法商研究 Studies in Law and Business
Vol. 42 No. 2(2025)

网络与信息法

数字化背景下公共数据的刑法保护

苏 永 生*

摘 要:数字化从广度和深度上大幅提升了公共数据的价值,形成了值得刑法保护的公共数据法益。我国现行刑法虽然为公共数据提供了一定程度的保护,但是保护的专门性、完整性和体系性明显不足。应对关涉国家安全的数据予以绝对保护,对关涉其他国家利益和社会公共利益的数据予以相对保护,并采用多元保护、专门保护、附带性保护相结合的保护模式,在危害国家利益和社会公共利益的犯罪中增设危害公共数据犯罪。应将危害公共数据犯罪的行为类型构造为毁坏公共数据、非法利用公共数据和不形成公共数据3类;将基本犯构造为对公共数据的实害犯,只能由故意构成,且属于微罪,配置1年有期徒刑以下刑罚,同时配置选处罚金;将加重犯构造为对国家利益或者社会公共利益的实害犯,罪过形式包括过失,根据不同的情况配置1年以上3年以下有期徒刑和3年以上7年以下有期徒刑两个刑罚幅度,同时配置并处罚金。

关键词:公共数据法益 数字化 刑法保护 危害公共数据犯罪

一、问题的提出及研究思路

数据是数字化的基石,一切数字技术都建立在对数据的利用之上。离开数据,数字化则无从谈起。因此,在数字化时代,数据是最基本的生产要素,保护数据是数字化时代最基本的要求。为此,2020年3月30日《中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见》明确提出,要加快培育数据要素市场,并将数据与土地、劳动力、资本、技术并列为生产要素。2021年《中华人民共和国数据安全法》(以下简称《数据安全法》)将数据安全提升到运用法律予以保护的层面。2022年12月2日《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》对数据基础制度的建构作出总体部署,其目的就是要通过制度化、法治化的方式来

* 河北大学法学院教授
基金项目:国家社会科学基金资助项目(23BFX118)

保护数据，并为整个数据制度的建立指明方向。[①]《意见》明确指出："数据作为新型生产要素，是数字化、网络化、智能化的基础，已快速融入生产、分配、流通、消费和社会服务管理等各环节，深刻改变着生产方式、生活方式和社会治理方式"，提出要"构建适应数据特征、符合数字经济发展规律、保障国家数据安全、彰显创新引领的数据基础制度"。显然，在数字化时代，数据在整个国家和社会治理中居于极其重要的地位，数据法律制度的建构必须遵循数据以及数字化运行的基本规律。

虽然根据数据的形成主体和控制主体的不同可将数据分为个人数据与公共数据，但是在数据法学中，个人信息通常被视为数据法的基本范畴。[②] 在此种背景下，个人数据成为当前数据法学讨论的重点问题。相比之下，对公共数据的讨论则明显不足。《数据安全法》第 1 条将立法目的明确规定为"规范数据处理活动，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，维护国家主权、安全和发展利益"。[③] 由此不难看出，公共数据与个人数据应当受到同等保护，甚至可以说，如果没有公共数据的安全，就没有个人数据的安全。"数字科技是一把'双刃剑'，数字化带来的不仅是权利的福音，还伴随着权利的危机。"[④]数字化在提升公共数据利用价值的同时，也增加了公共数据利用所带来的风险。那么，数字化从哪些方面提升了公共数据的价值？是怎样提升的？公共数据作为数字化背景下的新型法益，包括哪些内容？这是分析公共数据刑法保护的逻辑前提和基础，也是公共数据刑法保护的基本动因。

在一国法律体系中，刑法一般属于保障其他法律得以实施的法律。因此，刑法具有法益保护范围的广泛性和制裁手段的严厉性的特点，这些特点构成了刑法区别于其他法律的重要属性。这就意味着刑法必须是其他法律的后盾，在刑法中应当有与其他法律规定的违法行为相对应的犯罪；否则，因一般违法行为的程度增加而导致其他法律不足以制裁该行为时，法律体系和法律制裁就会出现断裂。因此，与数据法相适应，应当有数据刑法，即刑法中以保护数据为目的的罪刑规范。那么，我国当前的数据刑法对公共数据提供了怎样的保护？能否满足数字化背景下保护公共数据的基本要求？还存在哪些不足？如何予以改进？这是数字化背景下数据制度建设亟须解决的问题。对此问题，我国刑法学界却很少予以分析和讨论。

在本文中，笔者首先对数字化提升公共数据之价值和公共数据法益的内容予以分析和讨论，廓清公共数据刑法保护的基本动因；其次，通过研究我国数据刑事立法，分析我国刑法对公共数据的保护现状，指出其不足之处；最后，提出公共数据刑法保护的改进对策。

---

① 参见时建中：《数据概念的解构与数据法律制度的构建——兼论数据法学的学科内涵与体系》，《中外法学》2023 年第 1 期。

② 例如，有学者在"数据法的基本范畴"的章标题下仅讨论个人信息的概念和法律属性，个人信息与隐私、数据的关系，以及个人信息的类型化等问题。参见何渊主编：《数据法学》，北京大学出版社 2020 年版，第 41～55 页。也有学者指出，数据法体系包括数据安全、数据跨境流动、重要数据保护、个人信息保护等许多内容，重中之重是个人信息保护。参见马长山主编：《数字法治概论》，法律出版社 2022 年版，第 59 页。

③ 由此规定可将我国数据安全法的立法目的解读为以下 5 个：(1)规范数据处理活动；(2)保障数据安全；(3)促进数据开发利用；(4)保护个人、组织的合法权益；(5)维护国家主权、安全和发展利益。第一个立法目的可谓直接目的，其他 4 个立法目的均属于最终目的。

④ 张文显：《"无数字 不人权"》，《北京日报》2019 年 9 月 2 日。

二、公共数据刑法保护的基本动因

刑法是法益保护法。法益既是实定法上的概念,也是前实定法上的概念。因为在立法承认某种法益之前,法益本身是存在的,[①]所以法益具有指导刑事立法的基本功能,保护法益就成为刑法的基本动因。在数字化时代,数字技术提升了公共数据的价值,更新了公共数据法益的内容,强化了公共数据刑法保护的现实需要。

(一)数字化对公共数据价值的提升

公共数据是人类社会生活不可或缺的资源,因而其本身就是一种法益。在数字化时代,数字技术的迅猛发展不但拓宽了公共数据的范围,而且强化了对公共数据的利用,大大提升了公共数据的价值。

1.数字化拓宽了公共数据的范围

在数字化时代,数据和算法是最基本的生产要素。数据是算法交易的一种最基础的现代商品。[②] 各种数字技术依赖算法得以施展,大大拓宽了公共数据的范围,集中体现为公共数据从之前的局部数据、抽样数据和非系统数据转变为完整数据、全面数据和系统数据。从公共数据的形成或获取看,在传统信息社会,人们所能获取的只是局部数据,通常难以获取关于某一事项的全部数据。数字技术的迅猛发展和广泛运用大大提升了各项公共数据的形成和获取能力,使得公共数据能够更全面地反映某一事项而非局部信息。从公共数据分析看,在传统信息社会,人们所分析的公共数据通常是通过抽样而获得的数据,即抽样数据。“在信息处理能力受限的时代,世界需要数据分析,却缺少用来分析所收集数据的工具,因此随机采样应运而生,它也可以被视为那个时代的产物。”[③]随着数字技术(特别是大数据技术)的迅猛发展,人们具备了对全部数据的分析能力,使得其分析和利用的数据不再是抽样数据而是全面数据。从公共数据的利用向度看,在传统信息社会,人们利用的公共数据通常是结构性数据,对非结构性数据和半结构性数据的利用非常有限。在数字化时代,数字技术的发展使公共数据的利用不再囿于因果性而是转向相关性,为非结构性数据和半结构性数据的利用创造了条件。同时,通过对公共数据进行分级分类管理,进一步增强了其系统性。

