E-Commerce Letters 电子商务评论, 2026, 15(4), 408-414
Published Online April 2026 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2026.154412

Hans汉斯

电子商务平台公开数据爬取的刑法规制研究

徐佳靓

扬州大学法学院，江苏 扬州

收稿日期：2026年3月2日；录用日期：2026年3月13日；发布日期：2026年4月8日

摘　要

如今电子商务高速发展，数据已成为平台的核心生产要素。公开数据爬取在电商价格监控、竞品分析等场景下频发，不仅引发了商业竞争争议，更对刑法规制体系提出了挑战。虽然爬取行为在技术上有中立性，但涉及电商平台权益的恶意爬取极易跨越民刑边界。公开数据作为被爬取对象，虽可被公众浏览，但因其仍有一定的法律保密性，故有些爬取仍可能侵害数据权益，甚至危害计算机信息系统安全。司法实践对这类行为采取刑民分治的规制策略，而面对爬取行为入罪标准模糊、数据权属不清等问题，应坚持技术中立与刑法谦抑性原则，同时完善量化危害评估体系，以实现数据流通与安全保护的平衡。

关键词

平台数据，公开数据，网络爬虫，计算机网络犯罪

Research on Criminal Regulation of Publicly Available Data Scraping on E-Commerce Platforms

Jialiang Xu

Law School, Yangzhou University, Yangzhou Jiangsu

Received: March 2, 2026; accepted: March 13, 2026; published: April 8, 2026

Abstract

Against the backdrop of rapid e-commerce development, data has become a core production factor for platforms. Public data scraping frequently occurs in scenarios such as e-commerce price monitoring and competitor analysis, sparking commercial competition disputes while challenging existing criminal regulatory frameworks. Although crawling activities possess technical neutrality, malicious scraping that infringes upon e-commerce platform rights readily crosses civil-criminal boundaries.

文章引用: 徐佳靓. 电子商务平台公开数据爬取的刑法规制研究[J]. 电子商务评论, 2026, 15(4): 408-414.
DOI: 10.12677/ecl.2026.154412

While publicly available data may be accessible to the public, it retains certain legal confidentiality protections. Thus, scraping may still constitute infringement of data rights and even jeopardize computer information system security. Current judicial practice adopts a dual regulatory approach for criminal and civil remedies. To address issues like ambiguous criminalization thresholds and unclear data ownership, authorities should uphold the principles of technological neutrality and criminal restraint. They must prudently define the boundaries for criminal intervention while refining quantitative harm assessment systems to achieve a balance between data circulation and security protection.

Keywords

Platform Data, Publicly Available Data, Web Crawlers, Computer Network Crimes

1. 问题的提出

在电子商务生态中，商品定价、用户评价和库存信息是平台经营的核心数据。频繁且大规模的恶意爬取不仅会耗尽平台服务器资源，还会破坏电商行业的正常价格体系和竞争平衡。通过司法案例可以看出，有关数据争夺的侵权行为与违法犯罪时有发生，而作为数据搜集工具的爬虫技术的应用带来了很多争议，也对现有的法律秩序带来了冲击。

公开数据的爬取是否应由刑法予以保护？哪些过当的爬取行为才需动用刑法？刑法介入的边界在哪？刑法介入后应如何对法益进行保护？一旦刑法过度和不当介入，势必会减损信息交互的灵活性以至于产生数据垄断的风险，进而对数字产业的良性循环产生负面影响，所以如何合理地规制爬取公开数据行为成为了法律界亟待攻克的时代命题。

2. 公开数据应受刑法保护的必要性

(一) 公开数据与开放数据

公开数据与非公开数据的区分关键就在于是否设置了访问权限，公众是否能够轻易浏览并获取。但公开数据与开放数据之间的区分就更值得关注，因为这是公开数据是否应受刑法保护的关键所在。

公开不代表可被无偿获取。电商平台展示的商品详情等修饰工作是商家投入大量劳动成本后的智力成果，尽管是公开的，但其商业价值仍属平台和商家，而非竞争对手可以随意盗用的公共资源。电商平台的商家可将自己拍摄的视频或图片发到店铺中，但其他商家不可直接获取并使用，这就是公开数据但非开放数据。所以爬取公开数据的行为不一定合法。

