中州学刊

数据犯罪的双重法益及其保护路径

袁　彬　　薛力铭

摘　要：大数据时代数据的重要性日益凸显，但当下我国刑法对数据法益的保护依然存在一些问题，包括数据秩序法益的内涵过于抽象，难以承担保护数据法益、保障数据技术平稳健康发展的使命；单一的数据安全法益说，会导致利用公开数据不当入罪。数据犯罪所侵犯的法益是双重法益，其外壳是数据安全，内核是数据自决权。以数据犯罪的双重法益为基础，我国在立法上应当通过修改旧罪、增设新罪的方式对数据进行刑法保护，在确立数据法益独立保护的基础上，修改《刑法》第285条第2款，同时增设专门针对数据的破坏、滥用数据罪；在司法上应当以双重数据法益合理界定侵害数据行为的入罪门槛和处罚范围，实现对个人数据及社会公共数据、国家数据的体系化保护。

关键词：数据安全；数据自决权；双重法益；破坏、滥用数据罪

中图分类号：D924　　**文献标识码：**A　　**文章编号：**1003-0751(2024)06-0070-09

随着科技的不断发展，数据在人们日常生活中占据着越来越重要的地位。数据作为数字经济时代最核心的生产要素，正加速成为城市智慧构建、政府流程再造、经济创新驱动的新引擎[1]。但是海量的网络数据不仅蕴藏着丰富的经济价值，也成为违法犯罪分子觊觎的对象[2]。例如，数据攻击者通过窃取执法部门邮箱等官方账号，向互联网平台发送“紧急数据申请”，从而套取用户敏感数据。在政府数据层面，巴西里约热内卢州的财政大臣披露，该州的财政系统遭到勒索软件攻击，420GB数据遭窃取，并收到威胁说如果不支付赎金将马上公开数据。围绕着数据处理而形成的数据犯罪正呈现出严重的社会危害性和前所未有的复杂性[3]。

如何有效开发利用数据、保障数据安全的平稳运行是当下面临的一个重要问题。目前国务院正准备组建国家数据局，“负责协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，统筹推进数字中国、数字经济、数字社会规划和建设等”[4]。2021年9月1日正式实施的《中华人民共和国数据安全法》(以下简称《数据安全法》)，也为数据的保护提供了法律保障。其中《数据安全法》第1条明确规定：“保障数据安全，促进数据开发利用，保护个人、组织的合法权益。”当前，数据已经具备了刑法保护法益的基础，而刑法如何保护数据的开发利用并为数据的良性发展保驾护航，是未来数据技术发展所绕不开的重要议题。

当前，数据犯罪逐渐成为学界的研究热点之一，但在部分问题上仍然存在明显的分歧和争议。首先，对于数据犯罪所侵犯的法益，当下并未有一个统一的认知，而由此产生的法益保护抽象化问题，不仅可能使数据犯罪的治理走向规制泛化的误区，也会对数据的体系性保护造成不利影响，进而无法有效地指导司法实践。其次，对于数据保护的前提，学界一直存在争议。有观点认为，数据与信息等同，并无

收稿日期：2024-03-07

基金项目：国家社会科学基金重大项目“当代中国刑法基础理论研究”(21STA003)。

作者简介：袁彬，男，北京师范大学刑事法律科学研究院教授、博士生导师(北京　100875)。薛力铭，男，北京师范大学法学院博士生(北京　100875)。

保护独立数据法益的必要。如何区分数据与信息的概念,不仅关系到法律术语的表达,同时也是确立数据法益的重要前提。最后,当下刑法对数据的保护还存在一定的缺位。《数据安全法》第 52 条第 2 款明确规定:“违反本法规定,构成违反治安管理行为的,依法给予治安管理处罚;构成犯罪的,依法追究刑事责任。”但是,刑法的适用在当前存在一定的困境。例如,行为人侵入政府系统后对数据进行修改删除操作的,只能依据《中华人民共和国刑法》(以下简称《刑法》)第 286 条第 2 款进行处理,然而该条款在保障数据安全、应对纷繁复杂的数据侵害行为方面力有不逮,难以有效应对数据技术快速发展所带来的新情况、新特点、新问题,数据安全的刑法保障效能还需要进一步提升。厘清数据犯罪所侵犯的具体法益,并在社会的高速发展中保护数据安全,确立合理的数据犯罪规制路径,是当下亟须解决的问题。

一、既有的数据法益观及其反思:秩序法益观的否定与安全法益观的局限

犯罪是侵犯法益的行为,而刑法的目的则是保护法益[5]85。解决数据犯罪刑事治理问题,首先需要厘清刑法意义上的数据法益概念及其内涵。如果数据法益的内涵和外延界定不清,将导致数据犯罪的刑事规制失去“准星”[6]。目前我国学者对数据犯罪的法益主要采取传统的法益界定方法,形成了以数据秩序法益观、数据安全法益观为代表的既有观点。笔者认为,数据秩序法益观过于抽象且无法还原为具有实质内涵的具体法益,数据安全法益观无法为数据提供周延的保护,二者都存在一定的局限性。