2.数字化加大了对公共数据的利用

数字化不但拓宽了公共数据的范围,而且强化了对公共数据的利用。

其一,数字化使得对公共数据的利用从局部性、片面性和非系统性利用转向完整性、全面性和系统性利用。在传统信息社会,受技术的限制,被利用的公共数据通常不是关于某一事项的完整数据、全面数据和系统数据,而是局部数据、抽样数据和非系统性数据,在公共数据的利用上通常呈现出局部性、片面性和非系统性。进入数字社会后,数字化的深入推进,特别是大数据技术的广泛运用,使得公共数据通常以整体数据、全面数据和系统数据的形态呈现在利用者面前。对

① 参见[德]弗兰茨·冯·李斯特:《李斯特德国刑法教科书》,徐久生译,北京大学出版社 2021 年版,第 6 页。

② 参见 [英]汉娜·弗莱:《算法统治世界》,李英松译,贵州人民出版社 2021 年版,第 27 页。

③ [英]维克托·迈尔-舍恩伯格、[英]肯尼思·库克耶:《大数据时代:生活、工作与思维的大变革》,盛杨燕、周涛译,浙江人民出版社 2013 年版,第 37 页。

公共数据的利用突破了因果性限制进而以相关性为指导，除结构性数据之外，半结构性数据和非结构性数据也成为被利用的重要对象。显然，正是在数字化的推动下，出现了对公共数据的完整性、全面性和系统性利用。

其二，数字化使得对公共数据的利用从幕后利用转向从幕后到前台的全过程利用。在传统信息社会中，公共数据的开放程度有限且未能实现生产要素化转型。因此，对公共数据的利用通常具有幕后性，其仅是人们从中分析和总结公共信息的资料。甚至在有些情况下，社会管理者为了制造出某种具有“政治正确性”的公共信息而将公共数据掩盖起来。在数字化时代，公共数据既是公共信息的载体，又使公共信息数据化；与此同时，在各种数字技术的加持下，公共数据被生产要素化，强化了公共数据的公开性。在此背景下，公共数据不但在幕后而且在前台发挥着重要作用，随着公共数据平台的广泛建立，对公共数据的全过程利用得以实现。

其三，数字化使得对公共数据的利用从传统的附带性利用转向专门性利用。在传统信息社会，人们看重的是对公共数据经过分析后所形成的公共信息而不是公共数据本身，故对公共数据的利用是一种附带性利用。换言之，公共数据是在保护公共信息的过程中附带受到了保护。在数字社会，不但公共数据被数字技术大量催生，而且公共数据的信息载体功能被其生产要素功能超越，出现了公共信息的数据化。“ICT 技术的革命性成果就是创造、开发和利用电子数据这一新兴信息载体，并使之成为人类社会前所未有且取之不尽、用之不竭的新兴生产要素。”[①]显然，在数字社会，谁掌握了数据，谁就掌握了生产的主动权。为此，应通过构建数据基础制度，“激活数据要素潜能，做强做优做大数字经济，增强经济发展新动能，构筑国家竞争新优势”。[②] 在此种背景下，对公共数据的利用必然从附带性利用转向专门性利用。

其四，数字化使得对公共数据的利用获得了主体性。在传统信息社会中，受技术条件的限制，公共数据的巨大价值难以得到充分发掘，公共数据资源在经济发展和社会管理中的作用远不如其他资源重要，通常处于边缘性地位。因此，传统信息社会对公共数据的利用具有非主体性。在数字社会，“随着数字技术的蓬勃发展和广泛运用，数据呈几何级数增长，数据存储和计算的技术和能力突飞猛进”。[③] “在大数据时代，数据就像一个神奇的钻石矿，在其首要价值被发现之后仍不断产生价值。数据的潜在价值有三种最为常见的释放方式：基本再利用、数据集整合和寻找‘一份钱两份货’。”[④]可见，数字技术不但提升了公共数据的采集和挖掘能力，而且揭示了公共数据的巨大潜在价值，并将其广泛运用于经济发展和社会管理中，在数字经济、数字政府和数字社会的基础上形成了数字文化。在公共领域，一切事务均以公共数据为中心而展开，公共数据获得了主体性地位。

（二）公共数据法益内容的型构

---

① 时建中：《数据概念的解构与数据法律制度的构建——兼论数据法学的学科内涵与体系》，《中外法学》2023年第1期。

② 《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》，https://www.gov.cn/gong bao/content/2023/content_5736707.htm，2024－08－26。

③ 时建中：《数据概念的解构与数据法律制度的构建——兼论数据法学的学科内涵与体系》，《中外法学》2023年第1期。

④ ［英］维克托·迈尔－舍恩伯格、［英］肯尼思·库克耶：《大数据时代：生活、工作与思维的大变革》，盛杨燕、周涛译，浙江人民出版社2013年版，第135～136页。

数字化大幅提升了公共数据的价值,这不仅增强了将公共数据作为实定法上法益的必要性,也型构了公共数据法益的内容。公共数据既承载着经济利益,又是一种新秩序,更为重要的是,它还关乎安全。

1.公共数据利益

对作为公共数据法益之内容的数据利益,可以从以下两个方面来理解。

其一,公共数据属于信息载体。国际标准化组织将数据定义为“信息的形式化表现,可展现其背后的意义,用于沟通、含义展示或处理”。① 我国有学者指出,在信息链中,数据无疑是最为基础的要素,只有通过数据处理,数据才能具有明确的意义,方可成为更具价值的信息。② “无论是《网络安全法》《数据安全法》抑或《个人信息保护法》以及《民法典》,均坚守了数据是信息载体这一科学认识,并将其内涵与外延法定化。”③显然,数据是信息的载体或形式,信息是数据所展现的内容。没有公共数据就不可能有公共信息。这是公共数据利益的重要表现。

其二,公共数据属于生产要素。在数字化时代,数字技术的广泛运用有力地促进了公共数据的资源化或生产要素化,公共数据被界定为数字经济的基础性生产资料。为此,我国提出通过推进实施公共数据确权授权机制,鼓励在保护个人隐私和确保公共安全的前提下,按照“原始数据不出域、数据可用不可见”的要求,以模型、核验等产品和服务形式向社会供给公共数据,对不承载个人信息和不影响公共安全的公共数据,推动按用途加大供给范围,推动用于公共治理、公益事业的公共数据有条件无偿使用,探索用于产业发展、行业发展的公共数据有条件有偿使用。④

