不存在传统意义上的实行共犯行为。这是由网络犯罪“互不见面”的特点决定的，犯罪人员不仅互不认识，甚至不需要像在物理空间那样必须在同一时间、同一地点形成合力去实施某一行为，而是可以在网上各自行动。（2）客观行为的共同性在逐步消解。如“帮助行为”往往针对大量或不特定的群体实施，即形成“一对多”的关系，因而造成网络行为交融性、分散化和碎片化。（3）主观意思联络的日益消解。网络空间结构是分布式的，信息交互以必要性而非以整体性为目标，在网络犯罪产业链中行为人只是各自实施相应行为，无需了解下游犯罪具体内容或形成双方意思联络。⑲ 对此，《刑法修正案（九）》增设《刑法》第 287 条之二的帮助信息网络犯罪活动罪，但该罪性质自增设以来争论不断。尽管参与结构发生了变化，但多数学者还是试图在共犯立场下进行理论调适，代表性观点有“中立帮助行为说”⑳、“帮助犯的量刑规则说”㉑ 和“正犯化的帮助行为说”㉒。在传统共犯理论中，共犯从属性说是共犯可罚性的通说。从行为结构来看，网络犯罪参与行为与实行行为存在分离之势，造成传统共犯理论在解决网络犯罪参与行为时存在困难，故这些网络犯罪行为对传统刑法理论的冲击和挑战值得关注。

（三）违反网络空间管理义务型犯罪

基于以信息网络为工具或者为对象的类型化思路，有学者认为，“传统犯罪场所从物理空间转移到了网络空间”㉓，由此出现以信息网络为空间的犯罪。问题是，空间型网络犯罪缺乏明确的内涵与外延，几乎可以涵盖将信息网络作为对象、工具的所有犯罪。㉔ 如在网络空间实施的寻衅滋事、开设赌场、侮辱、诽谤、传播淫秽物品，以及元宇宙沉浸体验下模拟性侵等，这其实不过是传统犯罪在网络空间的展开，事实上仍属于将信息网络作为工具的犯罪形式。笔者认为，应将在此之外利用信息网络实施的犯罪界定为违反网络空间管理义务型犯罪。理由有二：（1）信息网络空间秩序需要独立化保护。随着人类社会生活从现实世界逐步进入虚拟空间，网络空间也由单纯的“信息媒介”向“生活平台”转变。在此过程中，网络行为具有社会意义，其造成的负面影响极有可能扩散到现实社会中，因此网络空间秩序维护的必要性逐渐凸显。而且，信息网络空间既具有虚拟性，其秩序又极易被影响，危害具有较大的扩散性，故需要特殊保护、专业保护甚至是独立保护。（2）信息网络犯罪主体具有特殊性。网络社会建构在网络平台上，其服务提供者作为“网络社会生态环境的主要创建者、网络活动规则的主要制定者”㉕，能够通过自身技术实现对信息的管理与控制。我国法律、法规对网络服务提供者在网络空间特殊领

⑲ 参见王肃之：《网络犯罪原理》，人民法院出版社 2019 年版，第 376-377 页。
⑳ 参见刘艳红：《网络犯罪帮助行为正犯化之批判》，载《法商研究》2016 年第 3 期，第 18 页。
㉑ 参见张明楷：《论帮助信息网络犯罪活动罪》，载《政治与法律》2016 年第 2 期，第 5 页。
㉒ 参见刘宪权、房慧颖：《帮助信息网络犯罪活动罪的认定疑难》，载《人民检察》2017 年第 19 期，第 9 页。
㉓ 刘艳红：《Web3.0 时代网络犯罪的代际特征及刑法应对》，载《环球法律评论》2020 年第 5 期，第 104 页。
㉔ 参见前注 ⑥，苏青文，第 83 页。
㉕ 皮勇：《论新型网络犯罪立法及其适用》，载《中国社会科学》2018 年第 10 期，第 132 页。

域的网络安全管理义务已有规定。《刑法》第 286 条之一拒不履行信息网络安全管理义务罪，明确了网络服务提供者不履行法律、法规规定的管理义务，经监管部门责令采取改正措施而拒不改正，造成相应严重后果时的刑事责任。该罪名体现了督促网络服务提供者履行网络安全管理义务的立法意图，有利于推动信息网络特殊主体主动完善技术安全措施，提高网络治理的质效，起到事前防范的效能。然而，该罪自出台以来在司法实践中“全面遇冷”，几乎沦为“僵尸条款”。[26] 这表明该罪名的设置与规范可能存在问题。

有学者认为，非法利用信息网络罪实际上是传统犯罪预备犯在网络犯罪背景下的正犯化，同时基于传统犯罪的共犯立场理解帮助信息网络犯罪活动罪，认为这两个罪名仍与传统犯罪存在紧密联系，属于利用信息网络实施传统型犯罪的范畴。[27] 诚然，非法利用信息网络行为表现出“一对多”的特征，往往是为他人违法犯罪活动提供准备，但在多数情形下行为人与下游实行犯不存在意思联络，甚至下游实行犯不构成犯罪，那么这种准备行为便不满足实质预备犯下游的实行犯条件，并不具有侵害重大法益抽象危险犯的条件，因此也就难以确认为预备犯的正犯化。同时，无论从法益侵害抑或行为结构看，网络犯罪参与行为与正犯行为均存在分离之势，故难以在传统共犯立场下理解帮助信息网络犯罪活动罪的类型性质。有学者提出两罪名侵害法益并不从属于下游犯罪，是独立的公共法益——信息网络秩序，以论证这两个罪名的独立性，并主张以积量构罪的方式来完善其罪行构造。[28] 对此笔者表示赞同，在此基础上，将两个罪名纳入违反网络空间管理义务型犯罪范畴更为恰当。

综上所述，违反网络空间管理义务型犯罪主要指向刑法分则中的拒不履行网络安全管理义务罪、非法利用信息网络罪及帮助信息网络犯罪活动罪，该类罪的特点表现在犯罪主体的特殊性，作为义务内容与行政法律、法规的依附性，以及行政处罚的前置性等。

二、网络时代我国刑法立法模式的再检视

所谓刑法立法模式，是指立法机关在制定刑法规范过程中采用的具体立法方式或标准样式，如典籍式、散在式及其结合，单一刑法抑或附属刑法等。[29] 就我国刑法立法模式而言，在刑法典之外既有单行刑法也有附属刑法，只不过附属刑法是宣告式的。自 1997 年《刑法》系统修订后，主要是以修正案形式进行修改，附属刑法仍然保持着 1979 年《刑法》宣告式的特点。可以说 1997 年《刑法》奠定了我国单一法典化的立法模式，该模式显然不能完全适应网络时代犯罪多元化和活性化的特点，需要认真梳理和再次检视其症结与缺陷。笔者所主张的三元立法模式及其改造是对现行刑法立法模式的大幅整合、调整、修正与完善，并非完全意义上的新创，当然就其具体方案而言一定程度上体现了对