公开数据和开放数据的差异导致了受法律保护的程度的不同。公开数据并不等同于公共数据，也不是对数据进行开放[1]。公开数据更倾向于有个人性质的数据，其通常允许浏览但限制浏览者进一步地获取数据行为。开放数据则有公共性，可浏览亦可获取，更倾向于政府等公共部门的数据。显然公开数据的公开程度和可再利用程度没有公共数据那么彻底。

(二) 公开数据的技术保密性与法律保密性

爬取公开数据的用途与加工结果不可控，可能会导致隐私或商业秘密泄露。这是公开数据的固有矛盾，技术上可被公众浏览，法律上却限制信息的获取与加工，由此产生实践冲突。

公开数据的公开性是相对的，其包含法律层面的保密性，所以爬虫获取或加工可能会引发危险，当

行为危害超出民事范畴时，仍需刑法介入。数据保密性是数据安全法益的重要内容，所谓数据的保密性就是指，在特定情形下，系统维持一种自上而下的权限，并控制那些有权获取信息的人[2]。所以公开数据在一定情况下仍有其保密性，应由刑法进行保护。

数据的开放与受保护的状态应区别看待。前者关乎信息能否被随意检索，后者则通过平台技术防护手段阻断非法爬取，这也是公开数据与公共数据的本质区别。所以允许在线浏览信息不等于授权第三方爬取数据，二者无必然因果关联。在我国首例爬虫入刑案中，晟品公司因为不当使用爬虫手段而被认定侵犯了数据的保密性。对此法院认为，虽然其爬取的数据为公开数据，但其数据载体仍具有保密性，所以刑法有必要介入进行保护[1]。

3. 公开数据爬取行为的刑法规制现状及问题

(一) 手段与内容二分视角下的司法实践评析

(1) 使用数据内容违法的规制

在淘宝诉淘数公司案中，法院的规制重点在于数据内容本身的竞争性法益，聚焦于数据被获取后的非法利用行为，而非单纯的爬取技术手段[2]。

原告为浙江淘宝网络有限公司、浙江天猫网络有限公司及淘宝(中国)软件有限公司。被告是淘数有限公司、泰数有限公司等六家关联公司及自然人李某、林某。原告主张了三类数据权益，合法收集加工的原始数据集合、未公开的属商业秘密的经营数据和“生意参谋”等衍生数据产品。被告的“小旺神”软件主要提供三项功能，一键还原“生意参谋”脱敏数据、以小时级频率监控竞品信息以及一键下载商品素材，同时被告通过“数小易”API 批量售卖爬取的数据。

本案争议焦点有三个。第一，原告是否享有涉案数据权益及商业秘密。第二，被告行为是否构成不正当竞争。第三，若构成侵权，各被告如何担责。

法院认定原告对涉案数据有竞争性权益，未公开的经营数据属商业秘密，“生意参谋”的数据利用模式也受法律保护。被告破解脱敏算法、获取并披露商业秘密，构成侵权且实质性替代和破坏原告商业模式，竞品监控、素材下载及 API 服务属于绕过技术防护措施大规模爬取数据，超出合理使用范围，构成不正当竞争，各被告人格混同，承担连带责任。

可见这是一起涉及数据权益与商业秘密的网络不正当竞争案件，法院的判决明确了以技术手段非法获取、使用平台数据的行为是绝对违法的。本案深刻反映了电商平台数据资产的衍生性特征，生意参谋这类产品是平台在海量原始交易数据基础上，投入巨大算法和算力资源加工而成的商业情报。可见内容违法的评价核心不在于爬取技术本身，而在于数据内容所承载的商业价值与竞争秩序。若此类行为对数据内容法益的侵害达到刑事门槛，应通过侵犯商业秘密罪、侵犯公民个人信息罪等路径予以规制。

(2) 爬取手段违法的法律规制

王某案中，当爬虫行为通过破解加密算法、绕过技术防护等具有技术对抗性的手段实施时，其规制核心转向计算机信息系统的访问控制秩序[3]。

被告人王某明知其下载、购买、开发的爬虫程序及接口具有破解“得物”App 安全保护措施并获取商品数据的功能，仍进行网络售卖并提供维护服务长达近 3 年，违法所得 60 余万元。涉案程序具有通过破解“得物”API 的加密算法、校验签名算法、图形验证码，使用虚构的设备信息等技术绕过防护机制，未经授权获取“得物”服务器数据的功能。

