

“网络犯罪专章化”观点之探析

余云霞

中南民族大学, 湖北 武汉

收稿日期: 2022年5月27日; 录用日期: 2022年7月5日; 发布日期: 2022年7月13日

摘要

在互联网犯罪已经成为常态的大背景下, 有学者提出应当将我国刑法中的网络犯罪单独列为一章。就目前情况而言, 一方面, 现有刑法体例尚能应对网络犯罪难题, 另一方面, 网络犯罪专章化的条件暂不成熟, 实际操作较为困难, 且易引发新的问题。实际上, 对于网络犯罪的特别规制并非只有专章化这一条路: 在立足现行刑法分则体系的基础上, 梳理归类法益、进行前瞻性立法, 并设计犯罪情节的衡量方法以遏制重刑倾向亦是可取之策。

关键词

网络犯罪专章化, 刑法分则, 立法体例, 规制路径

Explorations toward “the View of Cyber Crime Specialization”

Yunxia Yu

South-Central Minzu University, Wuhan Hubei

Received: May 27th, 2022; accepted: Jul. 5th, 2022; published: Jul. 13th, 2022

Abstract

Under the background that the cyber crime has become the norm, some scholars propose that the network crime in China's criminal law should be classified as a separate chapter. However, as far as the current situation is concerned, one hand, the existing criminal law style can still deal with the problem of cyber crime well, on the other hand, the conditions for cyber crime specialization are not yet mature, and the practical operation is more difficult, and it is easy to cause new problems. In fact, the special regulation of cyber crime is not only a special way. The feasible method is: on the basis of the current criminal law rule system, sort out the legal benefits, carry out forward-looking legislation, and design the measure of criminal circumstances to curb the tendency of heavy punishment.

Keywords

Special Chapter of Cyber Crime, Separate Provisions of Criminal Law, Legislative Style, Regulatory Path

Copyright © 2022 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 问题的提出

网络犯罪专章化，是指在刑法分则中单独确立网络犯罪章节，使其与分则其他章节并列。在大数据时代，网络犯罪呈现侵害法益多元、手段多样的特点，而我国刑法对于网络犯罪，仅作散见于多个章节的具体罪名规定，故现阶段是否有必要通过网络犯罪专章化来强调对网络犯罪的规制，已然成为刑法典面临的重要问题。

1.1. 文献综述

许多学者认为需要进行“网络犯罪专章化”。例如陈兴良教授在《网络犯罪立法问题思考》一文中认为，不同于传统犯罪所导致的危害，网络犯罪所导致的危害具有“连锁性反应”。在互联网时代，惩治多元的网络犯罪、维护网络环境安全已然成为必要，故应当对《刑法》有关计算机犯罪和网络犯罪的法律规定予以整合，增设网络犯罪专节，规定相关罪名[1]；于志刚教授在《网络犯罪的代际演变与刑事立法、理论之回应》一文中认为，在刑法分则中，“计算机和网络犯罪”应独立成章[2]；孙道萃、王燕玲等学者亦主张对网络犯罪“专章化”、“确定单章体例”，乃至创制网络刑法典[3][4]。但仍有学者认为不应“动辄立法”，比如张明楷教授认为，应尽可能通过解释应对网络时代的各种犯罪[5]。

若要专设网络犯罪章节，首先应明确，何种网络犯罪在该章节之列。陈兴良教授指出，网络犯罪应当有广义和狭义之分：广义网络犯罪，指利用网络来实施传统犯罪，对此，并无必要另设新罪名，可以仅在《刑法》中规定提示性条款，以传统犯罪论处；狭义的网络犯罪指那些虽然发生在网络空间，但不能被传统犯罪所涵括的犯罪，或者具有不同于传统犯罪的特殊性的犯罪，对此，则应当在《刑法》中予以专门规定[1]。

1.2. 立法现状

1979年《刑法》由于时代局限性，并无计算机犯罪的规定。我国97年《刑法》第285、286条，是关于保护“计算机信息系统安全”与“计算机信息系统的管理秩序”的规定[6]，第287条中规定了与计算机关联犯罪的适用界限，可大致划分为两种类型，一是“针对危害计算机信息交流安全的行为”，二是“针对利用计算机技术的危害行为”[7]。《刑法修正案(七)》增加了侵犯公民信息类的犯罪，其所保护的法益由计算机安全扩充到公民个人信息权，扩容了信息网络安全保护的范围和力度。《刑法修正案(九)》将网络犯罪的预备行为、帮助行为及信息网络安全管理义务均予以正犯化[1]，同时进一步充实网络犯罪的罪名体系[4]。此外，司法解释亦对网络犯罪相关问题作出解释。由此可见，目前刑法并未设立专章来规制网络犯罪，而是通过在现存章节中增加具体罪名或出台相关司法解释对典型行为进行规定。