1.数据秩序法益观及其缺憾

数据秩序法益观认为,数据犯罪所侵害的法益是一种独立于传统法益的新型法益,即国家数据管理秩序。而国家数据管理秩序的内涵也并非传统法益的集合,而是数据犯罪的共有法益[7]。将数据犯罪侵犯的法益认定为数据管理秩序,意味着只有破坏数据管理秩序的行为才能构成数据犯罪。而数据管理秩序存在的前提是数据管理存在前置性的秩序规定,同时在数据管理上,是以政府为主导来进行的。

笔者认为,数据秩序法益观以数据管理秩序为核心,存在着明显的缺陷。首先,秩序法益成立的前提在于国家是否对数据存在一定的管理秩序;而数据管理主要是指对于数据的流通、使用存在一套完整的管理方案,包括何种类型的数据可以流通,应当如何流通,数据应当如何储存等。2021 年 12 月国务院印发的《“十四五”数字经济发展规划》指出:“充分发挥市场在资源配置中的决定性作用,构建经济社会各主体多元参与、协同联动的数字经济发展新机制。结合我国产业结构和资源禀赋,发挥比较优势,系统谋划、务实推进,更好发挥政府在数字经济发展中的作用。”但是,这里只是提出针对数据开发、数据利用等应当加强多元主体的协作,形成完备的治理格局,并没有具体说明政府在这个治理格局中应当承担何种职能,如何对数据的开发、利用等实施统一的行政管理。其次,由于去中心化等网络发展的特色,管理职能已经分散到多元主体,例如企业、平台、政府、行业、社会公众等,完全中心化地对数据的集中支配式管理已经不现实,也不具备可行性。同时,数据犯罪也并非侵犯管理秩序类犯罪,如其他妨碍管理秩序类犯罪,都或多或少地具有明确的管理秩序,而在虚拟空间如此散布的数据管理上,是否存在集中的管理秩序,笔者认为存在疑问。当下公民在进行数据交流、数据存储等活动时,均取决于公民的自主决定。尤其是在当下数据创新蓬勃发展、多元主体参与的时代,国家只是加以引导,并不需要普遍掌控,当然也谈不上管理秩序。最后,侵犯秩序法益的犯罪多属于法定犯,对法定犯进行刑事处罚时,需要完备的前置法的评价与认定,而数据法益的保护是一个新兴的领域,其前置认定处于缺位的状态。

可见,数据秩序法益说的内涵过于抽象且缺乏明确性,未能充分考虑到数据主体的多元化,忽视了平台、企业、社会公众等主体在数据管理中的地位和职能。同时,前置法的认定也存在缺失。采用数据管理秩序作为数据犯罪的法益,可能会为数据的发展设置较多的限制条件,难以切实承担起保护数据法益、保障数据技术平稳健康发展的使命,因此,将数据秩序作为数据犯罪所侵犯的核心法益并不适宜。

2.数据安全法益观及其局限

随着网络技术的发展以及数据技术的迭代,数据安全的脆弱性与易受攻击性越发凸显,数据安全也成为数据法益保护的重要内容[8]。在信息化时代,数据成为一种重要的生产要素,互联网企业之间的数据争夺大战纷争的核心便是用户数据[9]。数

据泄露、数据攻击现象频发,对信息社会的安全发展构成了严重的威胁。正因为如此,数据安全法益观是当下研究数据犯罪的学者们所认可的主流法益观。我国《数据安全法》第2条规定:“数据安全,是指通过采取必要措施,确保数据处于有效保护和合法利用的状态,以及具备保障持续安全状态的能力。”数据安全法益观提出,从数据安全的保护目的出发,将数据安全作为数据犯罪所侵犯的法益之一,具有相当的合理性。

但是,数据安全具有明显的抽象性,需要对其实质内涵加以分析。按照我国《刑法》分则的规定,可以将安全作为同类法益的罪名,在《刑法》分则第一章和第二章中,分别设立危害国家安全罪和危害公共安全罪。细究《刑法》分则第一章与第二章下的条文,这两项罪名下的相应危害行为类型均会对社会的安全带来风险。且其具体行为,如放火、爆炸,都会直接侵害某些具体个人的法益[5]82。在还原为具体的法益时,爆炸等行为会使个人生命安全受到侵犯,可具体还原为《刑法》分则第四章侵犯公民人身民主权利罪中的故意杀人罪的法益等。但与此相比,数据安全常常面临还原的困难。从内涵上看,安全本身就是一种抽象性的表述,如果数据安全法益不能还原为具体的个人法益,就意味着对数据安全状态造成侵害的轻微风险都可以认为侵犯了数据安全法益。安全法益这一特殊性决定了如果想要证立数据安全作为数据犯罪的法益,就必须有可被还原具体内涵的个人法益。

当数据与安全结合时,数据安全法益所保护的就应当是,数据能够被有效保护、合法利用,并具备持续地维持安全状态的一种能力。在对数据安全内涵的还原上,有学者将其还原为数据具备持续安全状态的能力[10],即数据在系统内部平稳运行不被他人侵害的权利。也有学者以数据安全三要素,即数据的保密性、完整性与可用性作为三种可被数据安全法益所还原的具体法益[11]。其中,数据的保密性强调对数据外部状态的保护,即侧重保护数据储存、运行的私密状态。数据的完整性与数据的可用性则强调对数据内部状态的保护,前者侧重保护数据内容的完整、真实,不会因他人的行为而导致数据内容的缺失、存伪;后者则侧重保护数据内容的有效使用,不会因他人的行为而导致数据无法正常使用。