㉖ 参见陈洪兵：《拒不履行信息网络安全管理义务罪条款“僵尸化”的反思》，载《学术论坛》2022 年第 3 期，第 2 页。

㉗ 参见前注 ⑲，王肃之书，第 408-409 页。

㉘ 参见皮勇：《新型网络犯罪独立性的教义学分析及司法实证》，载《政治与法律》2021 年第 10 期，第 98-100 页。

㉙ 参见李晓明：《再论我国刑法的“三元立法模式”》，载《政法论丛》2020 年第 3 期，第 23 页。

未来我国刑法立法模式的前瞻。

（一）一元模式易造成打击网络犯罪的法网疏漏

1979 年《刑法》是我国首部刑法典，面对改革开放带来的政治、经济剧变，立法机关又先后制定了 25 个单行刑法和 130 多个附属刑法。由于单行刑法与刑法典规定不一致，曾造成司法上的不统一甚至混乱。鉴于此，我国 1997 年对刑法进行系统修订，将 25 个单行刑法并入刑法典，此后又颁布 2 个单行刑法和 11 个刑法修正案，“形成了以刑法典为单一形式的大一统的刑法格局”[30]。

就网络犯罪而言，1997 年《刑法》修订时仅设有非法侵入计算机信息系统罪和破坏计算机信息系统罪。2009 年《刑法修正案（七）》增设非法获取计算机信息系统数据、非法控制计算机信息系统罪。2015 年《刑法修正案（九）》增设帮助信息网络犯罪活动罪、非法利用信息网络罪和拒不履行信息网络安全管理义务罪。为应对网络犯罪行为方式及其对象的变化，最高司法机关出台了大量司法解释以扩张刑法规范的适用范围，即便如此也难以应对迅速发展的网络犯罪。

以破坏信息网络安全的技术型犯罪为例，近年数据安全问题日益突出，随着网络时代数据收集及处理技术的发展，数据安全与个人信息、企业秘密、公共安全乃至国家安全密切关联。如数据采集不当，传输阶段的损害、篡改、泄露，以及数据分析应用中的滥用、未经授权的访问、转让、共享等会产生损害国家安全、侵犯商业秘密等风险。域外国家对数据犯罪的规制往往涵盖了数据流通的诸多环节及侵害手段。如欧盟《网络犯罪公约》第 1、4、5 条分别规定“非法存取”“数据干扰”“数据窃探”等以数据为对象的犯罪。《德国刑法典》第 202a 条规定了“数据窃探”，即未经授权为自己或他人非法窃探受特别保护的数据犯罪。此外，德国刑法对数据犯罪的规制涵盖了数据流通的诸多环节，包括非法探知、截留、预备探知或截留、窝藏、变更数据等犯罪，全方位加大了对数据犯罪的打击力度。[31] 我国非法获取计算机信息系统数据罪和破坏计算机信息系统罪，所针对的主要是与计算机信息系统安全紧密联系的静态数据，仅仅是对数据的非法获取、删除、修改及增加等行为予以规制和惩处，明显存在着立法上的潜在漏洞。

在我国大一统典籍化的刑法立法模式下，应对网络犯罪有两种方式：一是通过出台司法解释，以扩张传统刑法规范的适用范围涵盖网络犯罪新问题；二是通过刑法修正案增设新罪名来规制网络犯罪。前者不仅会造成司法解释对立法的逾越，还会造成法律适用的不确定，从而动摇“罪刑法定”的刑法根基。后者将新型网络犯罪都纳入刑法典也不现实，因为这些犯罪随着社会的变迁呈现出极强的易变性，频繁修改刑法典不利于其稳定性和权威性。显然，一元化的典籍模式将严重阻碍网络时代刑法立法活性化的进程，不可避免地导致犯罪圈的狭窄，造成刑事法网的疏漏，使刑法的滞后性日渐凸显。

---

[30] 刘之雄：《单一法典化的刑法立法模式反思》，载《中南民族大学学报（人文社会科学版）》2009 年第 1 期，第 108 页。

[31] 参见张勇：《数据安全分类分级的刑法保护》，载《法治研究》2021 年第 3 期，第 23 页。

（二）一元模式易催生网络犯罪刑罚结构的重刑化

除工业革命及其技术带来的安全风险“无时不在，无处不在”外，[32] 网络时代网络技术异化的风险也在不断扩张，无论传统犯罪的网络异化还是新型犯罪的网络渗透均颇为复杂，催生网络犯罪刑法规制的早期化甚至重刑化。由于信息网络技术更新迭代迅速，加之新兴技术极有可能被滥用，导致信息网络安全面临严重威胁，必须及时严密刑事法网，通过增设新罪将其纳入刑法的规制范围。但另一方面，网络技术风险也意味着社会发展机遇，网络犯罪圈即使进一步扩张，也不可过于严苛而遏制网络技术发展。

从域外看，死刑废除、自由刑限制、财产刑提升、资格刑丰富等都是网络犯罪刑罚制度发展的趋势。从美国《电脑欺诈与滥用法》看，非法获取国家安全信息犯罪的最高刑为 10 年；非法侵入政府计算机系统而未破坏系统或实施其他犯罪被视为轻罪，最高刑为 1 年；未经授权登录计算机系统后实施其他犯罪，包括破坏计算机或破坏数据等被视为重罪，最高刑为 5 年。《德国刑法典》第 202b 条规定拦截数据罪，刑期为 3 年以下；第 202c 条规定预备窥探和拦截数据罪，刑期为 1 年以下或并处罚金。可见，美国、德国的计算机或数据犯罪均根据不同情形、危害大小形成重刑轻刑、层级分明的刑罚体系。

从我国刑法对网络犯罪规定的最高刑期看，纯正网络犯罪中非法侵入计算机信息系统罪为 3 年，非法获取计算机信息系统数据、非法控制计算机信息系统罪为 7 年，提供侵入、非法控制计算机信息系统程序、工具罪为 7 年，破坏计算机信息系统罪为 15 年，拒不履行网络安全管理义务罪为 3 年，非法利用信息网络罪为 3 年，帮助信息网络犯罪活动罪为 3 年。包括不纯正网络犯罪在内的其他犯罪则呈现重刑化特征：（1）目前刑法有 46 个死刑罪名，保留死刑的罪名仍然较多；（2）刑法分则每个罪名都配置有自由刑，许多罪名都配置 3 年以上的重刑，自由刑在整个刑罚结构中占据绝大部分；（3）财产刑仅规定为附加刑，与其他国家财产刑多处于主刑地位形成对比，且我国还有没收财产刑。

