网络信息安全犯罪的定量评价困境和突围路径

——大数据背景下网络信息量化标准的反思和重构

田　刚

(中央民族大学 法学院,北京 100088)

摘　要:刑法对网络安全的保护立场,正由网络运行安全转向网络信息安全。刑事立法更新不断增设网络信息安全专属罪名的同时,刑事司法的定量评价体系却未能一体构建,成为网络安全刑法保护的薄弱环节。当前网络信息安全犯罪的定量评价体系缺乏明确的逻辑主线,同时适用错位的"传统法益侵害程度"量化标准和模糊的"数据规模"新型量化标准,无法满足网络信息安全专属罪名司法适用的准确性和统一性需求,导致了司法适用的困境。消弭规范和技术之间的差异,以"信息规模"为定量评价核心的基础上,建构信息价值的分层评价模型,并将"组信息"作为基础的数据规模计量单位,是大数据时代背景下,突破网络信息安全犯罪司法定量评价困境的合理路径。

关键词:网络信息安全犯罪;定量评价;量化标准;信息价值;信息计量单位

中图分类号:DF62　　**文献标志码:**A　　**文章编号:**1009-1505(2020)03-0063-14

DOI:10.14134/j.cnki.cn33-1337/c.2020.03.007

信息化是当前法学发展的时代底色,移动互联网、云计算使网络无处不在、无所不能,几乎所有的现实利益和法定权益都可以信息化为电子数据,以信息网络连接、经信息网络运算、借信息网络展示。因此,网络信息安全的保护是我国法律更新的重要方向,而刑法在诸多部门法中无疑走在前列。[①]近年来,刑法在网络空间中大举扩张,大量危害网络信息安全的行为实现了入罪化,网络信息安全犯罪罪名体系逐渐成型。然而,网络信息安全的刑法保护不仅是犯罪定性评价的扩张,定量评价亦需要实现体系化变革,网络信息安全犯罪定量评价模型的重构,成为当前迫切需要解决的问题。

收稿日期:2020-02-12

基金项目:国家社会科学基金重点项目"大数据侦查的程序控制与证据适用研究"(19AZD024);国家社会科学基金青年项目"大数据交易信息安全的刑法保护"(16CFX026)

作者简介:田刚,男,中央民族大学法学院讲师,华东政法大学博士后流动站博士后,法学博士,主要从事网络法研究。

①我国刑法中并没有直接引入"网络信息"或"网络信息安全"概念,而是使用了"信息网络"和"信息网络安全"概念,二者的内涵和外延并不一致,刑法中的"信息网络""信息网络安全"实际上是《网络安全法》中"网络""网络安全"的刑法语言表达。

一、网络信息安全刑法保护的立法扩张和司法挑战

我国网络安全法将网络安全分为了网络运行安全和网络信息安全，前者是“网络处于稳定可靠运行的状态”，后者是“保障网络数据的完整性、保密性、可用性的能力”。二者互为支撑，共同缔造了网络安全。而刑法对网络安全的保护立场，正明显由网络运行安全向网络信息安全转向。近期的相关刑事立法更新，实际上都是围绕着网络信息的生产、传播、收集、储存、利用的刑法评价。[①]然而，在刑事立法将各种严重危害网络信息安全的行为不断入罪的同时，如何准确定量评价不具有实体形态的网络信息，特别是大数据背景下网络信息安全危害程度量化标准的确定，也给刑事司法带来了全新的挑战。

（一）刑事立法更新带来的网络信息安全犯罪外延扩张

信息并非是从未进入刑法视线的全新事物，1997年刑法立法之初，就规定了内幕交易、泄露内幕信息罪和编造并传播证券、期货交易虚假信息罪，两个以信息为犯罪对象的罪名，而侵犯商业秘密罪中，也将特定的技术信息和经营信息作为了犯罪对象。然而，早期的刑事立法中，信息并非是网络安全刑法保护的重点，甚至未曾同网络安全明显联结在一起。1997年刑法立法时，非法侵入计算机信息系统罪和破坏计算机信息系统罪作为两个超前性的“预设罪名”[1]，实际上关注的是网络安全中的网络运行安全。刑法视阈下的网络信息数据，仅是作为计算机信息系统运行安全的组成部分[2]，不具有独立的保护价值。

然而，在互联网技术和大数据技术的双重作用下，信息安全对网络安全的价值开始凸显，2009年《刑法修正案（七）》增设了出售、非法提供公民个人信息罪和非法获取公民个人信息罪，可以视为刑事立法对网络信息安全的正式关注和回应。但是《刑法修正案（七）》同时亦增设了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的程序、工具罪，两个主要保护网络运行安全的罪名。而从保护范围来看，刑法仅对特定的公民个人信息安全进行了保护，而对网络运行安全的保护则明显更为全面，因此，此时刑事立法对网络安全的主要关注点依然是网络运行安全。直到2012年《全国人民代表大会常务委员会关于加强网络信息保护的决定》的颁布，提出了明确的网络信息安全全面法律保护要求，而刑法却受制于前期立法准备的不足，缺乏个人信息以外的信息安全保护专属罪名，不得已采取了扩张传统罪名的方式。两高于2013年颁布了《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》，将编造、传播虚假信息，危害网络公共信息安全的行为，纳入传统“口袋罪”寻衅滋事罪的制裁范围。[②]

随着网络信息安全地位不断地提升，网络安全领域的刑事立法更新，也开始从网络运行安全向网络信息安全转向，网络信息安全犯罪的犯罪圈迅速扩张[3]。2015年的《刑法修正案（九）》将出售、非法提供公民个人信息罪和非法获取公民个人信息罪，合并为侵犯公民个人信息罪，进一步加强了网络个人信息安全保护。[③]与此同时，新增设的拒不履行信息网络安全管理义务罪，非法利用信息网络罪，编造、故意传播虚假信息罪，几乎都可以视为网络信息安全的专属罪名，仅有帮助信息网络犯罪活动罪，

---

①“网络信息”是“信息”的下位概念，特指在网络场域中存在的信息。

②部分学者对司法解释进一步扩大寻衅滋事罪的适用范围提出了批评。详见陈兴良：《寻衅滋事罪的法教义学形象：以起哄闹事为中心展开》，载《中国法学》2015年第3期。

③侵犯公民个人信息罪中的“个人信息”，并不仅限定在网络空间中以电子方式记录的网络个人信息，也包括在现实空间中以其他方式记录的信息，但网络个人信息安全毫无疑问是侵犯公民个人信息罪保护的核心关注。这一点从《网络安全法》第76条第5款和《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（以下简称《侵犯个人信息刑事案件解释》）第1条中对“个人信息”概念的界定中都得到了明确的体现。

是兼顾网络信息安全和网络运行安全的罪名。刑事立法对网络安全的关注开始转向,大量严重危害网络信息安全的行为被纳入刑法的制裁范围。①

(二)建构全新网络信息安全犯罪定量评价体系的司法挑战

网络安全犯罪的犯罪圈不断扩张,在大数据时代演化为全新的犯罪形态。如图1所示,网络安全犯罪的模型,从计算机信息系统犯罪到网络信息安全犯罪再到传统权益犯罪,呈现出纵向发展的复杂态势。而作为中间核心环节的网络信息安全犯罪的五个罪名,除了非法获取计算机信息系统数据罪,②其余四个罪名都属于2015年新增的罪名,需要司法机关明确具体量化标准,成为整个网络安全犯罪司法适用的薄弱环节。

