Dispute Settlement 争议解决, 2025, 11(3), 204-211
Published Online March 2025 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2025.113115

Hans汉斯

论网络爬虫的刑事违法性认定基准

汪婧怡，陈馨悦

上海政法学院刑事司法学院，上海

收稿日期：2025年2月19日；录用日期：2025年3月12日；发布日期：2025年3月24日

摘　要

网络爬虫技术的运用可以促进技术、信息的分享和信息检索的效率，但是爬虫行为的失范导致了恶意爬虫的出现，我国近年来对相关案件的处理也从原来的民事处罚转向了刑事惩处，但是在实践中由于不区分爬虫手段的技术特征和数据的类型导致了处罚范围的扩大。为了避免刑事打击的泛化，应依据行为的不法和对象的不法两个方面来判断网络爬虫的刑事违法性。从对象上，区分公开信息和公开数据、开放数据、限制访问数据作为判断刑事违法性的实质标准；从行为上，通过爬虫行为的技术性特征以及Robots协议作为判断刑事违法的形式标准。建议通过建立数据分级制度等明确网络爬虫犯罪的合法性边界。

关键词

网络爬虫，反爬虫措施，开放数据，刑法规制

The Criteria for Determining Criminal Illegality in Web Crawling

Jingyi Wang, Xinyue Chen

College of Criminal Justice, Shanghai University of Political Science and Law, Shanghai

Received: Feb. 19th, 2025; accepted: Mar. 12th, 2025; published: Mar. 24th, 2025

Abstract

The application of web crawler technology can promote the sharing of technology and information and the efficiency of information retrieval. However, the unregulated behavior of web crawlers has led to the emergence of malicious web crawlers. In recent years, the handling of related cases in China has shifted from civil penalties to criminal punishments. However, in practice, the lack of distinction between the technical characteristics of web crawler methods and the types of data has led to an expansion of the scope of punishment. To avoid the generalization of criminal crackdowns, the criminal illegality of web crawlers should be judged based on both the unlawfulness of the

文章引用: 汪婧怡, 陈馨悦. 论网络爬虫的刑事违法性认定基准[J]. 争议解决, 2025, 11(3): 204-211.
DOI: 10.12677/ds.2025.113115

behavior and the unlawfulness of the object. From the perspective of the object, the distinction between public information and public data, open data, and restricted access data should be made as the substantive standard for judging criminal illegality; from the perspective of the behavior, the technical characteristics of web crawler behavior and the Robots protocol should be used as the formal standard for judging criminal illegality. It is suggested that the legality boundaries of web crawler crimes be clarified through the establishment of a data classification system, etc.

Keywords

Web Crawler, Anti-Crawler Measures, Open Data, Criminal Regulation

Copyright © 2025 by author(s) and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

1. 引言

当下我国正着力强化数据安全理念，针对网络爬虫的司法规制呈现出愈发严格的态势，其法律适用范围也逐渐从民事范畴向刑事领域延伸。以一系列典型案例为例，如 2013 年的百度与奇虎之争、2015 年新浪微博与脉脉之间的诉讼等，法院判决将网络爬虫抓取数据的行为判定为不正当竞争行为，进而确立了企业数据不容竞争对手非法获取的司法准则。

在近年来的司法实践中，针对网络爬虫的刑事追责力度显著增强。如 2017 年的运满满诉货车帮侵犯个人信息案及晟名公司非法抓取视频数据案等，涉事主体均因数据抓取行为而被追究刑事责任。这些案例清晰地表明，司法层面对于网络爬虫行为的评价，正从以往单纯认定为侵权行为或不正当竞争行为，逐步向认定为犯罪行为转变，这已然成为数据企业必须面对的关键法律风险。