重刑化的刑罚结构缘于网络犯罪仍延续适用传统犯罪的刑罚体系。而在大一统的典籍立法模式下，因刑法典体量有限，规定的罪名必然是社会危害性明显、必须赖以刑法规制的行为，由此形成“既定性又定量”的构罪标准，造成犯罪圈过窄的同时，对危害性较大的行为的惩处也必然较为严厉，最终导致刑罚结构的重刑化。基于网络犯罪立法规制之需，随着网络犯罪圈的扩张，如果不对重刑化的刑罚结构作出调整，不仅严重影响对信息网络犯罪的有效规制，而且阻碍网络科技的良性发展。网络犯罪的技术性特征决定了传统刑罚中的死刑、自由刑的威慑力降低或有效性不足，不仅难以在网络犯罪治理上发挥效能，而且由于刑罚过重严重限缩了网络技术的发展空间。

（三）一元模式易导致网络刑法与前置法衔接不畅

我国行刑衔接不畅问题突出：一是行政执法与刑事司法在程序上缺乏有效衔接。二是实体层面刑法规范与前置法规范内容脱钩。这与我国大一统的刑法典籍模式有关，若将前置法中规定违法的相关条文搬入刑法典，必然导致刑法典条文冗杂、内容膨胀，显然

---

[32] 参见［德］乌尔里希·贝克：《风险社会——新的现代性之路》，张文杰、何博闻译，译林出版社 2018 年版，第 43-48 页。

是典籍化的立法模式难以承受的。[33] 三是对刑法中大量行政犯构成要件要素的理解需要参照前置法的规定，如非法持有枪支罪中的“枪支”等。典籍立法模式无形之中造成刑法与前置法规范的割裂，前置法中大量“情节严重的，依法追究刑事责任”的宣示条款，更是无法与刑法典衔接。

为有效规制信息网络犯罪，我国不仅持续增加新罪名，而且在前置法中出台了一系列围绕信息网络与数据安全制定的法律及规章。然而，由于缺乏立法理论的指导而难以形成有机的科学体系，造成前置法相互之间、前置法与刑法间的衔接存在许多障碍。表现为：（1）前置法与刑法的立法意旨和范畴不统一，在网络空间理念上差异甚大，导致两法在行为与规制及其认定上存在混乱。如《刑法》中拒不履行网络安全管理义务罪的责任主体是“网络服务提供者”，而《网络安全法》中承担信息网络安全管理义务的却是“网络运营者”，全国人大常委会《关于加强网络信息保护的决定》中相关主体又是“网络服务提供者”。[34]（2）前置法与刑法的体系结构和秩序归属严重失衡。《网络安全法》规制了危害网络安全、非法运营关键信息基础设施、侵犯个人信息、利用网站实施违法活动以及网络运营者、关键信息基础设施运营者不履行义务等不法行为，而《刑法》除涉及计算机信息系统犯罪相对集中在第6章妨害社会管理秩序罪外，其他罪名均散见于其他章节。（3）前置法与刑法的调整范围和边界差异甚大。突出表现在“网络”与“计算机信息系统”的概念上，《网络安全法》的“网络”是指由计算机或其他信息终端及相关设备组成的依据一定规则和程序对信息进行收集、存储、传输、交换、处理的系统，而《刑法》的“计算机信息系统”是指由计算机及其相关配套设备含网络、设施构成的，按照一定应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。前者可由计算机、信息终端与相关设备组成，后者可由计算机及相关设备组成，主体范围明显存在差异。[35]（4）前置法与刑法的处罚措施衔接、配套较为有限。《网络安全法》规定有责令暂停相关业务、责令改正、单处或者并处警告、关闭网站、吊销相关业务许可证或者吊销营业执照、处违法所得1倍以上10倍以下罚款、停业整顿等相关资格处罚条款，而《刑法》只包括有期徒刑、管制、拘役、没收违法所得等，行之有效的资格刑并没有得到普遍设置和规定。[36]

学界关于网络时代刑法与前置法衔接的讨论，多集中在拒不履行信息网络安全管理义务罪的争论中。表现在：（1）网络服务提供者管理义务的立法呈现多极化、分散化的特点。《网络安全法》《数据安全法》《个人信息保护法》《反恐怖主义法》《保守国家秘密法》《关于加强网络信息保护的决定》等法律规范中的规定并不一致。（2）关于网络

---

[33] 参见曹波、于世淇：《论新时代统一刑法典模式的辩驳与坚持》，载《重庆理工大学学报（社会科学）》2020年第10期，第83页。

[34] 参见童德华、马嘉阳：《拒不履行信息网络安全管理义务罪之“义务”的合理性论证及类型化分析》，载《法律适用》2020年第21期，第86页。

[35] 参见梁莉、王斑：《网络安全的一体化立法路径——基于〈网络安全法〉与〈刑法〉的对接展开》，载《湖北师范大学学报（哲学社会科学版）》2019年第5期，第45页。

[36] 参见前注[35]，梁莉、王斑文，第46页。

服务提供者的类型，只有《互联网直播服务管理规定》有细致化的类型规定，其他规范性文件中则比较粗疏。（3）各类网络服务提供者的管理义务差别甚小。有学者认为，互联网信息服务提供者和互联网接入服务提供者承担的管理义务最宽，而第三方交易平台服务提供者只承担与中间服务提供者相同的义务。[37] 尤其是在法律及相关司法解释尚未对“其他严重情节”进行明确阐释之前，容易造成兜底条款的无限扩张。[38] 针对“特定危害后果”的认定，其中“致使违法信息大量传播”“违法信息”的判断均应以法律的明文规定为依据，在坚守罪刑法定原则的基础上予以解释和判断。[39]

此外，刑法与前置法的脱钩还体现在定罪量刑标准上。以数据犯罪中的金融数据为例，参照《金融数据安全 数据安全分级指南》，以金融数据所涵盖的信息内容为标准，金融数据可分为客户、业务、经营管理、监管等四大类，在此基础上又可依据数据的影响对象、范围和程度细分为诸多子类，之后还需要依照分级原则进行定级。根据该指南对金融数据的定级规则，依据金融数据安全遭致破坏的危害对象及其程度，将数据安全级别划分为 1 到 5 级，不同级别的数据的安全要求、保护措施差距明显。尽管前置法对金融数据分类分级有着明确的规定，且对不同类别、级别的安全要求、保护措施、限制流动程度等也有所不同，但刑法的定罪量刑标准并未充分体现数据分类分级的内容，难以发挥前置法对定罪量刑的参考及合理限制范围之功能。