虽然数据安全三要素可对抽象的数据安全法益予以还原,但仅凭数据安全法益无法实现对数据的周延保护。主要原因在于数据安全法益无法满足数据保护的多元需求。保密性、完整性与可用性无法涵盖数据所有的安全问题,其仅仅涵盖了数据不被他人获知、数据处于完整状态、数据能够有效使用这三种特性。但是,现今的数据并不仅仅是单一的关乎系统运行的二进制比特数据,其也具有多种权利属性。例如,数据经济的发展使部分数据具有了经济价值,数据权利人可使用其所享有的数据获得收益,而收益权并不属于上述三种权利中的任何一种。即便是依据“侵犯该数据的可用性的行为却导致了权利人丧失了该数据及其背后利益的可得性”[12],也无法得出合理的结论。因为该观点其实已经将利益可得性与可用性放在了同等重要的地位,利益可得性是数据可用性产生的结果,如果该论点成立,就意味着数据的可用性也是由数据的完整性延展出来,这又会得出数据的完整性包含数据的可用性的不当结论。更何况即便是持数据安全三要素的观点,其对于数据可用性的理解也不包含数据的可得利益,而是仅指权利人能及时、有效地获取、使用数据的状态。所以,单独以数据安全作为数据的保护法益,无法为纷繁复杂的数据保护提供周延的保护。

二、数据犯罪的法益重塑:融合数据安全与自决权的双重法益观

1.重塑的前提:融内容与形式于一体的数据形态

信息和数据作为当代互联网法律中的基础概念,一直没有被有效地区分。在法律文件和法律论述中,两者被不加区分使用的情形居多[13]。但是,信息与数据的关系、数据犯罪的内涵边界,是研究数据犯罪绕不开的重要问题。如果不能对数据与信息的概念进行明确的区分,则数据犯罪这一概念就可能会被信息犯罪的概念所替换,数据法益的独立地位也就无从谈起。

目前学界关于数据与信息的关系问题的探讨,大致可以分为两类:一类是信息与数据的内容与形式区分论。有学者认为信息是数据的内容,数据是信息的形式,在大数据时代无法将数据与信息加以分离而抽象地讨论数据上的权利[14]。也有学者认为将两者等同视之不存在刑法法益确定上的障碍,且有助于充分实现对该类法益的保护[15]。另一类是信息与数据的范围区分论,其中又细分为信息与数据相对型[16]、信息小于数据型[17]、信息大于数

据型[18]三种类型。

笔者认为,数据不仅是信息的形式,也包含着信息的内容,是一种独立的存在,数据本身既是形式也是内容。在范围上,笔者不赞同将信息与数据等同的观点,认为应当对信息和数据作相对的区分。这主要基于以下三个方面的考量:一是区分信息与数据是立法的初衷。信息与数据的不同,其实在立法之初就已经确定。虽然在多数情况下,信息与数据可以相互替换,但是二者并不是等同的概念则毋庸置疑。例如《刑法》中有"非法获取计算机信息系统数据罪"的表述,也有"侵犯公民个人信息罪"的表述。二是信息与数据的内涵不同。信息犯罪与数据犯罪的界定,主要是信息与数据概念的划分,而不是强调隶属关系。《数据安全法》将数据定义为:"任何以电子或者其他方式对信息的记录。"所以,在能被人们解读的层面,数据是信息的载体。而在数据本身的层面,数据就是物理代码。如果将计算机系统中系统运行所需要的二进制代码解释为信息,似乎超过了信息原有的内涵。三是信息与数据存在转化关系。信息与数据在一定程度上可以相互转化。例如,在侵犯个人信息犯罪中,行为人存储在电脑中的旅游记录、生活轨迹等,这些都用数据的形式予以保存,但是这些数据却反映了人们的生活信息;国家环境监测所记录的环境污染数据,也反映了某地的环保情况;在侵犯商业秘密罪中,犯罪分子从竞争对手处非法获取的财务数据,也承载了公司经营的财务状况。立法中也明确使用了信息与数据的不同表述,"所以刑法中的数据犯罪也应该与信息犯罪有别。我们不应该因为有较早前将数据与信息混同的司法解释规定,而罔顾相关法规甚至刑法对数据与信息、数据犯罪与信息犯罪区别对待的立法原意"[7]。

立足于《数据安全法》对数据的定义,作为信息载体的数据,其范围应当大于信息。当下刑法所保护的数据主要具有两层含义:一是系统运行的比特数据,即不含有信息内容的二进制代码。二是作为信息载体存在,其形式上属于电子数据,但其内容可以被识别为不同信息。

