Dispute Settlement 争议解决, 2026, 12(7), 127-132
Published Online July 2026 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2026.127222

Hans汉斯

数据破坏型网络犯罪中“数据”范围的认定

金　晨

中国政法大学中欧法学院，北京

收稿日期：2026年6月17日；录用日期：2026年7月12日；发布日期：2026年7月21日

摘　要

由于《刑法》第二百八十六条第二款对“数据”范围缺乏明确界定，数据破坏型网络犯罪的司法适用面临罪质认定不清与同案不同判的困境。双重法益说通过区分系统安全法益与数据法益，明确该款所保护的数据法益兼具公共秩序属性与技术属性，从而为“数据”范围的界定提供规范基础。本文主张，第二款中的“数据”应限定为承载公共信任或具有社会价值的非功能性数据，原则上排除纯粹私人数据，同时将虽属个人数据但足以影响社会信任的数据纳入保护范围。为破解司法适用困境，应以数据法益的社会信任功能为指引，区分功能数据与一般数据，细化“后果严重”的判断标准，并结合数据的技术属性与规范属性构建第二款“数据”范围的认定框架，以实现本款适用的明确性与适度性。

关键词

破坏计算机信息系统罪，数据法益，数据利益，非功能性数据

Determination of the Scope of “Data” in Data-Destructive Cybercrimes

Chen Jin

China-EU School of Law, China University of Political Science and Law, Beijing

Received: June 17, 2026; accepted: July 12, 2026; published: July 21, 2026

Abstract

The ambiguous definition of “data” in Article 286 (2) of the *Criminal Law* of China has led to challenges in judicial application, including unclear offense classification and inconsistent rulings in similar cases. Grounded in the dual legal interest theory, the legal interest of data embodies both public order and technical dimensions, necessitating a shift from traditional static protection to recognizing the dynamic value of data in network interactions. This theory distinguishes system security from data-related legal interests, providing a normative foundation for defining the scope

文章引用: 金晨. 数据破坏型网络犯罪中“数据”范围的认定[J]. 争议解决, 2026, 12(7): 127-132.
DOI: 10.12677/ds.2026.127222

of "data". This article argues that the determination of "data" should focus on non-functional data that carries public trust or social value, excluding purely private data while including personal data that impacts social trust, thereby ensuring comprehensive protection. To address judicial challenges, the social trust function of data-related legal interests should guide the differentiation between functional and general data, with a quantified standard for serious consequences. By integrating technical and normative attributes, the scope of "data" under Article 286 (2) can be defined to achieve clarity and appropriateness in applying the offense.

Keywords

Crime of Disrupting Computer Information Systems, Data-Related Legal Interest, Data Interest, Non-Functional Data

1. 数据破坏型网络犯罪的"数据"界定困境

《中华人民共和国刑法》[1](以下简称《刑法》)第二百八十六条第二款对删除、修改、增加信息系统中的数据的非法行为，以破坏计算机信息系统罪予以规制。然而，由于"数据"范围界定模糊，司法适用中面临罪质模糊、同案不同判的问题。不同于第一款强调"造成计算机信息系统不能正常运行"的结果要件，第二款聚焦对数据对象的直接侵害，凸显数据在网络空间的独立保护价值。有学者指出，第二款适用偏差源于仅对构成要件作形式而非实质的解释[1]。例如，对于干扰信息系统并获得对数据控制权，但未影响系统正常运行的非法行为，刑事司法存在认定困难，忽视了数据在网络空间社会交互中的作用，又将不具有可罚违法性的行为错误认定为犯罪，偏离罪质。此外，由于数据犯罪和传统犯罪数据化的界限模糊，掩盖了数据本体的重要价值。厘清本款"数据"的范围不仅有助于明确数据在数据犯罪体系的刑法保护价值，还对界定数据犯罪与传统犯罪具有价值。因此，准确认定本款"数据"的范围是破解司法适用困境的关键。

1.1. 数据界定的规范困境

明确"数据"范围是本罪适用的逻辑起点。现行规范多作广义界定。《中华人民共和国数据安全法》[2](以下简称《数据安全法》)第三条对"数据"采取了最广义的定义，涵盖任何以电子或者其他方式对信息的记录。数据犯罪的"数据"事实上能够涵盖所有能以代码形式储存于计算机信息系统中的权利客体[2]。广义定义虽然便于涵盖多样化数据形式，但因缺乏具体标准难以满足刑事细致化、精准化保护的需求。数据的多维属性伴随技术更新，使得单一定义难以精准回应数据在"双层社会"的独立价值，无法为数据法益保护提供具体明晰的指导。

