数据犯罪的刑法规制研究

◆余益林

（西南科技大学法学院，四川 绵阳 621010）

【摘要】数据犯罪在我国目前的法律中尚无明确的定义和内涵，其行为类型广泛、犯罪手段智能、侵犯法益多元，会对个人权利、社会利益以及国家安全造成危害。现行刑法对数据犯罪的规制存在将数据依附于计算机信息系统加以保护、停留在保护数据背后的特定利益、数据罪名缺乏体系的问题，对数据安全保护不直接、不充分、不全面。因此需要对症下药，通过剥离数据对计算机系统的依附、承认数据的独立法益价值以及构建全链条数据犯罪刑法体系，实现刑法对数据犯罪规制路径的完善。

【关键词】数据安全；数据保护；数据犯罪；刑法规制

大数据时代，新技术产生的同时催生了数据安全问题，数据犯罪行为类型不断增多，不利于社会经济的发展，法律具有滞后性，现行《刑法》中关于数据犯罪的规定无法完全应对层出不穷的侵犯数据安全的行为，对数据安全保护不直接、不充分、不全面的问题亟待解决，如何与时俱进回应数据犯罪的规制问题也亟待解决。本文首先将明晰我国数据犯罪的内涵，然后对数据犯罪的规制现状进行分析，从而明晰不足之处并提出完善建议。

一、数据犯罪的内涵

（一）数据犯罪的概念

数据犯罪目前在各项法律规定及司法解释中尚无明确的含义界定。通过检索学术论文、司法判例等，可以将与数据有关的犯罪概括为三类：一是将数据作为犯罪工具，此类犯罪侵犯的依旧是传统法益；二是以数据本身的安全性和功能性作为犯罪对象的犯罪，以数据的管理秩序为法益；三是以数据内容为犯罪对象的犯罪，危害的是数据所涉及的人身安全、公共利益、国家安全等各种具体利益。不同学者对数据犯罪的定义和内涵有不同的见解。

第一种观点认为，应当将数据犯罪定义在最狭义的范围之内，即仅指以数据本身为犯罪对象的犯罪，主要关注数据作为物理载体的技术属性，破坏的是数据本身的机密性、完整性和可用性。第二种观点认为，数据犯罪是指以数据为犯罪对象的犯罪，即无论是数据本身的安全还是数据的内容所蕴含的其他价值，都是刑法要保护的。将数据安全法益定位为数据信息内容保护，能够合理限定数据犯罪的规制范围，符合刑法谦抑性的要求。第三种观点认为，数据犯罪不仅包含以数据为犯罪对象的犯罪，还包括以数据为犯罪工具的犯罪，即最为广义的数据犯罪。只要是与数据有关的犯罪，都可以纳入数据犯罪这一概念的范畴。

笔者认为，以上三种观点基于其研究的范围和视角的不同都具有一定的合理性。在本文中采用第二种观点，以此展开对数据犯罪刑法规制的研究不会过于狭窄也不会过于宽泛。倘若刑法将以数据为工具的犯罪包含进数据犯罪之中，那么将不能有效区分传统犯罪与数据犯罪，数据犯罪也将失去其独立的价值与意义。同样，如果将数据犯罪界定为仅针对数据本身安全的犯罪，我国刑法中尚且没有此独立罪名，其研究重点在于新罪名的构建，而本文侧重于对刑法中已有的与数据安全高度关联的犯罪罪名做出系统分析。因此，在本文中，数据犯罪是指以数据为犯罪对象的犯罪。

（二）数据犯罪的特点

在界定完数据犯罪的范围之后，通过分近年来数据犯罪的司法实务案例可以发现，数据犯罪具有以下特点。

首先，行为类型广泛。各类新型数据犯罪包罗万象，包括但不限于非法获取型数据犯罪、攻击破坏型数据犯罪、虚构造假型数据犯罪和其他关联型数据犯罪，既包括传统犯罪，也包括以数据本身安全和数据信息安全为法益的犯罪，其范围延伸至与数据信息相关的网络犯罪整体。