2.重塑的基础:数据自决权的提倡

随着科技的不断发展,双层社会的出现使网络空间已逐渐成为人们生产生活的第二空间。但网络空间不同于现实空间,人们所有的活动均是建立在数据正常运行的基础上,因而,人们在网络空间中的工作、交友、娱乐等活动均离不开数据的传输与运行。在网络办公场景中,人们依靠数据来展开工作,在网络交友聊天中,人们又需要数据传达信息。久而久之,数据已经不仅仅属于信息的载体,其也被赋予了多种意义,具有多重属性。例如,网络虚拟财产虽然由数据组成,但其被赋予了财产属性。《"十四五"数字经济发展规划》开篇就明确指出:"数字经济是继农业经济、工业经济之后的主要经济形态,是以数据资源为关键要素。"可见,数据已经成为经济发展的新动力。保障数据发展的合规、安全,刑法不能缺位,但数据安全法益的局限性,导致刑法无法周延地对数据进行有效保护。

立足于数据保护的现实需要以及数据安全法益的局限性,笔者主张将数据的自决权纳入数据法益的构造当中。数据自决权主要反映法定主体对其所享有的数据具有自由决定的权利。数据自决权的实质内涵是未经数据主体知情同意,其他人不得随意收集、破坏、使用该数据,主要包括数据的所有权、使用权、收益权和处分权等权利。其中数据的所有权表现为数据归数据权利人所占有,未经权利人同意,其他人不得随意收集该数据。但是,数据的所有权与有体物的所有权并不相同,因为数据的特殊性,行为人未经他人允许而获取他人数据的行为,虽然没有造成他人数据的丧失,但是也侵犯了他人的数据所有权。数据的使用权表现为数据可以被有效运用、传播以及利用的权利。数据的收益权表现为数据权利人通过对数据的加工使用,进而获得该数据所产生的收益的权利。例如,视频数据权利人可利用归其所有的视频获得的点赞获取一定收益。数据处分权表现为数据权利人可采用数据传输的方式,将该数据与他人共享等。数据自决权并不是仅为个体自然人享有的一种权利,法定主体同样可以享有数据自决权。例如,政府部门的政务依法不公开,如果行为人非法获取、传播该数据内容,同样侵犯了政府部门的数据自决权。

透过数据自决权,我们看到,它可以有效解决数据安全法益对数据收益、使用等行为无法周延保护的问题。但同时,也要注意到,原始数据的数据自决权与二次加工生成的数据并非同一数据自决权。例如,数据权利人甲许可企业收集自己的数据,企业可以对收集到的原始 A 数据进行加工使用,进而得到 B 数据,企业可自由转让 B 数据。但企业对原先收集到的 A 数据具有保管的义务,如果企业没有履行法定义务,造成 A 数据的泄露,或者超出原先个人同意的范畴进行传输、使用,那么就侵犯了数据权利

人甲的数据自决权。

数据自决权所强调的知情同意,与数据安全所还原的数据保密性存在一定程度的交叉,但二者也存在一定的区别。知情同意立足于数据权利人的角度侧重形式判断,即行为人获取数据前是否已经征得数据权利人的同意;数据保密性则立足于数据内容的保护角度侧重实质判断,即数据内容是否为私密的,是否未被他人知晓。在某种条件下,有可能存在数据保密性灭失,而数据权利人是否知情同意还尚需确认的情况。如数据权利人将数据上传至网络空间予以公开,此时数据保密性灭失,但行为人使用该数据需要征得数据权利人的同意。所以,知情同意并不仅仅包含数据内容的私密,还包含数据获取、使用等行为的知情同意。

对比数据安全与数据自决权可以发现,数据安全侧重于对数据本身的保护,数据自决权则侧重从数据权利人的角度对数据进行保护。作为推动数字经济发展的重要生产力,数据并非凭空产生,而是归数据权利人所有。因此,如果仅侧重数据本身的安全保护,就会导致对数据权利人相关权益保护的缺失。数据自决权的提出强调对数据权利人数据支配、使用权利的保护,可以在周延数据保护范围的基础上,使刑法进一步为数据经济的发展保驾护航。

3.重塑的核心:融数据安全与自决权于一体的双重法益

数据犯罪的双重法益,主要是指行为人对数据的侵害,必须同时造成对数据安全以及数据自决权的侵害,才能认定为犯罪行为。正如前文所述,单一的数据安全法益无法实现对数据的周延保护;同理,只强调对数据自决权的保护,也会阻碍数据的创新发展。只有提倡数据双重法益,才能在保证周延数据保护范围的基础上,避免刑法适用范围的不当扩张。

在大数据时代,科学研究成为一种典型的数据应用场景,在先进的技术条件下,可以对这些数据进行前所未有的细致分析,以挖掘其对于科学研究所具有的巨大潜在价值[19]。大数据能够快速、高效做出决断的基础在于其对海量数据的强大分析能力,而这种能力往往会侵犯到个人数据权利。如果过于强调对数据的排他性的权利,则无疑会妨碍数据的合理创新使用。同样,大数据的流通性、共享性特点,也决定了在某些数据的使用上只保护数据自决权并不现实。例如,驾驶员驾驶新能源汽车所产生的数据不仅会被车企记录,同样会上传至地方及国家监测平台[20]。此时,对于车主而言,因其车辆行驶所产生的数据并非私密数据,所以车企的记录行为并未侵犯到数据的保密性,但如果要求车企后续的使用行为需要以车主的知情同意为前提,则不利于新能源技术的进步。

