Advances in Social Sciences 社会科学前沿, 2026, 15(5), 398-407
Published Online May 2026 in Hans. https://www.hanspub.org/journal/ass
https://doi.org/10.12677/ass.2026.155413

Hans汉斯

数据安全法益视角下数据犯罪的刑法规制

李宗衡

苏州大学王健法学院，江苏 苏州

收稿日期：2026年3月27日；录用日期：2026年5月19日；发布日期：2026年5月28日

摘　要

随着数字化时代的到来，数据已成为社会进步和经济发展的关键要素。对于数据犯罪刑法应当如何作出回应成为理论聚焦的重要议题。当下数据犯罪研究中存在概念模糊不清的问题，应当认识到数据与计算机系统和信息等概念存在本质区别，不可混淆使用。我国刑法在数据犯罪的规制上存在不足，如存在数据全流程保护不力、数据犯罪构成要件认定模糊等问题。为了有效应对数据犯罪，应当首先厘清数据犯罪所侵害的法益，以独立的数据安全法益为中心，确立数据的独立地位，实现数据全流程保护，并区分数据犯罪与其他相关犯罪。

关键词

数据犯罪，数据安全法益，刑法规制

Criminal Law Regulation of Data Crimes from the Perspective of Data Security Legal Interest

Zongheng Li

Kenneth Wang School of Law, Soochow University, Suzhou Jiangsu

Received: March 27, 2026; accepted: May 19, 2026; published: May 28, 2026

Abstract

With the advent of the digital age, data have become a key element for social progress and economic development. How criminal law should respond to data crimes has emerged as a significant issue in theoretical discussions. Current research on data crimes suffers from conceptual ambiguity, and it is essential to recognize that data is fundamentally distinct from concepts such as computer systems and information, and should not be used interchangeably. China's criminal law exhibits deficiencies

文章引用: 李宗衡. 数据安全法益视角下数据犯罪的刑法规制[J]. 社会科学前沿, 2026, 15(5): 398-407.
DOI: 10.12677/ass.2026.155413

in regulating data crimes, including insufficient protection throughout the entire data lifecycle and unclear criteria for determining the constitutive elements of data crimes. To effectively address data crimes, it is necessary first to clarify the legal interests infringed upon by such crimes. Centering on independent data security legal interests, the independent status of data should be established, comprehensive protection throughout the data lifecycle should be achieved, and data crimes should be distinguished from other related offenses.

Keywords

Data Crimes, Data Security Legal Interest, Criminal Law Regulation

1. 引言

在数字化浪潮与人工智能技术爆发式的发展之下，互联网技术深度影响着民众的生活方式与行为习惯。在时代背景下，“数据”的重要性迅速上升，它不仅是进行人工智能模型训练与算法迭代的基础，更是驱动经济高质量发展的核心生产要素[1]。因此，数据安全不仅关乎传统的信息保护，更延伸至人工智能时代的算法安全与模型安全，这使得数据犯罪问题成为刑法学研究亟待深耕的前沿领域，引发了学界的广泛讨论。为回应数据治理的现实需求，我国不断推动立法，致力于为数据的收集、流通与利用提供完善的法律保护。在此过程中，《网络安全法》[2]《数据安全法》[3]等一系列法律法规相继出台，共同构筑起数据治理的规范体系。尤其是《数据安全法》的颁布施行，具有重要意义。作为首部专门聚焦于数据安全保护的独立立法，它标志着我国数据治理呈现出体系化、专门化的趋势，为保障数据要素的安全有序流转与合法合规利用，构建了坚实的规范基础[1]。然而作为社会治理体系中承担最后保障功能的刑法，在面对复杂多变的数据犯罪时，其规制功能却发挥不足。相较于民法、行政法等前置域的快速响应，刑法在数据安全保护方面呈现出显著的滞后性。具体而言，现行刑法规范尚未形成对数据全过程的周延保护机制，且对于实践中层出不穷的非法持有数据、越权使用数据等新型法益侵害形态，由于缺乏类型化的构成要件设计，导致大量具有实质危害性的数据滥用行为难以被有效纳入刑法规制的范围之内。随着数字技术的发展，数据犯罪的手段愈发呈现出智能化、隐蔽化与跨国化的特征，其社会危害性持续累积，对我国数据刑事立法与司法应对能力构成了严峻的考验。面对这一情况，刑法理论界应作出回应。

2. 数据犯罪的前提概念澄清

2.1. 数据的概念厘清

在对数据犯罪展开系统研究之前，首要任务在于对“数据”这一概念作出界定。在此前提之下，方能廓清数据犯罪所涵摄的行为类型及其对应的刑法规范，进而探讨各类行为所侵害的法益内容。需要特别说明的是，现行刑法条文中所使用的“数据”一词，其规范内涵与刑法解释学视角下“数据犯罪”这一学术概念中的“数据”，二者之间可能存在差异。若将这两种不同语境下的“数据”概念不加甄别地简单等同，进而将所有与数据存在形式关联的刑法罪名一概纳入数据犯罪的讨论范围，势必导致犯罪圈

[1]http://www.pishu.com.cn/skwx_ps/ps/literature?SiteID=14&ID=16441716.
[2]https://flk.npc.gov.cn/detail2.html?ZmY4MDgwODE2ZjNlOTI4MTAxNmY0MjUyMzE0OTJk.
[3]https://flk.npc.gov.cn/detail2.html?ZmY4MDgwODE3MjA3MTc2YzAxNzI3YzE3MTE1YTA3ODk.

