大数据法益刑法保护的检视与展望

孙道萃

(北京师范大学刑事法律科学研究院，北京，100875)

摘要：大数据时代衍生大数据犯罪，网络数据的代际属性正夯实其独立的法益地位。早期刑法保护表现出从属性与狭隘性，当前保护呈现为重信息网络、弱数据安全的差序格局。多头保护持续暴露数据法益专门保护的疲软。数据法益的专门化与非专门化保护各有利弊，财产化保护具有专属意义，但专门保护具有天然的优先性与后续统领的潜质。网络刑法学的知识转型可以提供终极的制度保障，立法整体转型与创制网络刑法典尤为关键，刑事治理的网络化转型是积极的推动力量。

关键词：数据法益；刑法保护；网络刑法学

中图分类号：D914 **文献标识码**：A **文章编号**：1672-3104(2017)01−0058−07

一、大数据安全与法益保护的刑法挑战

当前，网络空间独立化步步紧逼，大数据时代铺陈开来，大数据法益的刑法保护任务不期而至。而传统刑法学的思维桎梏横亘其中，引发一系列连锁反应。

(一) 大数据安全问题的形成

在互联网 1.0 时代，技术型的计算机犯罪是雏形阶段。但是，主导互联网 1.0 时代的技术、功能、程序等内容已显陈旧，以信息网络为标志的互联网 2.0 时代快速变革，对当前社会生产生活产生巨大的影响，促成现实社会与网络社会形成“双层社会”。在互联网 2.0 时代，信息互动成为主流，信息网络犯罪不断增容，挤压传统计算机犯罪的空间。在此背景下，网络作为犯罪对象、犯罪工具的固有格局正在扩容，网络空间犯罪形态正在扩大化。[1]在互联网 3.0 时代，网络全面渗透到生产生活，网络空间日益成为独立的犯罪时空维度。云计算技术促成大数据时代的到来，网络数据成为新的焦点和关键词。[2]数据安全的脆弱性与易受攻击性越发凸显，大数据犯罪渐成气候。数据法益日渐成为新型网络安全法益，保护网络数据安全成为刑法任务的重中之重。

(二) 数据法益的刑法地位释明

“当世界开始迈向大数据时代时，社会也将经历类似的地壳运动。”[3]数据是一种生产资料，大数据是新财富，价值堪比“石油”。大数据是下一个创新、竞争、生产力提高的前沿，大数据时代与智能化生产和无线网络革命将是引领未来繁荣的三大技术变革。[4]云计算的核心是服务，从大数据的广泛应用看，数据的生成与繁殖具有显著的动态性、开放性、无限延展性，数据应用功能具有无穷的自生性，蕴涵无限潜在的经济效益，是网络经济的动力来源，是网络社会财富资源的新“富矿”。大数据内在的技术优势、应用空间与功能范围、经济效应和财富价值是数据可以作为新型独立法益的基础，是刑法保护新型网络数据法益的认识前提、政策基础与价值依据，使数据拥有法律意义与规范价值，使刑法保障大数据安全具有正当性，奠定刑法积极介入的必要性前提。随着大数据时代逐步确立网络数据的代际主导地位，数据安全诉求急剧攀升，数据法益具有独立的代技术属性与刑法地位，并演化为网络刑法学的法益保护对象和主体内容。

(三) 数据法益保护与传统理论桎梏的碰撞

大数据的技术风险不断累积，传统刑法学以现实物理空间为主要规制对象，应对大数据风险的经验、能力和途径仍处在探索阶段。现行刑法仍保留规制计算机犯罪的陈旧内容，而信息网络安全作为主要保护内容，也间接遮蔽了网络数据的核心地位与独立保护问题，包括网络数据应当作为独立法益保护内容的意识和力度不够、网络数据是否属于刑法中的财产仍模

收稿日期：2016−06−24；**修回日期**：2016−11−05

基金项目：国家社会科学基金一般项目“科技风险的管理与公共安全的刑法保障”(11BFX106)；司法部中青年课题“网络犯罪的立法回应与刑法知识转型”(16SFB3020)；最高人民检察院理论研究所课题“检察机关保障网络安全机制研究”(GJ2016D41)

