重庆大学学报(社会科学版) 2025年第31卷第1期
JOURNAL OF CHONGQING UNIVERSITY(Social Science Edition) Vol. 31 No. 1 2025

Doi:10. 11835/j. issn. 1008-5831. fx. 2024. 01. 003

欢迎按以下格式引用:梅传强,盛浩. 数据安全刑法保护的模式转换:从管理安全到利用安全[J]. 重庆大学学报(社会科学版),2025(1):272-288. Doi:10. 11835/j. issn. 1008-5831. fx. 2024. 01. 003.

Citation Format: MEI Chuanqiang, SHENG Hao. Mode transformation of criminal law protection of data security: From management security to utilization security[J]. Journal of Chongqing University (Social Science Edition), 2025(1):272-288. Doi:10. 11835/j. issn. 1008-5831. fx. 2024. 01. 003.

数据安全刑法保护的模式转换:从管理安全到利用安全

梅传强[1],盛 浩[2]

(1. 西南政法大学 法学院,重庆 401120;2. 四川警察学院 侦查系,四川 泸州 646000)

摘要:数据安全关乎国家安全和社会稳定,通过刑法保护数据安全既有必要性也有紧迫性。经过修正案的完善和司法解释的补充,我国刑法形成了保护数据安全的"管理安全模式",即以静态数据的保密性、完整性、可用性为规范目的,以非法获取计算机信息系统数据罪、破坏计算机信息系统罪为规范依托的数据安全保护标准样式。"管理安全"保护模式的确立经历了数据作为计算机信息系统的保护附带内容、数据成为相对独立的刑法保护对象,以及借助司法解释扩大数据安全涵摄范围三个发展阶段。从规范上分析,"管理安全"保护模式具有封闭性、静态性特征,这难以适应数字社会数据动态化、共享化发展的趋势,未能实现与《中华人民共和国数据安全法》等前置法的有序衔接,并导致刑法中数据犯罪条款在司法适用出现"模糊化"的问题。数字社会的到来产生了新的数据安全风险类型,即分析数据所产生的风险,以及利用分析数据产生的知识和信息,作出决策而引发的风险。面对新的风险类型,数据安全保护亟需转向以动态数据的保密性、完整性、可用性、可控性、正当性为核心的"利用安全"模式:在保护理念上,应当将数据作为独立对象,从依附保护向专门保护、系统保护转变;在规制重心上,从注重数据收集、储存节点向其他节点拓展,从片面保护向全链条保护转变;在保护策略上,从笼统保护向分类分级保护转变。为此,应当在优化现有数据犯罪条款的基础上,增设新的数据犯罪,并引入数据分级分类保护制度。具体而言:一是在立法上明确数据与信息、计算机信息系统的关系,并剥离出独立的数据条款,实现数据安全的专门保护,同时,在《中华人民共和国刑法》分则中集中规定危害数据安全犯罪,实现系统化保护;二是增设非法公开、提供、出售、出境数据罪,非法分析数据罪、非法运用数据分析结果罪等犯罪,实现周延保护;三是构建数据安全分级分类保护制度,即在定罪层面,数据分级分类与数据犯罪的认定相结合,在量刑层面,数据分级分类与数据犯罪的刑罚裁量相对接,实现分级分类保护。

基金项目:2024年度教育部人文社会科学研究一般项目(24YJA820019);重庆市新型犯罪研究中心2022年度规划项目"个人数据权利刑法保护的立场及路径研究"(22XXFZ23)

作者简介:梅传强,西南政法大学法学院教授,1685807377@qq. com。

关键词:数据安全;数字社会;刑法保护模式;数据分级分类;数据合规
中图分类号:D914　　**文献标志码**:A　　**文章编号**:1008-5831(2025)01-0272-17

一、问题的提出

数据安全与国家经济运行、社会治理、公共服务、国防安全等领域紧密联系,事关国家安全和社会稳定,是一种极为重要的新兴安全类型。尤其是随着“滴滴事件”“领英数据泄露事件”“平台大数据杀熟”等涉及重大数据安全事件的发生,数据安全问题不仅迅速成为当前社会关注的焦点问题,而且一跃成为国家治理的核心议题。加快构筑数据安全法律保障体系,提升国家数据治理效能,这既是我国法治建设的重点,也具有现实的必要性和紧迫性。刑法作为数据安全保护的重要手段,在数据安全法律保障体系中扮演着“最后法”和“保障法”的角色。从现有规范来看,《中华人民共和国刑法》(以下简称《刑法》)在第285条第2款“非法获取计算机信息系统数据罪”、第286条“破坏计算机信息系统罪”及相关司法解释的基础上,形成了通过打击破坏型数据犯罪和获取型数据犯罪以保护静态数据安全的数据安全保护模式。在该模式之下,数据安全由保密性(confidentiality)、完整性(integrity)、可用性(availability)三个核心要素构成,数据犯罪被定义为“以数据为对象的非法获取、删除、修改、增加等行为”,刑法中数据犯罪条款的理解与适用也应以此为中心展开[1]。该模式的一个显著特征是,由于信息载体和计算机信息系统构成要素的双重限制,数据被视为不具有流动性的静态事物,数据安全也是一种旨在保持数据安宁状态的静态安全,因此,该模式也可称为“管理安全”模式。

尽管管理安全模式下的规范体系对静态数据的安全保护起到了积极的作用,但管理安全模式只是传统信息网络社会下数据安全保护需求的表达,并不能完全适用于正在到来的数字社会。数字社会的网络化、数字化、智能化进程,改变了人类社会的单一物理属性,带来了“物理世界—数字世界”“现实生活—虚拟生活”“物理空间—电子空间”的双重社会架构,且两重架构之间相互影响、相互嵌入、相互塑造,共同形成了数字社会的基本形态[2]。在数字社会中,数据作为重要生产要素正改变以往相对静止的状态,大量数据的衍生、流动、聚集甚至被分析,深刻改变人们的日常生活,甚至影响了人们各方面的选择和决策。在此过程中,“作为数据生产者和使用者参与‘大数据基本循环’的普通公民,对于这里所使用的信息技术基础设施既无法把握又无法施加影响”[3],数据极易脱离监管被滥用甚至被不法分子恶意利用,产生新的数据安全风险。显然,传统的保密性、完整性、可用性三要素,已经无法精准和完整地概括数字社会的数据安全价值诉求,在管理安全模式下建构的刑法规范框架,也无法适应数字社会的治理思维,数据安全刑法保护面临思维滞后、模式陈旧、规范供给不足等问题。本文将立足于数字社会数据发展的现状及安全诉求,探讨动态数据利用安全刑法保护的模式转变方向及规范实现进路。

二、数据保护“管理安全”模式的形成

刑法中的数据犯罪可以被分为“狭义的数据犯罪”和“广义的数据犯罪”,前者是指直接以数据为对象的犯罪,其被刑法中的数据犯罪条款专门规制;后者除了包括直接以数据为犯罪对象的犯罪之外,还包括将数据作为手段和工具的犯罪,其往往被刑法中的其他犯罪(如诈骗罪等)规制。从立法上看,我国刑法对于数据安全的保护,是随着立法者对数据认识不断深入而变化的,整体上可划分为三个

阶段。

(一)雏形阶段:数据作为计算机信息系统保护的附带内容

数据安全的刑法保护,最早可以追溯到1997年《刑法》修订,当时在第286条第2款增设了“破坏计算机信息系统罪”,即行为人违反国家规定,对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作,后果严重的,依照破坏计算机信息系统罪处罚。其中,“数据”是指计算机信息系统实际处理的一切有意义的文字、符号、声音、图像等内容[4],在客观方面,只有删除、修改、增加行为造成计算机信息系统不能正常运行时才能被评价为“后果严重”的情形[5]。这种将数据安全与计算机信息系统保护紧密关联的思路源自1994年《计算机信息系统安全保护条例》第2条、第3条的规定①,即借助维持内部数据的安定状态以保障计算机(信息)系统的技术安全与运行安全的立法思维。