过于强调数据的消极防御而忽视公开数据的实质使用需求,容易造成数据权利人为了谋求短期、极致的个人利益而做出妨害科技创新发展进程的行为,也可能会将不具备法益侵害性的数据使用行为纳入刑法惩治的范围。况且,个人数据的载体随着存储技术的发展而多样化,由此导致数据上相关权利主体众多,承载的利益也变得复杂化[21]。因而,不论是数据安全法益抑或是数据自决权法益,都无法涵盖既有社会属性,又有个人属性的数据犯罪,将其单独作为数据犯罪所侵犯的法益均会导致数据安全发展与个体自由使用发生对立冲突。

准确把握数据犯罪所侵犯的法益,是对保障数据利用良性发展的重中之重。应当认识到,在数据犯罪中,数据安全法益与数据自决权法益既具有存在的独立价值,又是相互联系的客观存在。首先,数据安全法益有其存在的独立价值根基。《数据安全法》对数据的合理使用提供了立法支持,该法注重对数据使用、传播等安全状态的保护,能够减少因过度强调知情同意,而阻碍数据创新发展的现象出现。其次,数据自决权法益作为对数据权利人数据权益的保护,可以防止出现以安全保护为由,进而泛化刑法适用范围的问题。数据自决权法益注重数据是数据权利主体的自由延伸,公民对自己所享有的数据具有使用、支配的权利。通过数据自决权法益的融入,可以保障公民的数据使用行为基于自由意志自主支配,避免以安全为由限制公开数据的使用。最后,数据自决权与数据安全共同存在于数据犯罪之中,侵犯私密数据的行为,不仅会打破数据的保密性,而且会损害数据权利人的数据自决权。对他人数据肆意修改,并加以使用的行为,不仅侵犯了数据安全法益,同时也损害了数据权利人对数据的排他性使用权。因而,立足于数据的双重法益,只有同时侵犯数据安全法益与数据自决权法益时,才能认定构成数据犯罪。

综上所述,以单一法益构造对数据犯罪的侵犯法益定型化,在实践中多少有些捉襟见肘。正是因为数据的特殊性,决定了一个不法行为造成双重法益侵害是难以避免的现实。因此,可以采用双重法益论,仅对实质侵害数据自决权法益与数据安全法

益的行为科处刑罚。这样不仅可以避免将不具有法益侵害可能性的行为解释为犯罪构成要件行为,而且也不会将侵犯法益的行为排除在刑法的评价之外,既能实现对数据的合理利用创新,也能兼顾对数据权利人的保护。

三、数据双重法益观的刑法实现:司法与立法并进的法益保护路径

数据双重法益观的实践路径包括司法路径与立法路径。相较于立法的稳定性,司法解释具有一定的灵活性,能够及时、有效地应对司法实践中常见、高发的问题。针对数据双重法益的实践保护,笔者建议,可以先通过出台司法解释的方式予以解决;对于数据法益保护的法条"漏洞",则应进行立法完善。

1.数据双重法益的司法保护路径

随着科技的发展,数据已经具备了独立保护的价值,《数据安全法》的出台和国家数据局的拟建立,都标志着数据是未来关系到国家发展、个人发展的重要因素,可以说在大数据时代,对数据的保护与利用被提升至国家战略的高度。目前学界对数据犯罪的研究,多集中于《刑法》第 285 条第 2 款与第 286 条第 2 款,但因破坏计算机信息系统罪,存在系统安全法益与数据安全法益的争论。例如,针对个人数据进行修改的案例中,被告人张某登陆法制晚报官方微博账号"法晚壹现场",删除约 3000 条微博,法院认为,其扰乱了社会公共秩序,产生恶劣的社会影响,最终认定为破坏计算机信息系统罪①。针对公共数据修改案例,被告人张某通过修改数据,影响排污系统监测,最终法院将其认定为破坏计算机信息系统罪②。但上述涉及对数据的修改行为,在适用破坏计算机信息系统罪时也并非不存在争议。主要原因在于,《刑法》第 286 条第 1 款与第 3 款均有"计算机信息系统正常运行"的表述,而该罪第 2 款仅规定了"后果严重"。因而,司法实践中将大量修改数据的行为统一认定为破坏计算机信息系统罪的做法饱受争议,认为不当扩张了该罪的适用范围。对此,笔者认为应当以数据双重法益为指导,对非法获取计算机信息系统数据罪的司法适用进行限制。

首先,以数据双重法益作为该罪的侵犯法益,符合法条的罪状表述。《刑法》第 285 条第 2 款非法获取计算机信息系统数据罪,主要规制的是数据的获取行为。根据罪状表述,"侵入"或者"采取其他技术手段"均要求行为人数据获取的行为,需要突破或避开数据权利人为数据所设置的安全保护措施,而数据权利人所设置的安全保护措施的目的,正是为了避免数据遭受不必要的侵害。如果行为人的数据获取行为事先经过数据权利人的同意,则完全没有必要采用"侵入"或者"采取其他技术手段"的做法。因而,行为人的数据获取行为,在侵犯数据安全法益的同时,也侵犯了数据自决权法益。