其次，犯罪手段智能。大多数数据类犯罪发生在网络空间，与网络犯罪相关，需要具备一定的专业性、技术性知识，涉及“数据劫持”“删库”“越权登录”“网络爬虫”等多种技术手段，尤其是人工智能、大数据、元宇宙、区块链等技术被实施于犯罪的各个环节，使得对数据犯罪的取证难度加大。同时，在智能化趋势下，对数据安全的保护提出了新的难题，例如，通过对骚扰电话所收集到的声音信息进行加工，然后虚假生成或通过技术修改人脸识别的数据，被用于在网络上实施盗窃或诈骗等犯罪。

最后，侵犯法益多元。数字化时代，数据融入了人们社会生活的方方面面，运行在数据生产、采集、存储、流通和开发的各个环节，数据的价值不再局限于数据本身，还承载着个人、组织、社会、国家多方利益，数据安全法益也更

加多元化、层次化。所侵害的不仅仅是传统社会管理秩序中的计算机信息系统管理秩序。数据法益犯罪所侵犯的法益突破了以往的单一法益，以法益综合体的面貌出现。

二、现行刑法对数据犯罪的规制现状

目前我国刑法中尚不存在以数据法益为规制核心的罪行规范体系，有关数据犯罪的条文分散于刑法分则的各个章节之中，对数据犯罪的规制存在以下问题。

（一）保护不直接

从数据载体来看，现行刑法是将数据依附于计算机信息系统加以保护，没有对“数据”进行直接保护。现阶段数据犯罪规制体系对数据的认识还停留在将计算机信息系统数据、信息数据等作为媒介和载体的阶段，涵射内容范围狭窄、不全面。例如“非法获取计算机信息系统数据罪”的犯罪对象仅限于使用中的计算机信息系统，而不包括脱离计算机信息系统存放的计算机数据，如光盘、U盘中的计算机数据等。当前，数据已经在技术层面与计算机信息系统区分开来，具有自己的独特性。但传统关于数据的认知理念已经落后于数据内涵扩展带来的变化，对于数据保护不直接的问题需要与时俱进更新理念，认识到数据的独立作用和价值。此外，从数据犯罪与关联犯罪之间的关系来看，现行刑法并没能很好地厘清数据犯罪与计算机犯罪、信息犯罪以及网络犯罪之间的关系，没能对“数据犯罪”进行直接保护。实践中存在的问题是对数据和对计算机信息系统的侵害行为以及其他侵害行为之间难以区分。

（二）保护不充分

随着《数据安全法》的出台，数据安全被单独作为一种法益类型，与个人信息安全进行明确区分，这也是数据法益独立性的实质体现，为建立健全数据安全管理体系指明了发展方向。法益是确定刑法处罚范围的价值判断标准，既是刑事立法层面判断是否将某种社会生活利益纳入刑法保护范围的决定性依据，也是刑事司法层面确定某一行为是否侵害了刑法所保护的法益、是否达到了应受刑罚处罚的程度的重要标准。但是，对数据安全法益的独立性没有全面认识。从法益保护视角来看，刑法对数据的保护仍然停留在数据背后的特定利益，体现的是将数据作为一种犯罪对象，目前特定信息数据罪名所保护的数据大体可以分为国家、公共以及个人三类。其立法思路为将表征数据内容的各种具体信息、秘密等作为犯罪对象，先判断数据的性质，再分析该类数据同种利益的直接相关利益，进而决定该利益是否需要刑法保护。数据是否受到保护由数据的性质决定，重要的计算机数据才能受到刑法保护，以此间接规制数据侵害行为，如侵犯商业秘密罪、非法获取公民个人信息罪等。立法目的侧重于对国家、社会法益的保护，对数据作为新型经济形态核心生产要素的独立性价值认识还不足。