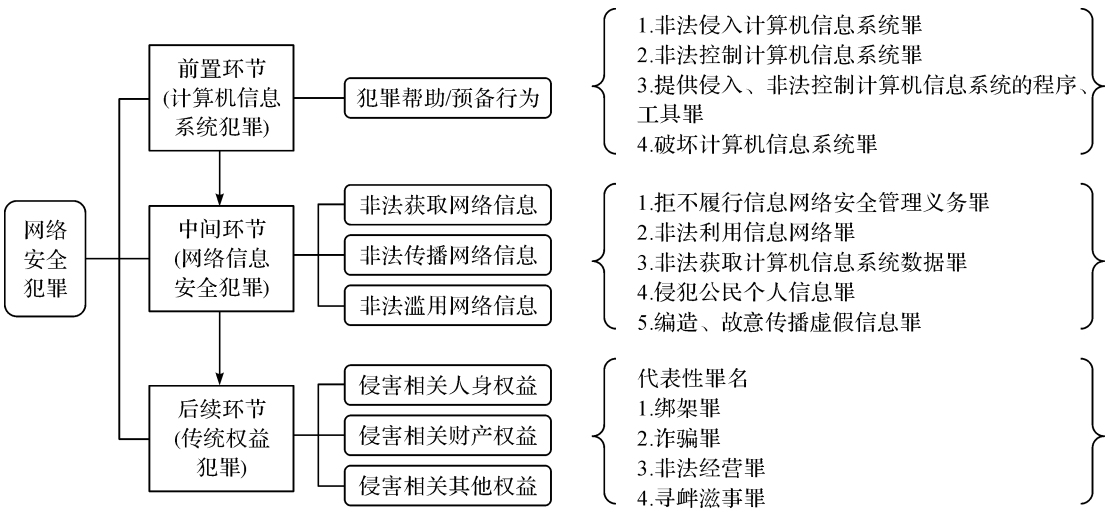

图1　网络安全犯罪纵向发展模型图

1. 网络安全犯罪前置环节的司法定量评价基准——计算机信息系统安全的危害性程度。网络空间中所有的权益都是以信息的形式存在,在大数据时代,绝大部分情况下,高价值的网络信息是非公开的,而是储存在个体、单位、国家的计算机信息系统之中,并采取了多重的技术防护措施。因此,行为人往往需要先通过一定的违法犯罪方式,获得非法接触信息的可能性。例如,非法侵入计算机信息系统、非法控制计算机信息系统、非法破坏计算机信息系统等危害计算机信息系统的犯罪。在互联网犯罪逐渐形成产业化,分工日益复杂化的背景下,早期的计算机信息系统犯罪,演化为广义网络安全犯罪的前置环节[4]。而对此类犯罪行为的司法定量评价基准,主要是根据行为对计算机系统的危害性程度,2011年《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》(以下简称《危害计算机信息系统安全刑事案件解释》)对此进行了集中解释。

2. 网络安全犯罪后续环节的司法定量评价基准——传统法益的危害性程度。在大数据时代,网络信息具有高价值属性,网络信息在被非法获取、非法传播和非法滥用之后,往往会伴随着进一步侵害

---

①网络信息安全为核心的刑事立法更新理念,还辐射到网络安全专属罪名之外的罪名之中。例如,《刑法修正案(九)》同时增设的宣扬恐怖主义、极端主义、煽动实施恐怖活动罪,泄露不应公开的案件信息罪,实际上也都将信息安全,作为恐怖主义犯罪和妨害司法秩序犯罪领域的刑事保护重点。

②值得注意的是,现有司法解释对该罪名适用范围进行了明显限缩,将立法上广义的"计算机信息系统数据"限定为"身份认证信息数据",导致了司法实践中非法获取其他类型数据的行为,无法纳入该罪名的制裁范围。详见田刚:《大数据安全视角下计算机数据刑法保护之反思》,载《重庆邮电大学学报(社会科学版)》2015年第3期。

相关权益的后续犯罪行为,这是网络安全犯罪产业链的最后一环。具体来看,可以分为三种类型:第一,侵害相关人身权利的犯罪。大量网络信息同个体人身权利密切相关,例如行踪轨迹、通讯信息等,利用此类信息实施的绑架罪、非法拘禁罪、侵犯通信自由罪已然出现[5]。第二,侵害相关财产权益的犯罪。在获取、控制网络信息后,犯罪分子开始利用信息实施后续的盗窃、诈骗、敲诈勒索等财产性犯罪,直接侵害信息主体的财产安全[6]。第三,利用信息数据实施的其他犯罪。在大数据背景下,信息中包含着多元的价值属性,例如获得身份认证信息后,行为人可以利用该信息同其他平台账户进行比对,俗称"撞库"行为,可以获得如邮箱账号、社交账号等大量新信息,进而利用上述信息实施多样化犯罪[7]。此类后续犯罪行为虽然成为大数据背景下网络安全犯罪链条中的一部分,但本质上依然是结合了网络因素的传统罪名,基本上可以继续适用基于传统法益侵害性程度的定量评价体系。

3. 网络安全犯罪中间环节的司法定量评价基准——尚未明确。网络安全犯罪的中间环节,是指直接作用于网络信息,危害网络信息安全的犯罪行为。整体上可以分为三种类型:其一,非法获取网络信息行为,包括非法从个体计算机信息系统中获取和从规模数据库信息系统中获取两种方式,后者往往会造成大范围的数据泄露事件。其二,非法传播网络信息行为,包括非法生产和传播网络信息,危害网络安全的行为。从网络信息的自然状态来看,信息生产和信息传播应当是两个相对独立的行为,但我国刑法对单纯编造但不传播的行为,普遍不评价为犯罪行为[8]。因此,我国刑法视阈下编造和传播是合并评价的,单独的传播可以构罪,而单独的编造则不能。遵循我国刑事立法的思路,本文将非法生产信息行为合并到非法传播信息行为之中。其三,非法滥用网络信息行为,是指合法获得、储存信息的单位和个人,非法滥用其储存管理信息数据权限的行为。部分机构和个人负有管理网络信息的职责,但其并不直接获得网络信息的所有权和处分权,随意滥用其管理的信息,将对网络信息安全造成危害。网络安全犯罪的前置环节和后续环节,对应的罪名并不属于网络信息安全专属罪名,前者同时亦是网络运行安全犯罪,而后者则普遍表现为传统犯罪,二者都是在大数据技术广泛运用的背景下,在定性评价的扩展中,被整合到广义网络安全犯罪之中的,在定量评价中依然基本遵循自身的定量评价体系。①而网络安全犯罪的中间环节,②普遍都是由刑事立法近期更新,而被划入到犯罪圈的,整个定量评价体系的基准尚未明确,这也是当前网络信息安全刑法保护面临的主要挑战。

二、网络信息安全犯罪定量评价体系的现状

我国刑法中罪名的适用,高度依赖司法解释所确立的量化标准。特别是刑法修正案增设的新型罪名,尽管都是回应社会治理的紧迫需求,但司法机关往往要等到相关司法解释明确定量标准之后,才会大量适用新罪名,网络信息安全专属罪名亦是如此。因此,司法解释明确量化标准,是网络信息安全刑法保护"落地"的关键环节。目前,网络信息安全犯罪所对应的专属罪名共计五个,包括非法获取计算机信息系统数据罪,侵犯公民个人信息罪,非法利用信息网络罪,拒不履行信息网络安全管理义务罪和编造、故意传播虚假信息罪,而司法解释所确立的量化标准,整体可以分为三种类型。

