数据犯罪法益的独立性批判与依附性证成

章艺林[1]

1. 澳门科技大学，yilinzhang0808@foxmail.com

摘　要：随着计算机和网络技术的发展，数据犯罪的法益定位问题日益凸显。本文针对司法实践中数据犯罪面临的法益定位模糊、罪名适用“口袋化”等困境，批判了主张数据安全法益独立性的观点，提出数据犯罪的法益应依附于传统法益。研究表明，数据作为信息的物理载体，其价值需要通过承载的内容实现，数据犯罪本质上是对数据所承载的信息内容的侵害，应当通过法益还原论，将数据犯罪的法益纳入传统犯罪法益的保护框架，通过厘清数据与信息的关系、实质化解释构成要件，现有刑法体系可有效规制数据犯罪，无需增设独立法益类型。

关键词：数据犯罪；法益独立性；法益依附性

一、引言

随着计算机和网络技术的发展，数据作为新的生产要素，其地位正在不断提高。数据的安全性和独立性已经成为法治领域的一个重要问题。近年来，我国颁布了一系列的相关法律，例如数据安全法、网络安全法以及个人信息保护法。这些法律的出台，确立了数据保护的基本框架。在刑法领域，通过第 285 条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等条款对数据犯罪进行规制。

然而，在司法实践中，数据犯罪却面临着诸多的挑战。例如，法益定位模糊。数据本身是传统法益的信息载体，是否蕴含着数据背后的财产权等法益；数据作为独立载体的安全需求，能否成为一种新型的法益，这些都是有待讨论的问题。因此对于数据犯罪所侵害法益的定位，实务界尚未形成统一观点。

其次，数据犯罪还有罪名适用“口袋化”的问题。从法院的判决书来看，我国司法所认定的“数据”不仅包括刑法中规定的“计算机信息系统中存储、处理或者传输的数据”，还进行了一定程度的对外扩张。在数据载体方面，判例突破了“计算机系统”的物理边界，将智能手机、物联网设备、云存储等新型载体纳入解释范围。在数据形态方面，数据的内容由二进制数字本身扩展到了各种数字化的权利客体。[1]对于“数据”认定的扩张化，使得数据犯罪所侵害的法益存在不确定性。

为了解决上述问题，必须明确数据犯罪所保护法益的定位。首先需要将数据犯罪的相关定义进行梳理。

二、数据的定义及犯罪类型

（一）数据的定义

对于数据的定义，在技术层面和法律层面有不同的规定。在技术层面，数据是计算机系统中存储、处理或传输的电磁记录。[2]数据是信息的电子形式，可以是文字、声音、图像等。数据和信息是载体和内容、形式和实质的关系。[3]可见，技术层面数据的定义强调了其物理属性和技术载体的功能。在法律层面，根据《中华人民共和国数据安全法》第三条第 1 款的规定：“本法所称数据，是指任何以电子或者其他方式对信息的记录。”该规定强调了数据的“记录形式”，而并非强调内容本身。[4]有批评的观点认为，数据安全法对数据的定义未明确区分数据与信息的概念，导致法律适用中二者存在混同的现象，进而模糊了数据权利保护的边界，导致了法律适用困难。

[1]杨志琼.我国数据犯罪的司法困境与出路:以数据安全法益为中心[J].环球法律评论,2019,41(06):151-171.

[2]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,2018,36(06):163-174.

[3]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(06):44-55.

[4]夏伟.论数据犯罪的立法重塑[J].法制与社会发展,2023,29(04):173-190.