其次,以数据双重法益作为该罪的侵犯法益,可实现公开数据的合理使用。在风险刑法观的影响下,刑法对安全、秩序价值的追求愈发迫切。但是,过度强调刑法对数据安全法益的保护,容易造成对数据支配权保护的漠视。例如,行为人"爬取"存储于数据权利人系统中的公开数据,通常会被认定为非法获取计算机信息系统数据罪。从行为外观上看,行为人的爬取行为符合"采用其他技术手段",属于绕开或突破安全保护措施的行为。但问题在于,行为人所爬取的数据属于公开数据,数据权利人将该数据予以公开,便意味着任何人可以获取该数据。此时,行为人的爬取行为只能认定为获取的行为手段违法,但并未对数据本身的内容及数据权利人享有的相关数据权益造成损害,也就不能认定为对数据法益造成侵害,进而适用非法获取计算机信息系统数据罪。此外,过于强调对安全状态的打破,有时又会不当放纵犯罪。例如,数据权利人未对数据设置相关安全保护措施,将其放置于办公桌上,此时行为人的获取行为,虽然没有对安全技术措施造成侵害,但并不意味着行为人的行为是合法的,应当认定为对数据保密性与知情同意的侵害。因此,对安全的理解不能仅侧重于对安全保护状态的突破,而应当立足于数据内容本身,结合数据的实质安全状态予以综合认定。

最后,针对国家、公共数据保护缺位的问题,可以先通过司法解释予以解决。《数据安全法》第 21 条明确提出,要对数据进行分类分级的安全保护,相较于《刑法》第 286 条第 2 款仅规定"后果严重"的情节要件,非法获取计算机信息系统数据罪分别以"情节严重"与"情节特别严重"作为基本的构成要件结果与加重的构成要件结果,可以通过解释的方式,实现数据的分类分级保护。但数据作为信息的载体,对数据的保护需要对信息的类型进行有效区分。目前针对国家数据的保护,多以"国家秘密"的认定为前提。《中华人民共和国保守国家秘密法》

第13条规定:“下列涉及国家安全和利益的事项,泄露后可能损害国家在政治、经济、国防、外交等领域的安全和利益的,应当确定为国家秘密:(一)国家事务重大决策中的秘密事项;(二)国防建设和武装力量活动中的秘密事项;(三)外交和外事活动中的秘密事项以及对外承担保密义务的秘密事项;(四)国民经济和社会发展中的秘密事项;(五)科学技术中的秘密事项;(六)维护国家安全活动和追查刑事犯罪中的秘密事项;(七)经国家保密行政管理部门确定的其他秘密事项。政党的秘密事项中符合前款规定的,属于国家秘密。”可见,仅有第1款规定的7项行为及符合第2款的规定范围的,才能认定为“国家秘密”。而对于不属于“国家秘密”的数据获取行为,可以通过《刑法》第285条第2款的规定予以保护。

2.数据双重法益的立法保护路径

随着大数据时代的发展,基于《刑法》与《数据安全法》相衔接的需要,以及法益保护原则的积极标准,有必要建立以数据为中心的,独立的罪名保护体系。有观点认为,我国目前没有针对数据犯罪采用专章或专节的立法方式,无法实现对数据法益的独立保护[22]。但问题在于,虽然当前刑事立法对数据法益的保护力有不逮,但也并不意味一定要通过增设数据犯罪专章的方式来进行调改。因《刑法》分则专章的增设,必然涉及大量罪名的调整,如将侵犯公民个人信息罪、侵犯商业秘密罪、非法获取计算机信息系统数据罪等涉数据类罪名予以调整,会导致刑法罪名体系的混乱。而如果采用增设新罪的方式则又需要通过增设大量罪名,设立数据犯罪专章,势必会导致刑法罪名数量的臃肿。

笔者认为,出于数据法益独立保护的需要,立法对数据双重法益的保护,应当分为两个部分:一是针对数据获取行为规制的完善,二是增设针对数据修改、使用行为的规制。前者主要是对非法获取计算机信息系统数据罪的修改,而后者主要涉及破坏、滥用数据罪的增设。

针对数据获取行为规制的完善,主要是要通过对《刑法》第285条第2款非法获取计算机信息系统数据罪的修改,确立以数据为中心的保护模式,将针对储存在计算机信息系统以外的数据予以涵盖。这是因为,随着科技的发展,部分数据并不存在于系统中,而是存在于云端网络、移动设备等,此时,行为人获取数据的行为并不一定要触及计算机信息系统安全法益,对云端数据等的获取、修改行为,以计算机信息系统安全为中心的罪名无法实现对数据的有效保护。例如,针对数据获取行为,因不属于侵入“计算机信息系统”的范畴,进而无法适用于《刑法》第285条第2款,导致“无法可依”的局面。同样,针对数据修改行为,《刑法》第286条第2款的法条中同样具有“计算机信息系统”的表述,如此,则行为人针对云端数据的修改,也无法通过适用破坏计算机信息系统罪来进行规制。在此基础上,针对情节严重的情形,应当设定不同的量刑标准,将非法获取国家数据、公共数据以及个人数据的行为予以分类分级保护。在罪名的适用范围上,主要针对不构成“国家秘密”“商业秘密”等现有信息类罪名以外的数据予以保护,避免因罪状的修改而导致罪名间的适用竞合。