我国司法在对网络爬虫进行严格规制的过程中，面临着诸多困境。一方面，司法实践时常忽略网络爬虫的技术特性，存在直接将其行为认定为犯罪的倾向。另一方面，在对待网络爬虫抓取的数据类型时，司法机关并未进行区分，而是普遍采用入罪化处理方式。鉴于此，为有效避免司法实践中出现“一刀切”的倾向，有必要从行为性质以及数据对象等多个角度，对网络爬虫的违法性展开深入剖析，以此防止相关罪名遭到滥用，避免其在新时代背景下沦为“口袋罪”[1]。

2. 刑事规制的必要性

2.1. 网络爬虫的处罚现状

网络爬虫，是现代互联网的一种信息检索工具，其效率远超手动搜索查找信息。它能够自动地对所查到的信息进行浏览、筛选并存储网站的数据，有助于在海量数据中提取所需信息并进行整合，它还能搜索到未被充分利用或者难以发现的网络资源，例如隐蔽的网址和站点。因此，在金融技术、气象预报、招标采购以及多媒体内容聚合等行业中发挥着重要作用。

网络爬虫被滥用并且有可能损害他人利益之时，不能以其“技术中立性”作为法律上的阻却或者免责的事由。我国对有关网络爬虫的案件的处理也逐渐从民事处理转向了刑事处罚。2013 年的百度诉奇虎 360 违反 Robots 协议案原被告双方基于 Robots 协议是否具有效力进行辩论，法院最后根据《反不正当竞争法》第二条，判决奇虎公司承担民事赔偿责任。而随着司法对于网络爬虫问题的关注和网络爬虫适用所出现的一系列问题，单单依靠民事责任规制恶意爬虫已经不能达到刑罚相当的力度了，恶意爬虫的相

关行为逐渐扩展到刑事领域，需要刑法对此加以规制。截止到2020年，有关网络爬虫的涉嫌刑事犯罪的案件共有31件[2]。

2.2. 严重的侵害后果需要刑法规制

随着人工智能技术日益强大，导致了人工智能为了快速收集数据信息而与网络爬虫技术相结合。大量运用这两种结合的技术一方面确实大大提升了收集和删选数据的效率，但是也对公众的信息、数据安全和网络空间秩序的稳定带来了挑战。网络爬虫不仅可以通过预设信息对目标数据进行收集、删选，导致了个人信息数据泄露的风险以外，而且网络爬虫为了快速收集信息会短时间大量访问网站，给网络带宽和硬件资源带来压力，压力超过硬件设施所能承受的范围以后会导致网站服务器的毁坏和崩溃，给网站经营者造成损失。这种行为如果不进入刑法规制的范围，继续由民法规制会导致大量类似的严重后果发生，正常的网络秩序被破坏，个人信息被肆意收集，民事赔偿与行政处罚均不能限制使用者通过网络爬虫敛财的欲望，所以需要更加严厉的刑法对这种措施进行规制。

网络爬虫的快速收集信息的能力，相比手动收集信息的范围更加广泛，不仅可以收集网络信息数据还可以收集数据库以及移动设备信息。它所收集的信息数据类别更加多样，行为人能通过所收集的各种个人信息全方位地了解到受害人的情况，为其实施其他犯罪提供帮助。例如，诈骗犯通过自己或者他人爬取的个人信息，运用现在的AI换脸技术通过微信等通讯软件和被害人进行视频通话伪装成被害人的父母、亲戚、朋友骗取被害人财物。虽然网络爬虫只能对数据、信息进行爬取，但是所爬取的信息已经成为下游犯罪的预备行为或者犯罪，不法分子可以通过这些数据信息，去完成例如诈骗、抢劫、恐怖活动等对社会造成严重损害的犯罪，如果不动用刑事规制，会导致个人信息被肆意索取并成为其他犯罪的摇篮。

3. 网络爬虫行为刑法规制困境

恶意网络爬虫行为因其快速收集数据的能力，与传统侵害行为相比社会危害程度更高，目前我国刑法虽然通过破坏计算机信息系统罪等相关罪名对其进行规制，但其在刑事违法性认定上仍然存在诸多困境需要探讨解决。