其一,非法获取网络信息犯罪的多元定量评价标准。非法获取网络信息犯罪对应的专属罪名包括非法获取计算机信息系统数据罪和侵犯公民个人信息罪。相关司法解释所确定的量化标准为:"组信

①网络信息安全犯罪前置行为的定量评价体系,在一定程度上存在着定位不清的问题。例如,《危害计算机信息系统安全刑事案件解释》第4条中,将对计算机信息系统中的数据进行删除、修改、增加作为破坏计算机信息系统罪"后果严重"的情形之一,实际上混淆了网络运行安全和网络信息安全。

②如未作特殊说明,本文中的网络信息安全犯罪特指狭义的网络信息安全犯罪,即构成网络信息安全专属罪名行为的集合。

息”“违法所得”“经济损失”[①]“犯罪相关信息”“条信息”“前科劣迹”,[②]共计六种量化标准。[③]

其二,非法传播网络信息犯罪的多元定量评价标准。非法传播网络信息犯罪对应的专属罪名包括:编造、故意传播虚假信息罪、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。相关司法解释所确定的量化标准为:“信息个数”“传播网络用户账号个数”“传播信息点击数”[④]“信息条数”“传播网站个数”“传播通讯群组个数”“违法所得”“前科劣迹”[⑤]“社会秩序损害程度”,[⑥]共计九种量化标准。

其三,非法滥用网络信息犯罪的多元定量评价标准。非法滥用网络信息犯罪对应的专属罪名包括:拒不履行信息网络安全管理义务罪和侵犯公民个人信息罪。相关司法解释所确定的量化标准为:

---

①《危害计算机信息系统安全刑事案件解释》第1条:“非法获取计算机信息系统数据或者非法控制计算机信息系统,具有下列情形之一的,应当认定为刑法第二百八十五条第二款规定的‘情节严重’:(一)获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组以上的;(二)获取第(一)项以外的身份认证信息五百组以上的;……(四)违法所得五千元以上或者造成经济损失一万元以上的;(五)其他情节严重的情形。”

②《侵犯个人信息刑事案件解释》第5条:“非法获取、出售或者提供公民个人信息,具有下列情形之一的,应当认定为刑法第二百五十三条之一规定的‘情节严重’:(一)出售或者提供行踪轨迹信息,被他人用于犯罪的;(二)知道或者应当知道他人利用公民个人信息实施犯罪,向其出售或者提供的;(三)非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的;(四)非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的;(五)非法获取、出售或者提供第三项、第四项规定以外的公民个人信息五千条以上的;……(七)违法所得五千元以上的;……(九)曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚,又非法获取、出售或者提供公民个人信息的;(十)其他情节严重的情形。”

③同一网络信息安全犯罪类型,不同罪名司法解释中相同的量化标准不重复统计,相关司法解释中的“其他”条款,由于并未设立明确的量化标准,也不纳入统计,下文亦同。

④2019年《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《非法利用、帮助信息网络犯罪刑事案件解释》)第3条规定:“拒不履行信息网络安全管理义务,具有下列情形之一的,应当认定为刑法第二百八十六条之一第一款第一项规定的‘致使违法信息大量传播’:(一)致使传播违法视频文件二百个以上的;(二)致使传播违法视频文件以外的其他违法信息二千个以上的;……(四)致使向二千个以上用户账号传播违法信息的;(五)致使利用群组成员账号数累计三千以上的通讯群组或者关注人员账号数累计三万以上的社交网络传播违法信息的;(六)致使违法信息实际被点击数达到五万以上的;(七)其他致使违法信息大量传播的情形。”

⑤《非法利用、帮助信息网络犯罪刑事案件解释》第10条规定:“非法利用信息网络,具有下列情形之一的,应当认定为刑法第二百八十七条之一第一款规定的‘情节严重’:(一)假冒国家机关、金融机构名义,设立用于实施违法犯罪活动的网站的;(二)设立用于实施违法犯罪活动的网站,数量达到三个以上或者注册账号数累计达到二千以上的;(三)设立用于实施违法犯罪活动的通讯群组,数量达到五个以上或者群组成员账号数累计达到一千以上的;(四)发布有关违法犯罪的信息或者为实施违法犯罪活动发布信息,具有下列情形之一的:1.在网站上发布有关信息一百条以上的;2.向二千个以上用户账号发送有关信息的;3.向群组成员数累计达到三千以上的通讯群组发送有关信息的;4.利用关注人员账号数累计达到三万以上的社交网络传播有关信息的;(五)违法所得一万元以上的;(六)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,又非法利用信息网络的;(七)其他情节严重的情形。”

⑥由于本罪名没有直接相关司法解释,因此参照2013年《关于审理编造、故意传播虚假信息刑事案件适用法律若干问题的解释》第2条的规定:“编造、故意传播虚假恐怖信息,具有下列情形之一的,应当认定为刑法第二百九十一条之一的‘严重扰乱社会秩序’:(一)致使机场、车站、码头、商场、影剧院、运动场馆等人员密集场所秩序混乱,或者采取紧急疏散措施的;(二)影响航空器、列车、船舶等大型客运交通工具正常运行的;(三)致使国家机关、学校、医院、厂矿企业等单位的工作、生产、经营、教学、科研等活动中断的;(四)造成行政村或者社区居民生活秩序严重混乱的;(五)致使公安、武警、消防、卫生检疫等职能部门采取紧急应对措施的;(六)其他严重扰乱社会秩序的。”

“信息条数”“人身权益损害程度”“财产权益损害程度”“社会秩序损害程度”[①]“犯罪相关信息”“违法所得”“前科劣迹”,[②]共计七种量化标准。

综上,在网络信息安全刑法保护不断扩张的背景下,为了满足新增设罪名的司法适用需求,最高司法机关近年来陆续出台了多部司法解释,对相关网络信息安全犯罪的量化标准进行了规定,看似是兼顾了传统犯罪量化标准和网络信息行为新特征,但由于缺乏系统的评价逻辑主线,实际上是一种多元标准混用的状态。值得注意的是,由于我国独特的“定性 + 定量”犯罪成立模式[9],网络信息安全犯罪的定量评价也会对定性评价产生影响。我国刑法公权近年来在网络空间中的迅速扩张,已经引发学界的关注和反思,[③]网络信息安全领域立法更新已经备受质疑的情况下,司法更应坚守刑法谦抑性,避免刑法适用过度扩张。但由于未能建立系统的定量评价体系,当前司法实践中多元标准的混用,反而进一步加剧了刑法公权在网络空间的无序扩张。

三、网络信息安全犯罪量化标准建构困境

网络信息安全犯罪的五个专属罪名之中,除了编造、故意传播虚假信息罪之外,其他四个罪名都已有专门的司法解释,明确了多元的量化标准。然而,网络信息安全犯罪的定量评价,却依然处于一种零散无序的状态,难以准确评价犯罪的危害性,严重制约着刑法的全面有效保护。现有司法解释一方面希望延续部分传统犯罪的量化标准,直接套用传统罪名的数额、法益损害程度等量化标准,另一方面又希望适应网络空间中的行为特征,创制了信息数据量、信息传播量等新型量化标准,结果反而受困于“传统”和“未来”之间,导致了上述量化标准在司法实践具体适用中面临困境。