1.3. 现存问题

现阶段，我国网络犯罪立法主要存在以下问题：第一，法益杂糅；不仅包括计算机信息系统中的数据安全，还包括个人信息等关联数据安全[3]。第二，立法被动；见招拆招的立法方式，引发了立法理念滞后、规定分散、内容支离等问题[8]。第三，重刑倾向；网络犯罪应对的不足，主要是法网不严密造成的，并不意味着必须用更严厉的刑罚手段处罚网络犯罪[9]。

2. 网络犯罪专章化之否定

根据陈兴良教授的观点，对于网络空间的行为，要作分流处理：首先要审视网络空间与现实空间的行为是否具有对应关系，若是，则可以按照利用计算机实施传统犯罪的模式，对这类网络犯罪以传统犯罪来进行定罪处罚；但如果某种行为只能发生在网络，或者其行为影响的只是及于网络空间的，就应当单独设置妨害网络秩序犯罪，而不能借用传统犯罪的罪名[10]。

在制定网络犯罪专章上，对于针对计算机信息系统的犯罪中的全部犯罪与妨害网络业务、网络秩序的犯罪中的部分犯罪，应当包含在网络犯罪专章中，而该种分类并无法解决上述问题。

2.1. 无法解决的问题

相对缺乏网络领域知识的立法者与日新月异的网络技术之间的矛盾，决定了网络犯罪立法将长期处于被动地位。一方面，立法者无法敏锐地感知到该领域将会发生何种新型犯罪，其“见招拆招”的立法方式是网络立法缺乏体系的根源；另一方面，网络技术高速发展，即便是专家，也可能无法预见技术发展过程中会产生何种犯罪行为，而现存的网络犯罪行为类型只是冰山一角。网络犯罪专章化，仅仅只对网络犯罪立法作形式上的调整，却无法改变立法者“见招拆招”的立法方式，也无法归纳出该种犯罪的大部分行为类型、设置对应罪名，网络犯罪专章化并无法改变立法被动的局面。

此外，法益杂糅是由网络犯罪侵害对象和犯罪方式的多样化决定的，重刑倾向是由“日渐猖獗的网络犯罪需要更严格的刑罚来规制”的时代背景决定的，网络犯罪专章化与此二问题的根源无关，故而并不能解决这些问题。

2.2. 导致的新问题

一是侵犯公民个人信息罪能否归入专章。根据陈兴良教授对网络犯罪类型的分类，侵犯公民个人信息罪并非仅能发生在网络，且其影响不仅仅及于网络空间，因此，其不属于“可单独设置的妨害网络秩序犯罪”，亦不能归入网络犯罪专章；亦有学者认为，网络安全之核心是数据安全[11]，而数据统指一切电子化的记录，包括数字、图形、文本、图片、音频、视频等各种形式，公民个人信息属于数据[12]，据此观点，公民个人信息的安全应当纳入网络安全的保护范畴，在制定网络犯罪专章时应将侵犯公民个人信息罪包含在内。制定网络犯罪专章，必须解决这一问题。

二是专章罪名过少。精通网络的罪犯往往是少数，故大部分罪犯所实施的网络犯罪，都属于“利用网络实施传统犯罪”，所谓“狭义的网络犯罪”在刑法典中都有规定，并能够归入相应的分则章节，如妨害社会管理秩序罪章节中的非法侵入计算机信息系统罪、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。若将此类犯罪单独抽出、形成专章，则该专章中的罪名可能寥寥无几。且不论如此处之会使刑法分则的结构欠妥——存在一个条文过少的章节，更重要的是，专章规制的本意是对其重点保护，但由于该专章条文过少，且相比“利用网络实施传统犯罪”而言并不常见，长此以往，该章在刑法分则中容易被忽视，被认为是不甚重要的章节。

三是法益难以确定。网络犯罪类型多种多样，呈现“跨罪名”的特点，这导致网络犯罪可能侵犯多

个法益。而刑法分则的划分依据在于犯罪行为所侵犯的法益，法益的杂糅势必带来设置专章的困难。法益的确定需要注意以下标准：第一，该章法益不能被刑法分则其他章节的法益所包容，否则就没有独立成章的必要；第二，这种法益划分应当对区分此罪与彼罪有意义，若仅仅为完成独立成章的任务，而将各类网络犯罪行为归集到一起，寻求其同质性并归纳出其侵犯的法益，是没有意义的；第三，对于不可把握的抽象客体，不能将其认为是法益，如“公共安宁”。而在刑法分则依据犯罪所涉法益，已经规定了较为完备的罪名体系的情况下，再遵循上述标准确立新的专章将非常困难。