2.公共数据秩序

秩序是法律所追求的重要价值目标。在社会发展的过程中,每一种事物的运行都离不开秩序。公共数据的形成和利用都以一定的秩序为基础,由此形成了数据秩序。公共数据法益所内含的秩序是公共秩序,即基于公共数据的形成和利用而形成的公共秩序,其内容包括公共数据关系的一致性、连续性和确定性。公共数据关系的一致性要求公共数据关系的主体、内容和客体在不同地区之间应当保持基本一致,即不能存在公共数据的“地方割据”状态,也不能存在公共数据的“数据孤岛”或“数据烟囱”。公共数据关系的连续性,即已经形成的公共数据关系应当在较长时间段内保持连续,不允许出现“朝令夕改”的现象,以此来实现以公共数据为基础的可预期性。公共数据关系的确定性,是指公共数据关系的主体、客体和内容都是确定的,不能出现模糊、模棱两可的情形。

公共数据法益所内含的数据公共秩序,实际上就是对公共数据的管理秩序,在法治实践中表现为公共数据管理制度的建立和健全。公共数据制度在我国目前尚处于探索与建构阶段,党和国家的政策性文件明确要求建立公共数据共享制度、供给制度、使用制度和管理制度 4 项基础性

① 转引自马长山主编:《数字法治概论》,法律出版社 2022 年版,第 49 页。

② 参见化柏林、郑彦宁:《情报转化理论(上)——从数据到信息的转化》,《情报理论与实践》2012 年第 3 期。

③ 时建中:《数据概念的解构与数据法律制度的构建——兼论数据法学的学科内涵与体系》,《中外法学》2023 年第 1 期。

④ 参见《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》,https://www.gov.cn/gongbao/content/2023/content_5736707.htm,2024-08-26。

制度。[①] 在此基础上，还需根据公共数据的基本特点，通过立法、执法、司法等实践活动细化公共数据制度，形成完备的公共数据制度。在数字社会，凡是涉及公共事务管理和公共服务的场所，都会涉及公共数据的形成和利用。因此，公共数据秩序是公共数据法益的重要内容。

3.公共数据安全

安全是法的基本价值目标。如果一部法律不能够保障人的安全需要，那么其合法性就值得怀疑。在传统社会科学中，利益被划分为国家利益、社会利益和个人利益；相应地，安全被划分为国家安全、社会安全和个人安全。利益与风险并存。在数字化时代，随着公共数据价值的明显提升，公共数据安全成为公共数据法益的核心内容。

根据《数据安全法》第3条第3款的规定，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。据此，可将公共数据安全界定为：通过采取必要措施，确保公共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。从字面意思看，公共数据安全包括公共数据处于被有效保护和合法利用的状态以及持续保持此种状态的能力两个方面的内容。但从实质看，公共数据安全实际上就是指确保公共数据处于有效保护和合法利用的状态，确保公共数据处于有效保护和合法利用的状态是一体两面的关系。确保公共数据处于有效保护和合法利用的状态，是公共数据安全本身，即内部安全，是手段层面的数据安全。公共数据承载的安全还包括外部安全，即国家安全和公共安全，是目的层面的数据安全。

三、公共数据刑法保护的现状与问题

由上可见，数字技术的广泛和深度运用对公共数据价值的大幅提升和对公共数据法益内容的型构，是刑法保护公共数据的基本动因。换言之，在数字化时代，保护公共数据成为刑法的重要任务，是刑法数字化发展的必然要求。那么，我国刑法对公共数据提供了怎样的保护？

（一）保护现状考察

关于刑法对公共数据的保护现状，可以从刑法分则的相关用语入手进行分析。从“数据”的内涵出发，可以以“数据”“信息”“信息网络”和“计算机（信息）系统”为关键词对现行《中华人民共和国刑法》（以下简称《刑法》）分则条文进行检索，[②]并据此对公共数据的刑法保护作出分析。

1.“数据”用语的角度

以“数据”为关键词在我国刑法分则中进行检索，罪状表述中含有“数据”用语的条款共有4个，即《刑法》第134条之一、第142条之一、第285条第2款和第286条第2款。这些刑法条款规定的内容对公共数据提供了一定的保护。除第142条之一规定的数据是虚假的数据，不涉及

① 参见《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》，https://www.gov.cn/gongbao/content/2023/content_5736707.htm，2024－08－26。

② 需要说明的是，从我国的立法看，数据和信息在很多情况下是并列关系。但从逻辑关系和实际情况看，数据与信息之间是有区别的。有学者指出，数据、信息、知识、智慧4者之间呈金字塔式层次关系，即从数据到智慧，依次呈现意义与价值从低到高、可编程性由高到低、属性由客观到主观的关系。参见马长山主编：《数字法治概论》，法律出版社2022年版，第51页。可见，数据是信息的基础和载体，保护公共信息，也就意味着保护公共数据，法律中的“信息”用语实际上相当于“数据”用语。

公共数据保护问题外,其他 3 个条款都涉及对公共数据的保护。首先,根据《刑法》第 134 条之一第 1 项的规定,在生产、作业中违反有关安全管理的规定,篡改、隐瞒、销毁直接关系生产安全的相关数据的,成立危险作业罪。这里的数据是指直接关系生产安全的相关数据,属于公共数据。虽然该项规定最终保护的是生产安全,但是公共数据也受到刑法的直接保护。其次,根据《刑法》第 285 条第 2 款的规定,违反国家规定,侵入国家事务、国防建设、尖端科学技术领域以外的计算机信息系统(以下简称"一般计算机信息系统")或者采用其他技术手段,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,成立非法获取计算机信息系统数据罪。① 这里的数据当然包括公共数据,因此该罪为公共数据秩序提供了一定的保护。最后,根据《刑法》第 286 条第 2 款的规定,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进行删除、修改、增加并且后果严重的,成立破坏计算机信息系统罪。据此规定,将计算机信息系统中存储、处理或者传输的公共数据进行删除、修改、增加且后果严重的,成立破坏计算机信息系统罪。

2."信息"用语的角度

以"信息"为关键词对我国刑法分则条文进行检索,罪状表述中含有"信息"的条款共有 10 个,即第 120 条之三、第 134 条之一、第 161 条、第 177 条之一第 2 款、第 180 条、第 181 条、第 182 条、第 253 条之一、第 291 条之一和第 308 条之一。其中,第 120 条之三、第 181 条和第 291 条之一所涉及的信息属于虚假信息,第 177 条之一第 2 款和第 253 条之一所涉及的信息属于个人信息,不涉及公共数据的保护,无须讨论。第 134 条之一中同时使用了"数据"和"信息"两个词语,且二者之间系并列关系,其对公共数据的保护具有同一性,不再赘述。因此,从"信息"用语的角度看,只有《刑法》第 161 条、第 180 条、第 182 条和第 308 条之一涉及公共数据的保护,需逐一展开分析。

第一,根据《刑法》第 161 条第 1 款的规定,依法负有信息披露义务的公司、企业向股东和社会公众提供虚假的或者隐瞒重要事实的财务会计报告,②或者对依法应当披露的其他重要信息不按照规定披露,严重损害股东或者其他人利益,或者有其他严重情节的行为,成立违规披露、不披露重要信息罪。前一种情形是隐瞒(未披露)基于真实、完整的数据或信息形成的财务会计报告,即隐瞒真实的或完整的数据或信息;后一种情形则是不披露真实信息。在这两种情形中,因隐瞒和不披露的对象均是股东和社会公众,且一般需要严重损害股东或者其他人的利益,故这里的重要信息或数据属于公共信息或公共数据。因隐瞒或者不披露重要信息或数据的行为属于对公共信息合理利用的危害,违反数据秩序,故将此类行为规定为犯罪是对公共数据的保护。