作者简介：孙道萃(1988−)，男，江西泰和人，法学博士，北京师范大学刑事法律科学研究院博士后研究人员，主要研究方向：刑法学，刑事诉讼法学

糊不清、数据法益如何独立保护等。刑事法治体系始终是社会技术创新、社会财富创造与社会进步的有力保障，而保护数据法益是网络代际更迭赋予的时代使命。我们应立足网络刑法学知识转型的宏观背景，理性回顾我国网络数据刑法保护的进程、现状与不足，明确保护的路径与策略等基本问题。

二、数据法益刑法保护的回顾与反思

通过回顾不同网络代际下数据保护的阶段性与渐进性，可以发现当前网络数据安全的刑法保护存在明显的滞后性，集中表现为意识不强、理念不新、制度不力等，大数据时代的数据法益地位有待正名。

(一) 早期：计算机信息系统数据保护的从属性与间接性

以 1997 年《刑法》的规定为依据，可以发现由于计算机技术立法思维的历史局限性，导致对计算机(信息)系统数据的专门、集中保护乏善可陈。

1. 计算机信息系统数据是网络数据的雏形

《刑法》第 285 条、第 286 条分别保护计算机信息系统安全与计算机信息系统的管理秩序，第 287 条规定与计算机关联犯罪的法律适用界限。[5]前两条将计算机信息系统作为犯罪对象，后者将计算机作为犯罪手段，立法思维可以概括为“针对危害计算机信息交流安全的行为”和“针对利用计算机技术的危害行为”两大类型。[6]第 286 条第 2 款规定“破坏计算机(信息)系统数据和应用程序”，是指对计算机信息系统实际处理的一切有意义的文字、符号、声音、图象等内容的组合以及用户按计算机数据库授予的子模式的逻辑结构、书写方式进行数据操作和运行的程序予以全部或一部分删除、更改或者增加。[7]该观点基本源自《计算机信息系统安全保护条例》第 2 条的规定。另有观点认为，数据是指计算机信息系统中存储、处理或者传输的信息资料。[8]据此，数据是“信息资料”，是计算机信息系统运行产生的“内部”信息系统资料。这既使计算机信息系统数据的内容具有封闭性、静态性和限定性，也使其与应用程序等相关内容区分时缺乏技术的操作性，导致实体内涵的虚无性、空泛性与模糊性。“计算机信息系统数据”是雏形阶段，与网络数据所处代际截然不同。刑法保护具有明显的狭隘性、静态性和封闭性、依附性。

2. 早期保护的不足

早期保护不足主要表现在：①专门、独立、直接的保护规定匮乏。第 285 条规定非法侵入三种特殊计算机信息系统的危害行为，而保护计算机数据并非立法直接意图。尽管第 286 条第 2 款直接规定“数据”，却和应用程序并合规定，忽视数据与应用程序的差异，降低保护数据的独立性。计算机信息系统数据具有明显的静态性、狭隘性等缺陷，无法充分呈现数据法益的独立地位与保护价值。尽管第 287 条具有保护的逻辑可能性，但其他条文并未单独或明确规定数据安全的具体内容，难以实现间接保护。②独立、专门的计算机(信息)系统数据法益保护理念阙如。计算机犯罪主要根植于以计算机技术、软件、程序及信息系统为主要标志的网络 1.0 时代，计算机(信息)系统的技术安全与运行安全成为保护的重心。计算机(信息)系统数据具有明显的依附性或间接性，并非独立的法益类型，独立保护意识和专门的立法规定被搁置不前。

(二) 中期：网络信息保护趋于专门化与扩容化

信息网络是互联网 2.0 代际的标志，经过两次刑法修改后，保护网络信息安全的规定日渐专门化，但保护范围仍略显狭隘，保护意识仍较为淡薄。

1.《刑法修正案(七)》的修改

《刑法修正案(七)》首次专门作出修改，为刑法保护信息网络安全奠定了规范基础：①增加出售、非法提供公民个人信息罪与非法获取公民个人信息罪。公民个人信息安全与网络信息安全高度融合，保护公民个人信息安全正是保护网络数据安全的重要举措[9]，尽管保护效果相对间接、辅助。②增加非法获取计算机信息系统数据罪。非法侵入特殊计算机信息系统或继续非法控制普通计算机信息系统往往是前期网络危害行为，后续一般表现为获取计算机信息系统数据或利用数据附着的信息实施其他关联犯罪，如盗取网络支付账户和密码等后实施盗窃、诈骗等犯罪行为。专门增设该款以强化信息网络安全的保护。③增设提供非法侵入、控制计算机信息系统专用程序、工具罪。力图从源头遏制提供非法侵入、非法控制计算机信息系统的技术行为，提前刑法介入的时间。[9]此外，其他刑法修正也间接扩容信息网络安全保护的范围与力度。