1.2. 数据认定的理论分歧

数据不仅是信息的载体，更因其独立性、非消耗性及增值效应，具备成为独立法益的意义。数据因保密性、可用性以及在流通中的利用价值，相较于计算机系统，具备独特的属性和独立地位。关于本款"数据"的对象范围，主要存在限缩论与扩张论两种理论观点。限缩论关注数据的规范属性，强调罪刑

[1]http://www.npc.gov.cn/npc/c1773/c1848/c21114/c25714/c25716/201905/t20190522_46193.html
[2]http://www.npc.gov.cn/npc/c2/c30834/202106/t20210610_311888.html

法定原则下的明确性与适度性；扩张论则聚焦技术属性，主张顺应数字化技术发展扩展保护范围。

1.2.1. “数据”范围限缩论

限缩论侧重规范属性，认为“数据”未被立法预设限制性条件，数据犯罪与关联罪名交叉重合，甚至溢出了整部刑法典[3]。因此，应当对“数据”予以限缩解释，以技术价值为标准，将第二百八十六条第二款中的数据限定为“计算机信息系统功能”的系统数据，而非一般数据，即与计算机信息系统功能运行无关的数据不能成为本罪的对象[4]。此外，有学者基于数据分级分类，提出将值得刑法保护的数据限定为《数据安全法》特别保护的重要数据或公共数据[5]，以实现精准规制。

1.2.2. “数据”范围扩张论

扩张论则聚焦技术属性，扩张论则强调数字技术网络化、云端化趋势已突破传统计算机系统的边界，数据存储不再局限于本地服务器，传统单一计算机系统已难以涵盖所有数据存在的空间。由此，“数据”不应局限于计算机系统内的数据，扩张论提出以下解释路径：一是不考虑对数据的规范价值施加限制，从而允许刑法制裁非法获取或破坏全部电子数据的行为[6]；二是倡导以网络数据替代计算机信息系统数据，成为数据犯罪的保护对象，从以系统技术安全为核心的保护思路向数据独立保护理念转变[7]。

1.2.3. 技术与规范属性的平衡

技术化用语、规范化用语需要进行规范性、技术性转化，“确保代码架构的设定合乎现有法秩序的价值设定”[8]。从罪状来看，删除、修改、增加数据的危害行为均属于技术行为，受限于技术架构，法律无法脱离技术架构实现对技术的规制[9]。限缩论与扩张论各执一端，但数据的技术属性与规范属性之间本是共存状态[10]。因此，数据的界定应当在技术价值与规范价值间寻求平衡。数据作为技术迭代的产物，刑法的保护范围难以避免地伴随着数字化技术的发展而扩大保护。随着对“计算机信息系统”外延拓展至所有具备自动处理数据，扩张论的解释路径可能在一定程度上已被现有规范所吸收，限缩论强调的数据技术意义在社会交互中也不断呈现出新价值。基于此，应当综合考量数据的功能性、社会性与法益保护需求，从双重视角诠释“数据”的内涵，实现技术属性与规范属性的有机结合。

2. 破坏计算机信息系统罪的数据法益建构

2.1. 破坏计算机信息系统罪的法益定位

“数据”范围扩张说与限制说的分歧不仅体现在条款适用范围上，更深层次地反映了对保护法益本质的不同理解。学界对本条款保护的法益主要有三种观点：法益秩序说、计算机信息系统安全说与双重法益说[11]。

秩序法益说试图将数据犯罪纳入“秩序犯罪”的传统刑法保护框架，主张本罪保护的对象是国家对计算机信息系统的管理秩序或社会公共秩序。然而，秩序法益在界定刑法保护对象时显得过于抽象，未能反映计算机犯罪保护法益的具体性和明确性([12], p. 217)，容易导致处罚范围不清。

