DOI:10.20270/j.cnki.1674-117X.2026.5011

治理范式转换视角下数据爬取行为的刑法规制

曲天明，孙志

（青岛科技大学 法学院，山东 青岛　266061）

摘要：数据爬取行为的刑法规制面临司法裁判标准不一的困境，其根源在于将传统产权范式简单套用于数据治理实践。从数据的自然属性与价值属性来看，原始数据并不具备赋予产权保护的理论基础，应归入非产权治理范式之下。就非法获取计算机信息系统数据罪的入罪标准而言，应舍弃合约授权、身份认证机制所具有的刑事违法性判断功能，转而回归以技术措施为表征的实质法益侵害标准。对于承载个人法益、社会法益或国家法益的数据所实施的非法爬取行为，应优先适用既有传统刑法罪名予以评价。在非产权治理范式下，数据犯罪所保护的法益应重新界定为数据使用秩序安全，爬取行为之入罪应以严重阻碍数据持有者对数据的使用、处理或传输为实质要件。此外，衍生数据因尚未上升为法定财产权利，不宜纳入财产犯罪范畴，而应交由专门数据罪名调整。

关键词：非产权治理范式；数据爬取行为；入罪标准；非法获取计算机信息系统数据罪；数据使用秩序安全法益

中图分类号：D924.3　　**文献标志码**：A　　**文章编号**：1674-117X(2026)05-0092-09

数据爬取是数据要素流通的重要手段，其刑法规制问题是数据安全治理的重要议题之一。现有研究主要围绕数据爬取的法律定性与治理范式选择而展开。一方面，学者普遍关注数据产权化保护路径，形成绝对化赋权、二元权利结构、独立数据财产权等多元观点，强调通过明确产权归属来界定爬取行为边界，但对传统产权范式与数据特性的适配性问题关注不足。另一方面，对于非法获取计算机信息系统数据罪的入罪标准，有的学者主张以合约授权为判断依据[1]，有的学者将身份认证机制视为授权与否的关键[2]，还有的学者将技术措施的突破作为入罪标准[3-4]，但学者们对标准背后的实质法益侵害缺乏统一认知。此外，学界已经关注到数据爬取行为在罪名适用、入罪边界、财产犯罪认定等方面的司法困境[5-6]，但未深入剖析问题的根源在于治理范式的错位。针对数据非消耗性、非排他性、价值聚合性的特殊属性，传统产权治理范式导致的过度规制，与数字经济对数据流通共享的需求形成结构性矛盾。既有研究在数据犯罪领域多聚焦于入罪标准或具体罪名的解读，对治理范式转换与法益重构之间的逻辑关联缺乏深度分析，未能形成适配数据特性的刑法规制逻辑。

本文立足于数据的自然属性与价值属性，重点探讨以下问题：其一，数据治理为何需要从产权范式转向非产权范式；其二，非产权治理范式下数据爬取行为的入罪标准如何界定；其三，非产权治理范式下数据爬取行为的法益应当如何重构。通过剖析非产权治理范式与数据爬取刑法规制的适配逻辑，以期为破解司法裁判标准不统一困境、平衡数据安全与流通价值提供新的理论视角与实践参考。

收稿日期：2026-03-20

基金项目：山东省社会科学规划基金资助项目“L3 级别自动驾驶中不作为犯适用问题研究”（25CFXJ09）

作者简介：曲天明，女，山东蓬莱人，青岛科技大学教授，博士，研究方向为数据法学。

一、问题的提出

《中共中央关于制定国民经济和社会发展第十五个五年规划的建议》提出，“十五五”时期，中国将持续筑牢网络、数据、人工智能安全屏障，加强网络安全体制建设。爬取行为的刑法定性是近年来数据获取与安全保障的重要议题，在实践中颇具争议。爬虫技术是按既定规则，从一个或多个网站上扫描和提取特定结构化数据进行存储的技术手段[7]。调查显示，自动化爬虫机器人已占全球网页流量约30%，这一现象标志着传统人力驱动互联网使用模式已发生重大转变[8]。从数据治理角度看，爬虫技术以预先设定的自动程序抓取网络数据，该行为一定程度上能够促进数据的获取与市场化流动[9]。网络爬虫技术虽为中立，但网络爬虫行为却有善恶之分[10]，并非所有爬取行为都必然构成违法犯罪，对其法律评价不应一概而论。