2. 刑法修正的进步

《刑法修正案(七)》增加了计算机信息系统数据保护的专门规定，明显提升保护力度：①首次规定专门保护。相比于第 286 条第 2 款，第 285 条第 2 款保护的对象范围更广、行为类型更具开放性、法益地位相对更独立，也不再被固化为静态的计算机信息系统的部分附属内容或其运行的计算结果，而是动态、开放性的网络信息群。②适度扩容保护范围。信息网络作为互联平台具有开放性与复合型特征，可以融合信

息、财产、利益等因素，客观上扩容计算机信息系统数据的外延，为数据法益的延伸保护提供一定的观念先导。

3. 刑法修正的不足

目前，仅有第 286 条第 2 款、第 285 条第 2 款涉及网络数据保护问题，两次修改也客观上形成了重信息网络、弱数据安全的差序保护问题：①制裁的行为类型范围不全面。诸如非法出售非法获取的数据、掩饰和隐瞒计算机数据及其控制权等行为是否处罚不明。②保护理念不清晰。网络 2.0 时代以信息网络为主导与核心，是对计算机(信息)系统数据保护理念的超越，但却未能兼顾大数据时代的数据安全保护，规范衔接不畅是其“硬伤”。③立法的整体规划滞后。由于网络数据保护的理念不明与立法规定的不足，导致网络数据的概念、保护范围、保护策略、罪名设计、罪状设置等均未正式纳入立法议程，严重影响以数据为未来核心的网络 3.0 时代的立法置换和司法对接。

(三) 渐进转型期：网络数据保护的过渡性与多头化

网络数据是大数据的核心。当前，数据法益的刑法保护与规范供给均处于动荡期，呈现出多头交叉保护的复合化趋势，暴露了数据专门保护的不力。

1. 司法解释的补强与不足

已有的司法解释优劣均沾，主要为：①司法解释的增补。一是厘定适用边界。为细化适用《刑法修正案(七)》，《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》(2011 年，简称为《计算机刑事案件解释》)重点规定具体的定罪量刑标准、刑事责任的范围，并对部分疑难问题作出解释。[10]此解释既解决了一些长期困扰司法机关的难题，也对数据保护产生直接的促进作用。二是确立网络空间安全与法益的独立属性。《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》(2013 年，简称为《网络诽谤解释》)为净化和规范信息网络空间的秩序安定和有序运营提供刑法保障[11]，正式确立了网络空间的独立属性。然而，信息网络安全的突出地位再次宣示信息网络的基础地位，信息网络立法应不断强化。②司法解释的不足。修改理念的代际迟延性导致以下代际缺陷：其一是身份认证信息是严格限缩的“网络信息”。《计算机刑事案件解释》第 1 条规定，数据是指“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或其他身份认证信息”。第 11 条第 2 款规定，“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。据此，“计算机信息系统数据”被限制解释为“身份认证信息”。尽管其具有明确的财产性和经济利益性，但仅是海量网络信息的极小部分，即使规定“其他身份认证信息”具有扩容性和解释空间，仍难以消除以偏概全的解释瑕疵，客观上容易产生信息网络主要保护“身份认证信息”的认识误区。其二是未充分重视和保护网络数据法益的独立意义。“信息系统数据”受制于“计算机技术”主导的时代性，造成数据的静态性与依附性。司法解释仍停留在网络 2.0 时代与成熟的网络信息格局，重在网络的“互联”及其附属功能，未能对大数据时代的数据法益作出释明。虽然“数据”可以表现为“信息”，但具有无穷性、流动性、经济性、社会性、公共性、财产性等特征。网络“数据”具备超越“信息网络”的技术优势和代际基础，亟待正式、独立、专门的保护。