的不当扩大，有损刑法谦抑性原则。一旦数据犯罪所涉及罪名的边界模糊，这一概念本身也将趋于泛化，此种概念边界的模糊化，不仅会使数据犯罪研究失去明确的聚焦方向，阻碍对其本质特征与运行规律的深度挖掘，更可能影响整体研究路径。因此，厘清“数据”概念的规范内涵，明确数据犯罪的范围，是推进相关研究的前提性工作。作为近年来新兴的法律概念，“数据”在法学理论体系中尚未形成成熟、系统的概念框架。在刑事立法与司法实践中，数据这一术语也时常与“计算机信息系统”“信息”等相邻概念混用，边界模糊不清。为厘清数据犯罪的规制对象，避免概念混淆导致的适用模糊，有必首先对“数据”及其相关概念的关系进行澄清。

数据是指在计算机信息系统中实际处理一切有意义的组合[32]，通过对数据的分析，可以从中提炼出具有特定价值的信息内容。在数据的处理中，计算机信息系统作为载体，承担着数据存储与运算的功能。然而需要明确的是，计算机信息系统虽为数据的主要载体，但其内部还包含诸多不属于数据范畴的构成要素。从本质层面来看，数据与计算机信息系统之间构成内容与载体的依存关系。在传统的技术环境下，针对数据的非法侵害行为，通常以突破计算机系统的安全防护为前提，行为人往往需要通过侵入或破坏系统的方式，实现对数据的获取或篡改。然而，随着云计算等新兴技术的持续演进与广泛应用，数据的存储、传输与处理方式日趋多元，其应用场景亦逐步突破传统计算机系统的物理边界。基于上述的技术变迁，在刑法规范层面，数据与计算机系统应当被明确区分为两种独立的犯罪对象。二者在侵害方式、危害后果及其法律评价上均存在实质性差异，不宜将其简单等同。

“信息”与“数据”在性质与语义层面具有高度相似性，部分法律规范中甚至将二者等同使用。例如，欧盟《通用数据保护条例》明确规定，个人数据涵盖任何能够识别特定自然人的相关信息[3]。在我国，《数据安全法》《个人信息保护法》[4]等法律的相继出台，标志着数据法律保护体系已初步构建并趋于稳定。然而，现行立法并未对数据与信息之间的关系作出清晰界分。根据《数据安全法》第三条的规定，数据在法律层面具有区别于信息的独立意义。该条将数据界定为“任何以电子或者非电子形式对信息的记录”，明确了数据作为信息载体的法律定位。在司法实践中，司法解释仍倾向于将数据与信息混同处理。例如，《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》[5]将“身份认证信息”直接等同于计算机信息系统中的数据。本文认为，数据与信息之间实则构成一种交叉关系。从表现形式来看，信息的载体较数据更为多元。数据仅能以二进制电子代码的形式存在，而信息除电子形式外，还可通过纸质记录、口头表达等非电子方式呈现与传播；从内容范围来看，数据的涵盖面较信息更为宽泛。数据主要指存在于网络空间中的电子记录，其中既包含承载具体信息内容的有意义数据，也包含不具有实际信息含义的冗余代码或无意义代码；从客体属性而言，信息往往蕴含一定的主观因素，这些因素可能源于社会认知、群体共识或主体需求，而数据则更强调其客观性与中立性，其价值主要体现于数据集合的规模体量与精细化程度，且使用价值会因应用场景与使用需求的不同而呈现差异化特征。

2.2. 数据犯罪的范围确定

当前对数据犯罪的内涵尚未形成明确的共识，其概念边界仍处于较为模糊的状态。在涉及数据犯罪的刑法研究中，概念混用现象屡见不鲜，突出表现为数据犯罪与计算机犯罪、网络犯罪、信息犯罪等之间的交叉重叠与混用。应当指出，无论是从现行法律规范文本中推导，抑或是基于理论层面的探讨，均尚未就数据犯罪的界定达成共识。数据犯罪并非刑法中明文规定的具体罪名，而是对一类具有共同特征的犯罪行为类型的概括。我国现行刑法虽未对数据犯罪作出明确定义，但在部分罪名的构成要件中，已

[4]https://flk.npc.gov.cn/detail2.html?ZmY4MDgwODE3M2I1ZjU0YzAxNzNiYjE0YmUxMDAxMjc.
[5]http://gongbao.court.gov.cn/Details/c6acdcf295a8ce63eb34a2444e67a8.html.