针对数据爬取行为的刑法规制，当前存在三个方面的适用困境。首先，侵犯公民个人信息等传统信息犯罪与非法获取计算机信息系统数据罪的界分标准模糊，导致罪名适用混乱。在多起爬取数据案件中，对于性质相近的行为，有的法院适用传统信息类罪名定罪处罚（参见湖南省怀化市鹤城区人民法院（2019）湘1202刑初530号刑事判决书，北京市海淀区人民法院（2018）京0108刑初770号刑事判决书），有的法院则直接以非法获取计算机信息系统数据罪论处（参见江苏省常州市中级人民法院（2023）苏04刑终240号刑事裁定书，山东省青岛市中级人民法院（2020）鲁02刑终108号刑事裁定书）。其次，关于非法获取计算机信息系统数据罪的入罪标准，各地存在明显差别，犯罪界限的认定不清导致该罪弹性空间过大，使其沦为学界诟病的“口袋罪”。最后，涉及数据资产价值的案件，在认定为财产犯罪还是数据犯罪之间存在争议。上海市静安区人民法院审理的一起非法获取计算机信息系统数据罪案引起了广泛的讨论。该案中，对于“非法抓取1800余万条数据，商业价值高达1400余万元”中的数据性质，即究竟为原始数据还是衍生数据，法院并未阐述清楚（参见上海市静安区人民法院（2025）沪0106刑初89号刑事判决书）。实践中数据概念的使用是宽泛的，需要对其进行类型化确认，比如区分原始数据、衍生数据的属性差异，否则刑法对数据犯罪的规制便会沦为“无的之矢”。以上问题的有效解决，首先需要回应数据是否确权的争议，即数据应当遵循何种治理范式。

二、爬取规制的理论修正：从传统产权到非产权的治理范式转向

（一）数据的特殊性：不适用传统产权治理范式

数据是数字经济时代的主要生产要素，其社会化的重复性使用是当今数据流通的重要目标。促进数据流通需要保障获取数据的便利性，而获取数据的方式除原始数据的直接收集、数据交易之外，更为普遍的是依靠技术手段抓取数据。数据爬取法律边界的界定，首先需回应的问题是：数据是否应当受到法律保护，以及应当如何保护。当前，学界与实践中对数据保护的思路，大多将数据纳入传统产权治理范式之下，试图通过明确产权归属解决数据赋权问题。学界支持数据赋权的观点，大致分为三派：其一主张绝对化赋权，即将数据归为物权之中[11]；其二主张二元权利结构，用户享有数据所有权，平台享有“数据用益权”[12]；其三则主张将数据财产权确立为与物权、知识产权并列的第三类对世权[13]。显而易见，这三种观点虽在权利设定的路径上存在差异，但本质上均将数据纳入传统产权治理范式之下，试图通过明确产权归属解决数据赋权问题。但是，《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》（以下简称“数据二十条”）的规定并没有沿用传统产权思维，而是采用“生产—持有—使用”这一有别于数据所有权的治理范式[14]。

传统产权治理范式下数据产权认定的不足，首先表现在其忽视了数据的自然属性。《数据安全法》

第 3 条中规定，数据是“以电子或者其他方式对信息的记录”，其本质是以 1 与 0 为二进制所构成的计算机符号语言。数据以数字形式存在，具备非消耗性、累积性与非排他性。不同于有形货物，数据不会因使用而消耗或者减损其价值，反而会随着使用次数的增加而增益。数据可通过持续采集、存储而不断累积，最终形成规模效应。非排他性指某物一旦被创造出来，就很难排除他人对该物的使用。在合法的前提下，对于信息或知识而言，一旦被他人浏览或收受即被他人使用；而对于承载信息与知识的数据而言，一旦被访问或爬取，也可以被使用 [15]123。同一数据可被无数主体同时使用，不会因使用产生损耗，这与传统产权“一物一权”“排他使用”的基础理论完全相悖。其次，从价值属性看，原始数据本身无固有价值，其价值产生于场景化使用与多源汇聚的条件下。有学者指出，实践中对新兴事物的法律保护常关注其价值，但具有价值并非法律保护的充分条件，故更应关注其是否具有“稀缺性”。（参见《人工智能对独创性的影响》，郭禾在 2025 国际版权论坛的发言讲话）而笔者认为，原始数据是否具有固有价值本就存在商榷之处。单独数据片段往往并无保护意义，只有经整合、分析的数据才能释放价值 [16]。所有法律，都是为某种利益而生，离开利益，就没有法的观念的存在 [17]。由此，将无固有价值的数据产权化实属不妥。最后，传统产权范式下，静态客体的排他权无法满足数据动态赋权的需求。现实中，大量的数据掌握于数据巨头手中，而当小微企业创新出智能模型需要投喂数据时，数据巨头会凭借数据垄断优势对其进行阻挠与打压 [18]。数据使用具有非竞争性和可分享性，赋予任何单一主体长期稳定的产权，保护其对数据的支配利益既不必要，也不利于数据价值的实现 [15]128。数据只有在流通中才能释放价值，若强行套用产权范式，会陷入数据垄断与价值梗阻的困境，即企业为维护数据所有权而设置壁垒，阻碍数据流通与复用，最终抑制数字经济的创新活力。