2. 《刑法修正案(九)》的最新刑法修正与遗憾

《刑法修正案(九)》仍立足网络 2.0 时代与信息网络的主导地位，首次大幅度修改网络犯罪及其关联犯罪，但仍有不足：①修改的内容。主要包括：一是大幅度增加网络犯罪规定。增设第 286 条之一、第 287 条之一和之二，再次强化网络信息的保护。二是同步调整关联规定。修改第 253 条之一、修改第 288 条、增设第 291 条第 2 款以及修改第 120 条之一等，通过规制公民个人信息犯罪、扰乱无线电通讯管理秩序罪、利用网络编造、传播虚假信息犯罪与网络恐怖主义活动犯罪，强化网络信息安全的保护体系。②修正的缺陷。主要包括：一是法益保护的对象具有杂糅性。既包括陈旧的计算机信息系统的“数据”，也包括信息网络中海量的信息，还包括个人信息、无线电信息等其他关联信息或特定信息，暴露保护理念的模糊与立法技术的交错性。二是网络数据法益的独立地位不明与保护意识淡薄。尽管信息网络安全仍占据网络安全的半壁江山，但大数据时代已全面嵌入和渗透到社会生产生活，网络大数据正成为社会生产生活的基本素材和核心动力。当前，由信息网络到网络数据的网络代际过渡正在加速形成，具有发展性和扩容性的网络数据正在确立统领地位，网络数据法益的独立属性也将不断显现和充实化。

3. 网络数据是网络信息的替代物

《网络安全法》第 1 条采用“网络”替代陈旧的“计算机(信息)系统”，宏观上确立网络(空间)安全保护的基础概念。当前，信息网络的成熟发达既确立了网络信息的主导地位，也达成了立法的基本共识。尽管第四章专章规定“网络信息安全”，凸显网络信息安全保护的基础地位与重要性，但是，根据第 2 条、第 9 条、第 10 条的规定，网络建设商、网络运营商、网

络服务提供商是与网络用户并行的主要网络参与主体，共同生成、使用海量信息并形成数据库。信息网络的核心是“互联”，与大数据时代的流动“数据池”及其广泛应用、经济利益不同。用户信息仅是网络信息的重要内容，而且，海量互动的网络信息通过云计算技术、扩张解释与立法修改等方式转换为网络数据。比如，《刑法修正案(九)》应将非法获取计算机信息系统数据罪的“数据”加以扩张解释和将“个人信息”调整为“信息数据”的观点便是印证[12]，也是网络代际变迁与大数据广泛应用的必然产物。但《刑法修正案(九)》仍主要聚焦网络信息安全，缺乏对大数据法益的足够认知和立法容纳，导致无法充分展现网络数据法益的地位、作用、功能。

三、网络数据法益的保护路径与策略

我国应立足信息网络并围绕网络数据法益这一核心，加快升级刑法保护的路径、策略，尤应立足于网络刑法学的知识转型，推动数据法益保护的终极蜕变。

(一) 专门化保护、财产化保护与路径研判

在网络 1.0 代际，保护策略分为专门保护(第 285 条、第 286 条)与非专门保护(第 287 条)，传统的财产化保护是主要方式。在网络 2.0 代际，专门化保护与非专门化保护(尤其是财产化)的二元保护模式不断巩固，财产化保护策略的地位上升。[13]但是，独立自主的数据法益专门保护理念和方式值得探索。