计算机信息系统安全说认为，本罪三款统一保护计算机信息系统的安全，以“系统正常运行”为违法性评价标准。该说虽更具司法可操作性，程序日志、数据变更痕迹、恢复难度等技术指标加以确认，并通过证据链技术认定“数据完整性”。然而计算机信息系统安全法益并不完全符合数据犯罪的技术实质和保护需求[2]该观点的单一法益立场存在两方面的局限：其一，将导致本罪第二款删除、修改数据行为与第一款语义重复；其二，忽视了数据本身作为独立法益地位，致使“未影响系统功能但严重损害数据利益”的新型犯罪(如流量劫持、域名劫持等)难以入罪，削弱了本罪的适应性。

双重法益说主张第一款、第三款保护系统安全，第二款保护数据的独立法益，包括数据的保密性、完整性、可用性，亦有学者提出“数据控制利益”，强调数据本身的价值性[13]。相较而言，该说在体系

解释上更具说服力。第三款并未将“造成计算机信息系统不能正常运行”作为结果要件，其规范重心在于规制对数据实施删除、修改或者增加的行为。若将系统功能受损作为第三款成立的必要条件，将不当限缩该款的保护范围。基于此，双重法益说更加契合规范定位，并为“数据”范围的界定提供法益基础。

2.2. 数据法益的双重属性

一方面，数据法益具有公共秩序属性。随着 Web3.0 时代的到来，网络与现实相结合形成“双层社会”，社会成员交往活动依赖信息数字化处理并以数据形式传播。数据不仅是信息交流载体，更承载了社会成员对网络沟通安全性的信任。这种信任表现为对数据的内容完整、价值可用产生诉求，构成了网络空间公共秩序的核心。网络系统运作原理与算法黑箱却并未被多数人理解掌握，社会成员对基于数据的沟通安全性的稳定预期构成网络空间的公共秩序体系。稳定的信任预期是社会交往得以持续展开的重要基础。如同刑法惩治伪造货币以维系金融信任，同样，网络社会数据安全、数据控制权同样承载着社会共同利益与公众的信任，这也契合将本罪置于“扰乱公共秩序罪”一节的逻辑。

另一方面，数据的法益属性根植于自身的技术特性。数据犯罪保护的法益经历了从附属法益逐步走向独立法益的转变过程，早期刑法仅将数据视为系统的附属客体和传统权利的间接载体([12], p. 112)，附属性保护模式削弱了其安全利益与流通利益。随着云技术发展，数据的非消耗性、增值效应与可复制性赋予数据独立的价值，催生了以数据安全为核心的法益保护需求[2]。要求刑法保护从系统导向转向数据导向，而网络空间的秩序问题也恰恰表现为对系统和数据的信任结构。数据的保密性、完整性与可用性不仅是技术指标，更是法益保护的核心维度。例如，非法删除关键数据虽未影响系统的正常使用，却破坏了数据形成的普遍性信任。

3. 数据破坏型网络犯罪的“数据”界定框架

3.1. 数据法益的多维构造

前文通过法益分析确立了数据安全的独立地位，强调公共秩序属性与技术属性的双重属性。在双重法益说的理论指引下，数据法益的构造需结合技术特性与社会功能，超越传统数据安全的静态保护模式，融入数据在数字经济与网络交互中的动态利用价值。传统的“数据安全”法益观侧重消极防御，强调数据的专有性和排他性，数据的保密性、完整性、可用性(CIA 原则)构成数据安全法益的技术基础[14]，维护数据作为信息载体的静态安全，保障数据能够被安全及时地获取，以确保从数据自身内容、使用价值和侵害风险等角度对数据犯罪进行独立规范评价。然而，静态保护模式难以应对数据动态利用过程中的多样化风险，无法实现刑法对数据双重价值的周延保护，未能充分体现数据在数字经济与社会交互中的增值价值与利用功能。随着数据的经济价值的上升，对数据权益的侵害不仅限于对数据系统的破坏或对数据的销毁，而逐渐转向对数据利用过程中的干预、操控和滥用行为。为适应数据犯罪的动态化趋势，保护数据流通中的利用法益的社会需求凸显。对此，有学者提出“消极预防 + 积极利用”观点，区分为“数据自身安全法益”与“数据利用安全法益”，强调前者侧重于静态保护，后者侧重于动态流转。数据利用法益不仅保障数据本身，更维系公众对数据社会秩序的信赖，构成了数据犯罪刑法保护的正当性基础。“利用法益”强调数据使用主体在使用过程中所应享有的权益，作为一项积极法益，旨在最大化实现其发挥生产要素的价值，过度强调数据安全层面的排他性与静态的防御，则与社会进步相悖[15]。