第二,根据《刑法》第 180 条第 1 款的规定,内幕交易、泄露内幕信息罪保护的是内幕信息,即涉及证券的发行,证券、期货交易或者其他对证券、期货交易价格有重大影响的信息,其属于公共信息,故在一定程度上直接保护了内幕信息这一公共数据,且保护的是公共数据秩序。根据该条

① 根据当然解释的原理,违反国家规定,侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统(以下简称"重要领域计算机信息系统"),获取该计算机信息系统中储存、处理或者传输的数据且情节严重的行为,一定成立非法获取计算机信息系统数据罪。但是,在立法者为保护重要领域计算机信息系统而设立了非法侵入计算机信息系统罪的情况下,获取重要领域计算机信息系统中储存、处理或者传输的数据的,应当成立非法侵入计算机信息系统罪。

② 虚假的或者隐瞒重要事实的财务会计报告,就是没有以真实和完整的数据或信息为基础而形成的财务会计报告,属于隐瞒数据或信息的行为。

第4款的规定，利用未公开信息交易罪中的未公开信息，是指内幕信息以外的其他未公开信息，行为主体是金融机构的从业人员以及有关监管部门或者行业协会的工作人员，故这里的未公开信息亦属于公共信息。因此，利用未公开信息交易罪的设置在一定程度上直接保护了公共数据。

第三，根据《刑法》第182条第1款第1项和第5项的规定，操纵证券、期货市场罪的手段行为是利用信息优势联合或者连续买卖，或者利用虚假或不确定的重大信息操纵证券、期货市场。因所涉信息的控制者并非个人，其指向具有公众性，故属于公共信息。此外，不论是利用信息优势联合或者连续买卖，还是利用虚假或不确定的重大信息诱导投资者进行证券、期货交易，都属于手段行为，其目的是操纵证券、期货市场。因此，该罪的设置在一定程度上为公共数据提供了保护。

第四，《刑法》第308条之一规定的披露、报道不应公开的案件信息罪保护的是案件信息。就具体案件而言，因案件信息通常是特定的，案件信息的控制者是作为公共机关的司法机关，并且泄露案件信息通常会给案件的公正处理和司法的公信力带来不利的影响，故案件信息属于公共信息。相应地，泄露不应公开的案件信息罪的设置在一定程度上对案件信息这一公共数据提供了直接保护。

3.“信息网络”用语的角度

信息网络是构成电子信息传输通道的线路、设备的总称。信息是以数据为载体的，是数据所表达的内容和意义。因此，信息网络实际上就是数据传输的网络化。以“信息网络”为关键词对我国刑法分则条文进行检索发现，罪状表述含有“信息网络”的条款共有5个，即《刑法》第246条第3款、第286条之一、第287条之一第1款、第287条之二和第291条之一第2款。其中，《刑法》第246条第3款规定的是利用信息网络实施侮辱和诽谤罪的证据提供问题，不涉及对公共数据的保护。《刑法》第291条之一第2款将“信息网络”作为虚假信息的传播媒体进行了规定，也不涉及对公共数据的保护。需要分析的是《刑法》第286条之一、第287条之一第1款和第287条之二的规定。

《刑法》第286条之一的规定旨在禁止拒不履行信息网络安全管理义务的行为。其实质是禁止不履行数据传输网络化管理义务的行为，即以不作为的方式违法利用数据。这里的数据当然包括公共数据，因为拒不履行信息网络安全管理义务罪的设置在一定程度上为公共数据提供了保护。《刑法》第287条之一第1款的规定旨在禁止非法利用信息网络。信息网络，说到底就是数据的网络化形成和利用。非法利用信息网络，就是非法利用数据的网络化。因此，非法利用信息网络罪的设立在一定程度上能够惩治和预防非法利用数据的行为，对公共数据的合法利用具有一定的保护作用。《刑法》第287条之二的规定旨在禁止帮助信息网络犯罪活动的行为。所谓帮助信息网络犯罪活动，就是为他人利用信息网络犯罪提供帮助。他人利用信息网络实施犯罪，实际上就是他人利用数据的网络化实施犯罪，包括他人利用公共数据的网络化实施犯罪，是对公共数据的非法利用。因此，帮助信息网络犯罪活动罪的设立在一定的范围内为公共数据提供了保护。

4.“计算机(信息)系统”用语的角度

在《刑法》第285条和第286条中出现了“计算机信息系统”或“计算机系统”。“计算机信息系统”在《刑法》第285条和第286条中分别出现了6次和3次，“计算机系统”仅在《刑法》第286条中出现过1次。2011年8月1日，最高人民法院、最高人民检察院发布的《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》第 11 条将“计算机(信息)系统”解释为“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”。一方面,计算机(信息)系统是用来处理数据的,是处理数据的基础设施;另一方面,在数字化时代,计算机(信息)系统是被网络化、数据化了的数据系统。因此,不论是非法侵入还是非法控制、破坏计算机(信息)系统,都会给数据秩序带来危害。

根据《刑法》第 285 条第 1 款的规定,只要违反国家规定侵入重要领域计算机信息系统,就构成非法侵入计算机信息系统罪。根据该条第 2 款的规定,非法控制一般领域的计算机信息系统,情节严重的,成立非法控制计算机信息系统罪。根据该条第 3 款的规定,提供专门用于侵入、非法控制计算机信息系统的程序、工具,或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具,情节严重的,成立提供侵入、非法控制计算机信息系统程序、工具罪。由此可见,我国刑法不但将非法侵入计算机(信息)系统的行为规定为犯罪,而且将为非法侵入计算机(信息)系统提供技术性帮助的行为(不限于共犯)也规定为独立的犯罪,实现了处罚的前置化,从而为公共数据秩序提供了重要保护。

《刑法》第 286 条规定了 3 种破坏计算机(信息)系统的情形:一是破坏计算机信息系统功能,造成计算机信息系统不能正常运行;二是破坏计算机信息系统中的数据和应用程序;[①]三是故意制作、传播破坏性程序,影响计算机系统正常运行。上述 3 种情形成立犯罪均需达到后果严重的程度,且前两种情形成立犯罪需违反国家规定,因而在一定程度上为公共数据提供了保护。

(二)存在的问题

从前文的分析不难看出,我国刑法从多层面、多角度对公共数据提供了保护,在一定程度上满足了数字化背景下公共数据的刑法保护需要。但从实际情况看,刑法对公共数据的保护还存在较为明显的问题,集中表现为保护的专门性、完整性和体系性不足。

1.保护的专门性不足

保护的专门性,是指通过设立罪刑规范为某种法益提供目的性保护而非附带性保护。由此可见,我国刑法对公共数据保护的专门性严重不足。

其一,把公共数据纳入其他保护法益中予以保护,导致保护的专门性不足。此种情形主要存在于《刑法》第 285 条和第 286 条规定的几个危害计算机信息系统的犯罪中。例如,非法侵入计算机信息系统罪、非法控制计算机信息系统罪和破坏计算机信息系统罪的行为对象都是计算机信息系统,保护法益是网络秩序。[②] 虽然计算机信息系统具有设备与信息(数据)一体化的特点,但是从这两个刑法条文的文字表述看,立法目的明显偏向于保护网络秩序,在保护网络秩序的过程中附带性地保护公共数据而非专门保护公共数据。

其二,未能将公共数据作为终极保护对象,导致保护的专门性不足。在刑法学理论上,通常从两个维度来界定法益,即从保护的维度将法益界定为保护法益,同时从侵害的维度将法益界定为侵害法益。[③] 相应地,可从保护和侵害的维度分别将对象界定为保护对象和犯罪对象(行为对象)。在立法层面,若将某种对象作为终极保护对象或犯罪对象规定下来,则是对该对象的专门