(一)“传统权益损害程度”量化标准的滞后

当前网络信息安全犯罪定量评价体系中,直接套用了大量传统犯罪的量化标准[10],如非法获取网络信息犯罪中的“违法所得”“经济损失”;非法传播网络信息犯罪中的“违法所得”“社会秩序损害程度”;非法滥用网络信息犯罪中的“人身权益损害程度”“财产权益损害度”“社会秩序损害程度”“违法所得”,实际上都属于财产权、人身权、社会秩序等传统权益损害程度的评价模式。[④]司法解释之所以规定上述标准,是基于网络信息安全权益内涵的丰富性,危害网络信息安全的行为,确实可能同时损

---

①《非法利用、帮助信息网络犯罪刑事案件解释》第4条规定:“拒不履行信息网络安全管理义务,致使用户信息泄露,具有下列情形之一的,应当认定为刑法第二百八十六条之一第一款第二项规定的‘造成严重后果’:(一)致使泄露行踪轨迹信息、通信内容、征信信息、财产信息五百条以上的;(二)致使泄露住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的用户信息五千条以上的;(三)致使泄露第一项、第二项规定以外的用户信息五万条以上的;(四)数量虽未达到第一项至第三项规定标准,但是按相应比例折算合计达到有关数量标准的;(五)造成他人死亡、重伤、精神失常或者被绑架等严重后果的;(六)造成重大经济损失的;(七)严重扰乱社会秩序的;(八)造成其他严重后果的。”

②详见《非法利用、帮助信息网络犯罪刑事案件解释》第5条。

③例如,有学者提出,刑法在网络的肆意扩张已然有“阻碍甚至窒息整个互联网产业的发展”的风险。参见车浩:《刑事立法的法教义学反思——基于〈刑法修正案(九)〉的分析》,载《法学》2015年第10期;又如,有学者提出大量网络空间中的刑法适用是一种情绪性过激反应,“单纯以互联网为工具进行的犯罪行为,刑法不必过于敏感。”参见刘宪权:《刑事立法应力戒情绪——以〈刑法修正案(九)〉为视角》,载《法学评论》2016年第1期。

④需要注意的是,“违法所得”同“经济损失”不同,其并不必然同财产权益损害相映射,刑法构成要件意义上的违法所得,是从“违法行为所带来的损害的角度来把握,即指理论上可以因实施损害公共利益和他人利益的违法行为而直接获得的利益。”参见肖泽晟:《违法所得的构成要件与数额认定——以内幕交易为例》,载《行政法学研究》2013年第4期。因此,“违法所得”同样也可以评价给其他权益造成损害的逐利行为。

害财产权、人身权、社会秩序等传统权益[11],从这个角度来看,似乎直接套用部分传统犯罪量化标准并无不妥。然而,司法解释却忽略了网络信息安全同传统权益之间,并非是单一指向关系,网络信息安全的权益属性是一种复合型权益。在大数据背景下,网络信息安全已然成为一种新型的重要法益,它不再依附于传统法益,而是具有自身独立的价值属性[12],其融合了人身权、财产权等传统私权的同时,也体现了经济秩序、社会秩序等公共利益,特定种类、特定规模的信息,甚至直接同国家利益紧密相连[13]。因此,司法解释直接套用传统权益损害程度的量化标准,显然是一种错位的片面性评价,局限性明显。进一步从技术角度来分析,上述量化标准中除了“违法所得”和“经济损失”可以进行明确的量化之外,其他标准普遍难以量化,标准本身的模糊性,也严重削弱了此类量化标准在司法适用中的可操作性。

(二)新型“信息规模”量化标准的模糊

最高司法机关亦意识到完全套用传统犯罪量化标准,难以准确评价新型的网络信息安全犯罪,因此也引入了基于“信息规模”的全新量化标准。然而,如何在刑法层面,准确评价网络信息的“信息规模”,我国相关司法解释进行了多种尝试,至今未能形成统一认知。

1. 信息传播量的“次数”评价模式。“次数”标准早期是司法解释为应对传统犯罪的网络异化而提出的[14],2004年《关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》(以下简称《淫秽电子信息刑事案件解释》)中,规定了制作、复制、出版、贩卖、传播淫秽电子信息的行为,可以通过信息实际被点击数来评价行为的危害性程度。目前,“次数”被司法解释普遍用于评价非法传播网络信息犯罪的危害性程度,除了“点击次数”还有“浏览次数”。①但此种模式的核心问题在于,仅能适用于非法传播领域,不能适用于其他领域,而且只能评价单一用户的传播行为,难以真实还原网络信息传播的拓扑结构。②

而结合网络信息传播学来看,当前刑事司法仅评价次数的模式,也无法准确界定信息传播的实际影响。因为仅考虑了信息传播的广度,无法评价信息传播的数据规模,缺乏了评价的基础变量。③例如,A 信息全部内容放置一个链接中,点击1次,和将 A 信息内容分割为10个链接,点击10次,传播的信息规模基本一致。

2. 信息本身数据规模的计数评价模式。此种模式直接指向信息的数据规模本身,从技术角度来看最具有合理性,但如何转化为统一的刑法规范化评价,则是困扰司法的难题。实际上,司法解释已经进行了多种尝试。(1)以“组”作为网络信息数据规模的计量单位。根据一定的标准,将犯罪所作用的信息划分为“组信息”,用“组信息”的数量来评价犯罪危害性程度。例如,《危害计算机信息系统安全刑事案件解释》中规定,非法获取金融身份认证信息十组以上的,构成非法获取计算机信息系统数据罪的“情节严重”。④(2)以“条”作为网络信息数据规模的计量单位。根据一定的标准,将犯罪所作用的信息划分为“条信息”,用“条信息”的数量来评价犯罪的危害性程度。例如,《侵犯个人信息刑事案件解

---

①2017年《关于办理组织、利用邪教组织破坏法律实施等刑事案件适用法律若干问题的解释》(以下简称《邪教组织刑事案件解释》)第2条第12款:“……4. 邪教信息实际被点击、浏览数达到五千次以上的。”

②网络信息传播具有拓扑式传导的特征,用户发布的信息被其他用户接收后,部分接收用户会再次发布相关信息,呈现出类似传染病的 SIR 传导模型。(SIR 模型是用于描述信息传导的经典模型,S 为未获得信息内容的个体,I 表示获得信息内容的个体,R 表示获得信息内容但未继续传播的个体)详见王金龙、刘方爱、朱振方:《一种基于用户相对权重的在线社交网络信息传播模型》,载《物理学报》2015年第5期。

③网络信息传播学中,信息传播的内容和广度是信息传播影响评价的两个基础变量。详见江成、刘室辰:《谣言网络多级传播路径下关键引爆点识别模型和算法研究》,载《情报杂志》2020年第3期。

④详见《危害计算机信息系统安全刑事案件解释》第1条。

释》规定,非法获取、出售或者提供可能影响人身、财产安全的公民个人信息五百条以上的,构成侵犯公民个人信息罪的“情节严重”。①(3)以“个”作为网络信息数据规模的计量单位。根据一定的标准,将犯罪所作用的信息划分为“个信息”,用“个信息”的数量来评价犯罪的危害性程度。例如,《非法利用、帮助信息网络犯罪刑事案件解释》规定,致使传播违法视频文件以外的其他违法信息二千个以上的,构成拒不履行信息网络安全管理义务罪的“致使违法信息大量传播”。②