3.2. 数据破坏行为的罪名体系定位

本罪设置在第六章“扰乱社会公共秩序罪”一节，表明其保护法益的公共性。本节罪名如招摇撞骗罪、伪造国家机关公文罪，均以维护特定社会信任与公共秩序为目标，反映社会信任基础的公共权利。

第二款的数据安全的社会信任亦属此列，承载社会成员对数据真实性与可靠性的集体信任，由此区别于保护人格利益和财产利益等私法益，明确数据犯罪和传统犯罪数据化的区别。从体系安排上，第二百八十六条的三款规制不同侵害对象与行为样态，体现分别规制的逻辑。立法中曾考虑将本条拆分为“破坏计算机信息系统功能罪”“破坏计算机信息系统数据和应用程序罪”“故意制作、传播计算机病毒等破坏性程序罪”三个独立罪名的考虑。第一款聚焦“功能性破坏”，以“系统不能正常运行”为结果要件；第三款针对“破坏性程序”的制作与传播；第二款则以“删除、修改、增加数据”为行为要件，突出数据自身的侵害后果。为避免重复评价，第二款的保护对象应与功能性数据相区别，严格限定为不直接影响系统运行的非功能性数据。

3.3. 数据范围的规范标准

第二百八十六条第二款非法删除、修改、增加行为的直接对象是数据，本款适用效果直接依赖于“数据”的精准界定。最高人民法院指导性案例 145 号“张某杰案”将破坏计算机信息系统罪的保护对象界定为“有价值的数据”。具有重要价值的数据的价值体现在经济价值、使用价值等方面，其自身因利益重大、不可复制或者高度机密等特性而需要刑法介入保护[3]。从数据安全和社会信任法益出发，界定破坏计算机信息系统罪第二款中“数据”的范围，数据的价值性应当从数据的技术属性和公共秩序属性出发。

在技术属性角度，应当区分第二款与第一款、第三款保护对象的差异。应当准确区分“功能数据”与“一般数据”。第一款保护的“功能数据”指组成计算机系统正常运转的必要组成部分，诸如系统文件、程序代码和数据库文件。该部分数据受损会造成计算机系统崩溃、运行中断。例如陈丽、刘效实案中[16]，涉案人员修改服务器文件及门禁系统 IP 端口，导致会员系统和门禁系统故障，法院认定为构成本罪的第一款破坏行为。

第二款保护非系统组成的“一般数据”，例如删改交通违章记录、考生成绩、购物评价等数据并未对计算机信息系统功能的可用性造成妨害，但破坏了系统存储数据的圆满状态[17]。在公共秩序角度，第二款的“数据”应当承载社会成员的集体信任，涉及公共服务、社会管理或经济流通等领域，一旦破坏数据的真实性、完整性和可用性便对集体信任造成损害。社会成员依据系统用于决策的目标直接相关或价值共通，最终指向社会对数据安全的共同信任与决策质量降低。第二款通过保护一般数据，保证了数据保护类型的周延性，并以“后果严重”加以限制，唯有破坏非功能性数据在具有重大规范价值时，才能与另外两款功能性数据的社会危害性相当。

基于计算机信息系统数据罪的利益维度限定在集体利益与社会利益，第二款“数据”的范围原则上排除为单方主体占有支配、不与外界交互的私人数据。一方面，这类私人数据往往承载的人格利益，已受到传统私法益罪名的刑事保护，若双重规制将导致刑罚不当扩张。另一方面，私人数据往往因单一主体所控制而无意运用于网络社会的交互，不构成社会交互的决策依据，无谈对信任的损害，对此类数据的删除或修改不构成社会信任法益指导下第二百八十六条的适格行为对象。然而，需要注意的是，数字化数据不仅可为计算机系统物理性地识别，也可能被使用此系统的人社会化地识别，此时数据与背后的社会化性质产生了不可避免的重合[3]。不能简单将数据切割为“私人数据”与“非私人数据”，将私人数据“一刀切”排除出本罪的保护范围。对于影响网络社会成员决策依据的个人数据，也应当经由集体法益的保护路径，受一百八十六条第二款保护，例如修改填报系统中院校志愿，虽然属于个人数据，但涉及教育公平与社会信任，志愿数据系统承载共同信任，因此对于擅自修改志愿数据属于破坏计算机信息系统罪的保护范畴。