1. 财产化与专门化共存的保护格局

主要包括：①专门保护与财产化保护相结合。大数据已经蕴含巨大的财富价值，客观上调整财产的形式或存在形态，为大数据的财产化与刑法保护奠定了基础。可以考虑将网络资源(包括所有权和使用权)直接增列为“财产”的新类型，确立数据的财产化立场。[14]鉴于数据作为核心将日渐取代信息的主导地位，可以增加“非法获取网络数据罪”(由“非法获取计算机信息系统数据罪”修改而成)、“非法获取数据罪”两个专门性罪名。“非法获取数据罪”主要由非专门性的关联罪名组成(涉及国家秘密、商业秘密、公民个人信息等)，最终形成完整的网络数据犯罪罪名体系。[15]该观点专门阐述大数据法益的刑法保护，强调网络数据资源具有现代财产的法律属性和价值性，主张可以沿用现代财产化保护方式并应根据网络犯罪的罪名体系进行专门保护。另有观点立足于网络财产性利益立场，主张专门化与财产化保护相结合、专门化保护是未来主流趋势。[13]“大数据”的财产属性、价值属性、财富意义客观存在，财产化保护无可厚非，但专门、专业、集中保护是必然趋势。②财产化保护。对非法获得他人虚拟财产的行为，不应全部作为计算机犯罪，而认定财产犯罪有其合理性，可以解决部分未利用计算机获取他人虚拟财产行为的处罚，避免处罚的漏洞和罪刑的不均衡现象。但前提是将虚拟财产认定为刑法中的财物，并应重点综合考虑判断方法、解释理念、现实世界的反映、财物的特征、罪刑法定的要求等。而且，可以根据不同的虚拟财产类型及其法益的主体(虚拟财产对法益主体的作用或价值)区分认定价值。[16]该观点仅限于“非法获取虚拟财产”的特定情形，但虚拟财产不等于大数据，因而对网络数据法益保护的意义有限。不过，该观点也间接肯定或扩张解释认定网络资源具有财产属性或价值属性，主张财产化保护符合理论和实践的需要。但可能导致过度放大网络资源的财产属性，弱化网络数据法益的独立地位及专门保护的作用。③专门化保护。针对采取非法侵入方式、窃取网络虚拟财产且情节严重的，因网游“虚拟财产”不属于刑法中的财产，并未侵犯财产所有权，按照盗窃罪论处与法理、司法规律相抵牾，应按照非法获取计算机信息系统数据罪论处。不属于利用技术非法侵入和窃取的，不能按照第 285 条第 2 款论处，对单位工作人员按照侵犯著作权罪论处。[17]该观点也仅限于“窃取虚拟财产”的情形。由于虚拟财产与数据法益不尽相同，该观点也属于间接强调数据法益具有独立于传统财产的内在特性，并倾向于第 285 条第 2 款提供的专门保护。但是，第 285 条第 2 款保护范围不足是其软肋。

2. 财产化保护的优劣研判

尽管财产化保护有其理论基础与司法实践，但仍面临以下难题：①财产化保护的理论基础不扎实。当前，尽管网络数据与传统现实物理社会的财产存在形式差异，却具备传统财产的实质内容[18]，民商法学界目前也持相似立场。即使理论上对网络数据资源的法律属性与财产价值存在分歧，对网络数据的财产化问题存有争议，然而，采取财产化保护有其必然性，可以有效辅助保护网络数据内在的经济属性、价值属性。②未充分制裁非法使用数据等危害行为。传统财产化保护的法益仍主要以所有权为主，使得网络财产化保护路径主要适用非法获取等危害行为。然而，在网络手段型、网络对象型或网络空间型犯罪形态中，网络数据具有显著的使用价值，而且网络数据的使用行为(滥用、乱用等)泛滥不止。[19]财产化保护难以有效规制网络数据使用行为，暴露财产化保护的非周延性，揭示网络数据的价值属性远超过狭隘的财产所有权，

应当至少延伸到使用行为。③数据的价值评估缺乏共识性方案。价值认定是传统财产犯罪的“疑难杂症”，财产化保护也必然重视网络数据的价值评估及其意义。当前，司法机关面临包括“数据是什么”、网络数据价值认定的技术操作瓶颈、数据被主观化后的现实物理价值具有明显的波动性和不确定性等难题。财产化保护路径应当首先解决价值认定问题，否则，财产化保护容易在司法环节出现虚无化、标准不统一等现象。为了超越价值认定难题，网络数据法益的独立化与专门保护是根本出路，同步制定独立的网络犯罪定量因素及其体系予以配套亦不可少。