[1]广东省高级人民法院(2017)粤 03 民初 822 号民事判决书。
[2]江苏省南京市中级人民法院(2023)苏 01 民初 4082 号民事判决书。
[3]上海市普陀区人民法院(2024)沪 0107 刑初 501 号刑事判决书。

本案争议焦点有两点。第一，提供爬虫程序是否属单纯的技术行为。“得物”在用户协议及 Robots 协议中明确禁止数据爬取，采取了多重技术防护措施。被告人未经授权许可向他人提供爬虫程序破解防护机制并获取系统数据，属于提供“专门用于侵入计算机信息系统的程序”的行为，并非单纯技术行为。第二，允许访问的公开信息是否属于本案犯罪对象。涉案商品信息在“得物”客户端可被浏览，但在后台对其所对应的代码进行了加密保护，并设置了多种反爬措施，未经授权许可绕过或突破保护措施获取上述数据的，仍属于侵入计算机信息系统。故王某构成提供侵入计算机信息系统程序罪，情节特别严重。

此类行为规制的重心在于计算机信息系统的访问控制秩序与系统数据安全，而非数据本身的价值。刑法在此类场景下打击的是以专门技术手段强行侵入系统的行为，通常落入非法获取计算机信息系统数据罪等罪名的评价范畴。

两案都涉及未经授权的公开数据爬取，但在法律层面的评价与规制截然不同，关键就在于行为侵害的法益性质以及社会危害性程度。王某案中，王某明知程序具有破解“得物”安全防护措施的功能，仍出售并予以维护，以批量获取未经授权的服务器后台加密代码，明显超越了正常用户访问范畴，属于对计算机信息系统安保措施的实质性突破。此案规制核心在于计算机信息系统的访问控制秩序与系统数据安全，刑法守护的是网络空间秩序的底线，打击的是以专门技术手段强行突破防护机制的行为。反观淘宝案，被告虽也涉及爬取平台数据，功能亦需突破平台反爬措施并对数据再加工，但其行为直接冲击的法益并非系统整体的运行安全，而是原告的商业秘密与竞争性数据权益。其行为虽对平台服务器造成一定压力，但未影响平台整体的正常运行，危害主要体现在窃取他人劳动成果、破坏他人商业模式以及破坏公平竞争秩序，故由《反不正当竞争法》评价，通过侵犯商业秘密与网络不正当竞争行为予以规制。

通过对比可以看出当前刑法规制数据爬取行为的现状与边界。刑法并非规制所有不当数据爬取行为的首选，其介入有严格的门槛。刑法仍主要指向技术攻击性强烈、对计算机信息系统运行安全造成直接或严重破坏的行为。对于只是通过不当爬取手段侵犯数据内容本身权益的行为，主要通过民事法律救济，若使用行为的危害性达到刑事门槛，应通过侵犯商业秘密罪、侵犯公民个人信息罪等路径予以规制。

(二) 公开数据爬取行为入罪的问题

(1) 刑法介入的谦抑性不足

在面对爬取公开数据行为时，刑法是不能提前介入与过度保护的。一方面，刑法应坚持谦抑性原则，仅在其他法律手段不足以应对时作为最后手段介入，严防过早介入阻碍数据流通。刑法作为最严厉的法律制裁手段，其介入能够有效震慑数据爬取中的违法行为，维护数据安全与秩序。另一方面，公开数据在特定条件下同样具有保密性并应纳入刑法保护范围，但若过度保护，可能会因过于严苛而阻碍数据正常流通与利用[3]。司法实践中，部分案件将违反爬虫协议的行为直接认定为非法获取计算机信息系统数据罪就忽视了爬虫协议本身的私力规则属性，可能导致刑法干预范围的不当扩大[4]。

且刑法过早介入会产生一连串负面影响，过度强调数据安全可能导致数据资源被数据大厂垄断，进而阻碍数字经济的健康发展。同时刑法针对此类犯罪门槛要求较高且诉讼成本高，在针对轻微数据爬取违法行为时无法有效处理和解决。而且刑法过度干预可能会削弱其他法律规制手段的效用，破坏和影响多层次全方位数据治理体系的完整性[5]。