① 由此规定不难看出,破坏计算机信息系统中储存的数据的行为也属于破坏计算机信息系统。

② 参见江溯主编:《网络刑法原理》,北京大学出版社 2022 年版,第 59～62 页。

③ 参见张明楷:《刑法学》,法律出版社 2021 年第 6 版,第 78 页。

保护;反之,若将某种对象作为过程性保护对象(即在保护其他对象的过程中受到保护的对象),则对该对象而言不是专门性保护而是附带性保护。综观我国刑法分则中与公共数据保护相关的规定不难发现,除了《刑法》第285条第2款对非法获取计算机信息系统数据的禁止性规定能够为公共数据提供终极保护之外,其他对公共数据的保护均系过程性保护,[①]这充分反映出我国刑法对公共数据的专门性保护不足。

其三,未能明确区分数据与信息,导致保护的专门性不足。一般认为,数据与信息之间虽然存在紧密联系,但是也存在很大的区别。就认知程度而言,数据属于原始资料,并且属于事实和认识的材料,[②]信息是对数据加工后形成的。数据与信息之间系阶层关系,即信息是在数据的基础上形成的,但不能说数据是在信息的基础上形成的。因此,从概念看,数据的外延大于信息的外延,但数据的内涵小于信息的内涵。值得注意的是,随着数据技术的迅猛发展,出现了信息的数据化发展趋势,但这只是认识和处理信息的方式,不会颠覆数据与信息的基本区别。相应地,在保护机制上,对数据的保护主要侧重于事实性保护,而对信息的保护侧重于价值性保护。但在我国法律中,数据和信息的混用[③]导致用保护公共信息的方式和方法来保护公共数据,进而使得对公共数据的保护缺乏专门性。

2.保护的完整性不足

在刑法保护中,受保护的利益或者对象应当具有完整性,否则就违反平等保护原则。对公共数据的保护应当保持完整性,不能顾此失彼。然而,我国刑法对公共数据的保护在很大程度上表现出片段性或碎片性,凸显出保护的完整性不足。

从宏观层面看,公共数据包括涉及国家安全、公共安全、公共秩序、国防利益、军事利益等领域的数据。但在我国刑法中,危害公共数据的犯罪被规定于危害公共安全罪、破坏社会主义市场经济秩序罪和妨害社会管理秩序罪中,在危害国家安全罪、危害国防利益罪和军人违反职责罪中,均未规定危害公共数据的犯罪。也就是说,我国刑法侧重于保护涉及公共安全和公共秩序(包括市场经济秩序和社会管理秩序)的公共数据,从而凸显出对公共数据保护的完整性不足。

从微观层面看,在同一类公共数据中,有的数据受到保护,有的数据则未受到保护。例如,在涉及公共安全的数据中,应当说刑法只保护与生产安全直接相关的数据(危险作业罪),而涉及其他公共安全的数据均未受到保护。从保护的重点看,刑法注重保护对公共数据的占有而非对公共数据的利用。例如,在《刑法》第285条和第286条规定的以信息网络为对象(目标)的网络犯

① 例如,根据《中华人民共和国刑法》第134条之一的规定,篡改、隐瞒、销毁直接关系生产安全的数据,具有发生重大伤亡事故或者其他严重后果的现实危险的,成立危险作业罪。直接关系生产安全的数据属于公共数据,但此公共数据属于过程性保护对象,而生产作业制度才是终极性保护对象。

② 参见张敏主编:《数据法学》,中国政法大学出版社2023年版,第6~7页。

③ 从我国的立法看,混用数据和信息的情况主要表现为以下3种情形:(1)数据与信息并用。例如,《中华人民共和国电子商务法》第25条、《人类遗传资源管理条例》第24条、《废弃电器电子产品回收处理管理条例》第17条、《消耗臭氧层物质管理条例》第28条均采用“数据信息”的表述,《志愿者服务条例》则使用“信息数据”的表述。(2)信息包含数据。例如,《中华人民共和国环境保护税法》第15条第2款、《中华人民共和国国际刑事司法协助法》第26条第5款、《中华人民共和国监察法》第25条、《中华人民共和国食品安全法》第17条、《人类遗传资源管理条例》第2条第3款采用“数据等信息”或类似表述。(3)数据包含信息。例如,《中华人民共和国数据安全法》第38条采用“个人隐私、个人信息、商业秘密、保密商务信息等数据”的表述,《中华人民共和国电子签名法》第2条第2款、《快递暂行条例》第34条以特定信息分别界定“数据电文”与“电子数据”的内涵。

罪中,[①]注重惩治非法侵入、控制和获取行为,而不惩治对公共数据的非法利用行为,亦凸显出对公共数据保护的完整性不足。

3.保护的体系性不足

公共数据保护的体系性,即在危害公共数据犯罪的设置上应当呈现为一个有机统一的整体,主要通过对个罪和类罪的设置呈现出来。我国刑法分则中的任何一个具体犯罪,都是对事实上难以穷尽的犯罪现象的抽象,是一个具体的犯罪类型或者犯罪"轮廓"。因此只要立法者针对某种对象或者法益设置了具体犯罪,那么对该对象或者法益的保护就具有了体系性,且其体系性通过严密的犯罪构成得以体现。如果根据所保护对象或者法益的类型性设置多个具体犯罪,那么其体系性更加凸显。当然,法益的错综复杂性,使得立法者只能根据客观上的主要法益或者其认为的主要法益来确定个罪在刑法分则体系中的位置。[②] 然而,我国刑法对公共数据的保护严重缺乏体系性,主要体现在以下 3 个层面:(1)虽然立法者在危害公共安全罪、破坏社会主义市场经济秩序罪、妨害社会管理秩序罪等类罪中设置了能够对公共数据起到保护作用的个罪,但是这些犯罪难以形成一个数据犯罪体系。(2)我国刑法没有设立任何将公共数据设置为独立的犯罪对象或者将公共数据作为直接且终极的保护法益的个罪。换言之,刑法既没有针对危害公共数据的行为设立独立的犯罪构成,也未形成一个直接保护公共数据的犯罪类型。(3)既然刑法未针对危害公共数据的行为形成独立的个罪,也未形成一个由若干独立个罪构成的数据犯罪体系,那么就没有形成由间接保护与专门保护构成的体系性保护。

四、公共数据刑法保护的改进对策

在数字化的背景下,通过刑法保护公共数据是数字化赋能公共数据的基本要求,但我国刑法在公共数据的保护上表现出明显的不足。为此,应当明确公共数据的刑法保护范围和保护模式,并在此基础上构造危害公共数据犯罪的体系。

(一)明确公共数据的刑法保护范围和保护模式

1.公共数据的刑法保护范围

刑法保护的是重大利益,对非重大利益,刑法不予保护,即刑法具有不完整性。[③] 这是由刑法谦抑主义延伸出来的刑法的基本性质。因此,并非所有的公共数据均由刑法来保护,值得刑法保护的只能是具有重大利益性的公共数据。换言之,在公共数据的刑法保护上必须坚持公共数据的重大性原则,以此来确定公共数据的刑法保护范围。

当前,我国公共数据的形成主体主要有 3 类,即国家机关及其职能部门、企事业单位和提供数字技术服务的企业或组织。据此,可将公共数据分为 3 类,或者说公共数据主要由 3 部分组