综上，在我国单一典籍刑法立法模式下，容易形成规制网络犯罪的法网疏漏、刑罚体系重刑化以及刑法与前置法的衔接不畅等问题。单一刑法典也难以适应网络犯罪活跃化、涉及领域广泛化、责任主体多元化的趋势。该模式呈现出的低效性及规制目的落空，究其原因正在于片面追求典籍立法的统一性和稳定性，忽略了网络时代刑法立法的多元化需求。故笔者建议立足于立法技术、社会发展现实和网络犯罪的类型，反思与重构适合网络时代特点的刑法立法体系。

三、网络时代我国刑法立法模式的应然选择

针对网络犯罪的特点，对其进行针对性、体系化的刑法规制已是学界达成的共识。那么，刑法立法应采取何种模式就是问题的关键。

（一）网络时代刑法立法模式的类型

一定程度上，选择什么样的立法模式直接决定着刑法立法的科学化程度，甚至影响到刑法治理网络犯罪的效能发挥。对于刑法立法模式的选择，学界的代表性观点如下：

一是坚守刑法典的一元模式论。该观点主张继续维持刑法典的模式，不赞成另外制定网络刑法。理由是：（1）网络犯罪是庞大的犯罪类群，若将所有的网络犯罪规定在网

---

[37] 参见皮勇：《论网络服务提供者的管理义务及刑事责任》，载《法商研究》2017 年第 5 期，第 17-18 页。

[38] 参见李世阳：《拒不履行网络安全管理义务罪的适用困境与解释出路》，载《当代法学》2018 年第 5 期，第 76 页。

[39] 参见谢望原：《论拒不履行信息网络安全管理义务罪》，载《中国法学》2017 年第 2 期，第 245 页 。

络刑法中，将导致另一部网络刑法典的形成而非单行刑法；（2）若制定网络刑法，将面临网络犯罪与传统犯罪划分的难题，造成对刑法典的冲击和混乱；（3）改变刑法典模式特别困难，需要特别长的时间，故应继续通过修正案的方式，在刑法典增设网络犯罪。[40] 然而一家独大的刑法典难以系统规制复杂领域罪名，对新型犯罪易产生疏漏。特别是在网络时代，会导致刑法典的不断修改，既损害刑法典的稳定性又无法满足社会秩序的应急之需。

二是增设刑法典的专门章节论。该观点主张，面对网络犯罪在定义、特征上与传统犯罪的差别，将其归类于刑法典的“妨害社会管理秩序罪”章节，既不利于法律规范的完整性，也不利于司法实践中对网络犯罪的认定处罚。故应对有关计算机犯罪和网络犯罪的规范予以整合，增设“网络犯罪”专章或专节。[41] 显然，该主张仍是在维持刑法典一元论模式基础上对现有立法进行修补，属于刑法典的结构变化，重视对网络犯罪的系统化整合，但无法克服网络犯罪扩张带来的刑法典膨胀以及刑法与其他部门法之间的衔接不畅问题。

三是打造网络刑法典的独立论。该观点主张，鉴于网络刑法学所引发的知识变革尤为剧烈和全面，整体修订刑法典作重大调整应为首选，其目标是制定独立的网络刑法典。[42] 也有学者认为，从发展的眼光来看，传统犯罪与网络犯罪的分流指日可待，这就要求传统刑法典彻底转变为全新的网络刑法典，从而真正固化网络刑法学理论体系。[43] 显然，这是在专门章节论基础上更激进的主张，实现网络犯罪领域的大一统。然而，网络刑法典的构建主要是通过搬移现有刑法典里的相关罪名，在此基础上进行补充和体系化，并未涉及刑法与前置法的衔接问题，故该主张仍存在疑问和障碍。

四是完善三元立法的模式论。该观点主张，在网络犯罪新类型不断涌现，一元立法模式弊端日益凸显，单行刑法既可将部分技术型犯罪纳入其中，又可针对网络犯罪规定专门程序的前提下，推进网络犯罪规制的刑事一体化。而附属刑法也能将与互联网相关的诸多行政犯罪吸纳到部门法中，由此法律适用时刑法与前置法之间的衔接不畅也可得以缓解。[44] 故有必要在维持刑法典统一性的基础上发展刑法典、单行刑法与附属刑法三者并立的刑法立法体系。[45] 反对者认为，单行刑法容易导致刑法条文形式有效却实质无用，进而架空刑法典的原有规定。同时认为，采取附属刑法立法模式缺乏相应的法律基础，时机尚不成熟。即便再次启用附属刑法，也需要对其进行更新改造和完善，否则难以解决其“附而不属”问题。[46] 但这恰恰是重构和完善三元立法模式应着重改进的地方，

---

⑩ 参见张明楷：《网络时代的刑事立法》，载《法律科学》2017 年第 3 期，第 75-76 页。

⑪ 参见陈兴良：《网络犯罪立法问题思考》，载《公安学刊》2016 年第 6 期，第 11 页。

⑫ 参见孙道萃：《网络刑法知识转型与立法回应》，载《现代法学》2017 年第 1 期，第 126 页。

⑬ 参见王燕玲：《中国网络犯罪立法检讨与发展前瞻》，载《华南师范大学学报（社会科学版）》2018 年第 4 期，第 136 页。

⑭ 参见姜瀛、储宜彬：《论网络犯罪治理中的刑法立法模式选择——基于立法实质走向与形式契合的分析视角》，载《铁道警察学院学报》2022 年第 2 期，第 46-47 页。

⑮ 参见李怀胜：《论多元化刑事立法模式的构建及方向》，载《山东大学法律评论》2010 年第 7 辑，第 70-74 页。

⑯ 参见卢建平、姜瀛：《犯罪“网络异化”与刑法应对模式》，载《人民检察》2014 年第 3 期，第 10 页。

而非反对该立法模式的真正理由。实际上，没有一种立法模式是一劳永逸或完美无缺的，都是各有利弊，立法模式也必然随着社会对犯罪治理需求的变化而变化。在网络时代背景下，有必要重视三元立法模式治理网络犯罪的合理性与科学性，并在此基础上推动我国未来刑法立法体系的科学化、规范化。尽管三元立法模式的尝试、改造与完善或许会对现有立法模式形成巨大冲击，可谓牵一发而动全身，但却是具有前瞻性和发展空间的。

（二）网络时代三元立法模式的形态及其优越性

前文对具有代表性的刑法立法模式进行了讨论和比较，显然，刑法典的一元模式论在体系与内容安排上存在较大的局限性，而专门章节论与网络刑法典论无法实现刑法与前置法的有效衔接。笔者认为，重构和完善“三元立法模式”是最佳选择，故有必要对该项立法模式的形态及其优越性展开讨论和证成，尤其是论证网络时代我国未来刑法典、单行刑法与附属刑法并立的科学性和合理性。