将数据明确列为犯罪对象。

综观学界现有的研究成果，关于数据犯罪的概念界定主要存在广义与狭义两种观点。狭义说认为，数据犯罪是指以数据为侵害对象，实施非法获取、删除、修改、增加等行为的情形。在我国刑法体系中，此类狭义数据犯罪主要体现于两个条款：其一为《刑法》第 285 条第 2 款规定的非法获取计算机信息系统数据罪；其二为《刑法》第 286 条破坏计算机信息系统罪第 2 款中关于删除、修改、增加数据的相关规定[4]；广义说明主张将数据犯罪的范围扩展至所有与数据存在关联的犯罪行为[5]。持此观点的学者认为，数据犯罪的研究范畴不应局限于《刑法》第 285 条第 2 款及第 286 条第 2 款所规定的具体罪名[6]。凡是以数据为工具或媒介实施的犯罪行为，均宜纳入数据犯罪的讨论范围。依此逻辑，侵犯公民个人信息罪、泄露国家秘密罪、侵犯商业秘密罪等传统罪名，在特定情形下均可归入数据犯罪的范围[7]。

在确定数据犯罪的概念时，本文倾向于采纳狭义说，认为该视角下的界定方式在理论逻辑上更具精确性与合理性。数据犯罪这一概念是数字时代发展的产物。若以广义说作为规制重心，极易导致数据犯罪的边界过度扩张，使其涵盖范围过于宽泛。在传统犯罪形态中，虽不乏以数据为工具实施的行为，但彼时所涉的数据与大数据语境下的数据存在本质差异。当下数据不仅承载着更为丰富的信息内容，更被赋予独特的经济价值、社会价值与战略意义，呈现出鲜明的时代属性。此外，从法律适用的效果考量，狭义的数据犯罪界定更有利于实现精准的规制。将《刑法》第 285 条及第 286 条所涉行为明确锚定为数据犯罪，有助于清晰呈现数据犯罪与传统犯罪之间的结构性差异。此种区分方式可为司法实践提供更为明确的裁判指引，避免在罪名适用过程中出现混淆与偏差。同时该路径亦有助于对现行刑法规范进行体系化的审视，确保其在应对新型数据安全风险时能够充分发挥应有的规制功能。综上，相较于广义说，狭义的数据犯罪概念更契合当前数据犯罪的实际样态，无论在理论建构层面抑或实践操作层面，均展现出更强的理论优势。

3. 数据犯罪的刑法规制现状及问题

3.1. 数据全流程保护的缺失

2019 年发布的《信息安全技术数据安全能力成熟度模型》将数据生存周期系统划分为六个环节，即数据采集、传输、存储、处理、交换与销毁[6]。2021 年施行的《中华人民共和国数据安全法》[7]则从宏观层面将数据生存周期统一概括为“数据处理活动”，并具体列举了涵盖收集、存储、使用、加工、传输、提供、公开等多个环节。由此可见，数据的利用并非单一行为，而是一个贯穿多个阶段、具有完整周期性的过程。在数据生命周期的各环节中，均潜藏着法益侵害的可能。然而，审视我国现行刑法对数据的保护不难发现，其规制重点主要集中于“获取”与“破坏”两类行为，对于数据生存周期中其他阶段可能出现的侵害行为，则呈现出规制不足、规范缺位的状态。以“魔蝎公司爬取数据案”为例，该公司在未获用户明确授权的情况下，将爬取所得的数据存储于其云端服务器[8]。该案在法律定性上引发较大争议，争议焦点集中于应认定为非法获取计算机信息系统数据罪，抑或构成侵犯公民个人信息罪。法院最终认定，本案存在非法获取计算机信息系统数据罪与侵犯公民个人信息罪的想象竞合关系，并以非法获取数据定性。然而，该裁判结论仍存疑点，其一，魔蝎公司的爬取行为在某种程度上已获得用户的默示同意，能否直接认定为“非法获取”有待商榷；其二，该公司行为的实质问题在于未经同意擅自存储数据，其违法性应更多体现于“非法存储”层面。再看“滴滴数据出境案”，滴滴公司为实现海外上市目的，将所收集的大量用户行程轨迹、个人信息等敏感数据擅自提供给境外机构。此类非法使用数据的行

[6]《信息安全技术 - 数据安全能力成熟度模型》(GB/T 37988-2019)。
[7]http://www.npc.gov.cn/npc/c2/c30834/202106/t20210610_311888.html.
[8]浙江省杭州市西湖区人民法院(2020)浙 0106 刑初 437 号刑事判决书。