在刑法中，数据的定义没有作出明确的解释。从数据在刑法条文中的定位来看，数据犯罪主要位于刑法分则第 6 章第 1 节，属于妨害社会管理秩序罪中的扰乱社会秩序犯罪。在司法解释中，对数据的外延进行了细化。根据《最高人民法院、最高人民检察院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），数据包括用户身份认证信息、金融数据、其他重要电子记录。[5]

有学者认为，刑法分则规定的数据的外延过于狭窄。现行刑法中，数据的定义仅仅局限为计算机信息系统数据，这与目前的数据类型和数量相比显得过于狭隘。这意味着有很多具备显示危害的实际上的数据犯罪行为无法被包容进刑法的评价范围。[6]

不过，也有学者指出，数据的定义范围过于宽泛，现行法律对数据的定义未限定载体形式，也未明确数据的具体类型，导致司法实践中难以界定保护范围。李怀胜教授指出，数据的定义过于宽泛，导致其与信息、系统安全等概念重叠，从而弱化了数据犯罪的独立地位。[7]

两种观点的对立，实际上反映了立法规定不明确与司法上的过度扩张之间的矛盾。一方面，刑法将该罪中“数据”的范围局限于计算机信息系统之中，难以应对大数据时代多样化的数据类型，导致具有实质危害性的新型数据犯罪的行为规制缺失。另一方面，司法解释虽然通过开放列举拓宽了外延，但并未建立起类型化判断的标准，使得数据与信息、计算机系统等法益的边界处于模糊状态。两者的冲突共同指向了数据犯罪法益的定位问题。对于这一问题，尚未形成统一的认识，这也成为了制约数据犯罪规范体系建构的关键所在。

（二）数据犯罪的概念与类型

数据犯罪的概念有狭义和广义之分。狭义的数据犯罪是指刑法上直接规定的，直接以数据作为侵害对象实施的犯罪行为，具体罪名为非法获取计算机信息系统数据罪和破坏计算机信息系统罪。广义的数据犯罪是指一切涉及数据的传统犯罪，如与数据相关的知识产权犯罪、个人信息犯罪、财产犯罪等犯罪，也可称之为“数据化的传统犯罪”。在刑法理论的语境下，数据犯罪通常采用狭义上的概念，专指《中华人民共和国刑法》《刑法》第 285 条第 2 款非法获取计算机信息系统数据罪及《刑法》第 286 条第 2 款破坏计算机信息系统罪中针对数据的行为。

对于数据犯罪的类型，依据划分的标准不同存在不同的分类方式。例如，根据犯罪对象划分，可分为对计算机信息系统信息的犯罪、对个人信息数据的犯罪、对企业数据的犯罪、对公共数据的犯罪；根据行为方式划分，可分为数据获取型犯罪、数据破坏型犯罪、数据滥用型犯罪、数据传播型犯罪；按数据的作用划分，可分为数据作为犯罪对象的犯罪、数据作为犯罪工具的犯罪；数据作为犯罪结果的犯罪。

虽然数据犯罪的类型划分呈现出多元化的视角，但是可以结合研究的目的选择较为合适的划分方法。其中，按照数据在犯罪中所起到的作用来划分数据犯罪的类型，最能明确研究数据犯罪的范围，以论述法益的定位。

1. 工具型数据犯罪

工具型数据犯罪是指通过数据内容的运用或加工来实施犯罪。数据在此类犯罪中起到一个犯罪工具的作用，其核心在于将数据技术特性用于违法目的。例如，通过非法获取公民的个人信息后通过所获得的信息实施诈骗行为，数据是其犯罪过程中的一个零件，其侵害的法益其实是诈骗罪的财产法益。在此类犯罪中，数据作为工具或者手段对犯罪起作用。行为人所实施的是传统类型的犯罪，数据只是起一个帮助或者强化犯罪效果的功能，其社会危害性仍然需要通过下游犯罪的实施来实现。因此其刑法评价需要回归对传统法益的侵害结果来进行认定。

2. 结果型数据犯罪

在结果型数据犯罪中，数据是犯罪行为的危害结果。结果型数据犯罪的具体表现有数据泄露、数据篡改和数据滥用等。对于不同的犯罪，侵害的法益类型有所不同。例如，非法获取公民个人信息后贩卖牟利，所侵害

[5]张明楷.网络时代的刑事立法[J].法律科学(西北政法大学学报),2017,35(03):69-82.

[6]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+207.