此外，前述的法益杂糅会带来网络犯罪的界限不明，难以划分此罪与彼罪，在司法认定的过程中，存在这样的可能：当出现疑难案件难以认定时，只要涉及网络，都将其归入“网络犯罪”，适用网络犯罪专章的内容。

四是成本过高。改变现有刑法典体系的成本过高。从立法成本来看，网络犯罪专章化抛出了这样一个难题：将何种类型的网络犯罪归集到一起，设定以何种法益为侵犯对象的专章？这需要投入相当大的人力物力，进行长期研究设计。从司法成本来看，若打乱刑法典现有体系，重新对所有罪名进行分类组合、设置专章，则会带来司法的不适应，造成司法者的误判，影响司法公正性；此外，司法机关还需要投入成本组织司法者学习新法、适应新模式，这会给任务繁重的司法机关与司法者增加更多负担，影响司法效率。

综上，虽然从表面上来看，制定专章更有助于对网络犯罪进行专门规制，但实际上，网络犯罪专章化无助于解决法益杂糅、立法被动和重刑倾向等问题，且改变行之有效的刑法分则体系、增加网络犯罪专章会带来新困境，因此，暂且无需对网络犯罪进行专章规制。

3. 网络犯罪的立法规制路径

一条可取的立法规制路径为：立足现行刑法分则结构，不改变各网络犯罪的章节归属，优先出台司法解释应对实践中的难题，或出台刑法修正案“小修”刑法，在各分则中增设、修改条款。对于前文提出的问题，本节将以这种规制路径为基础加以解决。

3.1. 立法体例的选择

目前，理论上关于网络犯罪的立法体例有两条路径。第一条路径是将其专章化，乃至制定专门法；第二条路径是只需进行个别修改，其中包括在现存法条中增加新的行为类型和行为对象，使现存法条包括新类型网络犯罪的“一元模式”，也包括在现存法条之外增加新条款以规制新型网络犯罪的“二元模式”，此两种模式能够交替进行[5]。

张明楷教授认为，面对网络时代的新型犯罪时，能够通过刑法解释路径予以应对的，就不需要再采取刑事立法路径。就网络犯罪的案发特点而言，利用网络实施犯罪，很多时候与现行刑法规定的各种犯罪并没有明显的界限，且自现行《刑法》颁布以来，不论是增加新犯罪类型，还是修改具体罪状、修改法定刑，均是通过刑法修正案方式对刑法典进行的修改[5]。

因此，本文认为，应立足于“一元模式”，直接适用现行刑法惩治网络犯罪，或以现行刑法分则结构为基础，在各分则之内增设、修改条款，对于实践中的难题，应优先出台司法解释，网络犯罪专章化并无必要。同时，在相当长的一段时间，网络犯罪都无法完全替代传统犯罪，以网络专章化为过渡阶段制定新的网络犯罪法律也并非现阶段的任务。

3.2. 法益的归类与梳理

首先应当对造成法益杂糅的原因进行分析。表层原因包括：第一，网络常常介入传统犯罪；第二，

即便是狭义的网络犯罪,也散见于不同的章节。深层原因是立法的被动性,当出现新的网络犯罪行为时,人们首先想到的是立法,而非将其归类。在法益的梳理、归类中,应把握以下几点:

一是要看到网络犯罪与传统犯罪是相容的概念。首先,许多“网络犯罪”本质上仍然是传统犯罪,网络手段和数据的参与仅仅改变的是犯罪对象的性质,而非犯罪行为的性质,且数据化的法益与同类型的普通法益并无本质区别[13],因此,对于这类犯罪,仍然属于传统犯罪体系。其次,利用网络所实施的传统犯罪也有其体系——刑法分则各章。最后,对于狭义的网络犯罪而言,刑法亦已经形成了分类,若要将其进一步体系化,则可以通过司法解释规定跨罪名犯罪的处理方式,建立二者之间的联系,从而使其形成有机整体。