虽然数据概念在客观上得到了规范表达,但以下几个特征决定了该阶段只是“自身保护”模式的雏形阶段:(1)地位上的从属性。虽然“数据”作为新兴的概念被写入刑法规范之内,但刑法禁止删除、修改、增加数据行为的目的在于保证计算机信息系统的有效运行,数据自身的完整性、有效性、可用性只是计算机信息系统安全的附带性内容之一。(2)状态上的封闭性。受制于Web1.0时代的低互联性所带来的限制,当时的计算机信息系统之间处在相对隔离的状态,彼此之间很难实现自由的信息交流,这使得计算机信息系统数据具有封闭性、限定性和静态性。(3)概念上的含混性。虽然《刑法》第286条第2款明确规定“数据”,但其却与“应用程序”同句并列,这导致司法适用中难以区分“数据”与“应用程序”,继而引发数据实体内涵的空泛性和模糊性问题[6]。

(二)成形阶段:数据成为相对独立的刑法保护对象

管理安全模式的成形标志是《中华人民共和国刑法修正案(七)》增设“非法获取计算机信息系统数据罪”。根据《刑法》第285条第2款规定,行为人采取非法侵入或者其他技术手段,获取该计算机信息系统中存储、处理或者传输的数据,情节严重的,按照非法获取计算机信息系统数据罪定罪处罚。进入Web2.0时代后,网络世界的互联性和开放性明显增强,计算机网络犯罪的形态也随之变化:非法侵入或者利用其他技术侵入他人计算机系统的主要目的,是窃取计算机系统存储、处理和传输的数据。其中,网上银行的数据信息又是窃取的重点,包括个人在网上银行的账户、密码等,这给公民的金融财产安全带来极大威胁[7]。因此,刑法才调整以往的规制内容,在破坏型数据犯罪的基础上增加了获取型数据犯罪。

归纳来看,该阶段的数据安全刑法保护呈现以下特征:(1)地位上的相对独立性。《刑法》第285条第2款的增设使得数据的从属性地位得以改变,数据概念的轮廓感得以加强。一方面,刑法为获取型数据犯罪设置独立罪名,并把“数据”写入罪名之中进行表述,这意味着数据概念的独立规范意义得到进一步承认;另一方面,虽然该罪的罪名被概括为“非法获取计算机信息系统数据罪”,但考查规范内容可以发现,该罪禁止非法获取行为的直接目的并不是保证计算机信息系统安全,而是侵入计算机系统成为非法获取数据的途径之一,数据安全在某种程度上摆脱了原来相对于系统安全的辅助性、依

①《计算机信息系统安全保护条例》第2条、第3条规定,“本条例所称的计算机信息系统,是指由计算机及其相关的和配套的设备、设施(含网络)构成的,按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统”;“计算机信息系统的安全保护,应当保障计算机及其相关的和配套的设备、设施(含网络)的安全,运行环境的安全,保障信息的安全,保障计算机功能的正常发挥,以维护计算机信息系统的安全运行”。

附性地位。(2)价值上的重要性。数据概念的相对独立性也征表了数据安全在价值上的重要性,有学者认为非法获取计算机信息系统数据罪的犯罪客体是计算机信息系统及其中数据的安全[8],数据安全法益观开始出现。(3)内容上的完全性。虽然破坏计算机信息系统罪禁止针对数据的删除、修改、增加行为可以保证数据安全的完整性、有效性、可用性,但这在客观上并不周延,正是由于非法获取计算机信息系统数据罪的增设,才形成了"破坏型+获取型"数据犯罪的格局,数据安全的核心内容被更全面地揭示出来。

(三)扩容阶段:借助司法解释扩大数据安全的涵摄范围

在该阶段,数据安全涵摄范围通过司法解释和司法适用的双重叠加实现了扩张。为依法惩治危害计算机信息系统安全的犯罪活动,维护正常的计算机网络运行秩序,最高人民法院、最高人民检察院于2011年出台《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《解释》)。根据《解释》第1条规定,非法获取计算机信息系统数据行为的情节严重程度可以通过其所涉及的"身份认证信息"数量进行判断,并且《解释》第10条规定,"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"。可见,身份认证信息被定性为数据的下位概念,数据概念的外延也扩张至个人信息的范畴。同时,根据《解释》第10条规定,《刑法》中的"计算机信息系统"和"计算机系统",指的是"具备自动处理数据功能的系统,包括计算机、网络设备、通信设备、自动化控制设备等"。在司法适用过程中,数据概念也出现了一定的扩张现象,司法人员在具体案件中的扩大化解释使得作为犯罪对象的"数据"范围极广,其几乎涵盖了身份信息、网络虚拟财产、网络知识产权、数据产品等一切可在电脑系统中储存、显示、获取的权利客体[9],数据安全的涵摄范围也随之扩容。

该阶段形成了数据安全保护泛化的格局,缓解了相关条款以往被局限于特定场域而适用受限的局面。总体来看,该阶段的数据安全刑法保护呈现以下特征:(1)概念上的模糊性。由于数据概念借助解释的方式不断扩张,承载于其上的数据安全的概念轮廓也不断拓展并随之虚化,数据安全在客观上已难以与信息安全、网络安全等概念区别开来。(2)地位上的兜底性。由于新型网络犯罪的不断更新发展,以及前述的数据概念的扩张,《刑法》中的数据条款也随之开始迎合更多的刑法评价需求,出现了网络犯罪认定的数据犯罪化。以盗窃网络虚拟财产犯罪为例,虽然不少理论学者和实务专家主张该行为成立盗窃犯罪,但最高人民法院研究室的研究意见却认为"虚拟财产不是财物,本质上是电磁记录,是电子数据,这是虚拟财产的物理属性",所以对该行为应以非法获取计算机信息系统数据罪定罪量刑[10]。

经过三个阶段的修正案完善和司法解释补充,数据安全刑法保护的管理安全模式得以形成。《刑法》中的两条数据犯罪条款互为补充,基本满足了获取阶段和存储阶段静态数据的保密性、完整性、可用性的保障需求。其中,非法获取计算机信息系统数据罪旨在保护数据的保密性,以确保数据利益主体对数据的排他性获取、复制、使用与处分等权益;破坏计算机信息系统数据罪重在保护数据的完整性与可用性,以确保数据不被其他主体破坏以及数据权利主体可随时访问和使用数据[11]。

三、数据保护"管理安全"模式的问题检视

"管理安全"保护模式所针对的数据安全风险,主要是利用计算机网络系统环境的漏洞来侵害数据的保密性、完整性和可用性,其在客观上主要表现为非法获取、删除、修改、增加等行为。通过回顾数

据刑法规范的演变历程可以发现,在信息网络犯罪更新迭代以及人们安全诉求升级的推动下,刑法借助立法和解释两种方式不断提升自身的包容性和延展性,这对完善数据安全刑法保障体系具有十分重要的意义。然而,刑法是随着新兴的社会风险、人们日益增长的安全需求,以及用刑法来调控社会风险的期待而变革的[12],根植于传统信息网络社会的规范样式难以适应数字社会中的数据治理需求,以及数据安全法的修订步伐,“管理安全”保护模式面临时代性的拷问。同时,囿于“管理安全”刑法保护模式的内容模糊性等固有缺陷,刑法中的数据安全概念逐渐丧失自身的独立性,相关刑法条款也显现出“模糊化”的趋势。

(一)难以满足数字社会的数据治理需求

得益于物联网、互联网等技术的不断驱动,万物互联化、数据泛在化成为社会进步的大趋势,数字时代已经到来[13]。数字社会在本质上是信息革命的后现代性给其现代性带来的挑战,在客观形态上,数字社会表现为社会本身的全面数字化,这与传统信息网络社会中数字技术的局部化运用存在明显区别。所以,传统的信息网络社会到数字社会的发展过程是从特定行业向全社会扩张、从静态连接向动态连接、从技术主导向内容主导、从以设备为中心向以人为中心的数字化过程[14];在技术语境上,数字社会的典型技术表达是人工智能、大数据分析、自动化决策等智慧化科技,它们在现实社会中的应用场景极为广泛,在诸如自动驾驶、公共管理、司法等领域与场景中,发挥着举足轻重甚至是决定性的作用[15]。总之,数据是数字社会的核心要素。但是,数字社会赋予数据全新意义的同时,也在治理上提出了优化数据归集共享、提高数据供给质量、健全数据标准规范、完善数据管理职能等新的要求[16],原有的数据治理模式需要适时转换。具体到刑法层面,传统的“管理安全”保护模式具有封闭性、静态性,这既无法满足数字社会背景下数据安全的周延保护要求,也无法满足数据治理的共享化、动态化、多元化等需求。