（三）保护不全面

目前，直接保护数据的罪名呈现出“口袋罪”的倾向。在数据的内涵方面，非法获取计算机信息系统数据罪规制的“数据”范围广，几乎涵盖了一切可在电脑系统中储存、显示的客体，还涉及个人信息权、财产权等权利，数据犯罪保护法益的内涵和外延较为模糊。在司法实践中，司法人员也未能厘清“数据”的技术属性与法律属性。例如，在网络虚拟财产案件中，涉及的网络虚拟财产属于财产还是数据的认定以及犯罪数额的认定，实务中有的为了回避其性质判定难题选择，直接将盗窃虚拟财产的行为认定为非法获取计算机信息系统数据罪。这种做法更加体现了将其作为“兜底罪名”的性质。除此之外，间接保护的数据犯罪罪名缺乏体系。刑法规制数据犯罪的行为链条和行为类型并不完整，大量新型数据犯罪并不能得到规制，导致对数据犯罪的刑事管理陷入困境。我国刑法对数据犯罪的管理，主要集中在规制编造、传播虚假数据的行为，非法获取或泄露真实数据的行为以及删除、篡改、隐瞒、销毁数据的行为等，也即刑法对数据犯罪的管理重点集中于数据获取阶段而非数据利用阶段。刑法主要关注上游和中游的数据转移与流动，而忽略了下游对数据加以非法处理、利用的行为。但是，数据的获取、泄露等行为只是犯罪链条的起点与发端，而通过利用数据获得非法利益，往往才是数据犯罪产业链的落脚点与最终目的。

三、数据犯罪刑法规制的完善路径

针对上述现行刑法对数据保护的不直接、不充分、不全面的问题，需要对症下药，采取针对性的措施进行改进和完善。

（一）剥离数据对计算机系统的依附

受技术发展水平限制，以前的数据几乎都存储在计算机信息系统中，而现在，数据犯罪所侵害的对象主要类型已经由媒介、载体性数据扩展为内容及类型多元化的网络数据等。针对数据犯罪的刑事立法理念也应及时更新，要转变传统的立法思维。首先，要准确界定数据犯罪的概念以及其构成要件。这是将来在刑法中增设与数据相关的犯罪罪名无法回避的问题，需要审慎地证成后予以明确。这样也有利于司法机构在运用时准确地对数据犯罪中数据本身的性质和内容、数据可能遭受的侵害风险进行规范评价，做到正确定罪量刑。同时，明确数据犯罪与计算机犯罪、信息犯罪以及网络犯罪之间的联系与区别。数据犯罪与其他犯罪是强相关的概念，相互之间的关系盘根错节，在罪名范围上可能存在一定的交集，但是在本质上是有一定差别的，所强调的重点不同。只有从理论上划分清几个罪名之间的界限，才能保证司法人员在具体案件中在法律适用包括犯罪罪名选择上的准确性。

其次，要合理确定需要保护的数据范围。数据与国家的经济运行、社会管理、公共服务、国防安全等方面密切相关，一些个人隐私信息、企业运营数据和国家关键数据的流出，将可能造成个人信息曝光、企业核心数据甚至是国家重要信息的泄露，给国家安全带来各种隐患。所以，对于哪些数据是需要保护以及值得保护的，要根据时代的发展不断补充和完善。要避免应当保护的数据被排除，重点关注具有社会危害性的数据犯罪。同时，数据虽具有独立价值，但并不是所有的数据都值得保护，也要避免不应保护的数据被纳入，例如虚假数据、涉及犯罪的数据等。

（二）承认数据的独立法益价值

既有的数据法益内容是一种典型的传统法益依附性模式，数据法益要么完全依附于个人信息法益、财产法益、社会秩序法益，要么折中依附于多元传统法益内容组合和数据性质法益。在大数据时代的数据不再依附于计算机信息系统或者信息内容而具有价值意义，其自身包含了大数据时代所独有的某类重要的利益和价值导向，具有自身的独立价值属性。在此背景下，也开始主张应将数据本身的安全作为独立的新型法益加以保护。具体而言，首先应当在刑法中构建信息安全、数据安全和计算机信息系统安全并行的保护体系，专设“数据犯罪”专章或专节。同时，针对目前无法得到规制的对数据的非法提供、泄露、利用行为，增设相应的新罪名。