3.1. 爬取对象边界认定不清

在现行司法实践过程中，存在将信息与数据不加以区分，等同运用的情形，这种现象虽然在一定程度上彰显了数据价值的日益凸显，但却忽略了信息与数据在本质上的差异以及它们各自所具有的独立性。无论从范畴归属、立法导向、法益角度哪一方面出发，信息与数据二者皆有所区别，数据与信息不能作为等同概念，两者虽然联系紧密但依旧有所区别，盲目将二者混同在一起将会导致罪名认定的扩张。同时，实践中还存在未区分数据类型的认定困境。当前我国针对非法爬取数据行为分别通过民法、行政法与刑法进行规制。在司法实践中，唯有对侵害对象的性质进行准确归类，才能准确判断法益的侵害程度，使得行为人承担相应的法律责任。然而，目前有关立法中缺乏对数据类型的准确划分，导致司法实践中容易产生不区分数据类型而一律入罪的情形，造成同案不同判现象的增加。

3.2. 爬取行为边界认定不明

在数字经济时代的大背景下，数据天然具有流动共享的特性，然而，数据的权利化和共享性存在内在冲突，赋予数据所有者权利保护，必然会在一定程度上对数据共享形成限制，“限制行为”的合理尺度往往难以精准把握。一方面，出于数据安全保护的考量，不能仅仅聚焦于数据的静态安全维护，还需兼顾其动态安全，保护范围面临从个人私密领域走向公共领域的扩张，但另一方面，数据的流通共享是实现数据价值的必由之路，数据的获取正是数据得以流通共享的起点，网络爬虫技术能够加快数据获取

效率，但其行为既包含经授权同意的合理利用行为，也涵盖违反网站协议、规避或突破反爬虫措施的爬取行为。近年来，刑法日益重视对数据安全法益的保护，但对于爬虫行为的入罪边界把握仍然不够明确，司法实务中往往出现“一刀切”的情形，虽然有利于对数据的保护，但过度规制的行为将导致数据流通渠道受阻，造成数据垄断等情况，减损数据自身的价值。因此，需要进一步明确恶意爬取与合规爬取之间的界限，从而明确恶意爬虫行为的刑事入罪门槛。

4. 侵害对象的不法性认定

如果按照网络爬虫的技术定义对其合法性进行界定，即要维持网络爬虫的技术中立性，就要通过法律规定明确网络爬虫技术的合理使用边界。从对象角度来看，数据的开放性程度决定了网络爬虫行为的正当性和有效性，因为数据安全主要保护数据的保密性、安全性、可用性，也就是数据越是开放，数据的独占性和数据的价值也就相对较低，法益保护的力度也随之减弱，网络爬虫构成犯罪的可能性也相应降低。所以，数据的开放性程度就成为了认定网络爬虫合法性界限的一个重要的维度。

4.1. 数据与信息的区别

在研究网络爬虫技术后台所采集数据对象时，存在一对核心且必须予以高度重视的概念，此即数据与信息之关联。数据与信息犹如双生花，彼此依存，难以割裂。当信息的接收者对其进行辨识之后，那些用以表示信息的符号便被称作数据。数据作为可识别的符号，其呈现形式丰富多样，或数字，或文字，或图像，然而其所蕴含的信息内容却始终如一，绝不会因载体设备之形式变迁而有所改变。信息则是对数据的阐释，是运用过程中的解码，即便数据已历经加工处理，只有借助解释方能使之下落成为真正意义上的信息。从本质层面而言，数据是客观事物之载体方式，而信息是承载着数据内容的外在表现方式。数据与信息的区别而言主要表现为其问题归属、立法导向以及法益归属的不同。

从其问题归属来看，信息与数据的差异不仅体现在表象之上，更在于它们所属的法律范畴截然不同：信息主要关联着公开与分享的议题，而数据则更多涉及到操作规范的领域[3]。例如，“政府信息公开”意味着政府依据特定条件和范围，将某些信息公之于众，使其为社会公众所了解，且不拘泥于具体的呈现形式；“政务数据开放”指的是社会公众可以进入公共网页或者平台，对相关数据进行自主浏览、下载、搜索以及分享。