1. 管理安全保护模式的封闭保护逻辑脱嵌于数据的共享化发展趋势

数据的重要资源地位并非一直受到重视,在数字社会到来之前,由于认识能力的局限性,数据往往被视为物理事物的电子形式,法律定性为数据权利保护的物权化思维,即将数据权看作是特定主体对特定数据的排他性支配权利,并针对性地制定规范予以保护。具言之,该思维将数据界定成存储在特定载体上的数据文件,一旦行为人对数据文件进行侵犯,同时也就构成了对载体所有权的侵犯,数据文件“拥有者”即可“通过诉诸对数据载体所有权的侵权,来迂回地向侵犯数据文件者主张权利”[17]。物权保护思维具有明显的滞后性,因为云存储时代的数据文件常会存储于云端,甚至分别储存于不同地方的服务器上,这使得数据文件“拥有者”与云存储供应商(或者是为云存储供应商提供具体数据文件储存服务的独立第三方企业)并非同一主体,此时数据文件的“拥有者”便无法诉诸数据载体所有权来保护自己的数据。刑法层面的管理安全模式与物权化思维具有同质性,二者都强调了数据在封闭环境中的载体依附和私人所有特性:第一,正如前面所总结的那样,无论是现行《刑法》第285条规定的获取型的数据犯罪,还是第286条破坏型数据犯罪,其在发生领域上都强调了“计算机信息系统”条件,而脱离此场域的存储于移动设备中的数据、流通中的数据等则不能被直接包括在刑法保护圈之中;第二,从《刑法》第285条和第286条的规范表述看,行为构成数据犯罪都要求其“违反国家规定”,以及使用了违背被害人意志的“侵入”“破坏”“获取”行为,这旨在保证数据在特定主体排他支配下的安宁状态,恰好是保护数据私人所有的规范体现。

但不同的是,数字社会基于物理时空又超越物理时空,既包容物理世界又是对物理空间的数字化

重建[18]，由物理世界衍生的物权保护思维不能完全适用于数字社会。数字社会中，数据价值的增长主要依靠流动、共享实现，其在法律层面的数权也不再表现为“一数一权”的客观占有，而是一种排他性质的共享权，往往呈现出“一数多权”的现象[19]。共享权是数字社会中数权的本质，它的实现方式是公益数权与用益数权，数据的所有权和使用权的分离因此成为可能，形成一种“不求所有，但求所用”的共享格局[20]，这决定了传统的物权化保护思维难以把握住数据的共享化发展脉搏，不能回应新社会背景下数据安全保障的全部诉求。与之对应，刑法层面的“管理安全”保护模式强调数据安全保护的载体依附性和私人所有性，从理论上讲，这极易导致规范内容的迟滞化问题，即“管理安全”保护模式下的数据犯罪条款仍困守于私人所有和空间封闭的桎梏之中，造成了非法提供等实质上值得处罚的行为脱离刑法规制范围，刑法立法的迟滞化问题凸显。

2. 管理安全保护模式的静态保护逻辑难以和数据的动态化发展趋势兼容

传统的信息网络社会向数字社会的转变不但推动了数据的共享化发展，还推动了数据的动态化发展。传统的信息网络社会是一个中心化的“有限型”社会，由于人们缺乏有效的传播、获取渠道，数据的获取和运用活动往往具有不均衡性，所以数据常常处于《刑法》第 285 条和第 286 条所描述的“计算机信息系统中存储、处理或者传输”的封闭状态，无需法律制度的链条化、动态化保护。但性质迥异的是，数字社会的关系结构决定了其内在的机理是去中心、扁平化、无边界，基本精神是开放、共享、合作、互利。进入数字化时代后，互联网为人们构筑了蜂巢式的社会结构，任何个体之间在理论上都可以实现点对点的连接和沟通，随着电信网络技术的不断迭代发展，数据流通更加便捷。数字化时代的大数据不再是一个静态的状态，而是处于实时高速流动之中，数据安全也相应地处于一个动态过程，其中涉及数据的收集、处理、存储、共享、跨境等各个环节的安全以及数据处理平台的安全等。

数据的动态化发展在两个方面突破了管理安全模式：一是突破了“计算机信息系统”这种特殊载体。社会全面数字化所带来的“万物互联”令数据的载体形式更加多样化、普遍化，这使得传统需以侵入或者破坏计算机信息系统为前提的数据犯罪如今却不必以此为前提。行为人可能入侵的只是他人手机[21]、各种类型的传感器，甚至是“云存储”端；二是突破了“存储、处理或者传输”这种特定的存在状态。社会的全面数字化也带来了数据存在形态的多元化，数据既可以被收集、聚拢，也可以人际共享、有偿转让、跨境传播，而不是仅仅局限于“存储、处理或者传输”这三种状态。无论是非法破坏计算机信息系统罪还是非法获取计算机信息系统数据罪，其设置的构成要件内容都只足以对在计算机信息系统中存储、处理或者传输的数据进行保护，现行刑法无法满足数据动态化发展的安全保障需求。虽然《解释》第 10 条规定将“计算机信息系统”和“计算机系统”的含义扩张为“具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备等”，但该解释结论是否违反罪刑法定原则，以及能否从长远上解决刑法规范供应不足的问题，仍然存在疑问。

（二）难以实现刑法与前置法的有序衔接

数据安全法律保障体系中不仅包括刑法，还包括以《中华人民共和国网络安全法》（以下简称《网络安全法》）和《中华人民共和国数据安全法》（以下简称《数据安全法》）为代表的前置性法律。尤其

是《数据安全法》的出台,被定位为保护人民群众数字权益、促进数字经济健康发展的重要举措②。从规范内容上看,《数据安全法》对数据分类分级管理、安全风险评估、安全审查等基本制度作了规定,明确了相关主体的数据安全保护义务,其在保护静态数据的管理安全的同时,更加注重保护动态数据的利用安全:其一,在规制节点上,《数据安全法》涵盖了数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁各个节点,实现了动态环节的全链条保护。其二,在规制行为上,《数据安全法》的规制范围包括不履行安全保护义务、非法向境外提供、非法提供交易中介服务、拒不配合国家机关合法的数据调取要求、未经主管机关批准向外国司法或者执法机构提供数据,国家机关工作人员不履行法定的数据安全保护义务,数据安全监管人员玩忽职守、滥用职权、徇私舞弊、窃取或者以其他非法方式获取数据等行为类型,实现了安全风险的全方位防护。其三,在规制主体上,《数据安全法》的规制范围包括了开展数据处理活动的组织和个人,特别是对关键信息基础设施的运营者、数据出境企业、涉及处理重要数据的企业、数据交易服务机构等主体的数据合规义务作了要求,落实了数据利用的主体责任。总之,《数据安全法》突破了以往局限于一般主体在数据采集、储存节点实施的窃取、删除、修改等行为的规制逻辑,在规制的节点、行为和主体上加以延展,提供了契合数据动态化、共享化发展趋势的法律治理框架。