3. 专门化保护的困题

网络专门保护以网络数据法益的独立地位为前提，但也面临一系列问题：①对网络数据法益内涵的确认与直接规定不明。目前，立法理念仍处在计算机 1.0 时代与网络信息 2.0 时代，犯罪客体主要是计算机信息系统安全与信息网络安全管理秩序，犯罪对象主要是计算机信息系统或信息网络[20]，实践中主要援引第 285 条第 2 款的非法获取计算机信息系统数据罪以及第 286 条第 2 款的规定。刑法中的“网络数据是什么”仍未知，使得数据法益的刑法内涵模糊不清。然而，此举直接混淆不同网络代际的数据法益，既使得专门保护的对象不明确，也导致大数据法益的保护容易流于形式。我国应当加快《中华人民共和国信息数据法》的立法工作，为合理圈定网络数据法益提供前提和依据。②专门保护的规范竞合助长司法内耗。当前，网络立法的内在缺陷使网络犯罪客体与犯罪对象高度重合，网络危害行为的界限模糊，网络罪名频现竞合。比如，在“流量劫持”案中，虽都采取 DNS 攻击方式，却分别论处破坏计算机信息系统罪与非法控制计算机信息系统罪，说明第 286 条规定的“破坏”可以包括第 285 条规定的“侵入”“非法获取”“非法控制”“提供”。[21]在网络立法明显供给不足时，专门化保护的内部竞合虽难以避免，却增加了司法保护方式的复杂性与非规律性，也暴露出专门化保护的制度瓶颈。③专门保护的立法意识与司法适用序位偏低。大数据法益地位正处在形成期，网络刑法立法暂时无法提供充足的规范供给，专门化保护客观上无法全面保护网络数据法益，导致财产化保护占据很大比重，间接压制专门保护的司法序位。专门化与非专门化组成的复合型保护格局有其合理性，但网络信息数据是未来网络刑法立法的核心内容[22]，保护网络财富资源应首选专门化保护且兼顾财产化保护，并应加大司法适用的频次。

4. 专门保护的统摄

我们应考虑最终确立专门化保护的统领地位，理由为：①网络代际变迁与刑法知识转型的必然性。由传统现实物理社会彻底过渡到网络社会、从传统计算机信息系统与信息网络的时代到网络数据时代的全面覆盖，不仅注定了从传统刑法学到网络刑法学的知识变革命运，也必然导致传统犯罪的绝对主导时代逐渐切换到网络犯罪的统领时代。犯罪本质的蜕变决定犯罪形态、刑法理论体系及保护方式的转型。②财产化保护与专门化保护的分工与地位不同。目前，难以科学预测网络代际的变迁速度、频率与连锁反应，过渡期应避免路径的单一化。网络代际切换与更迭导致传统财产的概念、形式及其保护方式不断发生变换，现代财产的概念及其形式变动不居，加剧财产化保护的司法不确定性与法理的不稳定性。网络数据和刑法财产概念时刻在变动，短期内难以形成固定且唯一的专门保护或财产化保护模式，复合型保护格局则有其存续意义。数据的网络安全法益与财产法益可以并行不悖，专门保护和财产化保护却应有主次之别。③专门保护的优位性。数据是核心，兼具技术属性与财富属性，数据可以包容网络财产利益，但更是独立的网络利益与财富的增长点。保护网络数据往往便保护了网络财产法益，专门保护与财产化保护并非对立关系，但保护财产法益并不必然保护数据法益，财产化保护方式并不能直接等同专门保护。专门保护立足网络数据法益的独立地位，在兼顾与包容财产化保护方式时，更凸显独立保护意识，强调数据法益整体上的包容性与统摄性。

(二) 网络刑法学知识转型的驱动

网络刑法立法转型具有突出的引领作用，但“网络刑法学”作为传统刑法学全面“网络化”的远景形态，是大数据法益刑法保护的终极供给方案。

1. 网络刑法立法转型的要务

刑法立法是推动网络刑法学稳步前进的主要动力，更是保护网络数据法益的优先选项。首先，是网络立法理念的重构。从国际发展趋势看，计算机犯罪已并非发展主流。[23]传统立法过度以计算机技术及其运行为重点，立法思维的陈旧已经严重制约刑法规范的更新与有效性，既与信息网络时代的保护主题摩擦不断，也导致大数据保护的代际落差愈来愈大。大数据时代正在确定网络数据的核心地位。保护数据应当作为新的立法任务，数据安全法益的刑法立法实现应当占据关键地位。其次，是网络法益扩容。法益内容应当随着犯罪形态及对象的延展实现同步的扩容。围绕计算机技术或信息网络的立法应主要聚焦计算机信