（二）理论协调性：非产权治理范式的逻辑基础

数据由社会成员可自由使用的资源演变为一种经济资源，需要法律介入确立其流通利用秩序，在保护数据承载的并存利益前提下，实现数据资源的有效利用。在这一视角下，“爬”与“反爬”是数据无序且低效的利用状态，其不利于数据的权益保护和社会公共利益的维护。数据重用亟待走出当前缺乏明确规范的粗放模式。为解决数据可获取与有效供给的现实难题，应当在尊重数据持有者合法权益与合理贡献的基础上，建立有效的激励机制，引导其主动向社会分享或提供数据，使数据在有序流通中实现持续增值，真正释放数据要素的应有价值。但是，法律又不能赋予数据持有者以排他支配权，这是因为数据具有社会性，我们需要保护数据使用者的利益。如果像物权法规则那样，基于先占或加工使用而赋予排他性数据产权，在先使用者就会妨碍其他使用者获取和使用数据的权利。针对这一问题，有学者提出的“权利束”观点存在一定合理性。所谓“权利束”是将财产权去“物”化改造，成为一束没有核心、可随意抽取的“权利束”[19]。在数据资产的“权利束”上存在“个人信息利益”“数据处理者经济财产利益”“社会公共秩序及国家安全利益”等多元法益 [20]。

数据作为客观世界的映射，承载着数据主体、物主、组织乃至社会、国家的多元利益，其获取与使用并非单纯的财产交易，而是涉及公共福祉与社会秩序的复杂活动。公共数据的开放利用关乎社会治理效率，个人数据的流通涉及隐私与发展的平衡，其中利益的平衡无法通过传统产权的私权自治实现协调。作为认知世界、生产知识的媒介，数据与公民的信息自由、社会文明进步绑定在一起。信息自由是个人独立自由的基础，数据的社会化复用是知识生产的源泉。互联网与人工智能时代，数据虽存放于网络端，但无损于我们对其应归属社会共享的基本认知——数据的价值在于流通，而非独占。

（三）实践适配性：治理范式的运行验证

数据治理范式的落地有赖于完整的数据基础制度体系，该制度一方面需要通过权利配置激励数据持有者对外供给数据，另一方面需要保障数据使用者的权益获取。实现该制度的设计目标在于承认和维护数据持有者的使用权。数据持有者的使用权不具有排他性，每个合法获取数据并进行加工使用的主体均

享有独立的数据使用权。治理范式以类型化的权利配置为核心。数据从原始获取到知识生产的过程中，价值形态不断演进：原始数据强调开放获取，加工后的数据侧重流通治理，知识产品则需要产权激励。治理范式通过赋予不同环节的主体，即初始生产者、加工者、产品生产者差异化权利，实现价值创造与利益分配的动态匹配。例如，数据加工者可获得流通使用权，数据产品生产者可通过知识产权实现权利保障，这种差异化的权利配置既避免了一权到底的僵化模式，又保障了各环节的合理利益[9]。数据交易过程中应当坚持去标识化流通，数据持有者应采取针对个人信息安全的保护技术和管理措施，规避个人信息的非法收集、获取等安全风险。因此，对于未经加工的数据，应当允许爬虫技术对其获取，但是爬虫行为不能侵害数据持有者的流通使用权，即爬取行为不得减损数据持有者正常开展数据流通、利用的权益。因此，从数据的特性、社会性与价值目标方面而言，非产权治理范式是适配数据时代需求的必然选择。这样，有利于实现数据的社会化利用，使数据在不断流通和汇集利用中最大化地实现其社会价值。

三、非产权治理范式下数据爬取行为的入罪认定检视

《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》）第1条将非法获取身份认证信息作为入罪情形之一，但又在第2条第1款将突破系统安全保护措施以及未经授权或者超越授权，作为侵入、非法控制计算机信息系统程序、工具的认定。基于此，研究者对入罪标准的理解产生了明显分歧。

（一）突破身份认证机制为入罪认定的检视

有观点认为，“身份验证机制”才是判断授权与否的核心技术标准[2]。《解释》第1条将“计算机信息系统数据”解释为“身份认证信息”。该解释的规范逻辑源于计算机信息系统安全这一保护法益，其论证基点在于身份认证信息的完整性与保密性是计算机信息系统正常运行的基础屏障。然而，随着大数据时代数据价值维度的拓展与数据犯罪样态的演进，这一以系统安全为单一导向的法益观逐渐显现出司法适应性不足的问题。