从立法导向而言，从刑法规定的罪名而言，有关个人信息的犯罪例如侵犯商业秘密罪属于破坏金融管理秩序犯罪、侵犯公民个人信息罪属于侵犯公民人身权利、民主权利犯罪。可见，有关信息的犯罪保护的法益主要是经济、金融秩序和人格权，而有关数据犯罪保护的法益是社会管理秩序，所以两者的保护法益不同，也导致了保护方式的差异。

从法益的角度而言，信息保护的主要是特定信息即保密信息可以不被他人所知悉；数据则不同，因为它属于无形物，主要保护的是数据的控制权和使用权。所以，信息安全主要在于防止他人未经授权获取、披露未公开的信息；而数据安全则主要为了保护数据权利人对相关数据的控制权、使用权。在数字化技术日益成为人们不可或缺的一部分的当下，维护数据的保密性不仅仅通过对数据文件进行加密或者采取安全预防措施，更主要的是维护信息系统数据的安全，换句话说就是维护数据权利人的控制权，防止他人篡改、毁坏、盗取。数据安全不仅仅是为了数据本身的机密性，而且更主要的是维护数据控制的安全。不被他人知悉主要是为了维护适格主体访控用数据的权利，而保护特定信息秘密性虽为核心，但并非全部内涵。

根据上述几个方面的区分，数据和信息不是混同的概念，两者的虽然联系紧密但依旧有所分别。换而言之，信息公开不意味着数据公开，网络上公开的浏览信息也并非都是公开数据，不能以抓取的是网

页公开信息为由，就认定不具备刑事违法性。

4.2. 数据的开放程度

4.2.1. 抓取公开数据不属于刑法规制的范围

抓取公开的数据不属于刑法规制的范围，是秉持着刑法谦抑性原则。因为一旦数据的信息内容公开，意味着有关数据的机密性下降，不能以保护数据的保密性为由，运用刑法罪名对相关爬取行为进行刑法规制，但是如果该数据是被刑法重点保护的数据，比如著作权，应当根据具体情况，即著作权人是否授权，进行刑法评价，不宜以该著作权数据属于公开数据为由主张免除处罚。

开放数据，是数据权利人自己放弃了控制权，允许公众对数据进行自主浏览、下载、搜索以及分享。换句话说，私人主体已经失去了对该数据的支配力，丧失了独占价值与保密性。权利人同意他人访问、获取并自愿承受其不利的后果，属于“同意不产生违法”。在刑事领域上，其属于被害人承诺，不能以“未经授权”为由，主张承担刑事责任。而且，这种同意不仅阻却了刑事违法性，而且也规避了民事责任。因为，在民事领域，被害人同意是侵权责任的免除事由。个人的开放数据公众可以进行公开使用，数据主体不能因网络爬虫技术而追究侵权责任。企业的开放数据也不应当因为获取使用该数据而进行刑事惩罚，例如互联网的相关企业因为互联网市场的市场特性和运营模式，许多的网站就是通过免费数据资源、无须充值会员等噱头吸引大量用户，再通过增值服务或广告盈利，这已经成为了互联网相关公司的一种运营模式的成功范本。对于为了吸引用户而免费开放的数据资源，属于公开的商业数据，抓取公开商业数据的行为不具有刑事违法性。

并非信息一旦公开，其权利就一定无法保护，可以被肆意进行网络爬取。从法律保护来看，有些数据被刑法所重点保护，单独定罪量刑，比如侵犯著作权罪。刑法将网络上公开的著作权数据予以重点保护，即使在网站上对内容予以公开，只要未经过著作权人的授权或者许可，擅自复制著作权作品的，仍属于侵犯著作权罪，应当受到刑罚处罚，因为该罪保护的是未经许可不得复制其作品的权利，与一般数据保护的法益为数据的保密性不同。而对于刑法没有专门保护的一般数据，不能不辨认所抓取数据的类型而将爬取数据的行为都认定为非法获取公民个人信息数据罪，不然就有违刑法的谦抑性原则。