(2) 爬取行为违法性与危害性认定困难

现在对于公开数据爬取行为的违法性和危害性认定的标准并不清晰。正因没有统一标准可以遵循，法官在判断这类爬取行为是否构成犯罪时有较大的自由裁量空间，进而让同类案件的处理结果出现差异，这也会影响司法的公正性和权威性[6]。

一方面，司法实践中爬取行为的违法认定标准模糊。第一，违反爬虫协议是否属于犯罪，要看协议内容和爬取表现形式，但爬虫协议是私力规则，其法律效力及处罚力度不具有确定性，加剧了违法认定

的复杂性。第二，关于如何对公开数据爬取行为做类型化区分，也没有明确的操作和认定标准，这就导致刑法规制在实际执行中，很难做到精准实施和有效保障[4]。且还存在针对爬虫技术进行有罪推定的倾向，往往就会忽略爬虫技术本身的中立性和复杂性。

另一方面，针对公开数据爬取行为危害结果的量化评估体系不够全面，也加剧了入罪界限不清晰的问题。实践中的常见危害结果因没有统一的量化评估标准，所以其具体严重程度很难准确衡量，这也影响入罪判断的科学性和合理性。在某些案件中，数据爬取行为可能导致少量数据的丢失，但其对数据主体、系统的某些核心节点造成的破坏和潜在风险却难以估量，这种情况下是否构成犯罪，成为司法实践中的难题[7]。

(3) 数据权属界定模糊

当前我国在数据权属界定方面的法律规范处在初期阶段，相关条款散见于《民法典》《数据安全法》及地方性法规。《数据安全法》明确了“保障数据依法有序自由流动”的宗旨，但并未对数据权属的具体分配作出明确规定[8]。所以数据爬取行为合法性认定存在争议，影响刑法规制的精确性与效果。数据作为新型资源，法律未赋予控制者绝对、排他的财产权，权利属性也未形成共识。法律侧重数据处理者的责任，但公开数据的生成、使用和传播涉及用户、平台等多方主体，权利边界相互交错，数据控制者是否完全放弃对公开数据的控制又不易确定，就会引发不同权利主体对数据权利的主张与数据公开性的冲突，更会加大爬取行为违法认定难度。

首先，数据权属界定模糊导致了公开数据爬取和滥用现象频发，并对个人隐私、商业秘密等造成了严重侵害。因为数据权属不明确，数据控制者往往倾向于过度收集和使用数据，以追求利益的最大化，不免忽视其他数据主体的合法权益。个别企业就会通过爬取公开数据的方式获取用户信息，但在后续使用中未能遵循合法、正当、必要的原则，导致用户隐私被泄露、滥用。

其次，数据权属界定模糊使数据授权的认定标准在公开数据爬取的场景下十分模糊。在现代刑法体系中，认定行为人获取公开数据的行为构成刑事犯罪的前提，是行为人的获取行为构成计算机犯罪[3]。需先认定突破防护措施的行为具有侵入性，再判断后续数据爬取是否构成非法获取计算机信息系统数据，这种递进审查机制保障了刑法评价的严谨与准确。《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》将侵入行为阐释为“避开或者突破计算机信息系统安全保护措施”和“未经授权或者超越授权”，只有明晰这两种情形，才能对公开数据爬取行为是否属于侵入行为进行判定[3]。为了网站的正常运转与数据竞争力，数据控制者通常会对针对爬虫采用协议和反爬技术手段来维护数据安全[4]。一是 Robots 协议声明爬取范围。仅违反网站 Robots 协议是否算“未经授权”并构成刑事犯罪存在争议，但 Robots 协议只是行业惯例，直接作为入罪依据会让数据控制者权利过大，不当限制数据的合理获取使用。二是反爬技术，主要限制访问频率、防止过度爬取，和计算机信息系统安保措施在防止未授权访问、保护系统安全之间有本质区别。未设置 Robots 协议或未采取有效反爬措施的公开数据，授权状态的认定存在争议。