为，不仅严重侵害用户隐私权益，更可能对国家数据安全构成潜在威胁，其危害程度甚至不亚于非法获取数据的行为。然而，该案最终仅以行政处罚结案，并未进入刑事追责程序。上述两起典型案例充分反映出，我国现行数据犯罪的刑法规制体系在数据存储、传输、处理等关键环节存在明显的制度盲区，难以实现对数据全生命周期的有效保护。

3.2. 数据犯罪构成要件模糊

数据犯罪与计算机系统犯罪之间存在着复杂的关联，二者在保护法益与构成要件要素的区分上，迄今尚未形成清晰统一的判断标准。在传统的立法模式下，数据能否纳入刑法规制，往往取决于其是否与计算机信息系统存在关联。具体而言，数据犯罪中的“数据”通常被限定为以计算机信息系统为载体的电子记录，未被系统存储的数据则被排除在规制范围之外。然而，随着信息技术的快速发展，数据存储方式已发生深刻变革。当前，大量新型数据可以存储于计算机系统之外的各类设备之中，例如蓝牙设备、移动终端等。对于此类数据的非法获取，实际与计算机系统的运行安全并无直接关联。但在司法实践中，却常将其与计算机系统数据混为一谈，导致数据本身缺乏独立、清晰的判断标准，这无疑为数据犯罪的准确认定带来较大困扰。同时，数据侵害与计算机系统侵害之间的界限亦较为模糊。在具体案件定性中，应适用非法获取数据犯罪的规定，抑或适用破坏计算机系统犯罪的条款，常常存在争议。例如，行为人采用技术手段获取数据的过程中，导致计算机系统出现短暂性功能迟滞，但并未造成系统不可逆的损坏，亦未实质破坏系统完整性。对于此类行为，究竟应评价为对数据的侵害，还是对计算机系统的侵害，目前尚缺乏明确的法律指引。此外，对于仅造成数据安全侵害，既未实际获取数据，亦未影响计算机功能正常运行的行为，如何作出准确定性，同样是亟待厘清的问题。

当前对数据犯罪后果的判断过度依赖计算机功能是否受到损害。在破坏计算机系统罪中，对于删除、修改数据等行为是否构成犯罪，其判断依据应立足于数据侵害的严重程度，抑或着眼于计算机系统功能的完整性，目前尚无定论。当删除、修改数据的行为并未对计算机系统安全构成实质威胁时，不宜忽视该行为对数据安全本身所造成的严重损害。然而，现行刑法对于单纯的修改、增加数据等行为，并未设置独立的规制条款，司法实践中往往倾向于将其向非法获取数据犯罪或破坏计算机系统犯罪的方向靠拢。但以计算机安全作为法益保护基础来解释此类行为的可罚性，在法理上尚显薄弱，难以实现对数据安全的全面、精准保护。

3.3. 数据犯罪定性存在争议

有学者对 100 份涉及破坏计算机系统罪的司法裁判文书进行梳理后发现，在司法实践中，控辩双方就罪名适用问题产生争议的案件多达 56 起[8]。相关争议主要集中在以下两个方面：其一，数据犯罪与传统犯罪之间在罪名适用上存在显著分歧。由于信息与数据在概念范畴上存在一定程度的交叉重叠，信息既可能是数据经过加工处理后形成的产物，亦可能直接等同于数据本身。当通过干扰数据的方式获取信息时，便容易引发数据犯罪与侵犯公民个人信息罪之间的适用争议。例如，非法获取考生学籍信息、非法删除个人违法犯罪记录等行为，本质上均系通过干扰数据的手段侵害公民个人信息权益，从而导致两类罪名适用上的选择困境。此外，数据还可借助技术手段转化为知识、财产或商业秘密等形态。这一转化特性使得数据犯罪与传统的知识产权犯罪、财产犯罪以及侵犯商业秘密罪之间，在罪名适用层面亦产生诸多争议。某些行为虽表面上针对数据实施，实则可能同时涉及对知识产权、财产权益或商业秘密的侵害，在此情形下如何准确界定罪名，成为实务中的难点。其二，数据犯罪与刑法所规定的其他计算机犯罪之间在罪名适用上也存在争议。以数据犯罪与非法侵入计算机信息系统罪为例，二者在客观行为要件上均包含非法侵入计算机信息系统的行为。然而，二者对所侵入系统的类型以及

所涉数据的具体要求存在明显差异。倘若行为人并非通过侵入计算机信息系统的方式，而是采取其他手段获取了国家核心数据或重要信息系统数据，则该行为既不符合非法侵入计算机信息系统罪所要求的行为方式，亦不满足非法获取计算机信息系统数据罪在对象方面的特定要件。在此情形下应如何适用罪名，有待进一步明确。