4.2.2. 爬取限制访问、获取的数据具有刑事违法性

限制访问、获取的数据，指的是数据持有人仅允许特定的主体基于特定目的在其允许的范围内进行访问获取的数据。这种限制是数据持有人在通过一定条件对访问人、使用者进行一个删选，这种数据与公开数据不同，数据的持有人要求获取者要持有某种身份比如公司员工，或者预备将该数据卖于特定的买受人以获取合适的对价，或者属于某种商业机密防止竞争对手的不正当竞争。这类数据的目的主要在于禁止未经授权知悉或者使用该数据，通过刑法前线的前移来保护这些重要的数据信息，提前对网络爬虫行为进行干预和防范，所以未经授权或者许可获取限制访问、抓取的数据具有刑事违法性[4]。

但是，并非所有的同意或者授权，都意味着可以排除刑事违法的可能性。例如，在实践中，大型企业对于个人或者小型企业数据的收集具有一定的强制性，即除了同意之外，无路可走。尤其是平台的相关隐私免责说明文件，虽然强制勾选，通过主要内容不进行强调、故意放小字体妨碍阅读等手段，给用户带来了阅读理解的障碍。相反，平台通过协议无限拓宽其权限，将各种数据爬取手段尽数罗列其中，通过“包括但不限于”等类似表达，无限放大其协议范围，使得这些公司在数据采集上毫无阻碍，而协议的相对方与其从始至终未处于平等的地位，所以，这些被爬取方的授权不属于真正意义上的自由选择。所以，对于授权方的授权要考查授权方的授权是否是当事人真实意思的表达，包括授权的时候是否具有基本的辨认和控制能力等。

5. 爬取行为的不法性认定

判断网络爬虫刑事违法性的另一关键在于判断其行为是否符合刑法所规定的构成要件，从立法文件来看，我国刑法与司法解释中关于“侵入”的具体内涵未做明确规定，仅指出其相应的行为特征，相关司法解释虽然也体现了将“未经授权”作为侵入行为认定的标准，但仍然需要进一步细化，采用实质性的技术解释对我国刑法中“侵入”的定义进行限制和解读。

5.1. 爬虫协议的效力

要想对“侵入”行为进行类型化认定，还需明确的一点在于违反 Robots 协议等爬虫协议是否属于“违反国家规定”的范畴，目前学界对于爬虫协议法律属性一直是存在争议的。我国法律并未明确规定网络爬虫协议的法律性质，对于违反爬虫协议是否需要承担刑事责任的讨论，基本分为两派。第一种观点认为应当将反爬虫协议作为认定“违法”的前置标准。Robots 协议代表着数据控制者的授权意愿，理应受到爬虫行为人的严格遵循，违背 Robots 协议的抓取行为有着诸多危害性[5]。因此，应当将违反 Robots 协议作为形式入罪的条件，而后再根据法益侵害性判断其是否达到实质可罚的程度。另一种观点则认为爬虫协议并不具备刑法上的约束力。爬虫协议仅代表网站等网络内容服务商的单方意思表示，不构成技术上有效的保护措施[6]。爬虫协议不具有技术上的强制作用，效力较弱，违反合同约定的数据抓取只构成违约责任，应采取传统的合同法规则和补救措施予以规范和制止[4]。对于上述有关爬虫协议的性质及效力问题的争论，本文认为计算机信息系统权利主体公示的用户协议或设置的爬虫协议作为约定性的文字表述，并不能将其看作安全保护措施，无法作为一项标准对侵入行为进行判断。在司法实践中，若认为爬虫协议仅具备告知作用，而不具备法律上的约束力与强制力，将会减弱对恶意爬取数据行为的规制作用。然而在一般情况下，爬虫行为都无法获得网站授权，若赋予爬虫协议以法律上的意义，将违背单方声明爬取数据行为均认定为超越授权的行为，将会导致善意爬虫与恶意爬虫的界限更为模糊，无疑会扩大爬虫协议制定方的权利。将违反爬虫协议的行为一律入罪，虽然能够加强对恶意爬取数据行为的管制，但也会引发数据垄断等不正当竞争行为，减弱市场数据共享带来的良性竞争，影响公平、开放的市场秩序。