4. 公开数据爬取行为的刑法规制方向

(一) 明确刑法规制数据爬取行为应坚持的原则

(1) 技术中立原则

技术中立原则的源头和法律奠基可追溯到 1984 年美国环球电影制片公司诉索尼公司案[9]。技术本身被视为中立的工具，法律责任的认定关键在于人的意图和行为，不过技术中立也并非绝对的免责金牌。虽说工具本身并无道德属性，但工具应用手段的社会评价却必不可缺，因为若是行为人假借技术之名行侵害法益之实，且该不法行为落入刑事法律的评价框架内，那国家权力就须通过强制性手段进行惩戒。

不过单靠技术中立免责往往难以成立，法理上更倾向于结合爬取时的主观意图与具体手段综合考量。一种典型的责任豁免情形是，若程序员受雇或应他人之托编写爬虫脚本，开发者若仅履行职业职能，即便用户后续违法爬取，仍可凭技术中立免于担责。但爬虫程序开发者需承担合理注意义务，因为技术中立豁免并非绝对。若技术员明知程序会用于非法爬取却仍然交付代码，或能够知晓用户的非法意图却疏忽放任，导致严重后果，违反了注意义务，会被认定存在主观过错并追究刑事责任。

(2) 刑法谦抑性原则

在爬取公开数据行为的规制上，遵循法秩序统一原理意味着不能将在民法上被认为合法的爬取行为认定为犯罪[10]。应研判特定爬取数据行为是否属于非刑事法律框架，不能直接认定该行为是计算机犯罪。我国刑法对数据犯罪的规制聚焦于技术手段与法益侵害程度，《刑法》第 285 条“非法获取计算机信息系统数据罪”的构成要件明确要求“侵入”或“采用其他技术手段”获取数据，其核心在于行为方式对数据控制权的实质性突破[3]。

因此要判断刑法对公开数据爬取是否过度介入，关键看行为是否突破民事与行政不法的边界，是否严重侵害刑法保护的核心法益。刑法介入需要满足两个标准。一是技术性危害，行为除了未授权访问，还包含技术上的规避性或破坏性。王某案中，嫌疑人用专门程序破解加密算法、图形验证码和设备指纹等防护机制，就非单纯数据浏览或获取，而是对计算机信息系统安保措施的实质性突破。二是法益侵害的程度。爬虫行为须有严重的社会危害性或达到法定严重程度。王某案中，被告人提供侵入计算机信息系统的专用程序，牟利 60 余万元，不仅严重侵害企业数据安全，还扰乱正常网络管理秩序，达到了刑法“情节特别严重”的标准，触及了核心法益。

刑法谦抑性和对数据爬取行为的规制并非对立，恰是谦抑性原则划定了刑法介入的边界，对于用技术手段产生严重社会危害性的数据爬取行为，刑法的介入反而是必要又正当的。

(二) 明确公开数据爬取行为入罪的标准

对于电商行业普遍存在的爬虫，应区分合理采集与恶意破坏。若行为人以破坏平台经营秩序、获取非法竞争优势为目的，模拟普通用户点击等手段绕过电商平台的反爬机制，其社会危害性已超越单纯市场竞争，具有入罪的必要性。

公开数据爬取的入罪判定应采用二分法，构建手段与内容的分层标准。手段违法适用破坏计算机信息系统类犯罪，我国刑法虽无明确规定何种行为属于“侵入计算机信息系统”的行为，但《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》[4]列明了什么是专用于非法侵入和控制计算机系统的程序和工具，可知侵入行为要满足两点：避开或突破计算机信息系统安保措施、未经授权或超越授权。若爬虫行为存在对防护机制的实质性规避并造成系统运行异常，则触犯刑法保护的系统安全法益。而内容违法适用侵犯秘密或信息类犯罪，即使手段不具有强烈的对抗性，若获取的数据涉及法定的特定法益，且行为人主观上具有非法获取商业秘密或个人信息的故意，则应依据数据内容的属性进行定罪。这样能有效避免因数据管控权界定模糊而产生的认定难题，在保障数据有序流动的同时，精准打击有严重社会危害性的行为。

在具体界定公开数据爬取行为的刑事违法性时，应建立以技术的对抗强度为核心的推定机制，通过行为人的客观行为判定其主观认知与行为非法性。

首先，通过技术对抗行为来推定主观明知。若公开数据的数据控制者已采取了实质性的技术防护措施，而行为人仍采用侵入性的技术手段强行突破，那就能推定其主观上明知自己的获取行为超出了正常访问授权，具备非法获取的犯罪故意。这种认定方式比要求行为人自证授权更合理。