该观点提出，身份验证机制，例如账号密码、生物识别的功能在于划定数据的公开与私密边界，是数据控制者对谁可访问其系统的合理管控，突破该机制意味着未经许可进入计算机信息系统的控制范围，直接威胁系统安全秩序。实践中，部分网站的信息虽处于公开状态，但未登录时复制粘贴功能会受到限制。那么，对于这种仅为突破复制限制而绕过身份验证机制的爬取行为，是否有必要动用刑法予以规制？目前，采纳数据安全法益的学者认为，该行为突破身份验证仅为方便批量获取，因未侵害数据的保密性与系统安全，不应认定为犯罪。部分学者主张，若数据依赖身份验证保持非公开状态，如后台数据库信息，那么，突破该机制则因实质侵害法益而具备刑事可罚性[21]。数据即见即可用的固有特性，决定了已公开的数据通常具备可被爬取的默许前提。然而，即便有学者试图通过增设“非公开数据”的限定性条件以完善身份认证机制的入罪标准，该完善路径仍未脱离数据非产权治理范式的框架，存在逻辑层面的局限性。

（二）超越合约授权为入罪认定的诘问

Robots.txt作为互联网行业通用的排除爬虫爬取的标准，内容涉及对网络爬虫的访问权限、爬取速度与范围的限制。但是Robots.txt仅为一种缺乏技术抵御能力的警告性声明，其是否被遵守完全依赖于爬虫操纵者的单方意志，这一固有局限决定了其难以具备强制约束效力。但主张超越合约授权为入罪标准的学者认为，爬虫协议作为网络平台对外声明数据爬取授权范围的直接意思表示，其主要功能在于明确“允许或禁止抓取的数据范围”，且在搜索引擎领域已成为普遍遵循的行业规范[1]。据此，绕过爬虫协议获取数据的行为，因违背数据控制者的单方意思表示，具有法律上的侵入性，应认定为“未经授权”。然而，这一观点在法理层面难以自洽：爬虫协议本质上是平台单方制定的行业规范，若将违反爬虫协议的行为一概纳入刑事评价，实则将数据控制权完全交予企业，可能导致企业借协议之名实施数据垄断，使

刑法沦为维护企业私利的工具，背离了数据流通的公共利益属性。我国司法实践也对这一标准进行了否定。例如在百度诉奇虎 360 不正当竞争纠纷案中，法院认定爬虫协议并非法律意义上的协议，仅为技术规范；温某某、贾某某非法获取计算机信息系统数据罪一案中也提到，“Robots 协议是针对搜索引擎的，且是一个类似于君子协定的东西，没有任何强制力”（参见江苏省常州市中级人民法院（2023）苏 04 刑终 240 号刑事裁定书）。连 Robots 协议都不能作为入罪标准，将网站服务条款协议（例如网站上的告知、弹窗等）扩展理解为合约授权则更显不当。例如，在美国 United States v. Drew 一案中，法院认为，控方提出以网站服务条款协议作为入罪标准的意见将可能使刑法的适用范围过度扩张，进而导致大量普通网络用户因日常行为而面临刑罚指控的风险（参见 United States v. Drew, 259 F. R. D. 449, 452(C.D. Cal. 2009)）。总之，合约授权是指通过意思表示允许或者禁止他人访问、获取数据，并不具有刑事违法性的判断功能。

（三）突破设备的安全技术措施为入罪认定的修正

有观点认为，授权判断应回归技术措施的实质违法性，唯有爬虫工具规避或突破技术障碍时，才能认定为“未经授权”。但争议的焦点在于：何种技术措施可作为判断基准？有观点认为，只要网站设置反爬虫措施，规避该措施的行为即构成本罪 [3]。此说忽略了反爬虫措施的技术属性——其本质是对访问方式的限定，如限制批量抓取速度（短时期、高频次的访问会增加服务器的负载，可能影响正常的网络服务，甚至导致服务器崩溃），而非对数据公开性的否定。已公开的数据仍可通过正常访问方式获取，此时爬虫工具仅是“自动化的信息收集手段”[22]，与人工浏览无本质区别，若仅因规避此类措施即入罪，显然扩大了刑事规制范围。安全技术防护措施成立的前提，是其背后存在所需保护的具体法益。正如德国刑法理论相关学说所指出的，数据爬取行为的刑事可罚性亦取决于所涉数据是否属于“特别保护”之对象 [23]。该理论可归纳为客观实质说，其主张保护范围应限于承载保密信息、具备“特别安全”属性的数据 [24]。因此，数据背后的信息，如若承载个人法益、社会法益、国家法益，如对其非法获取，则应当认定为非数据类的刑法罪名。如果所涉数据载有需法律保护的信息，而数据持有者并未设置安全措施时，也并不意味着未经授权可以被任意爬取。爬取者可能涉及侵犯公民个人信息罪、侵犯商业秘密罪等，而数据持有者可能因未履行信息保护义务而触犯拒不履行信息网络安全管理义务罪 [25]。非具备“特殊安全”的原始数据，不宜受法律保护，应当公开，即便突破技术措施获取也不应认定为违法。至于爬取具有经济利益的衍生数据，下文将着重探讨。