网络爬虫本质上是一种模拟浏览器并且高效率、大规模地获取数据的行为，其本身就容易受到网站禁止访问的声明，区分善意爬虫与恶意爬虫，将违反爬虫协议或规避反数据爬取措施作为前置标准显然有失偏颇，容易造成实务处理中的“一刀切”。爬虫协议并不属于任何规范性文件，违反爬虫协议行为的危害程度远不及避开或突破计算机信息系统的安全保护措施的行为，因此违反爬虫协议的行为仅具有民法意义上“未经授权”的效力，而不能将其判定为刑法意义上的“非法”。非法获取计算机信息系统数据罪的保护法益是数据安全，在涉及爬虫案件时，数据的保密性是否受到侵害才是入罪标准应当考察的，只有爬取非公开信息且达到情节严重的标准时，才能评价为不法。爬取公开信息但是违反网站规范或者突破反爬措施时，不具有该罪的法益侵害性，可运用合同法规则或者行政法规予以规制。

5.2. 规避反数据爬取措施的行为性质

认定网络数据爬取行为是否构成犯罪的关键在于明确反爬虫措施的性质，即规避反数据爬取措施的行为是否构成《刑法》第 285 条中的“非法侵入”。反数据爬取措施设置的目的是区分公开信息与非公开信息，以此形成一个相对私密的网络空间。相较于爬虫协议的“弱”保护意愿，反数据爬取措施的设立体现了对数据的“强”保护意愿，因此突破或规避反数据爬取措施的行为具有一定的法益侵害性基础，但不能仅以此作为认定违法的基础。我国司法解释中的表述为“计算机信息系统安全保护措施”，将反爬虫机制视为与用户身份信息机制同态的计算机信息系统安全措施的观点属于类推解释，由此得出的强行爬取数据构成侵入的结论也无法成立[7]。判断反数据爬取措施的性质，应当从技术性解释的视角出发，

采取实质性判断，通过验证用户身份以界定其是否具备相应权限，以此具体化计算机系统安全保护措施的概念。

本文认为应当将安全保护措施理解为访问控制机制，只有当某些数据资源处于对特定身份人员开放的保密状态时，才有安全保护措施存在的必要，应当将安全保护措施的内涵限定为根据访问者身份来判断其是否有访问或获取数据资源权限的控制机制[8]。安全保护措施的核心功能在于对用户访问权限的甄别与管控，旨在防止未经授权的个体访问特定资源。此类措施通常适用于封闭性网站或系统，且需预设访问权限机制。然而，反爬虫措施与访问控制系统存在本质差异，其并不涉及权限管理问题。例如验证码登陆机制或 User-agent 等方面的限制虽然在形式上表现为技术性措施，但其性质与安全保护措施之间仍然存在显著差异。User-agent 作为浏览器版本的标识参数，并不具备身份验证的功能属性，因此无法被认定为安全保护措施。验证码登陆机制的核心功能在于识别并排除自动化程序的访问行为，其本质是一种对用户进行能力验证的机制，而非对用户访问权限的实质性判断。因此，将反爬虫措施纳入计算机信息系统安全保护措施的范畴，属于类推解释，而基于该类推解释将网络数据爬取行为定性为侵入行为的观点显然缺乏理论依据。