《数据安全法》是数据保护的基础性规范,而刑法是《数据安全法》实施的重要保障。一方面,“法律是规范公民行为、调整社会生活最重要的手段,各个法领域之间各有分工,相互配合,形成了较为稳定的法律秩序”[22]。在法秩序统一的视角下,各部门法间是协调的有机体,如果某个部门法调整了处罚的范围,其他法律针对某种行为的评价也会相应变化[23]。虽然规范目的差异性决定了刑法中的犯罪认定不能完全依赖前置法,但立法者应当保证刑法与前置法之间交叉或重合部分的协调性与有序衔接,以达到法秩序统一的要求。另一方面,社会保障机能要求,刑法作为其他法律的保障法,应当对逾越前置法防线且具有法益侵害或侵害危险的行为予以规制。因此,刑法与《数据安全法》应当保持在数据安全风险种类与范围上的匹配关系,才能更好地实现数据保护法律体系的法秩序统一和刑法的社会保护机能。但正如前所述,当前刑法中的数据条款因受到管理安全保护模式的限制,在规制范围上仅限于数据采集、储存阶段的非法获取、删除、修改、增加行为,对《数据安全法》规定的其他危害行为完全缺乏规制,这导致《数据安全法》中的宣示性刑事责任条款形同虚设,数据安全保护的刑法规范供给不足,《数据安全法》与刑法无法实现有序衔接。

(三)导致刑法中数据犯罪条款的“模糊化”异变

如果仅从规范和学理的角度分析,管理安全模式下的数据条款存在规制行为类型不全面、规制节点不完整、数据安全保护不周延的缺陷。但在实践中,由于“数据”概念的含混性和案件事实的错综复杂,刑法中的数据条款的适用领域开始由数据犯罪领域向其他领域延展,出现了规范适用“模糊化”的趋势,造成立法意蕴与司法实践的脱节。对此,本文检索、分析了中国裁判文书网上非法获取计算机信

②数据安全法:护航数据安全,助力数字经济发展[EB/OL].(2021-06-10)[2023-05-06].http://www.npc.gov.cn/npc/c2/c30834/202106/t20210610_311894.html.

息系统数据罪的判决书加以验证③（见表1）。

表1　非法获取计算机信息系统数据罪判决书分析

犯罪对象	案件数量	百分比	具体内容
账号密码	61	30%	社交平台账号和密码、网游平台账号密码、短信验证码、支付软件账号密码、QQ账号、WiFi密码、手机解锁密码等
特定数据	46	22%	平台运行数据、房产数据、微信平台数据、医院处方数据、防伪码数据等
网络虚拟财产	48	23%	平台打赏礼物、游戏装备、比特币等
其他虚拟财产	8	4%	平台积分、车牌靓号等
知识产权	16	8%	网课视频、网站代码、软件源代码及美术资源文件、设备研发资料、游戏的脚本等
个人信息	26	13%	手机号码、居民居住证信息、平台用户个人信息、航空公司旅客信息等

通过表1的数据可知，在司法实践中，非法获取计算机信息系统数据罪中“数据”的指涉范围广泛，几乎涵盖了账号密码、虚拟财产、知识产权、个人信息等一切可在电脑系统中储存、显示、获取的电子内容。在205份判决书中，行为对象为账号密码、特定数据的判决书共107份，占比52%；犯罪对象为个人信息、虚拟财产、知识产权的案件共98份，占比48%。就前一类案件而言，账号密码和特定数据是典型的数据类型，以非法获取计算机信息系统数据罪定性没有争议，但就后一类案件而言，由于个人信息、虚拟财产以及知识产权不符合严格的数据定义，以非法获取计算机信息系统数据罪定性不甚恰当。第一，数据和信息存在巨大差别，这不仅体现为数据和信息的含义不同，“数据”侧重于突出载体或媒介本身，而“信息”强调的则是所要传达的内容与本质[24]，还在属性、状态上体现为数据兼具信息本体和信息媒介的双重属性，而信息必须与传送媒介相分离[25]。因此，表中26份判决书将能够“识别特定自然人身份或者反映特定自然人活动情况”的个人信息定义为数据④，并将非法获取的行为定性为非法获取计算机信息系统数据罪实属不当，应将此行为定性为侵犯公民个人信息的行为。第二，数据往往作为其他权利客体的载体形式，如果承载于数据之上的游戏装备、比特币、网课视频、网站代码、软件源代码等具体内容，能够被评价为法律意义上的财产、知识产权等，则应当优先考虑适用相应的财产犯罪、侵犯知识产权犯罪进行规制，更好地实现法律适用的针对性和精准性。因此，表中涉及虚拟财产和知识产权的72份判决书的定性结果也不尽合理。

通过以上的分析论证可知，虽然《刑法》第285条第2款对非法获取计算机信息系统数据罪的构成要件作了明确规定，但在司法实践中构成要件却囊括了不该囊括的行为类型，该罪名被不恰当地“模糊化”适用了。究其原因，一方面，是由于《解释》将数据扩大解释为“用于确认用户在计算机信息系统上操作权限的数据”的“身份认证信息”；另一方面，是由于实践中未对数据的技术属性（0/1二进制代码）和法律属性（权利客体）加以区分，导致案件裁判者极易在“避繁就简”的思维定式下，以技术属性判断取代法律属性判断，将凡是以0/1二进制代码为基础的电子信息内容都简单地评价为数据，而不

③数据检索过程如下：进入高级检索，案由选择“刑事案件——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”，文书类型选择“判决书”，审理程序选择“一审”，裁判时间选择2020年5月6日至本文写作之时即2023年5月6日（共计3年），共获得样本223份，排除仅以非法控制计算机信息系统罪定罪的样本18例，共获得有效判决书205份。

④最高人民法院、最高人民检察院《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》第1条规定，刑法第253条之一侵犯公民个人信息罪中的“公民个人信息”，是指“以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等”。

再去深入考察其包含的法益内容。此外,这与管理安全模式下的立法逻辑还存在极大的关联:管理安全模式下的刑法规范更加注重计算机信息系统中静态数据的保护,这使得数据难以摆脱作为计算机信息系统构成要素和电子信息形成基础的角色,数据作为一种权利客体也难以与信息、财产、知识产权等其他权利客体区分开来。换言之,正是囿于管理安全模式的范围限制,导致原本有更广适用场域的刑法数据条款被逼仄于"计算机信息系统"具体场景中,从而与侵犯公民个人信息罪、侵犯财产犯罪、侵犯知识产权犯罪等在行为规制层面产生更大的重合。再加上数据犯罪"以技术属性判断取代法律属性判断"的思维定式影响,以及数据与信息的模糊界分,非法获取计算机信息系统数据罪的模糊化适用才得以发生。

四、数据保护"利用安全"模式的提出及其实现

数据安全刑法保护模式的选择,不是立法者的随意决策,其背后隐含着深刻的背景因素和规范逻辑。在传统的信息网络社会背景下,数据只被简单地视为记录载体和初级生产要素,数据权利也被视为物权加以保护,所以保密性、完整性、可用性必然成为该阶段数据安全的核心要素。但是,数字社会的技术架构决定了其核心价值是去中心化、去边界化,即开放、协作、共享。这使得传统以保密性、完整性、可用性为核心要素的模式不再契合时代需求,数据安全的核心要素应当因应数字时代的数据安全保护诉求及时扩张和转变。在此基础上,数据安全的刑法保护也应当实现从管理安全模式向利用安全模式的转换,实现数据安全的专门保护、系统保护、周延保护、分级分类保护。

(一)数字社会下的数据安全核心要素转变

保护数据安全的前提是明确数据安全的构成要素。20世纪末,人类进入信息网络世界之后,数据就作为一种基础性的工具和材料被运用于信息记录、传输等领域。在传统信息网络社会阶段,人们更加重视数据中所包含的信息材料以及数据所依托的计算机信息系统的完整性和私密性,因此,数据自身的安宁状态成为数据安全的核心指向。例如,美国克林顿政府在1998年5月颁布了《第63号总统决策指令》,明确规定了计算机系统保护机制和"信息的准确、保密和可靠处理"⑤。2002年10月,美国《联邦信息安全管理法案》进一步将"信息安全"定义为"保护信息和计算机系统不被未经授权的获取、使用、披露、破坏、修改或者销毁",以确保信息的保密性、完整性和可用性⑥。自此,传统信息网络社会下数据安全的三要素被正式提出。根据当时我国相关国家标准,保密性是指信息数据不泄露给未授权的个人、实体、进程,或不被其利用的特性;可用性是指已授权实体一旦需要就可访问和使用的数据和资源的特性;完整性是指数据没有遭受以未授权方式所作的更改或破坏的特性⑦。因此,以传统三要素为背景的数据安全规范保护体系,主要着眼于数据自身的内容安全和数据所依托的载体、平台的安全,并禁止非法获取、删除、修改、增加等行为。

数字社会的到来,意味着"真实社会与虚拟社会相互交织、紧密互动,甚至互为因果"[26]。数字社会的网络化、数字化、智能化进程突破了物理的"时空体制",促进了世界"虚拟化",造成了时间和空间的"脱嵌"[27],这使得数据摆脱了以往信息载体的地位,成为一种流动的、拥有巨大价值的生产要素,成

⑤The Clinton Administration's Policy on Critical Infrastructure Protection:Presidential Decision Directive 63,May 22,1998.