对于爬取行为的规制需要通过明确、客观的标准平衡数据控制与社会利用，避免因主观判断的模糊性导致权利滥用。对于三种入罪标准，学者们大多将数据本身作为直接保护对象。该观点延续了传统产权治理范式的逻辑，本质上仍是对“数据自身安全”这一法益的确认。但这一法益观存在明显缺陷：其一，误将数据等同于传统有形财产，忽视其可复制、可共享的特性，过度保护易导致数据垄断，阻碍要素流动。其二，“数据自身安全”边界模糊，易引发入罪标准主观化、处罚范围不当扩大，违背刑法谦抑性原则。对于不承载传统信息法益的一般数据，其保护重心不应聚焦于排他性占有，而应在值得保护的数据流通与利用秩序中探寻保护的法益。

四、数据爬取行为侵犯法益的转向与适用

（一）数据爬取行为侵犯法益的争议与转向

1. 网络安全法益的反思

从刑法规制视角而言，若要对非法获取计算机信息系统数据罪作出合理解释，则有必要重新审视该罪所保护的法益内涵。刑事违法性的判断不应停留于形式化的协议违反或身份认证，而应结合非产权治理范式，回归法益侵害的实质判断，毕竟犯罪的本质是法益侵害。既有研究认为，数据价值的实现依赖

流通与复用，而网络安全是数据持有者使用与流通的前提。有观点主张网络爬虫严重妨碍网站业务、造成网站瘫痪，无法正常提供服务的，可以视为对网络安全的危害[26]。应以网络安全为法益核心，既通过保护网络的控制力与防御力，为数据流通与使用提供“安全基底”，又通过排除对数据本身的过度保护，为合法爬取行为保留空间。1997 年刑法增设该罪的初衷，是应对“非法侵入计算机信息系统、窃取账号密码、非法控制他人设备”等威胁网络安全的行为，其目的是维护信息网络的运行秩序[27]。故不应仅凭文义的可能性扩张其保护范围，否则将背离立法原意，造成刑法机能的错位。再者，网络安全直接关系到数据持有者能否持续、安全地使用数据。因此，通过保护网络安全间接实现对数据的保护，在技术与法理层面均具有合理性，无需将数据安全确立为独立法益。

当数据存储于跨国云平台且其价值实现已突破特定计算机信息系统边界时，若仍坚持系统安全或网络安全统摄数据安全的传统路径，则难以契合数据治理的新格局。并且随着数据流通秩序的发展，可信数据空间（可信数据空间是指基于共识规则，联接多方主体，实现数据资源共享共用的一种数据流通利用基础设施，具备数据可信管控、资源交互、价值共创等核心能力）的创建呼声日益高涨。以网络安全为法益未必能够囊括数据使用控制的全部情形。当前我国可信数据空间建设正经历从计划探索到实践试点的重要转折期[28]，在此背景下，若仅以网络安全法益来保障数据流通秩序，其保护范围将难以周延。

2. 数据安全法益的剖析

许多学者主张，数据安全法益应是数据犯罪独立保护的法益，如此，才能确保对数据犯罪进行独立规范评价[29-30]。但笔者认为，学界对“数据安全”的论证逻辑，其推理链条存在明显疏漏。主张数据应获独立保护的观点遵循如下思路：数字经济时代数据具有极高价值，故数据本身应受法律保护[31]。有观点认为，即便是不含有特殊信息的一般数据，爬取者也可以通过数据分析技术挖掘隐含在一般数据中的特殊数据，进而实施违法犯罪[32]。但数据的可挖掘性仅属事实层面特征，其与刑法责任的成立缺乏必要的关联。数据能否体现传统法益，在于其是否承载信息法益。刘宪权认为，数据安全法益在本质上是对信息法益的早期化保护，是服务于多类型信息法益的工具性集体法益[33]。秦雪娜进而提出完全否定的观点，“数据法益依赖于个人法益与集体法益既有的保护框架，试图将数据法益抽离并赋予其独立地位的观点，实际上过度放大了数据的技术属性在刑法评价中的意义”[34]。信息法益值得刑法保护，而不承载信息法益的数据是否具备刑法保护的正当性、应采取何种保护路径，则是另一个问题。

在非产权治理范式下，未经任何加工处理的原始数据不宜受法律保护，持有者并不享有任何权利，此时，持有仅是一种事实状态，因此对这部分数据的爬取行为并非违法行为，更谈不上刑法所规制的危害行为。若将数据本身的安全作为独立法益，可能导致“数据归属”优先于“流通价值”。这一立法思路可能会助推企业强化其技术壁垒，进而抑制小微企业的创新发展。反对泛化保护零散孤立、未形成体系的数据，是因为其未经系统性加工，流通更多依赖市场的自发调节。若将其纳入法律规制的范围，则会导致法律过度介入数据流通领域，阻碍数据价值释放进程。“数据本身安全”的法益是建立于传统产权治理范式之上的，传统产权治理范式的不适配性直接导致该法益的认定不适用于数据犯罪的规制。