6. 网络爬虫刑事违法性认定完善路径

6.1. 建立数据分级保护制度

根据我国《数据安全法》规定，要对数据采取分级分类保护，为确保刑事立法与前置法之间的有效衔接协调，解决运用刑罚条文处理网络爬虫类案件时罪责行不适应的问题，我国刑法也应当建立数据分级保护制度。建立数据分级保护制度，首先应当明确数据的重要程度以及遭受侵害后的危害程度，对于国家重点领域、新兴领域的核心数据进行重点保护，将通过恶意爬虫等行为非法获取该类核心数据的行为纳入刑法规制，将其作为破坏计算机信息系统罪的加重情形，对此设置更高的法定刑，实现对数据的分级保护。此外，对于其他领域的数据，应当以其授权开放程度作为依据进行分类保护，细化刑法对于数据开放程度的分级分类，对破坏计算机信息系统罪、非法获取计算机系统数据罪作更为详细的解释，避免在司法实务中出现一刀切，成为“口袋罪”。最后，除刑法规制外，还应加强行政机关对于信息网站的合规检查，强化行业间自律风气，提前防范由恶意爬虫行为引发的犯罪。

6.2. 明确行为不法的认定标准

进一步对破坏计算机信息系统罪、非法获取计算机系统数据罪作出解释，明确其行为不法的认定标准，即将是否避开或突破访问控制机制作为判断网络爬虫行为刑事违法性的认定标准。以是否避开或突破访问控制机制为行为不法的认定标准，与现有规制网络爬虫行为的相关司法解释之间具有一定共通之处。访问控制机制的设立目的为形成私密的封闭数据空间，以屏蔽非授权用户获取非公开数据。突破访问控制机制获得非公开信息的行为，与司法解释中“采取避开或突破计算机信息系统安全保护措施”相同，都是对“侵入”行为的进一步描述与解释。同时，明确行为不法的认定标准，有助于司法实践中有效区分刑事违法与民事违法，避免将违反爬虫协议或突破反爬虫措施获取公开信息等危害性并不高的行为认定为犯罪，有助于促进网络环境中数据的交互共享。

7. 总结

现如今，随着互联网大数据的迅速发展，数据安全愈发受到重视，网络爬虫行为也因此成为研究热点，近年来网络爬虫行为逐渐由民事规制转向刑事规制。网络爬虫行为作为抓取数据的技术基础行为，一方面能够促进数据流通共享，但恶意爬虫行为也会侵害数据安全，产生不良影响。我国现行立法上的

缺失导致司法实践中存在诸多问题，破坏计算机信息系统罪具有成为新时代“口袋罪”的风险。本文从对象和行为两方面入手，探讨如何对爬虫行为的刑事违法性进行合理认定。首先，数据的开放性程度是认定网络爬虫合法性界限的一个重要的维度，抓取公开数据不属于刑法规制的范畴，爬取限制访问、获取的数据才具有刑事违法性。从行为入手，违反爬虫协议不能作为网络爬虫行为刑事违法性的认定标准，只有规避、突破访问控制机制的行为才能被认定为具有刑事违法性的行为。最后，本文提出建立数据分级保护机制、明确行为不法的认定标准等措施，以期解决网络爬虫行为的民刑衔接，构建更为完善的网络爬虫行为规制体系。

参考文献

[1] 刘艳红. 网络爬虫行为的刑事规制研究——以侵犯公民个人信息犯罪为视角[J]. 政治与法律, 2019(11): 16-29.

[2] 苏青. 网络爬虫的演变及其合法性限定[J]. 比较法研究, 2021(3): 89-104.

[3] 孙杰. 数据爬取的刑法规制[J]. 政法论丛, 2021(3): 115-125.

[4] 杨志琼. 数据时代网络爬虫的刑法规制[J]. 比较法研究, 2020(4): 185-200.

[5] 曹阳. 我国对违反“爬虫协议”行为的法律规制研究[J]. 江苏社会科学, 2019(3): 159-167.

[6] 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.

[7] 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.

[8] 孙禹. 论网络爬虫的刑事合规[J]. 法学杂志, 2022, 43(1): 162-172.