⑥Federal Information Security Management Act of 2002,44 U.S.C. §3542(b)(1).

⑦参见:中华人民共和国国家质量监督检验检疫总局、中国国家标准化管理委员会:《GB/T 17532—2005 术语工作 计算机应用 词汇》2.1.1保密性、2.1.42完整性、2.1.20可用性。

就了数据资源到数据资本的转变。一方面,人们可以运用现代技术手段对收集、聚合而来的数据进行大数据分析,为反映现实、优化管理、科学决策提供主要依据;另一方面,一些制造商和平台可以通过数据的计算挖掘,形成数据用户画像,通过"精准投放"和"个性化定制"来影响用户的价值和偏好,从而创造更大的商业价值,实现数据增值。但是,数据在不断凸显价值的同时,其招致的风险也在不断增加。与传统的利用数据环境漏洞来侵害数据保密性、完整性、可用性的风险不同,数字社会背景下的数据安全风险是动态的、贯穿数据周期始终的、危害更为巨大的风险。其典型类型有:(1)分析数据所产生的风险。即采用因子分析、回归分析、相关分析、聚类分析等方法对掌握的数据进行分析,可挖掘出数据背后所隐藏的安全情报和涉密信息。即使这些数据在被分析之前无关紧要、平平无奇,但在被分析之后却能得出危害个人隐私、商业利益、社会发展甚至是国家安全的信息内容。例如,2017 年,美国一科技公司研发了一款可以记录运动路线的"斯特拉瓦"健身软件,由于其用户中有大量美军士兵,因此,无意中暴露了美国海外的军事基地位置,而这些信息内容可能被恐怖分子用来制造袭击⑧。(2)利用分析数据产生的知识和信息,作出决策而引发的风险。其不但表现为竞价排名、大数据杀熟、算法共谋、算法歧视等行为,还表现为一些严重危害公共安全和国家安全的行为。例如,2018 年发生的"剑桥分析公司事件"中,约 8 700 万名 Facebook 用户的数据被不当泄露给政治咨询公司剑桥,以此分析用户偏好,用以准确投放政治广告,从而影响了美国的政治安全⑨。该事件说明,即使数据分析结果本身不具有危害性,但滥用分析结果完全可能带来危害。显然,前述的数据分析风险和数据利用风险既不针对保密性,也不针对完整性,更不针对可用性。总之,虽然传统的数据安全三要素对于某一节点的数据管理安全依然适用,但其却无法涵盖数据安全在数字社会中的价值意蕴,应该提炼出一种以动态数据为中心的新的数据安全核心要素。

前述新型风险所对应的数据安全要素可以用"可控性"(Controllability)和"正当性"(Legitimacy)来加以概括。其中,可控性是指"在数据大规模流动聚合、分析的过程中,将安全风险维持在一种可接受水平的能力"[28];正当性是指在利用和处理数据时,要保持目的的正当性,不得损害国家安全、公共利益或者公民、组织合法权益[29]。数据利用的可控性要求刑法规制促使风险、敏感数据的流动和聚合的行为,避免这些数据被不当披露和聚合分析;数据利用的正当性要求刑法规制不当利用数据分析及分析结果的行为,避免数据分析滥用带来的危害。事实上,这种以动态数据的利用安全为中心要素的概括在相关规定中已经有所体现。例如,2015 年 1 月,我国与俄罗斯等国向联合国提交的新版《信息安全国际行为准则》中就强调,不得利用信息通信技术和信息通信网络"实施有悖于维护国际和平与安全目标的活动","干涉他国内政,破坏他国政治、经济和社会稳定"⑩,这体现了数据利用的正当性;我国《数据安全法》第 3 条第 3 款也规定,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。总之,数据安全的核心要素应当实现从保密性、完整性、可用性的传统三要素,向保密性、完整性、可用性、可控性、正当性五要素转变。

---

⑧跑步 APP 泄露美军事基地位置?五角大楼着手调查[EB/OL].(2018-01-31)[2023-05-06].http://world.people.com.cn/n1/2018/0131/c1002-29797384.html.

⑨马克·扎克伯格因数据泄露事件被起诉[EB/OL].(2022-05-24)[2023-05-06].http://www.chinanews.com.cn/gj/2022/05-24/9762313.shtml.

⑩信息安全国际行为准则[EB/OL].(2011-09-12)[2023-05-06].https://www.fmprc.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/fywj_674643/201109/t20110913_7668314.shtml.

(二)“利用安全”保护模式的提出

数据安全核心要素的转变,必然要求数据安全保护模式发生转变。如前所述,建立在保密性、完整性、可用性三要素上的管理安全保护模式,难以满足数字社会的治理需求,不能实现刑法与《数据安全法》的有序衔接,易造成刑法中数据条款的模糊化,亟需转向一种包含可控性、正当性要素的新的数据安全保护模式。本文将涵盖了保密性、完整性、可用性、可控性、正当性五要素的数据安全保护模式称为“利用安全”保护模式。从二者关系看,利用安全模式和管理安全模式之间并不排斥,后者是前者的进化形态,前者是后者的前期基础。管理安全模式向利用安全模式的转变主要体现在三个方面:(1)在保护理念上,从依附保护向专门保护、系统保护转变。即在利用安全模式下,刑法中涉及数据安全保护条文规范应当是系统的、独立的。这主要取决于两方面的因素,一方面,在数据的利用价值不断凸显的同时,危害数据安全行为的复杂性也在不断增强,从系统论的角度看,这决定了刑法应对的系统性,否则,数据安全法益内涵无法在分则条文中进行集中的、类型化的规范表达,更无法得到周延的保护;另一方面,可控性和正当性要素的加入使得数据安全的独立特性被释放出来,数据的地位不再仅是计算机信息系统构成要素和电子信息的形成基础,而是数字社会的生产资料和生产资本,这就要求刑法规范摆脱以往的依附保护思维,对数据安全加以专门保护。(2)在规制重心上,从注重数据收集、储存节点向其他节点拓展。即在利用安全模式下,刑法中数据条款的规制重心应当从针对保密性、完整性、可用性的收集以及储存行为节点,向针对可控性、正当性的其他数据处理节点拓展。这不仅是回应数字时代数据犯罪治理需要的必要性调整,也是满足刑法规范与以《数据安全法》为代表的前置法有序衔接的要求。根据《数据安全法》第3条第2款规定,数据处理包括收集、存储、使用、加工、传输、提供、公开等环节。因此,在利用安全模式下,刑法的行为规制范围应在非法获取、删除、修改、增加等行为的基础上,增加规范规制非法分析、提供、公开、出售、出境等行为。(3)在保护策略上,从笼统保护到分类分级保护转变。即在利用安全模式下,刑法中的数据保护条款应当是相对精细的、具体的,并针对不同种类和不同重要程度的数据提供不同的保护方案。与处于相对封闭状态的数据不同,数字时代的数据处于不断流动和被分析处理中,其表现形态更加丰富、多元,刑法应当结合不同种类、不同等级数据的可控性、正当性保护需求,设置不同的规范,否则,数据安全的刑法保护仅是泛泛而谈。同时,从规范完善的角度看,分类分级还有助于发挥数据安全法益识别功能,为认定数据犯罪提供罪质和罪量依据,有助于实现规范的衔接协调,完善数据安全保护法律体系。