综上，《刑法》第二百八十六条第二款“数据”范围的规范界定，应以数据安全的社会信任法益为指引，聚焦具有公共性、价值性与技术性的非功能性数据，并强调维护数据在社会交互与决策依据中的核

心功能。前文通过双重法益说的论证，确立了数据安全作为独立法益的地位，强调其公共秩序属性与技术属性的有机融合。在此基础上，第二款“数据”应当限定为承载网络社会公共信任或社会价值的数据，排除纯粹的私人数据；同时对虽属个人数据但影响社会信任的数据予以纳入，体现保护范围的周延性。为破解司法实践中罪质模糊与同案不同判的困境，可以建构以下认定路径：首先，通过程序日志、数据变更痕迹等技术手段，区分功能数据与一般数据，将侵害功能数据的行为归入本条第一款规制，明确第二款针对非功能性数据的独立保护价值；其次，以数据是否承载公共信任或网络公共秩序为规范标准，排除私人数据。再次，“后果严重”标准，量化数据侵害对社会信任与经济秩序的影响程度；最后，结合技术属性与社会信任法益的规范评价，确保罪名适用的明确性与适度性，防止刑罚不当扩张。

4. 结语

准确认定《刑法》第二百八十六条第二款的“数据”范围，是破解相关犯罪司法适用困境的关键。在双重法益说的指引下，明晰“数据”兼具技术与公共秩序的双重属性，将其界定为承载公共信任或社会价值的非功能性数据。司法适用中，应当借助程序日志、数据变更痕迹等技术手段剥离功能数据，排除纯粹的私人数据，并结合“后果严重”标准量化社会危害，兼顾数据的静态防御与动态利用。面对云存储等技术挑战，未来仍需持续探索数据分类的量化标准，完善规范评价体系，以周延应对网络空间的复杂风险。

参考文献

[1] 王禹. 计算机信息系统犯罪的行为透视: 以“破坏”和“非法控制”的界限与竞合为视角[J]. 江西警察学院学报, 2019(2): 108-113.

[2] 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.

[3] 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.

[4] 阎二鹏. 干扰型破坏计算机信息系统罪的司法认定[J]. 中国刑事法杂志, 2022(3): 122-137.

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

[6] 田刚. 大数据安全视角下计算机数据刑法保护之反思[J]. 重庆邮电大学学报(社会科学版), 2015, 27(3): 30-38.

[7] 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, 23(1): 58-64.

[8] 劳东燕. 网络时代刑法体系的功能化走向[J]. 中国法律评论, 2020(2): 101-114.

[9] 李刚, 李涛. 非法控制计算机信息系统罪与破坏计算机信息系统罪之辨析——以短缩的二行为犯为视角[J]. 中国检察官, 2021(14): 38-41.

[10] 阎二鹏. “数据安全法益”命题下虚拟财产犯罪的归责路径重构[J]. 政治与法律, 2022(12): 45-59.

[11] 徐春成, 林腾龙. 教义学视角下破坏计算机信息系统罪的法益论辩[J]. 科技与法律(中英文), 2023(4): 21-31.

[12] 高仕银. 计算机犯罪规制中美比较研究——以美国联邦《计算机欺诈与滥用法》为核心的展开[M]. 北京: 中国社会科学出版社, 2021: 112, 217.

[13] 于润芝. 数据犯罪刑法规制的价值选择、法益定位及利益识别[J]. 河南财经政法大学学报, 2024, 39(6): 78-89+100.

[14] 张明楷. 破坏计算机信息系统罪的认定[N]. 中国法院报, 2022-03-03(5).

[15] 高富平. 个人信息保护: 从个人控制到社会控制[J]. 法学研究, 2018, 40(3): 84-101.

[16] 辽宁省阜新市中级人民法院. 刑事判决书: (2021)辽 09 刑终 165 号[Z]. https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=vU+wdezk-KID4dex9U0CZ2Fc12363if/hqALOY0MrSBwO3wiFylAc7p/dgBYosE2gu0q3tOffVE2D6LQ7ng5tkF-stGoAjFVZqRtJuQajdYIl62JW+e064nnSaeHa0/mVl, 2022-01-07.

[17] 叶小琴, 高彩云. 破坏计算机信息系统行为的刑法认定: 基于最高人民法院第 104 号指导性案例的展开[J]. 法律适用, 2020(14): 3-14.