息系统安全或信息系统管理秩序等法益[24]，但数据安全法益使其逐渐陷入脱节与断代的边缘。大数据时代不仅奠定数据的统领地位，也间接弱化信息网络的优势，数据法益正成为刑法保护的核心法益。数据法益是新型刑法法益类型，是以大数据为保护对象的合法利益。在现有基础上，应围绕数据安全法益展开立法完善工作，并推动刑法理论体系的变革。再次，是网络危害行为类型的重组。网络危害行为是网络刑法学的逻辑起点与规制载体，危害大数据的行为变化较大。在推进网络空间的危害对象与法益内容的变革之际，危害行为类型的同步衔接与优化是必然的后续环节。[25]在大数据时代，设置数据安全的危害行为类型时，应以“数据”的技术特性、功能属性、应用特质以及经济价值等为依据。应当结合数据的具体载体与形式，灵活选择行为类型化的基准、标准与分类，主要包括窃取、转移、使用、传播、贩卖、提供、数据共享、技术支持与技术帮助等行为。最后，是独立的网络定量标准与体系。定量因素及体系是刑法评价的重要对象与依据。传统定量因素多以数额、次数、人数等为主，网络定量因素应在发展中更新，如注册人数、技术服务次数、点击次数、浏览网页数量等。当前，独立的网络定量因素体系正在生成，这为逐步确认和完善独立的网络数据定量因素体系提供参照。

2. 网络刑法典的有序创制

推动网络刑法典的最终生成才是立法转型的归宿，能为对接大数据时代和保护网络数据法益提供充沛的制度供给：一是“二元”立法格局的理性评价。从网络作为“犯罪对象”“犯罪手段”和“独立犯罪时空”三个维度看，当前主要专注前两者，第285、286条分别主要针对计算机信息系统作为“犯罪对象”的情形，第287条主要针对以计算机信息系统为“犯罪手段”的情形。据此，专门性立法和非专门性立法组成的二元模式有其必然性和合理性，非专门性立法对接和辅助适用第287条的规定。今后，网络作为“对象”“手段”的犯罪形态仍将发展，但网络空间犯罪类型必然是主流方向，网络数据犯罪形态不断成型。当前，对网络空间犯罪与数据犯罪形态缺乏足够关注和有效规制，未来围绕网络空间犯罪形态的立法规定尤为重要，既是超越“二元立法格局”的关键，也为逐步替代当前以信息网络为主导的立法格局储备力量，更为专门保护数据法益提供包容性的立法着力点。二是逐步创制网络刑法典的步骤。为了承接大数据时代与数据法益保护的任务，应分阶段推动网络刑法典的创制：首先是单节化。网络犯罪的单节设置尤为迫切，“妨害社会管理秩序”一章应同步增设“第十节”，整合并统领现有的“计算机犯罪”规定和“信息网络犯罪”规定，初步缓解网络犯罪规范体系的整体失衡现象。其次是专章化。随着网络2.0时代过渡到网络3.0时代，网络代际不断蚕食传统犯罪体系，应单独确立“网络(安全)犯罪”一章，对网络犯罪作出宏观布局，对新旧条文加以合理安排，对罪名体系进行重新布置，形成更独立与完整的法益保护网，对网络数据保护采取正式、直接、明确的独立规定。“网络安全犯罪”一章暂时可以置于第九章“渎职罪”后，既保护独立的新型网络安全法益，也对原有关联法益施以“兜底性”的间接保护，夯实过渡阶段的立法改良基础。再次是网络刑法典化。当网络3.0代际趋于成熟与大数据网络代际成型后，传统物理社会彻底被网络空间社会所取代，传统犯罪体系全面转换为网络犯罪体系，以网络数据法益为核心内容的新型网络犯罪体系最终定型，推动创生网络刑法典的时机已然成熟。

3. 刑事治理体系的网络化转型

为了有组织应对网络犯罪，刑事治理体系应当加速推进网络化，主要包括：①网络犯罪控制观。数据安全高度依赖刑事法治体系的保障功能，但不能过度化，应当客观看待刑法的功能及其发展变化，尤应慎重对待以犯罪化为主要表现方式的网络预防性立法理念。数据安全是网络技术创新与网络代际变迁中的必然伴生物，控制网络数据风险处于社会有机体的正常接受范围才是理性的刑法功能观，既可以保障网络技术自由创新与分享，也不妨碍积极防控数据安全隐患和确保数据安全。②刑事诉讼模式的网络变革。刑事诉讼法是保护大数据安全的“一翼”，刑事诉讼“网络化”转型势在必行，是衔接网络刑法学知识变革的程序载体。2014年，第十九届国际刑法学协会通过“信息社会与刑法”决议，着重阐明国际社会从刑法总论、刑法分论、刑事程序法以及国际法律形成四个方面的主要共识与举措。其中，刑事程序法方面的诸多内容值得参照，是我国传统刑事诉讼“网络化”转型的有益借鉴。③国际共治机制。大数据安全是全球性问题，我国应积极参与国际社会共治机制并发挥建设性作用，这是维护自身网络安全利益与保护数据法益的需要，也是在推动我国网络刑法学的知识生成与知识“输出”。欧盟2001年通过的《网络犯罪公约》与“信息社会与刑法”决议均值得参照，而推动制定国际公约是最迫切的任务。④网络犯罪案例指导制度。案例指导制度可以通过典型案例展现法理基础与适法要求，在刑法规范供给滞后于司法需要时，盘活案例指导制度可以解决新问题与推动法理的渐进，是实践中应对新型、疑难、重大司法案件的重要辅助手段。当前，