(三)“利用安全”保护模式的实现进路

1. 优化现有规范以实现专门保护和系统保护

从管理安全模式到利用安全模式的转变,是刑法规制危害数据安全犯罪基本逻辑的转变,首先涉及既有规范的调整问题。现行《刑法》第285条第2款非法获取计算机信息系统数据罪,第286条破坏计算机信息系统罪,以及《解释》的相关规定,是基于管理安全模式制定的,不能满足动态数据安全保护的需要,亟需根据动态数据安全系统保护和专门保护的需要作出优化。

一是在立法上明确数据与信息、计算机信息系统的关系,并剥离出独立的数据条款,实现数据安全的专门保护。在利用安全模式下,数据处于共享和流动的状态,只有明确了数据在刑法中的独立地位,才能有针对性地设计具体的刑法保护规范。然而,管理安全模式将数据定位为计算机信息系统的内容和信息的载体,模糊了数据自身的特征,导致刑法中的数据条款依附于其他罪刑规范,

无法实现数据安全的专门保护。因此,应当在界分数据与相关概念的基础上,从非法获取计算机信息系统数据罪、破坏计算机信息系统罪中剥离出破坏型数据犯罪的和获取型数据犯罪。

正如前文所述,在数字技术广泛运用的当下,计算机信息系统并非数据活动进行的唯一载体,数据可以借助云储存、云分享等形式存在于各式各样的载体之中,甚至实现物与物、物与人泛在连接的“物联网”世界。因此,数据与计算机信息系统之间并不存在必然的承载与被承载关系,刑法中的“数据”也不该被冠以“计算机信息系统”的前缀,而应在刑法中直接表述为“数据”,这样才能保证刑法数据条款的适用空间。同时,无论是在功能、作用上,还是在属性、状态上,数据和信息存在巨大差别,如果不加区分地表达在立法中会导致相关规范的适用混乱,这既不利于保护数据安全,也不利于保护信息安全。因此,《解释》对于非法获取计算机信息系统数据司法适用的规定也应相应地修改,删除第1条第1款第(一)项与第(二)项中与“身份认证信息”有关的表述,解决实践中数据与信息混淆认定的问题。

在明确数据与信息、计算机信息系统关系的基础上,刑法中的数据条款还应当实现“去杂糅化”,即将其从危害计算机信息系统犯罪中剥离出来,进行独立规定。数据犯罪的杂糅化体现为获取型的数据犯罪与非法控制计算机信息系统罪被规定在同一条文之中,破坏型数据犯罪被规定在破坏计算机信息系统罪当中。一方面,应当拆分《刑法》第285条第2款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,规定“非法获取数据罪”。正是由于数据和计算机信息系统之间并不存在必然的承载与被承载关系,非法侵入计算机信息系统也不再是获取数据的必然手段。因此,数据的保密性并不依赖于计算机系统环境的封闭性,获取型数据犯罪从现行《刑法》第285条第2款中剥离出非法获取数据罪十分必要。另一方面,应当从《刑法》第286条破坏计算机信息系统罪中剥离出“非法破坏数据罪”(对委托管理的数据进行破坏的也可以成立该罪)。从立法本意上看,《刑法》第286条禁止删除、修改、增加数据行为的目的在于保证计算机信息系统的有效运行[30]。但这既不契合当前数据与计算机信息系统的相互关系,也可能导致数据完整性、有效性、可用性沦为计算机信息系统安全的附带性内容之一,无法凸显数据安全的独有价值。事实上,即使是行为人非法侵入计算机系统之后删除其中存储、处理或者传输的数据,也不必然会造成“计算机信息系统不能正常运行”或“影响计算机系统正常运行”的结果,只是对数据的完整性和可用性造成了侵害。因此,破坏型的数据犯罪也没有必要规定在破坏计算机信息系统罪之中。

二是在《刑法》分则中集中规定危害数据安全犯罪,实现系统化保护。数据安全核心要素的扩充即可控性和正当性要素的加入,意味着刑法会通过增设新罪的方式来规制新的危害数据安全的行为类型,而如何明确新增犯罪的体系定位,则成为利用安全模式需要面对的问题。同时,实现利用安全模式要求从计算机信息系统犯罪中独立“非法获取数据罪”“非法破坏数据罪”,而剥离出的新罪也将面临在刑法分则中重新定位的问题。因此,从系统性和类型性的角度看,在《刑法》分则中集中规定危害数据安全犯罪是实现利用安全模式的必然延伸问题。刑法分则对某类犯罪进行集中规定有设置专章、设置专节、设置集中条款三种形式。就设置专章而言,虽然其是实现规范体系性、独立性的最有效途径,但当前危害数据安全犯罪无论在行为类型的丰富程度上还是在侵害法益的层次结构上,都未达到增设专章规制的程度;就设置集中条款而言,通过重新组合的方式将《刑法》分则中的数据条款调整为前后连续的罪刑规范集合体,并形成系列罪名,其最终效果则与现有的第285条第2款、第286条并列的格局无异,很难达到系统保护和专门保护的需求。因此,在《刑法》分

则中设置危害数据安全犯罪专章和集中条款,都不是实现利用安全模式专门、系统保护的最佳路径。笔者认为,当前可以考虑在妨害社会管理秩序罪的第一节扰乱公共秩序罪后增设“危害网络和数据安全犯罪”专节,集中规定危害数据安全犯罪和危害信息安全、计算机信息系统安全的犯罪。这样既能体现危害数据安全犯罪的系统性,又能兼顾危害数据安全犯罪与其他信息网络犯罪的共同性,进一步贯彻类型化原则。同时,在该节设专条,明确规定“通过危害信息网络和数据安全的手段实施其他犯罪的,依照处罚较重的规定定罪处罚”,从而理顺危害网络和数据安全犯罪与其他犯罪的关系,并在其他犯罪认定存在疑问时提供合适的兜底方案。

2. 新增覆盖数据生存周期的罪名以实现全链条保护

数据安全核心要素的拓展必然要求刑法规制行为类型的增加。管理安全模式下的数据条款只能涵盖数据收集、储存节点的非法获取、删除、修改、增加等行为,这既不符合数字时代数据犯罪治理需求,也无法满足法律衔接的需要,刑法亟需结合动态数据的可控性、正当性需求新增罪名以满足规范供给。根据2020年3月1日实施的国家标准《信息安全技术数据安全能力成熟度模型》规定,完整的数据周期包括数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁6个节点,每个节点都对应了不同的数据安全要求[31]。有必要参考相关标准和规范,在立法上补充后续节点的数据犯罪立法,覆盖数据的生存周期,形成数据安全刑法全链条保护格局。

(1)增设非法公开、提供、出售、出境数据罪。数据交换阶段利用的可控性和正当性极易受到非法提供、非法出售、非法出境等行为的威胁,对此,可以考虑在刑法中增设新罪以实现数据安全的全链条保护。从必要性上讲,一方面,数据的公开、提供、出售、出境意味着数据的流动和聚合过程,这本身就蕴含着数据利用活动脱离人的既有规则设计和发展预期,超出了数据利用的可控性。同时,公开数据,向他人提供、出售数据,以及将数据传输出境的行为,是对数据利用正当性的巨大威胁,极易导致危害公民权利,危害组织合法权益及公共利益,甚至是国家安全的严重结果,具有极强的法益危害性。另一方面,从我国现有立法看,《数据安全法》和《网络安全法》规定了非法提供、出境等违法行为类型及对应的处罚,而刑法却没有直接涉及这些行为。虽然基于谦抑性理念和规范性质的差异,刑法的行为规制范围不应与行政法保持一致,但就数据安全这一特殊领域而言,数据安全立法的发展变化影响着刑事立法,前置法规范具有刑事立法的参照系功能[32]。所以从法律衔接层面上讲,刑法积极回应前置法的立法动向并不完全是恣意性的体现,反而可能是保持立法前瞻性的手段[33]。只有刑法与前置法的有效配合,才能保证数据安全得到系统和周延的保护。