首先，固守传统刑法典的根基。三元立法模式的建构并不以牺牲现有刑法典为代价，刑法典仍可保留自身的魅力和优势。一部统一的刑法典是一个国家立法成熟的标志，以大陆法系为例，德国、法国、日本等虽然立有大量的单行刑法和附属刑法，但刑法典的地位仍十分重要。大量涉及国家安全、公共安全及传统侵犯人身、财产的犯罪规定于刑法典之中，这些国家也未见有人主张解构刑法典，尤其对于自然犯罪更是如此，故其地位不可动摇。当然，这并不影响我国刑法典的再造及刑法体系的完善。如有学者主张，“在新时代有必要按照法典化的更高要求打造刑法典的‘升级版’”[47]。

其次，开创单行刑法的体系化。单行刑法是指立法机关规定某一领域的犯罪与刑罚，并在形式上独立于刑法典的规范性文件。在我国，单行刑法是国家以决定、规定、补充规定等名称颁布的，但这种经验式的立法不可避免地带有盲目性，难以顾及单行刑法间以及单行刑法和刑法典间内容与体系的协调性，更难以对某一领域的犯罪通盘考虑以制定综合、系统的单行刑法，[48] 易与刑法典发生冲突，是导致法律适用混乱的主要原因。其弊端固然与相对粗疏的立法技术有关，同时也与其未能形成科学的规范体系有关。改造后的单行刑法有以下优势：（1）适用性好。能够根据犯罪态势及时、灵活地制定罪刑规范，严密刑法法网，有利于维护刑法典的稳定。（2）针对性强。能够对某一领域的犯罪进行专门性、针对性、系统性规制，有助于该领域的从业者完整地了解相关刑法规范。（3）有效衔接。能够将实体规范、技术规范与程序规范融为一体，对于规制和打击某些专业性较强的犯罪尤其是网络犯罪十分有效。（4）效能性高。能使刑法规范形成科学严密的有机整体，相互间不仅有科学边界和分工，且能实现相互衔接和有效配合，最终形成高效多能、灵活应变的刑法规范。

最后，完善附属刑法的罪刑规范。附属刑法是前置法中确立的罪刑规范的总称。[49] 学界普遍认为，我国传统的威慑式的附属刑法仅具有提示作用，既无罪名也无罪状和法

---

[47] 周光权：《法典化时代的刑法典修订》，载《中国法学》2021 年第 5 期，第 39 页。

[48] 参见前注 [45]，李怀胜文，第 72 页。

[49] 参见前注 [33]，曹波、于世淇文，第 84 页。

定刑，实际上是“附而不属”[50]，甚至有学者还将其解释为与罪状不相吻合的罪名[51]。笔者主张，散在于部门法中的附属刑法既要独立又要直接规定罪刑规范。其优点在于：（1）及时性强。尤其在规制新兴、复杂、多变的犯罪领域时，可以及时弥补刑法规范的空白和漏洞，既有助于维护刑法典的稳定性又能够增强刑法的及时性、实用性与前瞻性。（2）有机衔接。在前置法中既规定罪名和法定刑又明确构罪要素及其行为特征，增强了立法的协调性与专业性，能够形成有机统一、相互衔接的刑法体系。（3）快速高效。对某一特殊领域作出有针对性、刑行一致的制度设计，尤其是罪刑规范的明确扩充，完善了刑法体系，形成轻轻重重、快速高效的刑罚结构。

当然，不同立法形式的功能、价值取向均有较大差异，也表现出各自的效能和优劣，只有综合建构才能充分体现刑法规范价值维护的层次性和序位性。具体言之，刑法典维护的是国家、社会最重要的法益，与其稳定性、体系性相契合，通常规范那些违背人类基本伦理道德的杀人、放火、盗窃、抢劫、强奸等自然犯罪。单行刑法与附属刑法维护的是某一领域的社会秩序，其中单行刑法维护的是某一特殊领域的政治、经济、社会秩序，具有时代性、灵活性和易变性。附属刑法在加强刑法与前置法的衔接，尤其在维护法秩序统一性与协调性上发挥着其他立法形式不能替代的作用。三元立法模式显然与网络时代背景下犯罪类型化的发展及不同种类犯罪的治理诉求相适应，如利用信息网络实施的传统犯罪仍属于自然犯罪范畴，系传统刑法典理应关注的重点内容；破坏信息网络安全的技术型犯罪需要由针对性强的专门立法来调整，是单行刑法应重点关注的内容；违反网络空间管理义务型犯罪则需要强化刑法与前置法义务规范的衔接，是附属刑法应重点关注的内容。近年来与网络犯罪相关的立法呈现出明显的回应性扩张、预防性前置等特点，面对网络犯罪整体上的立法规制走向，未来的刑法立法模式应与之相契合。单行刑法最能彰显刑事一体化及规制刑法的基本功能理念，有助于实现刑法规制的整体价值目标，而附属刑法有助于在犯罪圈扩张中通过独立的罪名和刑罚种类完成统一的规制秩序，以实现轻轻重重及刑罚轻缓化目标，可见三元立法模式更契合网络时代的刑法立法走向，能够发挥出更大的刑法体系科学化效能。

（三）网络时代三元模式的立法原则

刑法立法的科学化应建立在对刑法立法模式的正确选择上。如上所述，三元立法模式更适合网络时代对刑法立法的实际需求，也更能发挥刑法的效能。在网络时代界分三元立法模式之功效，区别和确立刑法典、单行刑法及附属刑法各自的立法原则显然系重中之重。

首先，基于刑法典自身的地位，其在立法上应秉持理性、审慎的态度，力求法典具有长期的确定性与稳定性。在此两大原则下，再造后的刑法典以规制自然犯为主，此类犯罪罪名相对较为稳定和成熟，通常也不存在与其他法律的衔接问题。回顾近年来我国刑

---

[50] 储槐植：《1997 年刑法 20 年简要回顾》，载《东南法学》2017 年第 2 期，第 8 页。

[51] 参见前注 [33]，曹波、于世淇文，第 84 页。

法修正案的内容即可发现，修改最为频繁的多集中在网络犯罪、金融犯罪、市场秩序犯罪等领域。作为自然犯的传统犯罪，如盗窃、抢劫、杀人、放火、伤害等罪名相对较为稳定，刑法典大致保留危害国家安全罪、危害公共安全罪、侵犯公民人身权利和民主权利罪、侵犯财产罪、军人违反职责罪等类罪。随着网络时代的到来，或许这些传统犯罪可以利用信息网络手段进行，但其基本的犯罪内涵和构成要件不会有实质性改变，故适合规定在刑法典中。当然，作为整个刑法体系重中之重的刑法典再造，也需要在三元立法模式的统领下，做好与单行刑法和附属刑法的有机衔接与配合。特别是针对单行刑法和附属刑法没有规制或不便规制的行为，如果这些罪名已较为成熟或独立、单一，则可纳入刑法典。此外，与自然犯罪较接近的行政犯也可进入刑法典，不必过分机械。