由此可见,当前司法解释对网络信息本身数据规模的量化标准,依然是一种模糊混乱的状态,划分“一组信息”“一条信息”“一个信息”的标准不明确,三种计量单位之间的关系更是模糊,《非法利用、帮助信息网络犯罪刑事案件解释》甚至在一个司法解释中同时使用了“条信息”和“个信息”两种计数单位,令人无所适从。

四、网络信息安全刑法保护定量评价困境的突围路径

网络信息安全刑事立法不断扩张的同时,配套的定量司法评价标准应当一体化建构,目前暴露出的司法乱象和困境,究其根源就是量化标准的模糊和混乱。当前的定量评价体系,无法满足网络信息安全专属罪名司法适用的准确性和统一性需求,以“信息规模”为定量评价核心的基础上,建构信息价值分层评价模型,并设定统一的计量单位,是大数据时代网络信息安全犯罪司法定量评价困境突破的合理路径。

(一)确立“信息规模”为定量评价的核心

虽然不同司法解释规定存在冲突,在我国刑事司法体系中并非罕见[15],但是像网络信息安全犯罪定量评价这样的十余种标准混用还是首次。立法需要规划,司法解释的出台亦应当有体系性,司法解释不能总是以“救火队长”的身份出现,却忽视了司法解释之间的协调。当然,这种无序的司法定量标准本身,也说明了司法机关依然还在探索期,急需理论的指引。而当前理论界对网络信息安全犯罪定量评价的关注严重不足,也使司法机关缺乏足够的理论支持。

1. 网络信息安全犯罪定量评价的域内外基本理论立场。近年来,伴随着刑事立法的扩张,国内理论界围绕网络信息安全刑法保护的研究,呈现爆发式发展态势。然而,目前的理论研究基本围绕着信息的法益属性[16]、信息越轨行为的定性[17]、信息安全刑事立法保护的扩张[18]等网络信息安全犯罪的定性问题展开,基本上都未对定量问题展开深入探讨。即便是专门对网络信息安全犯罪司法解释进行研究时,也有意识地回避定量问题[5]。虽然有学者从宏观层面进行了初步思考,但亦属于凤毛麟角[19]。整体上来看,国内理论界对网络信息安全犯罪定量评价的关注严重不足。但是,司法实践对网络信息安全犯罪准确量刑的需求是客观存在的,并不会因为理论关注较少而削弱。值得注意的是,司法实务部门也对网络信息安全犯罪量化标准进行了总结反思,但要么是从证据认定的程序法角度[20],要么仅是对量化标准进行简单化的循环解释,例如,将量化标准“条”解释为“组”,却未进一步解释“组”的内涵和外延[21],整体上仍然处于零散化的认知状态。

域外大陆法系对信息犯罪的定量评价,理论上普遍认同在比例原则检验下的“强度原则”,即考察信息侵害对个体的外部社会评价带来不利影响的大小。评价信息犯罪危害性大小和刑事责任分配的决定性因素是“个人信息侵害强度”。③上述理论主张亦获得了司法机关的认可,德国宪法法院的判决

---

①详见《侵犯个人信息刑事案件解释》第5条。

②详见《非法利用、帮助信息网络犯罪刑事案件解释》第3条。

③“个人信息侵害强度”(Intensität der individuellen Beeinträchtigung)在德国刑法理论中已然成为专门的学术名词,详见 Stefan Drackert,“Die Risiken der Verarbeitung personenbezogener Daten”, Duncker & Humblot,2014,S. 209-210.

亦主张,网络信息安全犯罪的危害评价,要结合动机、匿名性、信息的个人相关性、信息恐吓的负面结果等侵害性强度来构建。[①]值得注意的是,大陆法系的传统理论观点中,私权是公权的边界,公权应当退让私权,[②]但在信息法益领域大陆法系理论界也认同,当个人信息同时具有了公共利益属性,信息安全犯罪的定量评价标准,则应当将“个体损害强度”转化为“公共损害强度”,信息的公共利益法律性质优先于个体利益法律性质。[③]而域外英美法系对信息犯罪的定量评价,同样强调不同信息价值差异的区分。例如,有学者主张对危害个人信息犯罪,要根据信息同隐私权联系紧密程度来进行定量评价[22];有学者提出,无论是个体还是商业机构,对自身生产、加工的元数据具有独特财产权利,相关信息安全犯罪的危害性评价,要根据信息的财产价值程度调整[23];有学者则主张,根据信息价值的大小,可以将其分为公开数据、半公开数据和非公开数据,刑事责任评价的严厉程度依次递增[24]。

2. 构建“信息规模”为核心的本土网络信息安全犯罪定量评价体系。网络信息安全犯罪定量评价体系的系统化建构,首先需要明确定量评价的核心。当前的司法解释,正是未明确评价的逻辑主线,才会导致传统量化标准和新型量化标准主次不分。笔者认为,诸如“违法所得”“损失数额”“法益侵害程度”等传统量化标准,只能作为辅助性标准,而“信息规模”应当确立为网络信息安全犯罪定量评价的核心。“信息规模”是指,网络信息安全犯罪行为所作用的犯罪对象信息中,蕴含的有价值数据的规模。一方面,从实体法角度来看,网络信息安全的法益蕴含在网络信息之中,网络信息安全犯罪在本质上,是以网络信息为对象的危害性行为,既然在定性层面的信息核心地位已然被学界所普遍认可[25],在定量评价层面,以网络信息安全犯罪所作用的“信息规模”作为量化核心,显然更加符合其法益本质和行为特征,更能实现准确评价。另一方面,从刑事一体化的视角来看,由于网络信息的无限延展性和数据永存性,想准确界定网络行为引发的权益损害极为困难,甚至是不可能的工作。以非法传播网络信息犯罪为例,非法信息一旦在网络空间中散布,理论上其传播的时间和范围都将永久性的延展。将信息蕴含的数据规模作为定量标准,比传统法益标准证明难度更低,更符合刑事诉讼法“事实清楚,证据确实、充分”的证明标准[9]。

更进一步来看,“信息规模”作为网络信息安全犯罪定量评价的核心,也可以避免多核心引发的不同种类量化标准,难以按比例折算问题。当前司法解释,对网络信息安全犯罪设置了多元的量化标准,自然会引发单一量化标准未达到,但是同时接近多个不同量化标准的情况。对此,《侵犯个人信息刑事案件解释》[④]《非法利用、帮助信息网络犯罪刑事案件解释》[⑤]中都规定了规模数据的按比例折算问题,但是这种折算仅限于规模数据之间,对于“违法所得”等传统定量标准,由于定量标准性质上的本质差异,在刑法逻辑上无法进行折算。

以信息的数据规模作为网络信息安全犯罪定量评价的核心,有必要明确“数据”和“信息”之间的

---

①德国联邦宪法法院判决,详见 BVerfGE 100,313;BVerfGE 109,279.

②德国法学界中大量关于刑法制定和适用中的公权和私权边界研究,实际上是在宪法学层面被探讨的。详见 Eric Hilgendorf, “Punitivität und Rechtsgutslehre: Skeptische Anmerkungen zu einigen Leitbegriffen der heutigen Strafrechtstheorie”, Neue Kriminalpolitik,2010,S. 127.