[7]李怀胜.数据安全的法益变迁与刑法规制[J].江西社会科学,2023,43(07):33-44.

的法益是个人的隐私权。而攻击交通信号灯系统篡改数据，导致路口瘫痪，所侵害的法益不仅包括数据法益，还包括公共安全法益。两者的区别在于，前者的侵害对象是数据本身，属于对单一法益的侵害，后者的侵害对象既包括数据，也包括其背后承担的公共安全，属于对复合法益的侵害。对于单一法益侵害的行为，可以直接适用数据本体相关的罪名，而对于符合法益侵害的行为，不能仅从数据本体法益进行规制，而可能需要结合计算机相关的犯罪罪名进行综合评价。理论上，可以首先用计算机相关犯罪的罪名来规制此类的犯罪行为，在无法完全包容评价具体行为的时候，再用数据本身的犯罪来加以规定。

（三）对象型数据犯罪

对象型数据犯罪，也被称为“狭义的数据犯罪”。在对象型数据犯罪中，数据是直接侵害的目标。具体而言，对象型数据犯罪是指非法获取或破坏数据的行为。根据行为的性质不同，可以进一步细分为获取型和侵害型两类。获取型行为是指未经授权或许可擅自取得受保护的数据，代表罪名为非法获取计算机信息系统数据罪；侵害型行为是指对数据的破坏，如对数据的删除、修改或增加，代表罪名为破坏计算机信息系统罪。有学者指出，无论是哪种行为模式，都体现了较为明显地对数据本体的侵害，应当区别于传统的计算机信息系统类罪名，设立偏向于数据本体的罪名。[8]

数据安全法对以数据为侵害对象的行为进行了规定。例如数据安全法第 32 条的规定：“禁止以窃取或其他非法手段获取数据，明确要求数据收集需要合法、正当。”然而，刑法和其前置法的协调和衔接方面存在一定的问题。例如，“情节严重”的认定标准不明确，社会危害性的评价标准不清晰。数据犯罪“口袋化”现象集中体现在该种类型的数据犯罪上。

综上所述，工具型数据犯罪和结果型数据犯罪实际上是披着数据外衣的各种传统犯罪，在保护法益的认定上可以直接参照传统犯罪的法益，并不具备特殊性，而对象型数据犯罪，即狭义的数据犯罪的法益较为特殊，且“口袋化”现象显著。因此，必须厘清该种类型数据犯罪的法益。

三、数据犯罪法益独立性的批判

支持数据犯罪法益独立论的学者主张，需要将数据安全作为独立法益进行保护。数据犯罪的法益独立于人身权、财产权等传统法益，需要将其与传统法益区分开来。数据犯罪与计算机犯罪或网络犯罪不同，其核心在于以数据为直接犯罪对象，而并非工具或者载体。

其中，有学者主张数据犯罪的保护法益是数据安全，认为数据犯罪侵害的法益是数据的保密性、完整性和可用性，即数据三性。其中，保密性是指数据未授权访问、知悉、泄露的状态。该罪的核心含义之一是保护“系统数据不为他人所知”。即使是在数据已经泄露的情况下，此时行为人如果使用技术手段获取数据，或者测试系统中的数据是否正确的行为，仍然属于侵害数据保密性的“非法获取”情形。完整性是指数据面授未授权篡改、破坏、删除，保持其真实、准确、完整的性状。非法获取计算机信息系统数据罪主要针对获取数据的行为，而数据安全说将该罪名的法益置于该罪名的上位概念“数据犯罪”来理解。我国刑法对于数据完整性的保护主要由刑法第 286 条第 2 款破坏计算机信息系统罪进行规定。可用性是指数据能够由授权用户及时、可靠的访问和使用。侵害可用性即令授权用户无法及时正常的使用这些数据。[9]