3. 数据使用秩序安全法益的转向

首先需明确，针对数据承载的传统法益所实施的犯罪行为，不应界定为专门的涉数据罪名，而应当归入传统的法益罪名，即侵犯个人法益、社会法益、国家法益罪名。例如某法院经审理认定，被告未经百度网盘运营方的授权，通过特定自动化程序非法收集平台用户存储的分享链接地址与提取码，并将其收录于自行运营的互联网平台以此牟利，构成非法获取计算机信息系统数据罪。（参见江苏省扬州经济技术开发区人民法院（2019）苏 1091 刑初 157 号刑事判决书）该案值得刑法保护的应当是网盘中的信息内容，而非数据符号本身；本案提取内容如若关联用户隐私信息、个人资料等具备身份识别或隐私属性的内容，可能触犯侵犯公民个人信息罪。同时，在上海市静安区人民法院判决的一起案件中，金某借助爬虫工具，实现避开上海某馆微信购票小程序的时间限制，提前进入购票信息页面进行抢票的功能；被

告人何某经金某等人纠集，使用上述方法抢购上海某馆分馆上海某馆 1、上海某馆 2 门票，后将入馆门票信息提供给金某等人对外出售，从中获利人民币共计 14 733 元。（参见上海市静安区人民法院（2025）沪 0106 刑初 593 号刑事判决书）金某与何某的犯罪意图虽指向门票转售的预期收益，但并不符合传统刑法罪名的成立条件。继而，需进行下一步判断，被非法爬取的数据是否蕴含刑法所值得保护的法益。

不承载传统法益的数据的某项利益能否纳入刑法法益的保护范畴，关键在于其是否蕴含值得刑法介入保护的价值。在非产权治理范式下，应当保护数据使用者对数据的持有与使用状态，以期保障社会层面的数据流通与利用。因此，非法获取计算机信息系统数据罪的法益保护应从对数据本身安全的保护转向对数据使用秩序安全的保护。上述金某数据爬取案，从涉及的数据本身而言并不宜受法律保护，但是其侵犯博物馆对数据处理与使用的行为，应当认定为非法获取计算机信息系统数据罪。非产权治理范式下，本质上原始数据的获取并不纳入法益的保护范围，但是对于数据持有者的加工、处理、传输等使用秩序的安全应当予以保障，如果对其使用秩序侵害达到一定程度，应当动用刑法予以规制。有鉴于此，笔者认为，无论是当前争议不断的非法获取计算机信息系统数据罪，抑或未来立法可能创设的数据相关罪名，均可从数据使用秩序安全法益予以考量。

问题的关键在于，对该秩序的侵害达到何种程度时，刑法才有介入的必要。从非产权治理范式的逻辑出发，该程度的界定应聚焦于侵害行为对数据使用秩序的破坏强度、影响范围与危害后果，以此建立兼具客观性与可操作性的判定标准。其一，需考量行为的干扰强度。若爬取行为直接破坏数据持有者的正常使用流程，如通过高频次访问挤占服务器资源导致数据处理瘫痪、篡改数据传输路径影响使用稳定性，或绕过合规授权机制批量获取数据导致使用秩序紊乱，即达到刑法规制的程度；轻微、零星的获取行为未对数据持有、使用的正常状态造成实质干扰，则应排除刑法介入。其二，需评估危害的辐射范围。当侵害行为不仅影响单个数据持有者的使用权益，还蔓延至行业层面的公平竞争秩序，如通过非法手段获取他人整理的结构化数据后批量复用，挤压合法数据处理主体的市场空间，或破坏公共数据的共享使用规则，导致社会层面数据流通效率下降，即具备刑法规制的必要性；若仅涉及个别主体的局部利益，未产生扩散性影响，可通过民事、行政手段规制。其三，需明确后果的严重性。若侵害行为造成数据持有者重大经济损失、社会公共利益受损，应认定为达到刑法规制的程度；反之，若损害后果轻微且可通过技术手段快速修复，未形成实质性秩序破坏，则应恪守刑法的谦抑性。