① 我国有学者将网络犯罪分为以信息网络为目标的犯罪、以信息网络为手段的犯罪和网络空间的总括性犯罪。以信息网络为目标的犯罪是指《中华人民共和国刑法》第 285 条和第 286 条规定的个罪。参见江溯主编:《网络刑法原理》,北京大学出版社 2022 年版,第 131 页以下。

② 例如,从高空抛物罪的立法过程看,该罪在第一次审议稿中被置于危害公共安全罪之中,在第二次审议稿中则被移至妨害社会管理秩序罪之中。这就表明,该罪既会给公共安全(公众的安全感)带来危害,又会扰乱公共秩序,立法者根据设立该罪保护的主要法益将其归类于扰乱公共秩序罪。

③ 参见张明楷:《刑法学》,法律出版社 2021 年第 6 版,第 23 页。

成，即国家机关及其职能部门在从事公共事务管理过程中形成的公共数据、企事业单位在从事生产经营过程中形成的公共数据和数字技术服务者在从事数字技术服务过程中形成的公共数据。公共数据涉及公共生活的各个方面，但可类型化为作为国家利益的公共数据和作为社会公共利益的公共数据。前者包括事关国家安全、国防利益和军事利益的数据，后者包括事关公共安全、市场经济秩序和社会管理秩序的数据。从现实情况看，作为国家利益的公共数据主要由国家机关及其职能部门来形成，作为社会公共利益的公共数据的形成主体则相对广泛，且各种主体之间并无主次之分。

从我国刑法对国家法益和社会法益的保护看，立法者对前者的保护强度整体上高于后者。这一差异具体表现为，在侵犯国家法益的犯罪中，侵犯国家存立的犯罪（危害国家安全罪）中的个罪均无罪量要素限制，只要行为人实施刑法规定的行为就构成犯罪，属于典型的行为犯；[①]在侵犯国家职能的犯罪（贪污贿赂罪、危害国防利益罪、渎职罪和军人违反职责罪）中，大多数个罪有定量因素限制。与此不同，在侵犯社会法益的犯罪（危害公共安全罪、破坏社会主义市场经济秩序罪和妨害社会管理秩序罪）中，大多数个罪有定量因素限制。由此来看，凡是关涉国家安全事务的数据，其本身就具有重大性，应当受到绝对保护，无须从程度上设置是否具有重大性的判断标准；相应地，在相关个罪中无须通过设置罪量要素来限制处罚范围。其他领域的公共数据应当受到相对保护，需要在程度上设置公共数据之重大性的判断标准；相应地，在相关个罪中需要通过设置罪量要素来限制处罚范围。

2.公共数据的刑法保护模式

在数字化的背景下，国家与社会生活中处处充满数据，由数字化带来的数据化“绑架”了一切，甚至连国家（数字主权）和社会（数字平台）本身都成为数据。[②] 公共数据的基本功用极为广泛，呈现出多元性特点。为此，在公共数据的刑法保护上应当采取多元保护模式。具体而言，在凡是涉及公共数据的类罪中，都应当设立危害公共数据的犯罪。在我国刑法分则规定的 10 大类罪中，有 8 类犯罪属于侵犯公共利益（国家利益和社会公共利益）的犯罪。其中，侵犯国家利益的犯罪有 5 类，即危害国家利益罪、贪污贿赂罪、危害国防利益罪、渎职罪和军人违反职责罪；侵犯社会公共利益的犯罪有 3 类，即危害公共安全罪、破坏社会主义市场经济秩序罪和妨害社会管理秩序罪。[③] 也就是说，此 8 类犯罪均涉及对公共数据的保护，故在这些类罪中均应当设立危害相关公共数据的犯罪。例如，在危害国家安全罪中，可以设立危害国家安全数据罪；在危害公共安全罪中，可以设立危害公共安全数据罪；在破坏社会主义市场经济秩序罪中，可以设立危害市场经济数据罪；等等。

在数字化时代，公共数据的价值借助数字技术而得以大幅度提升，使其本身也具有独特的运行机制和特殊的保护需求。因此，在公共数据的刑法保护上还需确立专门保护与附带性保护相

① 笔者在本文中所说的行为犯，是指不需要发生任何实害结果就可以成立的犯罪，相当于德日刑法学理论中的抽象危险犯；与此相对应的是结果犯，即需要发生实害结果或者危险结果才能成立的犯罪，相当于德日刑法学理论中的实害犯和具体危险犯。在德国，也有学者将抽象危险犯解释为行为犯。参见[德]乌尔斯·金德霍伊泽尔：《刑法总论教科书》，蔡桂生译，北京大学出版社 2015 年版，第 66～68 页。

② 参见马长山主编：《数字法治概论》，法律出版社 2022 年版，第 82～92 页。

③ 有学者指出，在妨害社会管理秩序罪中，妨害司法罪属于侵犯国家利益的犯罪，该类犯罪具体侵犯的是国家的司法职能。参见周光权：《刑法各论》，中国人民大学出版社 2021 年第 4 版，第 8 页。

结合的保护模式。所谓公共数据的专门保护是指设立专门保护公共数据的罪刑规范,而不能停留在将公共数据保护置于保护其他对象或者法益之下或之中。专门保护强调的是保护的独立性,要求针对公共数据设立独立的个罪,如危害环境数据罪。公共数据的附带性保护是指在保护其他对象或者法益时附带性地保护公共数据。如前所述,此种保护构成我国刑法对公共数据保护的基本特点,具有重要的现实意义,但也凸显出我国刑法对公共数据保护的不足。① 因此,在采用专门保护模式的同时,应当保留附带性保护,采用专门保护与附带性保护相结合的保护模式,对公共数据进行全面性、体系性保护。

(二)构造危害公共数据犯罪的体系

由于刑法对公共数据的保护只能通过犯罪化来实现,因此完善公共数据的刑法保护意味着必须构造一个合理的危害公共数据犯罪体系。为此,应当从行为类型和行为主体、罪行阶梯、主观罪过、刑罚设置以及该类犯罪在刑法分则中的分布情况等方面,对危害公共数据犯罪的体系予以构造。

1.危害公共数据犯罪的行为类型和行为主体

从危害公共数据的实践逻辑看,应当将危害公共数据犯罪的行为构造为以下 3 种基本类型。

一是毁坏公共数据。毁坏公共数据,就是非法获取、篡改、删除公共数据。② 非法获取公共数据包括违反国家有关规定提供公共数据和窃取或者以其他方法非法获取公共数据两种情形。篡改公共数据,是指违反国家相关规定修改公共数据,使公共数据失去原有的秩序和功能。③ 删除公共数据,是指违反国家相关规定删除已经形成的公共数据,包括全部删除和部分删除。就毁坏公共数据而言,其行为主体不应受任何限制,可以是公共数据的形成者、占有者和控制者,也可以是其他任何社会主体。