因此,基于数据安全保护现实需求和罪刑规范供给不足的现状,可以考虑适时在《刑法》增设非法公开、提供、出售、出境数据罪。在行为要件设置上,该罪有公开、提供、出售、出境四种行为类型:其中,“公开”是指将数据向多数或者不特定主体传播的行为;“提供”是指以复制、共享等方式向他人无偿传输数据的行为;“出售”是指以复制、共享等方式向他人有偿传输数据的行为;“出境”是指通过网络传输、存储介质、开展业务、提供服务与产品销售等方式实现数据跨境流动的行为。在犯罪性质上,该罪应当被定位为法定犯,即公开、提供、出售、出境构成犯罪要以“违反国家规定”为前提,具体应当根据《数据安全法》《网络安全法》等前置法来判断。例如,未经数据权利人(数据委托处理者、互联网平台用户、政府主管单位)同意或超出同意范围,将数据提供、出售给他人的,或向不特定多数人公开的;将履行职责中获取的数据泄露或者非法提供给他人的;未经国家主管部门批准,向他人提供、出售重要数据的;或者未经主管机关批准,向境外提供重要数据或者向外国司法或

者执法机构提供数据的;等等。在入罪条件上,该罪可将是否“情节严重”作为衡量标准,具体可以结合非法公开、提供、出售、出境数据的体量、类别、范围以及行为的次数等因素综合判断。

(2)增设非法分析数据罪、非法运用数据分析结果罪。所谓非法分析数据行为,是指以违法犯罪为目的,利用歧视性算法或其他非正当方式,对数据进行非法分析、处理的行为[34];非法运用数据分析结果行为,是指将非法分析的数据结果及合法分析数据的结果运用于违法犯罪领域的行为。在实践中,行为人实施数据犯罪往往是为后续的窃取国家机密、恐怖主义活动、电信网络诈骗、窃取商业机密等违法犯罪行为做准备。例如,在电信网络诈骗犯罪案件中,犯罪分子往往先是利用互联网的数据爬虫技术获取数据,分析出诈骗对象的详细身份信息和特征,并据此针对诈骗对象设计特定骗局,实施“精准诈骗”,提高诈骗犯罪的成功率[35]。倘若将后续犯罪的实施视为一个连贯的过程,那么非法获取、出售、提供、出境数据等行为只能是条件准备阶段,只有非法分析数据、非法运用数据分析结果才真正地打开了数据利用的“潘多拉魔盒”,对后续的国家安全、公共安全、公民财产安全等重要法益造成巨大的威胁。因此,有必要设立新的犯罪规制非法分析数据、非法运用数据分析结果的行为,以实现对数据利用安全正当性的周延保护,以及对国家安全、公共安全、经济安全等重要法益的前置保护。

在具体的构成要件设计上,首先,成立非法分析数据罪、非法运用数据分析结果罪仍应以“违反国家规定”为前提,即分析数据行为和运用数据分析结果的行为应当违反《数据安全法》等前置性法律。其次,在数据类型上,非法分析的数据应限于重要数据和核心数据,而非法运用的数据分析结果应限于对重要数据和核心数据分析的结果,因为数据分析是大数据价值链中的关键环节,正是它的存在才使得数据成为反映现实、优化管理、科学决策的主要依据[36]。刑法应当合理把握分析数据、运用数据分析结果行为的“双刃剑”特性,严格限制“非法”成立的范围和行为对象范围,在充分保障数据利用安全的同时,为数据行业和数字经济的健康发展留下充足的空间。再次,非法分析数据的行为和非法运用数据分析结果的行为应具有以违法犯罪活动为目的的主观心态,如果行为人以科学研究等正当使用用途为目的分析数据、运用数据分析结果的,即使其手段“违反国家规定”也不宜认定为犯罪,以免刑法过度介入社会生活,突破刑法的“最后手段性”界限。最后,在入罪条件上,仍应当以是否“情节严重”作为衡量标准,具体可以从行为涉及的数据体量、类别、造成的后果等因素等方面进行综合判断。

3. 建立数据安全刑法分级分类保护机制

类型化是人类认识和处理复杂事物的一种便捷、直观、有效的方法。在数据安全立法领域,数据利用具有广泛性和多样性,并非所有数据的安全状态都值同等保护,只有根据数据的属性进行区分和归类才能准确识别数据安全法益、合理配置立法司法资源。同时,与多样化的数据种类不同,刑罚作为一种严厉的法律后果,具有单一化和阶梯化的特征,这决定了数据安全既要保护分类,也要根据重要性程度的不同进行分级保护。在二者关系上,数据分类是数据分级的逻辑前提,只有在准确定位数据性质的前提下,才能对数据重要性程度进行判断[37],考虑到当前我国数据安全立法模式,刑法中的数据分级分类可以参考前置法和相关指南中的规定。根据全国信息安全标准化技术委员会 2021 年发布的《网络安全标准实践指南——网络数据分类分级指引》第 4. 1d) 条的内容,网络数据可以根据行业领域维度标准,分为工业数据、电信数据、金融数据、交通数据、自然资源数据、卫生健康数据、教育数据、科技数据等。根据《数据安全法》第 21 条规定,我国根据数据的重要程度

和滥用后的危害程度将数据分为一般数据、重要数据、核心数据,并在此基础上实行数据分类分级保护制度。在后续的规范完善中,刑法应当以此为基础,建立数据安全刑法分级分类保护机制。

(1)在定罪层面,数据分级分类与数据犯罪的认定相结合。即数据的分级分类的结果应当充分发挥罪质评价功能,与是否适用数据犯罪以及如何适用数据犯罪相关联。具体而言:一方面,将数据的类别和等级嵌入数据犯罪的入罪评价标准中。数据犯罪是严重侵害数据安全法益的行为,这种严重程度在不同类型和不同重要程度数据上应该有不同的征表。例如,同样的非法获取行为,在针对重要性程度不同的一般工业数据和核心公共卫生健康数据时,所造成的危害性大小不同。因此,为保证罪刑相适应原则在定罪阶段的贯彻,刑法应当借鉴《数据安全法》的分级分类保护制度,在同一个犯罪行为之下,为涉及一般数据、重要数据、核心数据的不同情形设置高低不同的入罪门槛。对此,需要立法和司法机关后续出台司法解释对相关的追诉标准进行细化。另一方面,将数据的类别和等级与数据犯罪成立范围大小相关联。刑罚的有限性决定了其运用应当有所侧重,这种侧重不但可以通过调整入罪标准来实现,也可以借助调整入罪对象范围来达成。具体到数据安全领域,刑法可以根据数据分级分类制度,区分一般数据、重要数据、核心数据三种行为对象,并通过保护对象的选择来合理划定数据犯罪的打击范围。以拒不履行数据安全义务罪为例,虽然保护数据安全是《数据安全法》明文规定的法定义务,但刑法不能不加甄别地将其吸纳进刑法义务的来源中,否则会对数据处理者苛加过重的义务,反而不利于数字经济和数据行业的发展。因此,建议后续的立法中,拒不履行数据安全罪的行为对象应当限制为“重要数据”“核心数据”。

(2)在量刑层面,数据分级分类与数据犯罪的刑罚裁量相对接。即数据分级分类的结果应当充分发挥罪量评价功能,在分级分类的基础上,根据数据安全法益的重要性程度,明确数据犯罪量刑的数额、数量标准和综合性情节等要素。应当注意的是,随着数字技术的广泛运用,数据犯罪的行为类型也会日趋复杂,《解释》中以数据数量(组)、数据违法所得数额、造成损失数额等要素衡量数据犯罪行为“情节严重”“情节特别严重”的思路已经滞后,难以满足数据犯罪行为法益侵害量化标准多元化的需求。本文建议,立法和司法机关在后续出台相关司法解释时,将更多能够反映数据安全法益侵害的因素,例如,数据流量、安全漏洞数,注册会员数、点击浏览或下载数量、系统正常运行时长、网络中断时长及影响用户数、网络故障导致的事故损害后果等因素,纳入数据犯罪“情节严重”“情节特别严重”的量化因素之中[38]。在确定量化因素的前提下,再根据一般数据、重要数据、核心数据安全的保护需要,为相应的数据犯罪行为设置“情节严重”“情节特别严重”的具体标准,以达到罪刑相适应原则的要求。