4. 数据犯罪的保护法益界定

4.1. 数据法益的适用现状

法益在立法与司法层面均发挥着关键性作用，其不仅是评判立法正当性的重要依据，也是解释刑法规范的核心指引，更是准确把握犯罪本质、科学开展定罪量刑工作的逻辑起点[9]。然而，当前理论界对于数据犯罪所侵害的法益究竟为何，尚未形成统一、明确的共识。数据本身具有多重属性，加之与数据犯罪相关的刑法规范呈现分散化特征，尚未形成完整、系统的制度体系。这一现状使得数据犯罪所侵害的法益难以获得清晰、精准的界定。从立法层面审视，一方面，如前所述，数据犯罪在形成初期以计算机信息系统安全法益作为规制对象。回顾《刑法》第 285 条的规定，早期对“计算机犯罪”的规制采取了混合模式，即同时兼顾计算机信息系统数据安全与数据本体。由此可见，数据犯罪在当时被置于“计算机犯罪”的框架之内，并未获得独立规制。尽管《刑法修正案(七)》[9]之后，第 285 条新增了非法获取数据等相关罪名，但数据犯罪仍未以单章、单节或单条的形式作出专门规定，仍受制于“计算机犯罪”的制度框架，未能实现对数据的独立保护。此种立法安排导致数据与计算机信息系统相互交织，进而使得数据犯罪法益的解释难以脱离既有体系而独立展开。与此同时，司法解释亦未能及时对数据犯罪所侵害的法益作出明确阐释。例如，《计算机安全解释》[10]仍以计算机信息系统为核心，仅通过扩张“计算机信息系统安全”法益的外延，来涵摄当前出现的各类针对数据的犯罪行为。此外，司法解释未能结合数据犯罪所侵害的法益对其构成要件进行细化说明，致使法益的解释功能未能充分发挥，数据犯罪的规制呈现明显的滞后性。另一方面，法益虽具备区分此罪与彼罪的重要功能，但在司法适用中却出现严重失位，导致数据犯罪的定性争议频发。从立法层面观之，现有数据犯罪规制体系存在制度缺陷，使得数据犯罪法益的内涵呈现多元化趋向。从既有司法实践来看，某一罪名出现“口袋化”倾向，往往源于刑法对该罪名的立法保护存在漏洞，现行规范难以对其进行全面、准确的覆盖。当前刑法在规制数据犯罪时，存在行为方式、处罚范围等方面的制度空白。然而，基于刑法谦抑性原则及维护法律稳定性的考量，不宜随意启动修法程序或增设新罪，而只能在既有规范框架内进行解释性适用。从司法层面观之，实践中司法人员往往倾向于对数据进行技术性判断，而忽视对其法律属性的实质把握[10]。由于技术性判断相对便捷，凡涉及数据的犯罪行为，司法实践中常未经充分的法律评价而径直认定为数据犯罪。此种做法既不利于对数据犯罪的精准定性，也在一定程度上影响了司法裁判的公正性与权威性。

4.2. 对现有数据法益理论的评价

当前，我国刑法对数据犯罪的规制仍主要依托于计算机信息系统安全的相关规范，集中体现于《刑法》第 285 条[11]与第 286 条所设定的计算机犯罪条款。学界普遍认为，上述条文以计算机信息系统安全为保护法益[11]，据此，部分学者主张将计算机信息系统安全作为数据犯罪的核心法益[12]。然而，伴随信息技术的飞速发展，计算机信息系统安全这一概念已难以完整涵盖数据安全的丰富内涵。在我国计算机犯罪立法之初，计算机系统主要以个人电脑为载体。随着智能手机、平板电脑等新型移动终端的普及，

[9]http://www.npc.gov.cn/zgrdw/npc/xinwen/lfgz/zxfl/2009-02/28/content_1476574.htm.
[10]同脚注 4。
[11]https://flk.npc.gov.cn/detail2.html?MmMwMDlmZGUtYWQzOS00Zjg5LWI4NzUtNzA4ZTA4YzFmZjUw.

司法解释对“计算机系统”作出扩张解释，将其界定为“具备自动处理数据功能的系统”。由此可见，计算机系统的本质在于具备数据存储、处理与传输能力，保护“计算机信息系统安全”的核心目标在于维持系统对数据的上述功能，保障其安全稳定运行，从而确保计算机能够被正常使用[6]。如前所述，数据除作为计算机信息系统的构成要素外，本身亦具有独立价值。若简单将计算机信息系统安全等同于数据犯罪的保护法益，实质上是将数据降格为计算机信息系统的附属物[4]。随着云技术的兴起，数据已可脱离特定计算机信息系统而独立存在，侵害数据安全的手段亦发生深刻变革。传统模式下，破坏数据往往需以侵入特定计算机系统为前提，而如今行为人可直接绕过系统对数据实施侵害。此外，以计算机信息系统安全作为数据犯罪的法益，易引发对犯罪对象的认识偏差。我国《刑法》第 285 条与第 286 条所规定的数据犯罪对象，被限定于“计算机信息系统内的数据”，即以计算机信息系统对数据范围作出前置性限定，将电子数据与其他形式的数据相区分，侧重于对电子数据的保护。值得注意的是，《刑法》第 286 条第 2 款对侵害数据行为的规定，并未要求该行为对计算机信息系统造成危险。由此可见，刑法在规范层面已对数据犯罪与计算机犯罪作出区分。若仍将数据犯罪纳入计算机犯罪的框架，此种立法安排将导致司法实践中不断扩张计算机信息系统的内涵，进而使数据犯罪面临“口袋化”风险。再者，以计算机信息系统安全法益为中心的保护模式，难以实现对数据安全的全流程覆盖。当前模式更侧重于静态防护，而数据犯罪的规制理应从数据的全生命周期出发，涵盖收集、存储、处理、利用等各环节。《刑法》第 286 条将删除、修改数据等行为入罪的标准设定为“危害计算机信息系统安全运行”，这一标准在一定程度上抬高了数据犯罪的入罪门槛，不利于对数据安全的充分保护。