还有学者主张，数据犯罪保护的法益是国家对于数据的管理秩序。支持该学说的学者认为，在数据之中存在一种具有社会属性的公法益，即国家对数据的收集、存储、运输、处理、分析等过程的管理秩序。这是所有类型的数据均拥有的法益，而并非特定种类的数据所专有的法益。数据是“为了社会管理便利而存在”的，具有鲜明的社会属性。数据法益具有集体法益的属性，其保护的对象是社会整体数据流通的安全性与规范性，而并非个体数据的私权。[10]在规范方面，《网络安全法》《数据安全法》等前置法确立了数据安全管理义务，刑法通过制裁非法获取和破坏行为来维护这一管理秩序。该法益观能够使刑法罪名与前置法有机衔接起来。然而，

[8]刘宪权.数据犯罪罪名体系建构之完善[J].国家检察官学院学报,2024,32(03):18-31.

[9]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,(01):64-76+63.

[10]刘宪权.数字经济环境下数据犯罪规制和认定模式的演变[J].上海大学学报(社会科学版),2024,41(02):1-14.

上述观点存在根本性的缺陷。以下将对其展开论述。

（一）数据安全法益无法脱离传统法益而存在

数据本身并非利益的载体，其价值完全取决于其所承载的信息内容。例如存储于数字载体上的姓名、身份证号、账户的账号和密码等。数据本身是由“0”和“1”组成的二进制序列，这些序列本身并不具有“意义”，只有他们按照特定的规律排布，并且可以被解读为有用的信息时，才具有价值。因此数据的价值具有间接性。[11]因此，并非所有数据的保密性、可用性和完整性都值得刑法的保护，数据的保护与否取决于其是否与数据所蕴含的实质法益，即各种信息内容法益。

数据犯罪与传统犯罪在法益的侵害方面具有高度重合性。在数据犯罪行为中可能会同时侵犯多种类型的数据法益。例如，在非法获取医疗数据的行为中，既有可能构成非法获取计算机信息系统罪，也有可能构成侵犯公民个人信息罪。可见数据安全法益与传统法益在内容上具有一定的同质性。[12]

（二）数据管理秩序是传统法益的延伸

首先，将“国家数据管理秩序”作为一种独立的法益进行保护，本质上依然是对于传统法益保护的一种延伸。值得刑法保护的数据，其价值源于数据所承载的具体内容。而对使用数据的过程中的秩序的保护，目的仍然是为了确保这些数据内容中的具体法益在使用过程中免受侵害。例如维护个人信息相关数据的管理秩序，是为了防止个人信息被泄露，从而保护人身权；维护支付信息相关数据的管理秩序，是为了防止虚拟财产被盗窃，从而保护财产权。可见，数据管理秩序并不能够脱离人身、财产等法益独立进行评价，如果将其设置为独立法益，反而使得数据犯罪的法益概念变得更加宽泛和抽象。

其次，如果将“秩序”作为法益，容易使刑法沦为行政管理的工具。刑法的任务在于保护法益，而并非维护行政管理秩序。如果将刑法意义上的法益认定为某种管理秩序，可能会模糊刑法与行政法的边界，甚至使得刑法沦为行政管理的工具。从法理上看，行政法旨在维护高效有序的管理流程，而刑法的核心任务是保障与公民个人、社会密不可分的各种实体性权益，如生命权、财产权、公共安全等。刑法介入的合理性在于对这些法益构成了严重的危险或者损害。如果将“违反行政管理秩序”与“严重侵害重大权益”划伤等号，实际上是降低了入罪门槛。

此外，“秩序”的概念过于抽象，无法为构成要件的解释提供一个切实有效的解释路径。究竟何种行为能够构成破坏“数据管理秩序”，缺乏一个客观的评价标准。并且“违反数据管理秩序”并不能给“技术手段”、“情节严重”等构成要件提供一个明确的解释，导致了构成要件的边界扩张，最终导致“口袋化”现象的产生。反之，如果将法益回归数据中蕴含的传统法益，反而能够更明确地判断行为的社会危害性大小，例如通过财产损失数额、个人信息泄露的数量与敏感程度等具体标准来量化不法程度，使刑法适用更加精确。