结语

刑法作为数据安全保护的重要手段,面对数字社会所蕴含的多元的、动态的数据安全威胁,应当及时完善规范,回应数据安全保护的最新诉求。由我国现行《刑法》中第285条第2款“非法获取计算机信息系统数据罪”、第286条“破坏计算机信息系统罪”及相关司法解释组成的规范体系是打击数据犯罪的直接依据,但其面对数字社会蕴含的新型数据风险,仍存在思维滞后、模式陈旧、规范供给不足等问题。究其原因,在于刑法未能准确把握数据安全核心要素的转变,相应地调整既有的规范保护模式。本文在分析管理安全模式缺陷的基础上,提出应当根据数据可控性、正当性保障的需要,构建数据安全刑法保护的利用安全模式,并设想了实现该模式的具体措施。当然,数据安全

保护是一个系统性工程,其不但需要在规范及制度完善的层面作出努力,还需要在具体落实的层面继续探索,对于这些问题,笔者将进一步研究和思考。

参考文献:

[1] 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):64-76,63.
[2] 马长山.智能互联网时代的法律变革[J].法学研究,2018(4):20-38.
[3] 罗纳德·巴赫曼,吉多·肯珀,托马斯·格尔策.大数据时代下半场:数据治理、驱动与变现[M].刘志则,译.北京:北京联合出版公司,2017:20.
[4] 赵秉志.新刑法教程[M].北京:中国人民大学出版社,1997:672.
[5] 刘家琛.新刑法新问题新罪名通释:根据最高人民法院最新司法解释修订[M].北京:人民法院出版社,1998:827.
[6] 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(1):58-64.
[7] 黄太云.《刑法修正案(七)》解读[J].人民检察,2009(6):5-21.
[8] 皮勇.论我国刑法修正案(七)中的网络犯罪立法[J].山东警察学院学报,2009(2):15-20.
[9] 杨志琼.非法获取计算机信息系统数据罪"口袋化"的实证分析及其处理路径[J].法学评论,2018(6):163-174.
[10] 喻海松.最高人民法院研究室关于利用计算机窃取他人游戏币非法销售获利如何定性问题的研究意见[M]//张军.司法研究与指导.北京:最高人民法院出版社,2012:135.
[11] 刘宪权,石雄.网络数据犯罪刑法规制体系的构建[J].法治研究,2021(6):44-55.
[12] BEATRICE BRUNHÖBER,冀洋.安全社会中刑法的功能变迁[J].刑法论丛,2020(1):80-103.
[13] 于施洋,王建冬,郭鑫.数字中国:重塑新时代全球竞争力[M].北京:社会科学文献出版社,2019:1-2.
[14] 王文,刘玉书.论数字中国社会:发展演进、现状评价与未来治理[J].学术探索,2020(7):48-61.
[15] 丁晓东.论算法的法律规制[J].中国社会科学,2020(12):138-159,203.
[16] 邱幼云,陶俊.建设数字社会亟须加强数据治理[N].中国社会科学报,2021-09-07(08).
[17] 纪海龙.数据的私法定位与保护[J].法学研究,2018(6):72-91.
[18] 马长山.数字时代的法律变革[J].浙江社会科学,2019(12):4.
[19] 连玉明.数权法2.0:数权的制度建构[M].北京:社会科学文献出版社,2020:149-153.
[20] 龙荣远,杨官华.数权、数权制度与数权法研究[J].科技与法律,2018(5):19-30,81.
[21] 姜涛.构建数字经济安全刑事规范新形态[N].检察日报,2021-08-23(003).
[22] 凯尔森.法与国家的一般理论[M].沈宗灵,译,北京:中国大百科全书出版社,1996:203.
[23] 王勇.法秩序统一视野下行政法对刑法适用的制约[J].中国刑事法杂志,2022(1):124-138.
[24] 劳东燕.个人数据的刑法保护模式[J].比较法研究,2020(5):35-50.
[25] 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):164-183,209.
[26] 王天夫.数字时代的社会变迁与社会研究[J].中国社会科学,2021(12):73-88,200-201.
[27] 马长山.数字社会的治理逻辑及其法治化展开[J].法律科学(西北政法大学学报),2020(5):3-16.
[28] 何波.中国参与数据跨境流动国际规则的挑战与因应[J].行政法学研究,2022(4):89-103.
[29] 刘金瑞.数据安全范式革新及其立法展开[J].环球法律评论,2021(1):5-21.
[30] 全国人大常委会法制工作委员会刑法室.中华人民共和国刑法条文说明、立法理由及相关规定[M].北京:北京大学出版社,2009:287.
[31] 国家市场监督管理总局,中国国家标准化管理委员会.信息安全技术 数据安全能力成熟度模:GB/T 37988—2019[S].北京:中国标准出版社,2019:6-7.
[32] 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.
[33] 梅传强,盛浩.新时代我国刑法典全面纂修的基本理念与建构路径[J].南京社会科学,2023(3):52-63.
[34] 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.
[35] 吕中伟.怎样治理大数据时代的精准诈骗[J].人民论坛,2018(11):68-69.
[36] 梅宏.数据治理之论[M].北京:中国人民大学出版社,2020:11.
[37] 熊波.数据分类分级的刑法保护[J].政法论坛,2023(3):155-167.
[38] 张勇.数据安全分类分级的刑法保护[J].法治研究,2021(3):17-27.

Mode transformation of criminal law protection of data security: From management security to utilization security

MEI Chuanqiang[1], SHENG Hao[2]

(*1. School of Law, Southwest University of Political Science and Law, Chongqing 401120, P. R. China*;
2. Department of Investigation, Sichuan Police College, Luzhou 646099, P. R. China)

Abstract: Data security is related to national security and social stability, and it is both necessary and urgent to protect data security through criminal law. After the improvement of the amendments and the supplementation of judicial interpretations, China's criminal law has formed a management security model to protect data security, which aims to regulate the confidentiality, integrity, and availability of static data, and relies on the crime of illegally obtaining computer information system data and the crime of damaging computer information systems as normative standards for data security protection. The establishment of the management security protection model has gone through three stages of development: data as an incidental part of computer information system protection, data becoming a relatively independent object of criminal law protection, and expanding the scope of data security coverage through judicial interpretation. The management security protection model has closed and static characteristics, which is difficult to adapt to the trend of dynamic and shared development of data in the digital society. It has failed to achieve orderly connection with pre-existing laws such as the Data Security Law, and has led to the problem of ambiguity in the judicial application of data crime clauses in the criminal law. The arrival of the digital society has created new types of data security risks, namely the risks generated by analyzing data, as well as the risks caused by using the knowledge and information generated by analyzing data to make decisions. Faced with new types of risks, data security protection urgently needs to shift towards a utilization security model centered on the confidentiality, integrity, availability, controllability, and legitimacy of dynamic data. In terms of protection philosophy, data should be treated as an independent object, shifting from dependent protection to specialized and systematic protection; In terms of regulatory focus, expand from focusing on data collection and storage nodes to other nodes, and shift from one-sided protection to full chain protection; In terms of protection strategy, there is a shift from general protection to classification and protection. Therefore, on the basis of optimizing existing data crime clauses, new data crimes should be added and a data classification and protection system should be introduced. Specifically, firstly, the relationship between data, information, and computer information systems should be clearly defined in legislation, and independent data clauses should be separated to achieve specialized protection of data security. At the same time, criminal offenses that endanger data security should be stipulated in the specific provisions of the Criminal Law for systematic protection. Secondly, crimes such as illegal disclosure, provision, sale, and export of data, illegal analysis of data, and illegal use of data analysis results should be added for comprehensive protection. Thirdly, a data security classification and protection system should be established, which combines data classification with the identification of data crimes at the conviction level, and connects data classification with the punishment discretion of data crimes at the sentencing level.

Key words: data security; digital society; criminal law protection mode; data classification; data compliance

(责任编辑 刘 琦)