此外，部分学者主张数据犯罪侵害的法益属于秩序法益范畴，认为数据安全本质上是公共秩序与社会管理秩序层面的安全。这一观点源于学界的普遍认知，即计算机犯罪主要侵害的是计算机系统数据安全运行的管理秩序以及网络安全管理秩序[13]。然而，数据秩序法益论存在诸多缺陷。从法益属性观之，具有公共秩序意涵的数据安全管理秩序属于整体性安全范畴，其并不直接指向个体信息权益，在法益类型上体现出社会公共法益与个人法益之间的显著差异[14]。数据安全管理秩序法益本质上是一种超个人法益，难以还原为具体的个人法益，因而无法充分发挥法益在立法批判与司法指引层面的应有功能。从秩序法益的内在特性来看，其具有较大的变动性与模糊性，内涵相对抽象。由于缺乏清晰界定，难以据此准确设定数据犯罪的入罪标准。在罪名区分方面，亦无法明晰界分计算机系统犯罪各罪名之间的法益内容，以及计算机系统犯罪与纯正网络犯罪、无线电犯罪之间的法益边界。此种模糊性易导致数据犯罪入罪标准的不确定性，司法实践中甚至出现将与数据安全无直接关联的转发次数、评论次数、点击次数等指标，作为判定数据犯罪入罪依据的不合理现象[15]。

4.3. 数据安全法益论的证成

杨志琼教授指出，将“计算机系统安全法益”作为数据犯罪的保护法益存在不合理之处，并在此基础上进一步提出，数据犯罪的保护法益应为数据安全法益。该法益的核心内涵涵盖数据的保密性、完整性、可用性，即通常所称的 CIA [4]。具体而言，数据的保密性旨在禁止未经授权者对数据内容进行访问、读取等操作，防止数据向非授权用户泄露，确保数据仅可为授权主体所知悉，其内容仅对授权主体公开。数据的完整性要求数据不受篡改或破坏，包括通过破解加密算法实施的数据劫持、修改以及数据欺骗攻击等行为。数据的可用性则主要涉及数据的使用权益，重点保障数据的服务与使用功能，对其侵害将干扰用户对数据网站的正常访问。于志刚博士与李源粒博士亦认为，数据犯罪的保护法益不应再局限于计算机系统安全，而应将关注重心置于数据本体。数据兼具人格属性与财产属性，对其保护法益的认定，应基于数据自身的内容、使用价值及侵害风险，展开独立的规范评价[16]。从国际立法层面来看，许多国家早已将数据安全作为独立对象加以保护。例如，欧盟《网络犯罪公约》第 3 条与第 4 条明确规定，该

公约旨在通过对数据保密性、完整性及可用性的保护，实现对网络犯罪的打击[17]。德国于 2007 年通过《为打击计算机犯罪的〈德国刑法典〉第 41 修正案》，增设了第 202a 条“获取数据罪”、第 202b 条“拦截数据罪”、第 202c 条“准备拦截数据罪”以及第 303a 条“变更数据罪”，奥地利刑法亦规定了滥用性数据截留罪、破坏数据罪等相关罪名[18]。

数据安全深深植根于社会生活的实践土壤之中。伴随信息技术的持续演进，数字经济时代已然来临，数据安全所蕴含的价值与日俱增。维护数据安全意义重大，不仅关乎国家与社会的稳定有序发展，亦是保障数字经济平稳运行的关键所在。数据源于社会生活实践，对生产生活具有积极的推动作用。为切实保障数据安全，我国相继出台了《网络安全法》《数据安全法》等一系列法律法规，构建起数据治理的制度框架。与此同时，数据安全亦面临现实侵害风险。随着计算机网络技术迈入大数据与人工智能时代，针对数据安全的侵犯行为所引发的法益损害后果日益复杂且难以控制。如前所述，数据的生存周期可划分为多个阶段，不同阶段的数据遭受侵害虽可能产生差异化的法律后果，但本质上均指向对数据安全的破坏。在当前时代背景下，数据安全极易受到不法侵害，无论是通过计算机信息系统对数据实施的不法操作，还是直接针对数据本体展开的攻击行为，抑或是对数据流转各环节的干预，均可能导致数据安全受损。最后，数据安全契合宪法价值，并在刑法现有规范体系中有所体现。前文在探讨数据犯罪时已多次提及，我国刑法对数据安全作出了明确规定。依据《刑法》第 285 条与第 286 条可知，数据安全已被纳入刑法保护范畴。同时，数据安全这一概念与宪法价值具有内在一致性。宪法作为根本大法，是制定其他法律规范的基本准则，将数据安全确立为刑法法益，并不违背宪法所设定的价值秩序。