二是对新型犯罪应当进行归类。本文认为,可以以犯罪对象为划分标准,将网络犯罪分为四大类:一是侵犯特殊数据的网络犯罪,如侵犯国家秘密、军事秘密的犯罪;二是侵犯计算机系统、计算机安全的犯罪;三是侵犯公民个人信息的犯罪;四是侵犯虚拟财产的犯罪。对于出现的新型犯罪,可以将其归入其对应的类别[14]。其意义在于:第一,能够进一步巩固网络犯罪体系,后期可以出台相关的司法解释,以此种分类为依据,规定新型网络犯罪的归属与处理方式;第二,在司法实践中,能够比照同质的传统犯罪,来进行定罪量刑,而无需出台新的规定。

三是要把握立法前瞻性。面对网络犯罪,人们总是出于消极防御的地位,新型网络犯罪行为出现,则紧锣密鼓制定法律、出台解释以弥补漏洞,而仓促的立法、解释会存在考虑不周的情形。为把握立法的前瞻性,可进行以下两种措施:第一,通过兜底条款,让新的行为能够被现存法律所囊括;第二,通过设置专门机构,通过研究犯罪、进行犯罪行为预测来制定对策,实现对网络犯罪的预防[15]。此外,还可以设置兜底条款,应对法律的滞后性。

四是要遏制重刑倾向。并非对于所有的网络犯罪都应严厉处之,在处理网络犯罪时,应综合考虑从严情节与从宽情节,且该类情节均可以在司法解释中进行明确规定。对于“情节严重”、“后果严重”可以设置如下衡量方法:第一步,考虑客观损失,对于能够予以量化的损失,则以数额来衡量严重程度,可以参照其他章节中对犯罪数额的分档进行严重程度的分级;如果客观损失难以估计,则进入第二步,从行为入主体条件出发,衡量行为入行为之恶劣程度。

4. 结语

对网络犯罪进行规制,无需伤筋动骨、大改刑法,较为高效可行的方法是立足于现行刑法,不改变分则体系,仅作部分条文的增删;面对司法难题时优先考虑采用司法解释细化法律规定,而非动辄考虑立法或改变现有刑法分则。值得注意的是,网络犯罪的特点不仅包括为手段的多样性,还包括行为空间的广泛性,各种跨国犯罪层出不穷,网络犯罪的规制呼唤着国际联合,因此,不能仅仅立足于国内网络犯罪规制体系的建设,还应寻求国际网络犯罪规制体系的建设,谋求合作,打击跨国网络犯罪行为。

参考文献

- [1] 陈兴良. 网络犯罪立法问题思考[J]. 公安学刊(浙江警察学院学报), 2016(6): 8-12.
- [2] 于志刚. 网络犯罪的代际演变与刑事立法、理论之回应[J]. 青海社会科学, 2014(2): 1-11+207.
- [3] 孙道萃. 大数据法益刑法保护的检视与展望[J]. 中南大学学报(社会科学版), 2017, 23(1): 58-64.
- [4] 王燕玲. 中国网络犯罪立法检讨与发展前瞻[J]. 华南师范大学学报(社会科学版), 2018(4): 128-136+191.
- [5] 张明楷. 网络时代的刑事立法[J]. 法律科学(西北政法学报), 2017, 35(3): 69-82.
- [6] 高铭喧. 中华人民共和国刑法的孕育诞生和发展完善[M]. 北京: 北京大学出版社, 2012: 512-514.
- [7] 赵廷光, 皮勇. 论我国刑法中的计算机犯罪[J]. 现代法学, 1999(4): 101-103.
- [8] 孙道萃. 网络刑法知识转型与立法回应[J]. 现代法学, 2017, 39(1): 117-131.

- [9] 单奕铭. 我国网络犯罪立法现状及其应然方向[J]. 河北法学, 2018, 36(6): 141-149.
- [10] 陈兴良. 网络犯罪的类型及其司法认定[J]. 法治研究, 2021(3): 3-16.
- [11] 于志刚, 李源粒. 大数据时代数据犯罪的制裁思路[J]. 中国社会科学, 2014(10): 100-120+207.
- [12] 刘一帆, 刘双阳, 李川. 复合法益视野下网络数据的刑法保护问题研究[J]. 法律适用, 2019(21): 109-117.
- [13] 刘宪权, 汤君. 人工智能时代数据犯罪的刑法规制[J]. 人民检察, 2019(13): 31-34.
- [14] 于志刚. “大数据”时代计算机数据的财产化与刑法保护[J]. 青海社会科学, 2013(3): 7-16.
- [15] 曹雅闻. 日本治理网络犯罪的法律对策及借鉴[J]. 中国人民公安大学学报(社会科学版), 2018, 34(2): 125-133.