其次，改变数据犯罪附属于信息犯罪、计算机信息系统犯罪条款的立法模式，强化数据犯罪罪名与刑罚的主体性和独立性。考察当今国际社会的刑事立法，各个法域无论是以附属刑法的形式还是增设罪名的形式，尽管各国关于数据犯罪的具体罪名等方面不尽相同，但是却具有立法的共同趋向，那就是不约而同地去强化数据保护的独立地位。这种数据安全保护的立法趋向，特别是以德国为典型的分类保护模式和以美国为代表的集中式立法，对于我国现行刑法具有参考和借鉴价值。对数据安全进行独立的刑法保护，是一种经过各国检验的立法思路，我国要与时俱进，取其精华、去其糟粕，吸取有益经验和政策，用于我国立法之中，这对我国保持与世界的数据共享、数据交流具有重要的现实意义。

（三）构建全链条数据犯罪刑法体系

我国目前关于数据犯罪的规制重点集中在“获取”型和“破坏”型等犯罪行为，对于数据存储、数据窝藏、数据滥用、数据泄露等行为则缺乏必要的规制，忽视了数据生存周期原理动态的刑法保护。要根据不同数据生存周期环节的不同特点，根据数据侵害行为的不同类型，如非法获取行为、非法传输行为、非法控制行为、非法破坏行为、非法处理行为等，在刑事政策的检视下对可类型化的其他数据侵害行为进行犯罪化考量，形成数据侵害流程前端、中端和后端的全链条规制体系，构建横向管理链条，形成对数据犯罪行为类型的全面规制。同时，在纵向上梳理数据犯罪的全流程，除了对数据犯罪的前端管理之外，对有所欠缺的危害性更大的数据泄露、数据滥用等末端犯罪的规制需要更加重视，实现对数据犯罪行为从上游到下游的有效管理，形成数据犯罪的立体化刑法管理体系。通过横向与纵向链条的衔接，构建针对数据犯罪管理的严密刑法体系。

同时，也要明确刑法介入针对数据的不法行为的界限。充分利用《数据安全法》所规定的“数据分类分级保护制度”，根据数据的重要程度以及对社会危害的严重程度，采用不同的保护手段和措施。针对重要程度一般的数据以及社会危害性不大的不法行为首先考虑用民事诉讼以及赔偿、行政处罚等非刑事手段来处理，对于严重危害国家安全以及公共权益数据的不法行为要通过刑法的及时介入来严厉打击。

四、结束语

数据对于个人、企业、社会而言都具有重要意义，需要各方的共同努力和维护。新技术与新应用总是在其中隐藏了过去未曾发觉的瑕疵与漏洞，刑法作为最后保障法在何时更为合适地介入，既不过于打击新技术的蓬勃发展，又不纵任其危害发展，是一门永远需要把握平衡的艺术。

参考文献：

[1]王惠敏.网络数据安全独立性之提倡及其刑法展开[J].法治研究，2023(03):117-131.

[2]王倩云.人工智能背景下数据安全犯罪的刑法规制思路[J].法学论坛，2019，34(02):27-36.

[3]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.

[4]刘智慧，张泉灵.大数据技术研究综述[J].浙江大学学报(工学版)，2014，48(06):957-972.

[5]刘双阳.数据法益的类型化及其刑法保护体系建构[J].中国刑事法杂志，2022(06):37-52.

[6]熊波.论数据法益独立性刑法模式[J].安徽大学学报(哲学社会科学版)，2023，47(02):67-76.

[7]苏桑妮.从数据载体到数据信息：数据安全法益本位之回归[J].西南政法大学学报，2020，22(06):97-108.

[8]蔡士林.我国数据安全法益保护：域外经验与立法路径[J].深圳大学学报(人文社会科学版)，2022，39(06):97-106.

作者简介：

余益林(1997—)，女，汉族，四川泸州人，硕士研究生，研究方向：中国刑法学。