针对数据修改、使用行为,我国可以考虑增设破坏、滥用数据罪。该罪规制的是非法对电子数据实施修改、滥用等侵犯数据自决权与数据安全的行为,其立法意义既是为了实现对数据的周延保护,也是为了与《刑法》第286条第2款的适用予以区别,实现数据法益的独立保护。其中,修改行为包括但不限于对数据的删除、增加操作,只要改变了原有数据的形态均属于修改;滥用行为主要是指对数据的非法使用,包括超越授权使用、无授权使用等情形。如此便能实现刑法对数据保护的周延,将滥用他人数据的行为,纳入刑法的规制领域。

根据数据的功能可以将数据分为两大类:一类是涉及计算机信息系统正常运行的数据,另一类是与计算机信息系统运行无关的数据,如存储于系统中的个人信息、商业秘密等均属于无关系统运行的数据。笔者在前文中提出,当下针对数据修改行为的规制,主要适用《刑法》第286条第2款,将所有涉及数据的修改行为,一概认定为破坏计算机信息系统罪。但该罪的适用是以计算机信息系统安全遭受侵害为主,其保护的法益是计算机信息系统的正常运行[23],如果将破坏计算机信息系统罪的保护法益解释为数据安全法益,则势必会造成《刑法》第286条第1款、第3款与第2款保护范围的割裂。因而,基于法条保护法益的一致性,应当将破坏计算机信息系统罪中的数据认定为,关乎系统正常运行的数据,将无关系统运行的数据予以排除。但因无关系统运行的数据也具有刑法保护的必要性,则适用破坏、滥用数据罪予以规制。

基于数据功能差异对数据类型作出的区分,笔者主张通过增设新罪的方式将针对无关系统运行数

据的修改行为从《刑法》第 286 条第 2 款中剥离。这样不仅可以厘清破坏计算机信息系统罪的适用范围,减少适用争议,而且能够填补刑法对数据滥用行为的规制空白,进而实现对数据法益的独立保护目的。同时,针对破坏、滥用数据罪的量刑幅度,可依据数据的分类分级,以个人数据、公共数据、国家数据分层量刑的模式,体现出对数据的分类分级保护。此外,新罪名的增设需要厘清与既有罪名的罪数问题。例如,行为人非法获取数据后,又修改、滥用该数据的应当如何处罚。笔者认为,对此应当区分两种情形:第一,行为人非法获取数据后针对该数据本身实施修改、滥用的操作,应当以牵连犯论处。此时行为人实施的前获取行为,是后续修改、滥用行为的必经阶段。第二,行为人非法获取数据后,通过修改数据,同时以修改后的数据为工具进行滥用,实施侵犯其他具体法益的行为,则应当以上游的非法获取数据行为和下游所实施的具体犯罪行为并罚。

以数据安全法益、数据自决权法益作为破坏、滥用数据罪的保护法益,不仅可满足科技发展对数据保护的紧迫需要,又能避免对数据的保护范围过宽,而导致相关罪名沦为“口袋罪”,不当地扩张刑法的打击范围。例如,针对破坏、滥用数据罪的适用,行为人使用他人公开数据的行为,是否构成犯罪,便可结合数据的双重法益予以分类探讨。如果数据权利人公开相关数据,但同时设置相应安全技术措施,避免他人肆意更改公开数据,并且事先言明,使用该数据需要征得其同意,此时因数据权利人公开了数据,数据的保密性灭失,而行为人完整使用该数据获得收益的情况,属于侵犯了数据自决权法益,但因行为人使用数据的行为,并未侵犯数据安全法益,则应当适用民事、行政处罚。如果行为人对数据权利人的数据予以修改并加以使用,造成了数据完整性受损和数据自决权遭受侵害,则可以适用刑法处罚。而之所以前者不构成犯罪,也是在严守刑法谦抑性底线的基础上,通过与《数据安全法》第 52 条衔接,确立针对相关行为的阶梯式治理模式。因此,以数据的双重法益可有效限缩非法获取计算机信息系统数据罪与破坏、滥用数据罪的成立范围,当行为单一侵犯数据自决权或数据安全时,并不构成犯罪,而是结合《数据安全法》的相关规定承担民事责任或适用行政处罚。

需要注意的是,在对数据安全法益加以保护时,不能仅关注数据保护的形式,也应当关注数据保护的实质需要。如果仅仅强调对数据安全措施的突破,而忽视了正当使用的必要,那么安全将会成为刑法适用泛化的依据乃至借口。

因此,数据安全法益的认定应当分为两部分:一是数据安全法益具体内涵的识别,二是数据安全法益的处罚必要性的判断。前者是保护数据不被侵害的安全状态,后者是数据被侵害后所造成的不利后果,即将数据安全的事后判断作为出罪事由予以考量。例如,未经企业授权的计算机安全人员主观善意地检测网络安全漏洞并提交第三方平台予以披露的行为,最终被检察院做出不起诉的决定,便是因为其行为并不会造成严重法律后果,缺乏刑事处罚的必要性[24]。此时,行为人虽然侵犯了他人数据安全法益,也侵犯了数据自决权法益,但是通过填补数据“漏洞”等方式,可以帮助企业完善系统运行,在这种情况下,因其法益侵害程度较为轻微,刑法也就没有介入的必要性。在此基础上,结合数据自决权法益,只有侵犯数据权利人相关权利的同时,同时造成数据内容本身安全的损害,方可认定为对数据法益的侵害。