网络犯罪的案例指导制度乏善可陈，更遑论针对大数据犯罪的指导性案例。这些都加剧了新型疑难数据犯罪的适法难度。今后应当从遴选范围上予以扩容，通过发布网络犯罪的指导性案例指导，强化网络司法保护数据法益的标杆效应，明确网络刑事司法的价值导向。

参考文献：

[1] 于志刚. 网络“空间化”的时代演变与刑法对策[J]. 法学评论, 2015(2): 113−121.

[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] 维克多·迈尔−舍恩伯格, 肯尼斯·库克耶. 大数据时代: 生活, 工作与思维的大变革[M]. 盛杨燕, 周涛 译. 杭州: 浙江人民出版社, 2013: 219.

[4] 邬贺铨. 大数据时代的机遇与挑战[J]. 求是杂志, 2013(4): 47−49.

[5] 高铭暄. 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.

[6] 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.

[7] 赵秉志. 新刑法教程[M]. 北京: 中国人民大学出版社, 1997: 672.

[8] 高铭暄. 新编中国刑法学[M]. 北京: 中国人民大学出版社, 1998: 826.

[9] 黄太云. 《刑法修正案(七)》解读[J]. 人民检察, 2009(6): 5−21.

[10] 陈国庆, 等. 《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》理解与适用[J]. 人民检察, 2011(20): 48−53.

[11] 最高人民检察院法律政策研究室. 《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》解读[J]. 人民检察, 2013(23): 22−27.

[12] 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.

[13] 孙道萃. 网络财产性利益的刑法保护: 司法动向与理论协同[J]. 政治与法律, 2016(6): 43−57.

[14] 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.

[15] 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.

[16] 张明楷. 非法获取虚拟财产的行为性质[J]. 法学, 2015(3): 12−25.

[17] 刘明祥. 窃取网络虚拟财产行为定性探究[J]. 法学, 2016(1): 151−160.

[18] 张智辉. 网络犯罪: 传统刑法面临的挑战[J]. 法学杂志, 2014(12): 65−70.

[19] 于志刚. 关于“使用盗窃”行为在网络背景下入罪化的思考[J]. 北京联合大学学报(人文社会科学版), 2007(3): 44−52.

[20] 高铭暄, 马克昌. 刑法学(第七版)[M]. 北京: 北京大学出版社、高等教育出版社, 2016: 532−535.

[21] 孙道萃. “流量劫持”的刑法规制及完善[J]. 中国检察官, 2016(8): 74−78.

[22] 于志刚. 中国互联网领域立法体系化建构的路径[J]. 理论视野, 2016(5): 37−42.

[23] 于志刚. 缔结和参加网络犯罪国际公约的中国立场[J]. 政法论坛, 2015(5): 91−108.

[24] 赵秉志. 中国刑法的最新修正[J]. 法治研究, 2015(6): 5−19.

[25] 孙道萃. 移动智能终端网络安全的刑法应对——从个案样本切入[J]. 政治与法律, 2015(11): 73−87.

Reflections and prospects of criminal protection of Rechtsgut in big data

SUN Daocui

(Research Institute of Criminal Law Science, Beijing Normal University, Beijing 100875, China)

Abstract: Data crimes are increasing in the big data era, while the network data is becoming the dominant Rechtsgut. The earlier protection was subordinate and indirect, while present protection focuses more on information. Multiple protection of big data constantly exposes the weakness of independent protection, the integration of protection through property and independent protection should be the general trend, and protection through property is necessary, but independent protection should be the leading form. The construction of network criminal law theory would be the ultimate resolution, the general transformation of legislation and the construction of network criminal law code should be the priorities.

Key Words: Rechtsgut of big data; criminal protection; network criminal law theory

[编辑：苏慧]