综上所述，数据犯罪法益独立论，问题在于其主张的“数据安全”或者“数据管理秩序”并非独立价值的法益，而是保护传统法益的一种手段。该观点在理论层面的抽象化，导致了实践层面处罚的泛化。因此，将数据视为传统法益的载体，采用较为保守的数据犯罪法益依附性说，或许更为恰当。

四、数据犯罪法益依附性的证成

对于数据犯罪法益依附论的构建，核心在于坚持还原法益的价值，区分数据与信息，并且采用实质解释的方法论。以下将从三个步骤进行展开论述。

（一）数据犯罪法益的识别与穿透

数据犯罪法益依附论的核心主张为，数据本身不是独立保护的法益客体，而是承载利益的一种工具，其价值必须依托于传统法益才能实现。数据法益实际上依附于传统法益，所谓的“数据犯罪”实际上都是针对传统

[11]阎二鹏,马光远.数据犯罪的教义学限缩：基于数据使用权法益的证立[J].北方法学,2024,18(04):111-126.

[12]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.

法益的犯罪。[13]首先，数据价值具有间接性。如前文所述，数据的价值由其所承载内容的价值而决定。数据本身是一连串的二进制序列本身并不具有意义，只有将数据进行解读，并转化为有用的信息，才具有实际的价值。数据的物理属性无法脱离其内容单独成为法益保护的对象。其次，数据法益的把握，必须始终遵从法益还原论的要求。刑法的任务在于保护法益，任何犯罪行为都是对法益的侵犯。法益必须是实际的、具体的，并且可以还原为个人法益。在数据犯罪领域，犯罪的危害性，需要通过其所侵害的传统法益来体现。例如，非法获取公民的个人信息数据的行为，侵害了公民的个人信息自决权；破坏企业生产的行为，可能侵害企业的财产权或市场竞争秩序。如果脱离具体法益的内容，单纯将数据安全作为定罪的依据，可能会造成数据犯罪法益的抽象化和空洞化。再次，刑法作为保障法，必须保证其谦抑性，避免对中立的技术行为进行过多的干预。对数据实施的侵害行为，只有在对传统法益造成严重侵害时，才具备刑事违法性。这也与刑法第 13 条“但书”规定中的“行为显著轻微，危害不大的，不认为是犯罪”相一致。

（二）数据与信息关系的厘清

数据与信息的关系，在司法实践中，经常出现混同的现象，必须对二者的关系进行梳理。在技术层面，数据是信息的物理载体。数据以电磁信号、代码等方式存在于计算机系统中，是信息的物理表现形态。[14]而在法律层面，信息是数据的规范内核。虽然刑法对数据和信息的内涵未作规定，但是可以参考民事法律的相关规定。民法典第 1034 条将个人信息定义为“以电子或者其他方式记录的与已识别或可识别的自然人有关的各种信息”，个人信息保护法第 4 条进一步明确“个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人的各种信息”。由此可以看出，法律对于数据的规制始终围绕其承载的信息内容展开。根据法秩序统一原理，刑法对数据的保护也应当从信息着手进行。

（三）构成要件的实质化解释

数据犯罪法益依附论要求对传统犯罪的构成要件将进行实质化的解释，其核心在于穿透数据的技术外衣，直接评价行为所侵害的实质法益，从而将数据犯罪纳入现有的刑法罪名体系之中。