③当特定信息同时具有个人利益属性和公共利益属性时,此时针对该特定信息的犯罪,将被认定为属于危害公共安全的犯罪。详见小西葉子:《テロリスムに対抗する予防的警察活動と比例原則(二)》,载《一橋法学》2018年第1号。

④《侵犯个人信息刑事案件解释》第5条规定:“非法获取、出售或者提供公民个人信息,具有下列情形之一的,应当认定为刑法第二百五十三条之一规定的‘情节严重’:……(六)数量未达到第三项至第五项规定标准,但是按相应比例合计达到有关数量标准的;……”

⑤《非法利用、帮助信息网络犯罪刑事案件解释》第3条规定:“拒不履行信息网络安全管理义务,具有下列情形之一的,应当认定为刑法第二百八十六条之一第一款第一项规定的‘致使违法信息大量传播’:……(三)致使传播违法信息,数量虽未达到第一项、第二项规定标准,但是按相应比例折算合计达到有关数量标准的;……”

关系。刑法视阈下的“信息”和“数据”是一对经常提及的概念,二者都在我国刑法条文规定之中存在,并且在大量的司法解释中互为解释,[①]在理论界也往往将二者视为同一概念混用。[②]但是从法律术语严谨性的角度来看,二者仍然存在一定差异。在内涵层面,根据刑法立法使用习惯,信息一词更侧重于内容属性,其普遍同特定的利益相联结,例如,“内幕信息”“虚假信息”“公民个人信息”,而数据更侧重于形式属性,泛指所有电子化的数据,例如,“计算机信息系统中存储、处理或者传输的数据”;在外延层面,信息更为广泛,信息泛指“现代科学指事物发出的符号系列(语言、文字、数据、状态等)所包含的内容,包括人和人、人和自动机以及自动机和自动机之间的消息交流,动、植物界的信号交流,细胞间和机体间的特征传输等。”[26]因此,信息可以储存在各种介质,包括实体形态的信息和非实体形态的信息,而数据主要是指信息电子化后的无实体形态,例如2019年5月28日公布的《数据安全管理办法(征求意见稿)》中,就直接将数据安全解释为网络数据安全。因此,刑法视阈下的“数据”是“信息”的电子化载体,数据本身不存在价值判断问题。

(二)建构网络信息安全犯罪的分层评价模型

关于网络信息犯罪的定量评价,域外大陆法系和英美法系的基本立场略有差异,前者是基于对公民个人尊严与基本人权的保护,后者则是基于对隐私与自由的保护,但二者普遍认同作为犯罪对象的信息,在实践中有差异化的价值属性,并影响刑事责任的具体分配。同传统犯罪对象的单一化价值不同,信息作为新型犯罪对象具有多元化价值,不同类型信息所体现出的价值层次也不同。从大陆法系的“法益原则”来看,[③]不同信息对权利主体保证其自由和发展的价值存在差异;而从英美法系的“危害原则”来看,[④]侵害不同类型的信息,对权利主体个人利益的损害也有明显不同。

我国最高司法机关对此亦持肯定意见,《危害计算机信息系统安全刑事案件解释》将信息分为“网络金融服务的身份认证信息”和“其他身份认证信息”两种,并设置了差异的量化标准,显然认为前者属于具有较高价值的信息;[⑤]《侵犯个人信息刑事案件解释》和《非法利用、帮助信息网络犯罪刑事案件解释》中将信息分为“行踪轨迹信息、通信内容、征信信息、财产信息”“住宿信息、通信记录、健康生理信息、交易信息等可能影响人身、财产安全的公民个人信息”“其他公民个人信息”三类,价值依次递减。[⑥]可见,我国现有网络信息安全犯罪的定量评价,对犯罪对象的信息在价值上进行了划分,并设置了不同的“信息规模”标准。然而,现有定量评价体系对信息价值划分的标准,存在着明显的缺陷。一方面,缺乏体系性,不同罪名“各自为政”,同一罪名中的划分标准亦不统一。《侵犯个人信息刑事案件解释》和《非法利用、帮助信息网络犯罪刑事案件解释》中,“行踪轨迹信息、通信内容、征信信息、财产信息”的划分,采用的是形式标准,仅根据信息的数据特征来确定。而“住宿信息、通信记录、健康生理信息、交易信息等可能影响人身、财产安全的公民个人信息”的划分,采用了实质标准,需要判断信息所关联的法益来确定。另一方面,理论基础薄弱,难以满足罪责刑相适应原则的严格要求。“行踪轨迹信

①《危害计算机信息系统安全刑事案件解释》第11条规定“本解释所称‘身份认证信息’,是指用于确认用户在计算机信息系统上操作权限的数据,包括账号、口令、密码、数字证书等。”

②许多学者直接将数据同网络信息视为同一概念,在学术研究不加区分地使用。详见单勇:《以数据治理创新社会治安防控体系》,载《中国特色社会主义研究》2015年第4期。

③“法益是在以个人及其自由发展为目标进行建设的社会整体制度范围之内,有益于个人及其自由发展的,或是这有益于这个制度本身功能的一种现实或者目标设定。”参见克劳斯·罗克辛:《德国刑法学总论》,王世洲译,法律出版社2005年版,第15页。

④“制裁损害他人利益的行为,保护个人自由”是刑罚权的唯一正当目的。参见博登海默:《法理学:法律哲学与法律方法》,邓正来译,中国政法大学出版社1999年版,第109页。

⑤详见《危害计算机信息系统安全刑事案件解释》第1条。

⑥详见《侵犯个人信息刑事案件解释》第5条、《非法利用、帮助信息网络犯罪刑事案件解释》第4条。

息、通信内容、征信信息、财产信息”四类信息具有最高价值位阶的依据何在?下一价值位阶的信息,例如“健康生理信息”是否在任何情况下,价值都必然小于“行踪轨迹信息、通信内容、征信信息、财产信息”?这些问题,现有划分标准难以合理回应。

因此,笔者认为有必要重构系统化的信息价值分层模型,以信息同信息安全的关联程度为标准,划分为三层:①第一层,同网络信息安全高度关联的信息,即不用通过数据分析,就可以直接危害重要权益的数据;第二层,同网络信息安全中度关联的信息,即可以直接危害一般权益,或者通过数据分析处理,可能损害重要权益的数据;第三层,同网络信息安全低度关联的信息,即上述两种信息以外的全部数据。重构的模型全部采用实质性判断,不再具体列举特定信息种类的价值阶层。一方面,避免司法解释的绝对化。实践中信息的价值是同应用场景紧密结合不断变化的。例如,同样是“通信内容”信息,根据具体内容的不同,信息价值将具有明显差异。当前司法解释默认所有“通信内容”信息都具有最高价值位阶,忽视了信息应用的复杂性和多样性;另一方面,避免司法解释的滞后性。我们依然处于大数据时代的开端,各类信息数据的价值还在不断发掘,特定信息的价值处于动态发展之中。例如,人的面貌信息,在人脸识别技术日益普及的背景下,价值正在不断提升[27]。法律和司法解释,都有必要给技术发展保留一定的空间。例如,德国立法机关对数据概念的内涵采用模糊态度,就是为了防止新技术发展引发法律概念的不断调整。②因此,我国网络信息安全犯罪定量评价的分层模型亦不应当采用形式标准,采用实质标准,有助于在技术变革期,保持一定的规范稳定性。