[4]参见《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》第 2 条。

其次，Robots 协议是主观恶性的补强证据。虽然 Robots 协议不属于刑法意义上有物理阻断功能的技术性防护措施，但其清晰表达了数据控制者的意愿，当网站通过 Robots 协议明确禁止了特定爬取行为，而行为人依旧采用绕过或突破反爬措施的技术手段实施爬取时，协议就可以作为证明行为人主观恶意的关键补强证据，协助认定行为的刑事违法性。

另外，要坚持获取行为需具有侵入性的实质评价标准。认定非法性的关键就在于获取过程有没有针对技术措施的破坏性，若行为人模拟普通用户的行为进行低频采集，属于普通用户正常使用的范畴，即使没获得明确的书面授权，基于公开数据的公共属性也应视作合理利用。只有当爬取行为存在对安全防护机制的实质性规避与突破，造成了系统运行异常、数据安全受损等严重后果时，才达到刑法要求的高度社会危害性。

爬虫技术动辄涉百万甚至亿级的信息量，现行司法解释中最高的数量标准往往也离现实中的海量数据有很大距离。且单纯凭金钱数额来衡量此类案件也不理想，可以建立一套分层数量评估体系，结合行为后果判定。若涉及商业秘密，既要考虑数据总量，也要兼顾数据本身的价值。如果涉及数据转卖，应综合考虑成交价格与数据自身价值。若某段时间内爬取的数据总量没达标，但频率显著超过正常访问范畴，也可追究刑事责任。量刑时可将多个指标结合，按照择一从重的原则进行处罚。

(三) 明确对违反 Robots 协议行为的刑法规制态度

Robots 协议是网站控制者的单方技术规则，是一种行业习惯，不属于技术手段，不能直接阻碍爬虫，亦无合同效力。但若数据爬取方未遵循 Robots 协议，其行为可视作侵害了网站控制者对网站数据的管控权，应承担侵权责任。

若要将违反 Robots 协议爬取数据的行为纳入刑法规制的范围不太妥当。因为 Robots 协议是一种单方声明，而非通过技术手段针对爬虫行为的防御。若网站控制者除了设置 Robots 协议以外，未实施其他任何技术性阻碍爬虫的手段，说明对其数据主观上的保护意志不强。刑法作为兜底性的保护手段，对于权利人保护意思本身就不强烈的情况，若轻易采取刑事措施，不仅有过度保护之嫌，对爬取数据一方也不公平。所以司法实践中应当审慎对待，一般不宜将其作为入罪的核心依据，但可在综合判断其行为对社会危害性时作为补强证据予以考量。

参考文献

[1] 陈兵, 姚俊羽. 公开数据保护的理念澄清与路径选择[J]. 中国特色社会主义研究, 2024(2): 38-52.

[2] 蔡士林. 我国数据安全法益保护: 域外经验与立法路径[J]. 深圳大学学报(人文社会科学版), 2022, 39(6): 97-106.

[3] 刘宪权. 非法获取公开数据行为的刑法规制[J]. 法律适用, 2025(8): 97-113.

[4] 陈毅坚, 曾宪哲. 网络爬虫刑法规制研究[J]. 广东社会科学, 2022(5): 240-253.

[5] 种政. 从附属到独立: 数据的刑法保护模式构建[J]. 公安学研究, 2023, 6(2): 50-70+123-124.

[6] 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.

[7] 智逸飞. 数据爬取行为刑事不法认定的应然转向[J]. 太原理工大学学报(社会科学版), 2024, 42(1): 1-11+53.

[8] 辛勇飞. 中国数据治理规则体系构建: 现状、挑战与展望[J]. 人民论坛·学术前沿, 2023(6): 6-12.

[9] Sony Corp. of America v. Universal City Studios, Inc., 464 U. S. 417 (1984).

[10] 石经海, 苏桑妮. 爬取公开数据行为的刑法规制误区与匡正——从全国首例“爬虫”入刑案切入[J]. 北京理工大学学报(社会科学版), 2021, 23(4): 154-164+172.