结　语

当今社会正处在一个飞速发展的时代,各种新生事物层出不穷,因而导致传统刑法在应对新兴技术手段时,多有捉襟见肘之感。但是刑法在介入新兴领域之时,应当保持克制的态度。所以,对于数据的保护,应当趋于理性,合理拓展刑法规制范围,不能一概将信息类犯罪、计算机犯罪、网络犯罪的概念同义替换为数据犯罪,而是应当在厘清数据犯罪本质内涵的基础上,进一步加以细化,同时力求确立数据犯罪所侵犯的具体的、含有实际内容的法益。在新罪的增设上,既要体现法益保护的现实需要,又要避免法益过度抽象化,减少回应式立法。因此,谋求以构建单行刑法或数据犯罪专章的方式来完善数据犯罪的刑事治理,并不契合刑法体系发展的逻辑理路和现实要求。基于当下保障数据发展的需要,合理的做法是,通过审慎增设新罪对数据进行分类分层的保护,同时以数据的双重法益限缩刑法的适用范围,使其既不阻碍数据的创新发展,又能使刑法为数据的合理利用保驾护航。

注释

①北京市丰台区人民法院刑事判决书,(2015)丰刑初字第 1964 号。

②湖北省枝江市人民法院刑事判决书,(2020)鄂 0583 刑初 236 号。

参考文献

[1]顾伟,孙伟,陈朝铭.数字化时代数据犯罪的刑法回应[J].上海法学研究,2022(1):268-282.

[2]张勇.数据安全分类分级的刑法保护[J].法治研究,2021(3):17-27.

[3]赵春玉.大数据时代数据犯罪的法益保护:技术悖论、功能回归与体系建构[J].法律科学(西北政法大学学报),2023(1):95-107.

[4]赵文涵.组建国家数据局[EB/OL].(2023-03-07)[2023-08-25].http://www.news.cn/2023-03/07/c_1129419141.htm.

[5]张明楷.刑法学[M].北京:法律出版社,2021:85.

[6]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(6):37-52.

[7]刘宪权.数据犯罪刑法规制完善研究[J].中国刑事法杂志,2022(5):20-35.

[8]张勇.数据安全法益的参照系与刑法保护模式[J].河南社会科学,2021(5):42-52.

[9]黄鹏.数据作为新兴法益的证成[J].重庆大学学报(社会科学版),2022(5):192-206.

[10]熊波.数据状态安全法益的证立与刑法调适[J].当代法学,2023(1):70-82.

[11]齐白.全球风险社会与信息社会中的刑法[M].周遵友,江溯,主译.北京:中国法制出版社,2012:308.

[12]郭旨龙.非法获取计算机信息系统数据罪的规范结构与罪名功能:基于案例与比较法的反思[J].政治与法律,2021(1):63-76.

[13]梅夏英.信息和数据概念区分的法律意义[J].比较法研究,2020(6):151-162.

[14]程啸.论大数据时代的个人数据权利[J].中国社会科学,2018(3):102-122.

[15]李婷.大数据时代的数据法益与数据犯罪[J].数字法治评论,2022(1):112-127.

[16]纪海龙.数据的私法定位与保护[J].法学研究,2018(6):72-91.

[17]李爱君.数据权利属性与法律特征[J].东方法学,2018(3):64-74.

[18]梅夏英.数据的法律属性及其民法定位[J].中国社会科学,2016(9):164-183.

[19]孙祯锋.比较法视域下科学研究处理个人数据的法律界限[J].科技进步与对策,2022(24):91-99.

[20]敬力嘉.信息网络犯罪规制的预防转向与限度[M].北京:社会科学文献出版社,2019:92.

[21]于润芝.非法获取个人数据犯罪的法益分析及处罚限定[J].大连理工大学学报(社会科学版),2023(2):56-64.

[22]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(6):97-106.

[23]江溯.环境监测中干扰采样行为的刑法定性[J].政法论丛,2024(1):107-119.

[24]孙道萃.网络"白帽子"的罪责边界审思:从袁某案说开去[J].法律适用,2017(16):75-81.

The Dual Legal Interests of Data Crimes and Their Protection Paths

Yuan Bin　　*Xue Liming*

Abstract: The importance of data in the era of big data is increasingly prominent, but there are still some problems in the protection of data legal interests in China's criminal law, including the abstract connotation of data order legal interests, which makes it difficult to undertake the mission of protecting data legal interests and ensuring the stable and healthy development of data technology. A single data security legal doctrine can lead to improper use of public data being criminalized. The legal interests violated by data crimes are dual legal interests, with data security as the outer shell and data self-determination as the core. Based on the dual legal interests of data crimes, China should protect data under criminal law by amending old crimes and adding new crimes in legislation. On the basis of establishing independent protection of data legal interests, Article 285 (2) of *the Criminal Law* should be amended, and special crimes targeting data destruction and abuse should be added. In the judiciary, the dual data legal interests should be used to reasonably define the threshold and scope of punishment for data infringement, and to achieve systematic protection of personal data, social public data, and national data.

Key words: data security; the right to data self-determination; dual legal interests; crimes of damaging and abusing data

责任编辑:一　鸣　　执　中