首先，需要将数据犯罪的“行为对象”和“行为手段”转化为传统犯罪的语言，将虚拟财产等具备交换价值和使用价值的数据解释为财产犯罪中的“财物”或者“财产性利益”，并将非法获取、篡改数据等技术行为，依照行为的主观目的和客观结果，解释为传统犯罪中的具体犯罪行为。例如，利用网络爬虫技术非法获取具有价值的数据，可以通过实质解释的方式解释为盗窃财产性利益。其次，需要将危害结果还原为传统法益的危害结果。例如，“数据保密性、完整性被破坏”这一数据安全层面的损害，应当被转化为“个人信息泄露”、“财产所有权灭失”等具体危害。再次，还应当厘清数据犯罪与传统犯罪的竞合问题。根据行为对法益侵害的种类不同，可以分为对单一法益的侵害和对符合法益的侵害。在对单一法益的侵害中，数据仅仅作为犯罪实施的工具。在此情形下，可以直接适用传统罪名。而对于侵害复合法益的情形，即数据侵害行为同时侵犯了数据本体和传统法益时，可以通过竞合理论进行处理。[15]例如，行为人非法获取患者的电子病历数据并出售牟利，既构成非法获取计算机信息系统数据罪，又构成侵犯公民个人信息罪。此时可以依据《中华人民共和国刑法》第二百八十七条第 1 款的规定“依照处罚较重的规定定罪处罚”。由此可见，在法益依附论的基础上，现有刑法规范能够解决数据犯罪与传统犯罪的竞合问题。

五、结语

本文通过对数据法益的独立性与依附性的系统性分析，得出了以下结论：数据犯罪的法益保护应当坚持依附性的立场，将数据犯罪的保护法益纳入传统法益的保护框架，不必增设新的法益类型。

首先，数据犯罪的法益定位必须回归到法益本质的还原论要求。数据是利益的载体，其价值必须依托于传统法益才能实现。其次，需要厘清数据和信息在技术上和法律上的关系。在技术层面，数据是信息的物理载体；

[13]黎森予.“数据犯罪”概念的否定与化归[J].南大法学,2024(04):30-47.

[14]刘宪权.数据犯罪刑法规制完善研究[J].中国刑事法杂志,2022(05):20-35.

[15]赵桐.一般数据犯罪的比较考察与体系建构[J].中德法学论坛,2022(02):83-103.

在法律层面，信息是数据的规范内核。数据作为无体物，其价值完全取决于其所承载的信息的内容，脱离具体信息内容的数据安全无法构成独立的刑法法益。再次，数据犯罪构成要件的解释应当坚持实质化解释，将行为对象、手段和结果回归到具体的传统法益之中。现有刑法体系已具备规制数据犯罪的基础框架。目前的刑法第 285 条、第 286 条已涵盖了大部分的数据犯罪行为。司法实践中对“数据”的扩展解释可以通过类型化路径规范，即区分单一法益侵害和复合法益侵害，从而避免“口袋化”的倾向。最后，在数字时代，数据犯罪的法益保护既要正视数据类型多样化带来的挑战，又要保持必要的开放性，实现保障数据安全与促进数字经济发展的有机统一。

参考文献：

[1] 杨志琼.我国数据犯罪的司法困境与出路:以数据安全法益为中心[J].环球法律评论,2019,41(06):151-171.

[2] 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,2018,36(06):163-174.

[3] 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(06):44-55.

[4] 夏伟.论数据犯罪的立法重塑[J].法制与社会发展,2023,29(04):173-190.

[5] 张明楷.网络时代的刑事立法[J].法律科学(西北政法大学学报),2017,35(03):69-82.

[6] 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+207.

[7] 李怀胜.数据安全的法益变迁与刑法规制[J].江西社会科学,2023,43(07):33-44.

[8] 刘宪权.数据犯罪罪名体系建构之完善[J].国家检察官学院学报,2024,32(03):18-31.

[9] 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,(01):64-76+63.

[10] 刘宪权.数字经济环境下数据犯罪规制和认定模式的演变[J].上海大学学报(社会科学版),2024,41(02):1-14.

[11] 阎二鹏,马光远.数据犯罪的教义学限缩：基于数据使用权法益的证立[J].北方法学,2024,18(04):111-126.

[12] 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.

[13] 黎森予.“数据犯罪”概念的否定与化归[J].南大法学,2024(04):30-47.

[14] 刘宪权.数据犯罪刑法规制完善研究[J].中国刑事法杂志,2022(05):20-35.

[15] 赵桐.一般数据犯罪的比较考察与体系建构[J].中德法学论坛,2022(02):83-103.