其次，单行刑法作为刑法典的重要补充，针对的是集中统一或新型领域的犯罪，不仅所涉领域特殊，而且所涉罪名群体化，该类犯罪具有针对性、协调性和时效性，甚至在某一领域具有体系性或系统性。为避免刑法规范的混乱，单行刑法应当充分考虑与整个刑法体系的衔接与配套，尤其与刑法典的分工相照应。其基本逻辑是：既能满足打击专业犯罪的需要，又能在特殊领域内建构逻辑严密、罪名结构清晰的刑事法网。随着信息网络技术的发展，网络时代的社会结构及利益形式不断变化，需要进行专门性、体系化规制的犯罪类型将不断涌现，如从破坏计算机信息系统安全的犯罪到数据犯罪，以及未来的人工智能、滥用算法等技术型犯罪。以日本为例，早在 1999 年就针对网络黑客行为制定有《不当入侵行为禁止法》等单行刑法，除规定相关刑事罚则外还将“识别符号”“入侵控制功能”等技术性概念纳入刑法规范。2012 年日本又出台《不当入侵行为禁止法部分修正案》，对不正当取得、不正当保管他人识别符号行为予以规制。[52] 我国现行刑法涉及计算机网络犯罪的条文相对较少，难以跟进当前技术发展与网络犯罪形势，呈现出明显的滞后性。当然，信息网络技术型犯罪领域的规制缺位也为我国未来网络单行刑法的立法预留了空间，尤其是将数据独立于计算机信息系统安全保护后，与数据安全相关的技术型犯罪更是未来网络单行刑法的核心内容，应引起立法者的高度重视。目前而言，刑法典再造后应考虑进行单行刑法立法的内容主要有：反走私犯罪立法、妨害社会管理秩序罪立法、公司及企业犯罪规制立法、破坏市场经济秩序罪立法、侵犯知识产权犯罪防治立法、网络犯罪治理立法、危害环境犯罪防治立法、危害税收管理秩序罪立法等。

最后，附属刑法既是刑法典和单行刑法的重要补充，也是保障经济法、行政法等贯彻执行的有效手段，还能处理好前置法与刑法典、单行刑法的有效衔接，故应具有立法上的独立性和依附性。独立性是相对于刑法典或单行刑法而言的，附属刑法是独立于二者之外的单独罪刑规范。依附性是指附属刑法规范与前置法规范具有关联性，要求附属刑法在设置罪刑规范时依附于前置法，这样更有利于刑法规范与前置法规范的有效衔接。在网络时代，尤其是针对违反网络空间管理义务型犯罪，判断是否成立犯罪要结合前置法所规定的义务规范的具体内容而定，近年来《网络安全法》《数据安全法》《个人信息保

㊷ 参见前注 ㊹，姜瀛、储宜彬文，第 43 页。

护法》等的出台，大大加重了网络服务提供者、数据控制者等主体的合规义务，这些义务内容极为庞杂且分散，若将这些义务违反型犯罪都置于刑法典之内，采用“空白罪状”的表述方式，势必造成“行刑割裂”和适用上的不便。故针对此类犯罪有必要充分发挥附属刑法立法模式的优势，必要时采取“一步到位”的立法策略与方案，直接在与网络安全、数据安全保护相关的前置法中，根据主体义务类型有针对性地设置独立的罪名和法定刑。

四、网络时代我国三元立法模式的建构

在明确三元立法模式的原则及刑法典、单行刑法、附属刑法各自功能的基础上，有必要进一步探讨网络时代背景下三元立法模式的具体建构方案，尤其结合网络犯罪的分类及其特征，深入思考网络犯罪的类型化与三元刑法立法模式间的关系，以及针对不同类型网络犯罪进行刑法立法的侧重点。

（一）利用信息网络实施的传统犯罪以刑法典为主体，以单行刑法、附属刑法为补充

利用信息网络实施的传统犯罪虽然在行为方式、行为对象、共犯归责等方面与现实社会的传统犯罪或有不同，但其法益的实质侵害与传统犯罪并无本质区别，仍在传统刑法典罪名构成要件的涵摄范围内，如网络盗窃、网络诈骗等。

有些方面也有争议，如网络犯罪中的虚拟财产，从最初游戏币、游戏装备等到区块链技术带来的比特币、以太坊、泰达币等加密货币，再到元宇宙的 NFT、数字土地等数字资产，这些虚拟财产是否属于刑法保护的财物，学界争议甚大。赞同者认为，我国刑法上的“财物”是包括有体物、无体物和财产性利益的最广义概念，完全能够涵盖虚拟财产，因此对于具有财产价值的虚拟财产应当按照财物予以刑事保护。[53] 反对者认为，虚拟财产“不是劳动创造的，没有价值，不属于财产”[54]。也有观点认为，作为盗窃罪对象的财物范围仅限于有体物，不包括财产性利益，而虚拟财产显然不是有体物，不属于刑法上的“财物”。[55] 另有学者提出不应将加密货币一律纳入虚拟财产范畴，而应当结合加密货币的类型与应用场景具体分析，从财产和金融资产两大维度来检视加密货币的刑法属性。[56] 随着信息网络的发展，虚拟空间的新兴财产种类持续出现，是否以新的立法一一应对存有争议。尤其我国刑法并未使用“财产性利益”概念，如果照搬德日刑法来解读我国的“财物”范围显然不妥。在罪刑法定原则下，只能从“财物”概念具有的含义去探讨窃取虚拟财产入罪的可能性。另外，新设立的罪名究竟放入刑法典抑或单行刑法或者附属刑法，有必要根据犯罪本身的类型、特征作出选择，虽然发生于网络空间但具有稳定性，且相对缺少专业性、技术性、变动性时，应纳入刑法典规制，以保持刑法典的稳定性。