数据安全法益应当作为单一法益予以独立保护。该法益的确立顺应了时代发展的客观需求。在互联网发展初期，计算机信息系统安全法益尚能涵盖数据安全的相关内容。然而，时至今日，数据的利用方式已逐渐摆脱对计算机系统的依赖，数据的存储与收集不再局限于计算机信息系统范畴。侵害计算机信息系统的行为与侵害数据安全的行为，二者并非必然同时发生。从数据自身所具备的价值属性来看，对数据法益进行独立保护具有重要现实意义。它不仅关涉个人隐私与企业生产经营活动，还与社会稳定、国防安全等重大利益紧密相连。复合法益论主张依据行为对象划分数据犯罪所侵犯的法益，此种观点虽看似周全，但容易导致数据犯罪法益的定位趋于模糊，难以充分发挥法益应有的功能。相较之下，对数据安全法益进行独立保护，能够更好地发挥法益的解释功能。通过对数据犯罪构成要件的细致阐释，可以有效解决数据犯罪与其他犯罪的区分问题，以及数据犯罪内部不同罪名之间的界限问题。例如，对于通过修改计算机信息系统数据以实现自动弹窗获利的行为，若该行为并未对计算机信息系统数据造成实质危害，则应在破坏计算机信息系统数据罪与非法控制计算机信息系统罪之间作出准确定性。若缺乏对数据安全法益的独立保护，容易陷入行为定性不明的困境。而在数据安全法益独立保护的视角下，该行为并未侵犯数据安全，仅系通过不当增加数据实现非法弹窗目的，应认定为非法控制计算机信息系统罪。在秉持数据安全法益独立保护的理念下，对于行为的入罪与出罪判断，应以是否对数据安全造成实质性侵害为标准，从而有效避免数据犯罪适用范围被过度泛化。

5. 数据犯罪的刑法规制

5.1. 确立数据安全法益的独立保护地位

欧盟《网络犯罪公约》针对侵害计算机系统与数据的行为分别设置了不同的罪名，充分体现了对计算机系统与数据实行分别独立保护的立法理念[19]。在科技持续进步的背景下，大量网络数据已可脱离计算机系统终端而独立存在。若仍以计算机系统作为界定数据范围的基本参照，将使数据概念的内涵趋于狭隘，难以适应大数据时代数据类型丰富多元、结构复杂程度较高的现实特征。换言之，在大数据时代，“计算机信息系统的储存、加工或传送”这一表述已无法精准涵盖数据概念的应有外延[20]。基于此，我

国刑法在立法层面应摒弃这一概念限制，不再将数据视为计算机信息系统的附属物，而应将数据概念从计算机信息系统的范畴中剥离出来[21]。在以计算机信息系统为核心的传统保护模式下，数据概念不仅范围狭窄，且较为抽象。因此，有必要明确将数据安全法益确立为数据犯罪的保护法益，使数据安全不再依附于计算机信息系统。

要确立数据安全法益的独立地位，首要任务在于立法层面区分数据犯罪与计算机犯罪、数据犯罪与信息犯罪。这要求对数据的概念内涵作出清晰界定，将数据与计算机信息系统及信息加以区分，准确把握数据犯罪行为的本质，从而降低刑法规定的不确定性，合理划定刑法的调整范围。具体而言，建议将《刑法》第 285 条与第 286 条中“非法获取计算机信息系统数据”及“破坏计算机信息系统数据”的罪名表述进行修改，删除“计算机信息系统”这一限定前缀，并将二者整合为“危害数据安全罪”，使数据摆脱对计算机系统的依附关系。同时，可将非法控制计算机信息系统与破坏计算机信息系统的行为，统一归入“危害计算机信息系统罪”罪名之下进行规制，实现刑法规范中“数据”与“计算机信息系统”的分离，进而达成对计算机系统与数据分别独立保护的目标。