(三)设定统一的“组信息”基础计量单位

“信息规模”是当前网络信息安全犯罪定量评价体系中的标准之一,但多种计量单位的混用和内涵模糊,严重阻碍了“信息规模”认定的司法效果,未来将“信息规模”作为核心标准,更需要设定统一的基础计量单位。

首先需要排除的是“次信息”计量单位。因为“次信息”被限定在信息传播领域,并且仅能体现传播的广度,无法真正体现非法传播信息的数据规模,其仅适合在非法传播网络信息犯罪中作为辅助性的量化标准。

同时,“个信息”也不适合作为基础计量单位。“个”普遍用于能够明确划分为最小独立单位的计数,例如“一个人”“一个字符”,并不适合以多样化电子数据为载体的信息规模的计数。《非法利用、帮助信息网络犯罪刑事案件解释》之所以将“个信息”作为计量单位,实际上为了对应信息物理载体电子化后的电子文件计数,所以才将“违法视频文件二百个以上”“违法视频文件以外的其他违法信息二千个以上”,③作为拒不履行信息网络安全管理义务罪中“致使违法信息大量传播”的认定标准。此种模式,最早在淫秽物品犯罪相关司法解释中就已有尝试,④然而,此种模式的核心问题在于,无法准确评价信息规模,特别是在电子图片拼接、剪切,电子书籍摘选与合并,网络音频、视频剪辑的情形下,尤为明显。例如,将一个时长一小时的视频文件,剪辑为10个6分钟时长的视频文件,此时相应的计数就从

---

①值得注意的是,刑法视阈下的数据分层本质上是数据关联的法益价值判断问题,不能直接等同于数据可挖掘性的数据分层,后者可以作为法益价值判断基础后电子取证辅助技术。卢志茂、冯进玫、范冬梅、杨朋、田野:《面向大数据处理的划分聚类新方法》,载《系统工程与电子技术》2014年第5期。

②参见 Vgl. Daniel Schuh, “Computerstrafrecht im Rechtsvergleich – Deutschland, Österreich, Schweiz”, Duncker & Humblot, 2011, S. 53–56.

③详见《非法利用、帮助信息网络犯罪刑事案件解释》第3条。

④《淫秽电子信息刑事案件解释》第1条规定:“以牟利为目的,利用互联网、移动通讯终端制作、复制、出版、贩卖、传播淫秽电子信息,具有下列情形之一的,依照刑法第三百六十三条第一款的规定,以制作、复制、出版、贩卖、传播淫秽物品牟利罪定罪处罚:(一)制作、复制、出版、贩卖、传播淫秽电影、表演、动画等视频文件二十个以上的;……”

“1个”变为“10个”,但信息数据规模并无变化。因此“个信息”计量单位同样应当予以排除。

目前网络信息安全犯罪相关司法解释中,“条信息”是运用最为广泛的计量单位,但其同样不适合作为“信息规模”的基础计量单位。①从形式层面来看,“条”单位普遍用于文字信息计量,不适合对视频、图片等其他形式的网络信息进行计数。“一条视频”“一条图片”显然不符合语言习惯,局限性较为明显。从实质层面来看,“条信息”的判断,高度依赖信息储存的客观状态,司法机关不宜基于价值判断对信息进行二次分割、组合,因为会改变原有信息的“条”数。对此,司法解释采取了一种“妥协性”的做法,《侵犯个人信息刑事案件解释》第11条第3款规定:“对批量公民个人信息的条数,根据查获的数量直接认定,但是有证据证明信息不真实或者重复的除外。”该规定实际上是按照犯罪人对“一条信息”划分的标准,来作为司法层面“条信息”的认定标准。“针对同一对象可能并存‘姓名 + 住址’‘姓名 + 电话号码’‘姓名 + 身份证号’等数条信息,但要求做到完全去重较为困难。为便于办案部门实际操作,突出对侵犯公民个人信息犯罪的从严惩治,《解释》明确对批量公民个人信息的数量根据查获的数量直接认定,但允许根据在案证据排除不真实或者重复的信息。”[28] 因此,如果犯罪人 A,将非法获取的一万名公民姓名、身份证号和住址的规模数据,按照主体标准,储存为一万条信息,那么司法实践中就将按照“非法获取一万条信息”来认定;而犯罪人 B 将非法获取的一万名公民姓名、身份证号和住址的规模数据,按照数据类型标准,以“姓名 + 身份证号”“姓名 + 住址”为内容,储存为两万条信息,那么司法实践中就将按照“非法获取两万条信息”认定。这种交由犯罪人自行决定司法量化标准的模式,显然是不可取的,也暴露了“条信息”计量单位的固有缺陷。

笔者认为“组信息”最适合作为“信息规模”的基础计量单位。其一,从技术层面来看,“组信息”作为计量单位,可以适用于全部网络信息类型,并且可以用于描述不同类型信息的集合。例如,一段文字、视频和音频可以共同构成“一组信息”,这是其他计量单位所不具备的优势;其二,从刑事实体法层面来看,网络信息在作为犯罪对象时,首先要根据信息蕴含的信息安全法益价值大小进行定性评价,然后才能进一步根据信息规模的大小进行定量评价。“组信息”作为计量单位,可以有效解决既需要定性评价又需要定量评价的难题。例如,以特定数据库作为犯罪对象时,无论数据库中信息的数量和形态如何,都可以按照上文的信息分层标准,将其整体划分为高价值信息、中价值信息和低价值信息三大类“组信息”,然后进一步统计每一大类别中有多少小“组信息”,最后对不同大类别的“组信息”数量进行按比例折算,可以充分兼顾信息的定性评价和定量评价。其三,从刑事程序法层面来看,“组信息”作为计量单位,本身就含有司法机关对信息进行分组选择的内涵,便于司法机关根据信息的内容和性质,对信息进行划分整合,使司法机关不再被动依赖犯罪人对信息的储存状态。

关于“一组信息”的数据规模,根据刑法视阈下信息类型的差异,可以分为两种。其一,有合法信息主体的信息,包括侵犯公民个人信息罪中的个人信息、非法获取计算机信息系统数据罪中的个人或机构信息、拒不履行信息网络安全管理义务罪中的用户信息。此类信息,要结合信息主体和信息分层结构共同确立一组信息的数据规模。以个人信息为例,犯罪人 A 非法获取了100名公民的个人信息,每名公民个人信息中包含的信息类别相同,此时将以100为基数,考察数据中是否包含不同价值分层的信息,如果都属于同网络信息安全高度关联、中度关联、低度关联信息中的一类,则直接认定为100组相

①侵犯公民个人信息罪是当前司法实践中适用最多的网络信息安全犯罪专属罪名,《侵犯个人信息刑事案件解释》中将“条”作为公民个人信息规模的单一计量单位,尽管司法解释中规定最少50条信息就可以成立犯罪,但实践中犯罪对象达上亿条信息的情形屡见不鲜。详见刘宏顺:《一两百元就可买上亿条个人信息》,载《四川日报》2016年9月30日第11版;盛望:《高中生窃取1亿条公民信息获利两万元黑客少年窃取的“数据帝国”》,载《西海都市报》2019年10月30日第 A11版。而最高司法机关对“条信息”单位本身亦并不完全认可,因此在后续颁布的《非法利用、帮助信息网络犯罪刑事案件解释》中才会选择多种计量单位混用。