---

[53] 参见前注 [14]，陈兴良文，第 146 页。

[54] 侯国云、么惠君：《虚拟财产的性质与法律规制》，载《中国刑事法杂志》2012 年第 4 期，第 51 页。

[55] 参见前注 [15]，刘明祥文，第 156-158 页。

[56] 参见马永强：《论区块链加密货币的刑法定性》，载《苏州大学学报（法学版）》2022 年第 2 期，第 105 页。

对传统犯罪在网络化过程中新出现的行为方式与侵害对象对现有规范的冲击，可通过完善法律解释和扩充罪征方式予以解决。针对传统犯罪在网络中的泛化，建议在刑法总则中增设“以计算机网络为工具犯罪”的定罪量刑原则，但以传统犯罪数额或数量标准来界定或区分网络犯罪的严重程度较为困难，故也需针对传统犯罪网络化呈现的特征，合理判断情节严重的标准。鉴于网络空间共犯归责的复杂性，建议对总则中共同犯罪的概念进行修改和完善，如在《刑法》第 25 条增加一款，“网络空间下的共同犯罪，本法有特殊规定的，依照特殊规定处理”[57]，以适应网络共同犯罪形式的变化及其认定需求。

当然，目前刑法典规定的罪名也有大量法定犯，这些犯罪通常与社会经济秩序和市场秩序有关，随着社会的发展与网络时代的到来，需要频繁修改才能适应社会的变迁。实际上，该部分犯罪并不符合刑法典的确定性与稳定性原则。故未来宜将破坏市场经济秩序、妨害社会管理秩序及信息网络等涉及经济法、行政法等易变性较大的罪名从刑法典中分离，或纳入单行刑法进行专门规定，或通过附属刑法调整或规制。另外，一些较成熟稳定的法定犯罪名也可以适当规定在刑法典中。比如有学者认为，“全面修订刑法典的任务包括整合反恐法、反间谍法、监察法等其他法律的处罚内容”[58]。这些内容虽然也可以进行单行刑法立法，但如果罪名成熟、稳定且数量又少，在刑法典中规制也是适当的。

（二）破坏信息网络安全的技术型犯罪以单行刑法为主体

在网络时代背景下，探求单行刑法的立法原则及涉及领域对有效规制网络犯罪意义重大。同时，单行刑法还可满足刑事政策对刑法立法的要求，使政策变化及时在立法中得到充分体现，在此应注意四点：一是确立稳定的有效规制网络犯罪之政策体系。国家安全是信息网络政策的重中之重，尤其在网络空间中国家的权利（力）、义务和责任更要在政策体系和立法规范中明确，以增强对国家基础设施的保护及相应的技术保障。同时，网络规制政策也应当考虑国际通则和惯例，以便与国际接轨。二是确立明确的网络犯罪规制政策之战略需求。宏观战略上，在追求高效打击网络犯罪的同时，逐步建立并巩固国家在信息网络建设与风险防控上的优位，进而制定有效的政策机制及运行规则，保持政策定力和持续性发展，最终保障国家安全。在这方面，既要体现打击犯罪又要保障对外开放，防止二者割裂。三是确立网络犯罪规制政策的具体落实。在信息网络安全领域与网络犯罪规制的政策建构过程中，找到我国网络安全的精准定位，尤其在关系国家核心利益时保持必要的自控权，构建公开透明、切实有效的程序安排与保障，使决策者能够制定出适应网络开放性环境的法律规制政策。四是确立网络犯罪规制政策的行刑控制。在行政监管上设定明确的网络信息流动监控及基础信息和数据科学使用的边界。具体通过透明度高的报告、政府信息公开及国家安全监控等予以保障，应链接相关法律资源，聚焦需要解决的问题，建构处罚标准，确保行刑的有效衔接。

显然，网络时代最为突出的是技术风险，打击网络犯罪的政策方向重点也是对技术

---

[57] 孙道萃：《应对网络共同犯罪还需完善立法》，载《检察日报》2015 年 10 月 12 日，第 3 版。

[58] 前注 [47]，周光权文，第 39 页。

风险的防控。以“信息技术”为基础的网络世界具有多变性、多样性、虚拟性、高速性、跨境性、全球性等特征，技术型网络犯罪的危害规模、传播速度与范围较之传统犯罪更甚，危害性更大。技术型网络犯罪还具有极强的专业背景，技术用语具有高度专业性，如2016 年 9 月法国的 OVH 公司（提供网站托管服务）遭遇了前所未有的大型 DDoS 攻击，攻击者利用物联网，黑掉多个摄像头后形成僵尸网络进行攻击，服务器被攻击的峰值甚至达到了每秒 1Tb。[59] 这还只是网络技术犯罪的冰山一角。未来的刑法规范一方面要针对这些技术难点和技术人群进行规制，另一方面刑法规范所使用的语言也要具有专业性，适时可以直接将技术规范和用语作为刑法规范予以规定，唯有如此才能有效制约该群体的行为。

此外，技术型网络犯罪具有鲜明的智能性、技术性、隐蔽性等特征，需要运用特殊的网络侦查手段来获取及保存作为证据的信息数据。同时，网络犯罪之跨国性会引发刑事管辖权的冲突与协调，需要国际刑事司法协助，这些都涉及刑事程序问题。因此，仅在刑法典中规定实体性条文难以达到实质性的威慑效果，为强化对此类犯罪的打击，迫切需要进行整体刑事法应对，构建刑事一体化的打击策略。单行刑法能够将实体法与程序法融为一体，是一种理想的针对某一领域的刑法立法模式。

综上，针对破坏信息网络安全的技术型犯罪，有必要采取单行刑法的立法模式，并对相关技术型侵害行为进行专门化、系统化的规制，包括加强单行刑法中的技术规范规制，以及刑法中技术规范与其他行业相关技术规范与用语的衔接。“技术规范是有关人类在利用各类技术时应当遵守的行为准则，由于技术的高度专业性，传统刑法规范难以完全适用其中，因此必要时技术规范也可以进入刑法规制。”[60] 在网络十分普及和人工智能迅速发展的时代，网络的高风险性日益凸显，在刑法规范中引入技术规范有利于有效应对相关风险。应结合网络治理实践及国际经验，整合我国刑法中破坏信息网络安全技术型犯罪罪名及相关司法解释，建构兼具程序的单行刑法。值得注意的是，为避免法条的混乱与适用困境，单行刑法不宜直接对刑法典原文进行搬移，立法时应注意单行刑法条文与刑法典条文间的协调性，以及单行刑法自身的系统性、统一性和严密性。

（三）违反网络空间管理义务型犯罪以附属刑法为主体

附属刑法依附于前置法，如经济法、行政法等，具有较强的专业性。将罪刑规范独立于刑法典和单行刑法，直接规定于前置法，便于相关专业人员了解刑法规定、统一掌握标准，从而实现统一规制及行政执法与刑事司法的有效衔接。同时，附属刑法所规定的是法定犯，其规制往往出于解决某一领域或特定时期的突出问题及国家刑事政策的考虑，这类犯罪的波动性很大，通过附属刑法立法，可以灵活地运用不同的刑事政策对相关行为进行犯罪化或非犯罪化处理，从而有效调节社会秩序。[61] 如有学者指出：“刑事立法应