5.2. 完善数据的全过程保护

综合前文所述，数据的生命周期可划分为采集、传输、存储、处理、交换及销毁六个阶段。在我国现行刑法框架下，数据犯罪的规制重点主要集中于“非法获取”与“破坏”两类行为，而对数据生命周期中其他环节的危害行为，规制力度明显不足。当前，我国尚未构建起覆盖数据全流程的完备法律保护体系，难以实现对数据犯罪行为的精准打击，进而使数据安全法益无法得到全面、有效的保障。有观点认为，数据犯罪刑法规制的核心不应局限于行为本身，而应聚焦于数据内容安全。换言之，对数据犯罪的规制，并非仅因其手段不合法，而在于其对数据内容安全造成了侵害[22]。然而，数据获取手段的不合法性，在一定程度上亦可反映数据来源的非法性。因此，以数据处理手段的合法性作为认定数据犯罪的依据，并非全无道理。在当前形势下，仍需以数据安全法益为核心，明确界定数据犯罪的手段行为，以实现对数据犯罪的全方位打击。鉴于我国刑法在数据犯罪全流程保护方面存在制度空白，从立法论视角出发，有必要适当增设罪名，以填补数据安全全流程保护的漏洞。具体而言，可将非法持有数据行为纳入数据犯罪范畴。该类行为是指行为人在合法获取数据后持续持有，超过授权期限且应销毁数据时仍拒绝销毁的情形。此外，非法访问行为亦应纳入刑法规制范围。非法访问是指行为人未经授权或超越授权范围浏览数据的行为[23]。此类行为虽在侵入计算机信息系统后未对数据实施破坏或盗取，计算机系统及内部数据亦未遭受物理性损害，但因行为人实施了非法浏览与复制数据的行为，已对数据的保密性构成侵害，理应受到刑法规制。再者，妨害数据正常利用的行为亦应被认定为数据犯罪。实践表明，数据犯罪中存在大量仅破坏数据而未破坏计算机信息系统的情形。若仅以破坏计算机信息系统罪对此类行为进行规制，显然不够妥当。同时，破坏计算机信息系统罪中关于数据保护的条款，仅规定了删除、修改与增加数据三种行为类型。然而，采用信号屏蔽等手段致使数据无法正常解码、数据系统无法正常运行的行为，同样会对数据安全造成实质性侵害。

参考文献

[1] 洪延青. 我国数据安全法的体系逻辑与实施优化[J]. 法学杂志, 2023, 44(2): 38-53.

[2] 高铭暄, 马克昌. 刑法学(2011) [M]. 北京: 北京大学出版社, 2011: 536.

[3] 张勇. 数据安全分类分级的刑法保护[J]. 法治研究, 2021, 135(3): 17-27.

[4] 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(6): 151-171.

[5] 马荣春, 宋相呈. 网络犯罪的类型描述、概念关系与立法完善[J]. 政法学刊, 2022, 39(1): 11-18.

[6] 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(2): 27-36.

[7] 付玉明. 数字足迹的规范属性与刑事治理[J]. 中国刑事法杂志, 2023(1): 125-141.

[8] 周立波. 破坏计算机信息系统罪司法实践分析与刑法规范调适——基于 100 个司法判例的实证考察[J]. 法治研究, 2018(4): 67-76.

[9] 夏伟. 对法益批判立法功能的反思与确认[J]. 政治与法律, 2020(7): 18-30.

[10] 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(6): 163-17.

[11] 高铭暄. 中华人民共和国刑法的孕育诞生和发展完善[M]. 北京: 北京大学出版社, 2012: 513.

[12] 王作富. 刑法分则实务研究(中) [M]. 第 5 版. 北京: 中国方正出版社, 2013: 1075.

[13] 高铭暄, 马克昌. 刑法学[M]. 北京: 北京大学出版社, 高等教育出版社, 2022: 539.

[14] 敬力嘉. 大数据环境下侵犯公民个人信息罪法益的应然转向[J]. 法学评论, 2018, 36(2): 116-127.

[15] 熊波. 网络违法信息传播次数作为入罪标准的困境与出路——基于 186 份刑事裁判文书和相关司法解释的思考[J]. 新闻与传播研究, 2020, 27(10): 77-94+127-128.

[16] 于志刚, 李源粒. 大数据时代数据犯罪的类型化与制裁思路[J]. 政治与法律, 2016(9): 13-29.

[17] 孙道萃. 网络刑法知识转型与立法回应[J]. 现代法学, 2017, 39(1): 117-131.

[18] 张婷. 互联网时代德国实体刑法[J]. 武汉公安干部学院学报, 2017, 31(2): 59-65.

[19] 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.

[20] 贾斯瑶, 郭旨龙. 数据犯罪刑事治理的新思路——以流量造假行为为切入点[J]. 中国检察官, 2022(7): 29-33.

[21] 冯卫国, 李婷. 论大数据和信息犯罪及刑法规制[J]. 犯罪与改造研究, 2020(10): 14-20.

[22] 童德华, 王一冰. 数据犯罪的保护法益新论——“数据内容的保密性和效用性”的证成与展开[J]. 大连理工大学学报(社会科学版), 2023, 44(3): 54-64.

[23] 蔡士林. “深度伪造”的技术逻辑与法律变革[J]. 政法论丛, 2020(3): 131-140.