对应的信息；如果同时包含高度关联、中度关联、低度关联三类信息，最后统计的“信息规模”便认定为，高度关联信息100组、中度关联信息100组、低度关联信息100组。而由于不同价值阶层信息的量化标准必然有差异，最后要按相应比例折算后合计。其二，违法、犯罪、虚假信息，包括拒不履行信息网络安全管理义务罪中的违法信息，非法利用信息网络罪中的违法、犯罪信息，编造、传播虚假信息罪中的虚假信息。此类信息由于不存在合法的信息主体，仅根据规模数据对法益的独立危害性，来确立一组信息的标准。以犯罪信息为例，犯罪人 B 在通讯群组发布了五种制造毒品方法的信息，每一种制造毒品方法数据的集合，都是可以独立对法益产生危害的信息，此时应认定为五组信息，然后再判断该信息所处的价值分层，而如果 B 在通讯群组仅发布了一种毒品制造方法信息，无论是否分多次发布，仅能认定为一组信息，然后判定该组信息的价值分层。

当然，“组信息”划定标准下，可能会出现不同个案中“一组信息”所包含的信息规模不一致的情形。笔者认为，在网络信息安全犯罪领域，由于信息的多样性和复杂性，按照量化标准划定的基础信息单元，无法做到在不同个案中完全一致。而该问题的解决，一方面，可以通过增设一些辅助性的量化标准，例如“违法所得”“信息传播量”“数据存储空间”[①]来帮助判定；另一方面，也应当赋予法官一定的自由裁量权空间。在民事网络侵权领域，司法解释明确赋予了法官以根据信息同权益的密切程度来判定责任，刑事犯罪领域同样可以适用该理念，[②]由法官根据个案“一组信息”对网络信息安全危害性程度的差异，来实现刑事责任的合理分配。

参考文献：

[1]于志刚. 青年刑法学者要有跟上时代步伐的激情和责任——20 年来网络犯罪理论研究反思[J]. 法商研究，2017(6)：7-10.
[2]李怀胜. 三代网络环境下网络犯罪的时代演变及其立法展望[J]. 法学论坛，2015(4)：94-101.
[3]白建军. 犯罪圈与刑法修正的结构控制[J]. 中国法学，2017(5)：69-90.
[4]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.
[5]庄绪龙. 侵犯公民个人信息罪的基本问题——以“两高”最新颁布的司法解释为视角展开[J]. 法律适用，2018(7)：16-23.
[6]时延安. 个人信息保护与网络诈骗治理[J]. 国家检察官学院学报，2017(6)：3-24.
[7]皮勇. 全国首例撞库打码案的法律适用分析[J]. 中国检察官，2019(6)：7-9.
[8]于志刚. 全媒体时代与编造、传播虚假信息的制裁思路[J]. 法学论坛，2014(2)：92-100.
[9]高艳东. 网络犯罪定量证明标准的优化路径：从印证论到综合认定[J]. 中国刑事法杂志，2019(1)：127-144.
[10]梁根林. 传统犯罪网络化：归责障碍、刑法应对与教义限缩[J]. 法学，2017(2)：3-13.
[11]欧阳本祺. 论网络时代刑法解释的限度[J]. 中国法学，2017(3)：164-183.
[12]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[J]. 环球法律评论，2019(6)：151-171.
[13]田刚. 大数据安全视角下计算机数据刑法保护之反思[J]. 重庆邮电大学学报(社会科学版)，2015(3)：30-38.
[14]于志刚. 网络空间中犯罪帮助行为的制裁体系与完善思路[J]. 中国法学，2016(2)：5-24.
[15]刘宪权，吴舟. 单位犯罪新立法解释与相关司法解释的关系及适用[J]. 法学杂志，2015(9)：24-31.

①《邪教组织刑事案件解释》中将电子文档的字符、电子音视频的分钟作为定量评价标准之一。从计算机网络技术的角度，“字符”等数据结构单元显然是最标准的信息规模计数单位，但基于规范和技术之间的研究视角差异，刑法学视野下的定量计数单位需要符合价值判断的需求，相同字符量的数据在刑法层面的价值可能完全不同，因此，类似“字符”大小等标准仅适合作为辅助标准，而无法成为核心标准。

②2014年《关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》第10条规定：“人民法院认定网络用户或者网络服务提供者转载网络信息行为的过错及其程度，应当综合以下因素：……(二)所转载信息侵害他人人身权益的明显程度；……”

[16]刘艳红.民法编纂背景下侵犯公民个人信息罪的保护法益:信息自决权——以刑民一体化及《民法总则》第111条为视角[J].浙江工商大学学报,2019(6):20-32.
[17]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.
[18]刘仁文.论非法使用公民个人信息行为的入罪[J].法学论坛,2019(6):118-126.
[19]于志刚,郭旨龙.信息时代犯罪定量标准的体系化构建[J].法律科学,2014(3):127-139.
[20]张铮.刑事推定在批量侵犯公民个人信息刑事案件中的司法运用[J].法律适用,2019(10):71-80.
[21]李静然,王肃之.侵犯公民个人信息罪的情节要素与数量标准研究[J].法律适用,2019(9):69-76.
[22]KIMBLE C,MILOLIDAKIS G. Big Data and Business Intelligence: Debunking the Myths[J]. Global Business and Organizational Excellence,2015,35(1):23-34.
[23]BOYD D,CRAWFORD K. Critical Questions for Big Data[J]. Information Communication & Society,2012,15(5):662-679.
[24]CRAMPTON J. Collect It All: National Security,Big Data and Governance[J]. GeoJournal,2015,80(4):519-531.
[25]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.
[26]董大年.现代汉语分类大词典[M].上海:上海辞书出版社,2007:578.
[27]高铭暄,王红.互联网+人工智能全新时代的刑事风险与犯罪类型化分析[J].暨南学报,2018(9):1-16.
[28]缑杰,宋丹.《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》理解与适用[J].人民检察,2017(16):35-40.

The Quantitative Evaluation Dilemma and the Breakout Path of the Crime of Network Information Security ——Reflection and Reconstruction of the Quantitative Standard of Network Information in the Big-Data Era

TIAN Gang

(*School of Law*, *Minzu University of China*, *Beijing 100088*, *China*)

Abstract: Currently, the protection status of criminal law protecting the Internet security is transforming from the operation security of the network to the information security. At the same time of increasing specific crimes for network information security in the updating of criminal legislature, the criminal justice has failed to build integrated quantitative evaluation systems, which become a weak area in the criminal protection for network security. The current quantitative evaluation system of the crime of network information security lacks clear logic mainline, and still uses the dislocated quantitative standard of "traditional legal interest degree" and blurred new quantitative standard of "data scale", which is unable to meet the requirements of accuracy and the uniformity of the judicial application of specific crimes of network information security, resulting in the judicial dilemma. Eliminating the difference of regulations and technologies, based on the quantitative evaluation as a core, constructing the hierarchical evaluation model of the value of information, and setting the "group information" as a measuring unit, will lead to the rational path of break through the quantitative evaluation dilemma of the crime of network information security in the historical big-data era.

Key words: crime of network information security; quantitative evaluation; quantitative standard; value of information; unit of measurement of information

(责任编辑 陶舒亚)