（二）财产犯罪认定纷争的化解

上文的探讨聚焦于未承载传统法益的原始数据，而具有经济价值的衍生数据在不同的治理范式下，存在以财产犯罪罪名抑或专门的数据犯罪罪名予以保护的争议。数据治理的核心并非对零散、孤立的数据进行排他性保护，而是对经过加工整合、形成体系的数据源进行规范，此类衍生数据应当成为数据治理的基本单元。衍生数据是通过分析处理而形成的创造性劳动成果，符合财产性利益需具备管理可能性、转移可能性和价值性的认定条件[20]。对其非法获取的行为是否可以纳入财产犯罪，学界存在不同意见。有学者认为，对其进行刑法保护可以参照与此类似的非法获取加密财产的行为，将其纳入财产犯罪保护的范畴，而不以数据犯罪进行论处[35]。

我国现行刑法中财产类犯罪的成立，需满足“以非法占有为目的”与“转移占有”两大构成要件。若数据经营者针对衍生数据所享有的财产性利益，无法被刑法意义上的“占有”概念所涵摄，亦不具备“转移占有”的可能性，则不能成立财产类犯罪。刑法中财产性利益需以财产权本身为内容，衍生数据对企业的价值是尚未上升为财产权利的经济利益。衍生数据既不具备有体物属性，也缺乏财产权利的归属效能、排除效能，无法认定为刑法规定中的“财物”[36]。进一步观之，若将非法获取衍生数据的行为纳入财产类犯罪的范畴，则可能导致司法实践中罪刑失衡之虞。以上文提到的上海市静安区人民法院审理的爬取案件为例，涉案数据经司法认定价值高达千万元，若依据盗窃罪定罪处罚，其法定刑最低应处十年以上有期徒刑，该量刑结果与爬取行为的社会危害程度及刑法谦抑性原则存在明显抵牾。因此，在不额外占

用立法资源的前提下，可通过适用非法获取计算机信息系统数据罪或非法控制计算机信息系统罪来实现该目标。除侵犯传统法益之外，若爬取行为未实质侵害数据使用秩序安全法益，即欠缺法益侵害的现实危险性，则可阻却违法性，应以此作为出罪事由，从而合理限缩刑罚权的介入范围。有鉴于此，数据使用秩序安全法益的认定可以化解财产犯罪认定的难题，对非法获取衍生数据的行为，宜以专门的数据罪名予以规制，即突破安全技术措施爬取非公开且具有经济价值的衍生数据的行为，可以作为数据犯罪的入罪事由。

爬取行为的刑法规制争议，本质上是数据的特质与法律传统产权范式之间结构性矛盾的集中体现。技术迭代催生的数据形态，天然具有非排他性、可重复利用性与价值聚合性等特质，而传统产权治理范式以物理资源的有体性、排他性占有为底层预设，难以有效涵摄数据的独特属性。基于此，我们应当超越传统产权治理范式的理论藩篱，转向一种以数据特质为起点的非产权治理范式。对于非法获取计算机信息系统数据罪，唯有厘清入罪标准，才能避免法律沦为数据垄断的工具，同时为网络安全筑牢防线，最终为数据有序流通与社会化利用提供稳定的规范预期，推动数字经济在法治轨道上行稳致远。应当明确，非法获取计算机信息系统数据罪的法益并非数据安全，而是数据使用秩序安全。一方面要避免将数据安全作为独立法益导致规制泛化，若原始数据成为产权直接保护对象，企业可能以数据所有权为由，阻碍数据流通；另一方面，只有当爬取行为侵害数据的使用与流通时，才可能构成违法，这为法律规制划定了清晰边界。如此，既可回应数据时代的发展需求，又能切中数据治理的核心要义。

参考文献：

[1] 王华伟 . 网络爬虫行为的罪责认定路径：数据确权与利益平衡 [J]. 环球法律评论，2023，45(1)：57-73.

[2] 李雪健 . 大数据时代下爬取企业数据行为的入罪标准及其司法限缩 [J]. 大连理工大学学报（社会科学版），2023，44(5)：79-87.

[3] 薛美琴 . 网络爬虫刑法规制的边界 [J]. 网络法律评论，2020，23(00)：227-248.

[4] 姜瀛 . 论刑法介入网络数据爬取行为的类型与限度 [J]. 浙江社会科学，2021(10)：37-45，156.

[5] 王惠敏 . 网络数据安全独立性之提倡及其刑法展开 [J]. 法治研究，2023(3)：117-131.

[6] 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.

[7] Boulanger M. Scraping the bottom of the barrel: Why it is no surprise that data scrapers can have access to public profiles on linkedin[J]. SMU Science and Technology Law Review，2018(21)：77.

[8] AI crawlers reshape the internet with over 30% of global web traffic[EB/OL]. [2026-03-17]. https://cybersecuritynews.com/global-web-traffic.

[9] 高富平 . 数据持有者的权利配置：数据产权结构性分置的法律实现 [J]. 比较法研究，2023(3)：26-40.

[10] 童云峰 . 大数据时代网络爬虫行为刑法规制限度研究 [J]. 大连理工大学学报（社会科学版），2022，43(2)：88-97.