二是非法利用公共数据。非法利用公共数据,是指将公共数据用于非法活动、以非法的方式利用公共数据或者超出规定的范围利用公共数据。将公共数据用于非法活动,如将公共数据用于诈骗、敲诈勒索等违法犯罪活动,即将公共数据作为违法犯罪的手段加以利用。以非法的方式利用公共数据,是指未按照规定的方式来利用公共数据。这里的规定包括国家规定、地方性规定、行业规定等。超出规定的范围利用公共数据,主要是指公共数据的占有者、控制者超越公共数据的利用范围利用公共数据。对公共数据的利用主要是一种权力性利用,或者说对公共数据的利用就是在行使权力。④ 对于权力而言,必须遵循“法无明文规定不得为”的原则。在利用公共数据的刑法规制上,必须将超过利用范围利用公共数据的行为纳入规制范围。非法利用公共数据的主体,主要是公共数据的占有者和控制者,其他主体难以实施该类行为。

三是不形成公共数据。不形成公共数据,是指有形成公共数据义务的主体,在应当且能够形

① 当然,附带性保护凸显出我国刑法对公共数据保护的不足,这并非附带性保护本身所导致,而是立法者在采用附带性保护的同时没有采用专门保护所导致。

② 非法获取公共数据是对公共数据合法占有状态的一种损害,也可以称之为对公共数据的毁坏。

③ 由于公共数据的基本功用是数据分析,因此公共数据必须具有真实性。非法修改公共数据会破坏公共数据秩序,使公共数据失去真实性,进而导致公共数据丧失基本功用。

④ 数字技术的迅猛发展,使得传统社会的“公权力—私权利”二元结构转向“公权力—社会权力—私权利”三元结构。参见马长山主编:《数字法治概论》,法律出版社 2022 年版,第 78 页。公共数据的公共性决定公共数据权既是公权力也是社会权力。

成公共数据的情况下不形成公共数据。公共数据是国家机关及其职能部门、企事业单位和提供数据服务的组织在从事公共事务管理过程中形成的数据，其目的在于实现对公共事务的有效管理。不形成公共数据就是指上述3类主体不形成公共数据。不形成环境数据是不形成公共数据的典型例证：(1)负有生态环境监督管理职责的国家机关及其职能部门应当通过生态环境检测形成环境数据，但滥用职权或玩忽职守而不对相关领域进行环境检测，属于不形成公共数据；(2)从事生产的企事业单位(特别是重点排污单位)有义务进行环境监测而不监测的，属于不形成公共数据；(3)负有生态环境监督管理职责的国家机关及其职能部门和从事生产的企事业单位应将检测或者检测到的环境数据上传数据平台而未上传的，属于不形成公共数据；(4)环境数据平台企业应当将环境数据上传生态环境保护平台而不上传的，属于不形成公共数据。

2.危害公共数据犯罪的罪行阶梯

罪行阶梯，是指对同一类行为根据法益侵害程度予以分级或分层之后形成的梯度。[①] 从实质看，罪行阶梯决定于罪行危害程度。[②] 危害程度跨度大的罪行，通常分为两个或者两个以上的罪行阶梯；危害程度跨度小的罪行，通常没有罪行阶梯。从形式看，罪行阶梯由法定刑来标识。有两个以上法定刑幅度的罪行，就有两个以上的罪行阶梯；只有一个法定刑幅度的罪行，就没有罪行阶梯。相应地，没有罪行阶梯的个罪，只有基本犯；有罪行阶梯的个罪，由基本犯和加重犯(或者减轻犯)组成。有两个以上加重犯的，可以分为一级加重犯、二级加重犯等；减轻犯通常只有一级。从我国刑法分则的规定看，少数个罪没有罪行阶梯，只有基本犯；多数犯罪有罪行阶梯，由基本犯与加重犯(减轻犯)构成。[③] 危害公共数据犯罪应当有罪行阶梯，由基本犯和加重犯构成。

危害公共数据的危害程度跨度较大，从危害结果看主要包括两种：(1)对公共数据本身的危害，即仅对公共数据利益、公共数据秩序或公共数据安全造成危害。此种危害相对较小，但仍能够达到应受刑罚处罚的程度，也是危害公共数据行为犯罪化的重点。(2)衍生性危害，即经由危害公共数据而对国家安全、公共安全、经济秩序、社会管理秩序等带来的危害。此种危害相对较重，完全达到刑罚处罚的程度。针对危害公共数据犯罪应当设立基本犯和加重犯。基本犯仅限于危害公共数据本身的犯罪。对公共数据本身的危害蕴含着危及国家安全、公共安全、经济秩序、社会管理秩序等的现实风险，这也构成了处罚危害公共数据行为的实质依据。危害公共数据犯罪的基本犯主要表现为危险犯，该罪的加重犯则是危害公共数据进而对国家安全和职能、公共安全、社会经济和管理秩序等造成危害的情形。

3.危害公共数据犯罪的主观罪过

犯罪的主观罪过包括故意和过失。一般认为，故意与过失之间在概念上属于并列关系，但在规范关系上则呈现出层级关系。从处罚的角度看，故意是基本的罪过形式，过失通常被赋予例外性。就某种个罪的罪过设置而言，需要优先考虑的是故意，并在故意的基础上考虑是否处罚过

① 罪行在分级或者分层之后，通常会配置轻重不同的刑罚，因此罪行阶梯也就是罪刑阶梯。只不过前者仅从罪的维度去考虑问题，后者同时从罪和刑的维度去考虑问题。

② 这里的危害程度，不限于行为和结果，还包括行为主体。例如，在有组织犯罪中，一般区分首要分子(或者罪行重大者)、积极参加者和其他参加者来设置罪行阶梯。

③ 我国刑法分则规定的个罪(罪名)共计487个，没有罪行阶梯的个罪有134个，占个罪总数的27.52%。

失。就同一行为而言,如果只处罚故意而不处罚过失,那是完全能够被理解的;但若只处罚过失而不处罚故意,则是不可想象的。从此种意义上讲,需要考虑的是个罪的罪过形式是否“包括过失”而不是“有无过失”。

就危害公共数据犯罪的主观罪过而言,不论是基本犯还是加重犯,首先应当处罚的是故意犯罪,在故意犯罪的基础上考虑是否处罚过失犯罪。应当在责任主义的指导下将危害公共数据犯罪的主观罪过设置为故意,然后根据危害公共数据犯罪之个罪的处罚必要性确定是否处罚过失。同时,应当分设基本犯与加重犯的罪过形式。对危害公共数据犯罪的危害,应当分两个层次来理解:(1)如果仅仅是毁坏、非法利用或不形成公共数据,并未对国家利益和社会利益造成实际损害,那么此时的危害公共数据犯罪仅仅具有损害国家利益和社会公共利益的风险;(2)毁坏、非法利用和不形成公共数据,给国家利益和社会利益造成损害,导致毁坏、非法利用和不形成公共数据的风险现实化。显然,第一层次的危害仅仅具有损害国家利益或社会公共利益的风险,属于危害公共数据犯罪的基本犯,且只处罚故意犯罪,即排除过失犯罪的可罚性。第二层次的危害表现为对国家利益或者社会公共利益造成实际损害,应将其设置为危害公共数据犯罪的加重犯,可以是结果加重犯、后果加重犯、情节加重犯或者数额加重犯。① 这些加重情形的出现,显然主要不是行为人意欲的结果,而是基于行为人的疏忽、自信或者放任。在危害公共数据犯罪之加重犯的罪过设置上应当坚持“包括过失”,即采取我国刑事立法的一贯方式,不明确规定罪过形式,而是交由司法者根据案件事实来判断究竟是故意犯罪还是过失犯罪。