---

[59] 参见《1Tbps！ OVH 遭遇史上最大 DDoS 攻击》，载搜狐网，http://www.sohu.com/a/115234042_465935，2023 年 5 月 1 日访问。

[60] 李晓明：《论人工智能刑法规制中的技术规范》，载《东方法学》2021 年第 2 期，第 54 页。

[61] 参见柳忠卫：《刑法立法模式的刑事政策考察》，载《现代法学》2010 年第 3 期，第 51 页。

当逐步过渡到多元立法模式，特别是应当在行政法、经济法等法律中直接规定行政犯的构成要件与法定刑。”[62] 如此可确保行政执法与刑事司法的一致性。

针对违反网络空间管理义务型犯罪，未来刑法立法的挑战是如何消解行刑规范的衔接不畅。以数据犯罪为例，数字经济时代，数据的获取、产生与应用成为互联网企业业务的主要组成部分，在此过程中，这些主体自然成为数据的获取者、存储者、处理者、传输者以及交易者，进而掌控海量的数据。[63] 然而，数据资源的集中导致数据控制主体一旦控制力度不够就会带来数据滥用的极大风险，而支配的另一面是追责，决定了数据控制主体在风险控制上所能发挥的能动性及其风险防范义务。对此，《网络安全法》《数据安全法》《个人信息保护法》及其他多部规范性文件均对数据控制者的数据安全保护义务予以规定，如建立健全全流程数据安全管理制度、开展数据安全教育培训、采取相应技术与管理措施保障数据安全、数据安全评估义务、数据跨境流动安全保护义务等。拒不履行信息网络安全管理义务罪为追究违反上述管理义务的数据控制主体的刑事责任提供了根据，该罪的适用须参照前置法中相关主体义务规定的具体内容。

目前有关数据安全保护义务的规定较为分散，义务内容间缺乏协调性，义务范围宽泛，使相关主体承担的安全管理义务范围呈无限扩大之势。尤其当前置法规定的安全管理义务与刑法上的作为义务界限不明确、不一致时，将增大罪名被滥用的风险。对此，除完善前置法有关数据安全保护义务的规定外，还需加强义务内容间的协调性。以金融数据跨境为例，还存在以下问题：（1）前置法仅原则性地规定数据分类分级制度及对数据控制主体的跨境安全评估、数据本土化、数据保密等安全保护义务，有关金融数据跨境流动的具体规则仍需参照金融监管部门出台的规范性文件。但在金融业分业监管模式下，监管机构分散、各行业对金融数据跨境安全保护义务的规定不一，甚至存在着大量重合与冲突之处，难以为数据控制主体提供明确的规范与指引。（2）金融数据分类分级标准、数据跨境安全保护义务规定散见于大量规范性文件甚至行业标准文件中，不仅规定混乱、标准模糊、国际国内标准不统一，而且法律位阶过低，甚至达不到《刑法》第96条“违反国家规定”中“国家规定”的标准。针对此，一方面应加强国内金融行业尤其是网络金融或金融数据的规范性建设与管理，实现各行业、领域和条线的金融网络管理与监督义务的科学、规范和明确，为刑法规范执行提供遵循和依据；另一方面要加强国际合作交流，研究借鉴相关国际标准和惯例，必要时可以建议或推动国际有关组织建立及完善相关规则。

另外，对于数据控制主体数据安全保护义务的设定，需要考虑数据处理的不同环节、主体的不同类型及其保护能力的差异等，为其配置不同的义务要求。故在前置法中设置义务罪刑规范时，应当受到刑法典和立法法的双重限制。一是应遵从刑法总则的规定，不能违背总则规范和罪刑法定原则。二是应严格遵循立法法的授权，防止不适格主体假

---

[62] 张明楷：《刑法修正案与刑法法典化》，载《政法论坛》2021年第4期，第3页。

[63] 参见于冲：《数据安全犯罪的迭代异化与刑法规制路径——以刑事合规计划的引入为视角》，载《西北大学学报（哲学社会科学版）》2020年第5期，第94页。

借附属刑法立法扩权。三是应把控附属刑法的立法条件，避免过度扩张对刑法典、单行刑法的冲击。为此，应明确只有在其他制裁措施无法奏效的情况下才可为其设置附属刑法规范，同时应限制附属刑法的最高刑罚上限，如限定为三年以下有期徒刑。

网络犯罪刑法立法的规制走向不可避免地带来犯罪圈的扩大，甚至背离刑法谦抑性原则，造成对网络技术未来发展的过度遏制。因此在附属刑法中，应当适当设置有针对性的罪刑规范，包括与之相适应的罪名和制裁措施。如未来智能机器人有可能成为新型犯罪主体，对其应设置卸载智能运行程序或终止“行动资格”等。再如针对网络平台主体，应设置禁止平台服务、取缔平台资格等刑罚。[64] 总之，规制网络犯罪的附属刑法既要兼顾传统更要凸显新需，充分发挥其灵活性、专业性、衔接性的特征，创设新型罪名与制裁措施，准确回应刑罚早期化、预防刑法和规制刑法的立法目的，拓展新兴网络刑事制裁功能，设置有针对性的罪刑规范，寻求科学的刑罚结构路径。

Abstract: Based on the different forms of information network crime, cybercrime is divided into three types: the technical crime of destroying information network security, the traditional crime of using information network and the crime of violating management obligations in cyberspace. Different types and characteristics of crime have different focus on governance. The unitary model of China's criminal code is difficult to adapt to the development of the Internet era, which can easily lead to the omission of the legal network of cybercrime, the heavy punishment of the penalty structure and the poor connection between the criminal law and the pre-law. The three-dimensional legislative model of the coexistence reflects the hierarchy and order of the maintenance value of the criminal law system. In particular, it has advantages in adapting to the typology of cyber crimes and differences in governance demands. The top priority of its construction is to clarify the legislative principles of the criminal code, the separate criminal law and the subsidiary criminal law, and select the type of crime according to the characteristics of each legislative model. Among them, traditional crimes committed through information networks are subject to the criminal code, supplemented by separate criminal law and subsidiary criminal law; Technical-based crimes that undermine the security of information networks are subject to separate criminal law; Crimes that violate cyberspace management obligations are subject to subsidiary criminal law. As a result, a specialized, targeted and effective scientific system of criminal law has been formed to meet the needs of crime governance in the Internet era.

（责任编辑：王　楷）

[64] 参见孙道萃：《网络刑事制裁范畴的理论视域与制度具象之前瞻》，载《西南政法大学学报》2019 年第 4 期，第 110 页。