[11] 朱宝丽 . 数据产权界定：多维视角与体系建构 [J]. 法学论坛，2019，34(5)：78-86.

[12] 申卫星 . 论数据产权制度的层级性：“三三制”数据确权法 [J]. 中国法学，2023(4)：26-48.

[13] 张新宝 . 论作为新型财产权的数据财产权 [J]. 中国社会科学，2023(4)：144-163，207.

[14] 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 [EB/OL]. [2026-03-17]. https://www.gov.cn/gongbao/content/2023/content_5736707.htm.

[15] 高富平 . 数据经济讲义 [M]. 北京：人民日报出版社，2024.

[16] 陈潭 . 国家治理的数据赋能及其秩序生产 [J]. 社会科学研究，2023(6)：12-30.

[17] 美浓部达吉 . 法之本质 [M]. 林纪东，译 . 台北：台湾商务印书馆，2012：44.

[18] 裴轶，韦武 . 企业间数据共享的垄断风险与规制进路 [J]. 湖南工业大学学报（社会科学版），2025，30(4)：77-85.

[19] 冉昊 . 财产权的历史变迁 [J]. 中外法学，2018，30(2)：379-392.

[20] 姚万勤，赵小勇 . “权利束”视角下数据资产的刑法保护 [J]. 法治研究，2024(1)：88-100.

[21] 孙禹 . 强行爬取公开数据构成犯罪吗 [J]. 国家检察官学院学报，2021，29(6)：121-139.

[22] Bifulco I，Cirillo S，Esposito C，et al. An intelligent system for focused crawling from Big Data sources[J]. Expert Systems with Applications，2021(184)：1-12.

[23] Stam F. Die strafbarkeit des Aufbaus von Botnetzen[J]. ZIS，2017(9)：547−552.
[24] 江海洋 . 数字时代数据爬取的刑法规制：法益界定与数据确权 [J]. 比较法研究，2024(2)：149−163.
[25] 刘嘉林 . 分置性权属视角下衍生数据的刑法保护 [J]. 西南政法大学学报，2025，27(4)：144−158.
[26] 任颖 . 数据立法转向：从数据权利入法到数据法益保护 [J]. 政治与法律，2020(6)：135−147.
[27] 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.
[28] 李林 . 基于可信数据空间的一体化数据市场构建 [J]. 中国特色社会主义研究，2025(2)：101−109.
[29] 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.
[30] 于润芝 . 非法获取个人数据犯罪的法益分析及处罚限定 [J]. 大连理工大学学报（社会科学版），2023，44(2)：56−64.
[31] 钱子瑜 . 论数据财产权的构建 [J]. 法学家，2021(6)：75−91，193.
[32] 张高月 . 数据安全法益的基本构造及司法运用 [J]. 江西社会科学，2025，45(6)：145−156.
[33] 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(2)：1−14.
[34] 秦雪娜 . 网络数据犯罪立法的三大重要问题 [J]. 北京理工大学学报（社会科学版），2024，26(1)：140−147.
[35] 赵拥军 . 论财产犯罪中数据资产的占有及转移 [J]. 东方法学，2023(3)：162−175.
[36] 欧阳本祺 . 要素市场中企业数据的法益识别与刑法保护 [J]. 法学研究，2025，47(6)：88−106.

Criminal Regulation of Data Scraping Behavior from Perspective of Governance Paradigm Shift

QU Tianming, SUN Zhi

（College of Law, Qingdao University of Science and Technology, Qingdao 266061, China）

Abstract：The criminal law regulation of data scraping is confronted with the predicament of inconsistent judicial adjudication standards, and the root cause lies in the simple application of the traditional property rights paradigm to data governance. From the perspective of their intrinsic and value attributes, raw data does not have the theoretical basis for property-rights protection and should be governed under a non-property-rights paradigm. Regarding the criminalization criteria for the crime of illegally obtaining data from computer information systems, the function of contractual authorization and identity authentication mechanisms in determining criminal illegality should be rejected; instead, the standard should revert to substantive infringement upon legal interests, as manifested through technical protection measures. For the illegal scraping of data that embodies personal, social or national legal interests, existing criminal law offenses should take precedence in evaluation. Under the non-property-rights governance paradigm, the legal interest protected by data crimes should be redefined as the security of data usage order. Its criminalization should be predicated on a finding that the scraping behavior substantially hinders the data holder's ability to use, process or transmit the data. At the same time, derivative data, as it has not yet been recognized as a statutory property right, should not be subsumed under property crimes but rather be governed by separate data-specific offenses.

Keywords：non-property-rights governance paradigm; data scraping behavior; criminalization criteria; crime of illegally obtaining data of computer information systems; legal interest in data usage order security

责任编辑：徐海燕