4.危害公共数据犯罪的刑罚设置

犯罪的刑罚设置不是一个纯形式问题,而是一个与犯罪危害程度紧密相关的问题,因而是一个本质性问题。随着刑事立法的发展,犯罪被分为危险犯与实害犯,危险犯被分为抽象危险犯与具体危险犯,甚至有学者提出了介于抽象危险犯与具体危险犯之间的准抽象危险犯的概念。② 持传统观点者认为,判断某种犯罪究竟是危险犯还是实害犯,关键在于对行为所保护的法益是否造成实际损害。③ 在制裁一种行为能够保护双重或多重法益的情况下,对危险的判断应当交叉进行。在危害公共数据的场合,危险包括两个方面:(1)毁坏、非法利用或者不形成公共数据的危险;(2)危害公共数据进而造成损害国家利益或者社会公共利益的危险。此种危险实际上同时表现为对公共数据的实害。显然,值得刑罚处罚的危险仅限于第二种危险。

与危害公共数据进而对国家利益或者社会公共利益造成实际损害相比,危害公共数据并具有损害国家利益或者社会公共利益的危险的危害程度要轻得多,故应当将此种情形设置为微罪,

---

① 在我国刑法学理论上,仅仅将加重犯区分为结果加重犯与情节加重犯,甚至刑法学理论通说只讨论结果加重犯。实际上,除结果加重犯和情节加重犯之外,还存在后果加重犯和数额加重犯。结果加重犯是指因造成严重后果而加重刑罚的情形,并且严重后果与结果之间存在很大的不同;数额加重犯是指因犯罪数额的增加而加重处罚的情形,与情节加重犯和结果加重犯之间存在较大的差异。

② 日本有学者指出,明文要求引起“危险”的犯罪是具体危险犯,法律条文上规定一般的、具有危险行为的犯罪是抽象危险犯。前者的危险是高度的,后者的危险包括比较缓和的情形。处于两者的中间状态是准抽象危险犯。参见[日]山口厚:《刑法总论》,付立庆译,中国人民大学出版社 2018 年第 3 版,第 46 页。我国有学者指出,传统的抽象危险犯与具体危险犯“二分说”存在缺陷,无法合理解释“足以”型危险犯、危险物质型危险犯、破坏公用设施型危险犯、暴力危及飞行安全罪、非法携带枪支等危及公共安全罪以及污染环境罪等,故应当提倡准抽象危险犯的分类。参见陈洪兵:《准抽象危险犯概念之提倡》,《法学研究》2015 年第 5 期。

③ 参见[德]克劳斯·罗克辛:《德国刑法学总论》(第 1 卷),王世洲译,法律出版社 2005 年版,第 221~222 页。

配置1年有期徒刑以下刑罚,同时配置选处罚金。危害公共数据且对国家利益或者社会公共利益造成实际损害的,属于危害公共数据犯罪的加重犯。对此种情形应当根据不同的情况配置1年以上3年以下有期徒刑和3年以上7年以下有期徒刑两个刑罚幅度,同时配置并处罚金。

5.危害公共数据犯罪的分布情况

公共数据主要涉及公共利益,包括国家利益和社会公共利益,具有综合性。危害公共数据的犯罪应当在危害国家利益和社会公共利益的犯罪中都有所分布。

危害国家利益的犯罪主要包括两类,即危害国家存立的犯罪和危害国家职能的犯罪。从我国刑法分则的规定看,前者仅指危害国家安全罪,后者包括危害国防利益罪、贪污贿赂罪、渎职罪和军人违反职责罪。[①] 在这5类犯罪中,最需要设立危害公共数据犯罪的是危害国家安全罪、危害国防利益罪和军人违反职责罪。例如,在危害国家安全罪中,可以设立危害国家安全数据罪,将危害关涉国家安全数据的行为类型化为个罪。又如,在危害国防利益罪中,可以设立危害国防数据罪,将危害关涉国防利益数据的行为类型化为个罪。再如,在军人违反职责罪中,可以设立危害军事数据罪,将军人危害军事数据的行为类型化为个罪。

在我国刑法分则中,危害社会公共利益的犯罪包括危害公共安全罪、破坏社会主义市场经济秩序罪和妨害社会管理秩序罪。在此3类犯罪中均应设立专门的危害公共数据犯罪。例如,在危害公共安全罪中设立专门的危害公共安全数据罪,将危害关涉公共安全数据的行为类型化为个罪。又如,在破坏社会主义市场经济秩序罪和妨害社会管理秩序罪中根据次类罪[②]保护法益的数据化情况设立专门的危害公共数据犯罪,如危害公共卫生数据罪、危害环境数据罪等。

五、结　论

在数字化背景下,数字技术的迅猛发展和广泛运用,推动了公共事务管理的数据化发展,使得公共数据的价值得以迅速提升。与此同时,危害公共数据的几率和风险也随之增加,赋予刑法保护公共数据的使命。然而,我国刑法对公共数据的保护明显滞后,集中表现为缺乏对公共数据的专门性、完整性、系统性保护。为此,需要强化公共数据的刑法保护力度。

在刑事立法上,应当超越当下对公共数据保护的过程性、间接性、片段性、碎片化等保护,突出对公共数据进行刑法保护的终极性、直接性、完整性和系统性。在现有保护的基础上强化对公共数据的专门性保护,需要在涉及国家利益和社会公共利益的犯罪中设立专门用于保护公共数据的个罪。一般而言,个罪应当由基本犯和加重犯构成。基本犯是仅危害公共数据并蕴含损害国家利益和社会公共利益之危险的犯罪,加重犯则是危害公共数据进而损害国家利益或者社会公共利益的犯罪。因此,危害公共数据的犯罪可分为以下3种情形:(1)原有的作为对公共数据进行过程性和工具性保护的危害公共数据的犯罪;(2)危害公共数据并创设损害国家利益或者社会公共利益之危险的犯罪;(3)危害公共数据并对国家利益或者社会公共利益造成实际损害的犯罪。第一种对公共数据的损害给予非专门性保护,后两者对公共数据的损害给予专门性保护。

---

① 参见陈兴良:《规范刑法学》(上册),中国人民大学出版社2023年第5版,第129～130页。

② 我国刑法中的类罪包括两个层次:第一层次类罪,即我国刑法分则各章标题所标识的10类犯罪;第二层次类罪,即我国刑法分则第3章和第6章中各节标题所标识的8类和9类犯罪,可称之为“次类罪”。

Abstract: Digitalization has greatly enhanced the value of public data in breadth and depth, forming a legal interest in public data that warrants protection under criminal law. China's current criminal law provides protection for public data in some degree, but specificity, comprehensiveness, and systematicity of protection are clearly insufficient. For this reason, absolute protection should be given to data related to national security, and relative protection should be given to data related to other national interest and social public interest; the protection model, which includes multiple protection, specialized protection and incidental protection, should be adopted; the crime of harming public data should be added to the crimes of harming national interest and social public interest. The types of behavior for this type of crime can be classified into three categories: destructing public data, illegally using public data and not forming public data. The basic offense of harming public data can be constructed as actual harm to public data, which can only be constituted intentionally, belongs to minor offense, and the penalty can be regulated imprisonment of up to 1 year with selected fine. The aggravated offense can be constructed as actual harm to national interest or social public interest, whose offence form includes negligence, should be regulated two penalty grades according to different circumstances: imprisonment of not less than 1 year but not more than 3 years with fine and imprisonment of not less than 3 years but not more than 7 years with fine.

Key Words: public data legal interest, digitization, criminal law protection, the crimes harming public data

责任编辑 田国宝