Dispute Settlement 争议解决, 2026, 12(1), 199-207
Published Online January 2026 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2026.121026

Hans汉斯

恶意网络爬虫行为的刑法规制研究

石郑晓

青岛大学法学院，山东 青岛

收稿日期：2025年12月20日；录用日期：2026年1月13日；发布日期：2026年1月23日

摘　要

网络爬虫作为互联网行业广泛应用的技术，极大地便利了人们信息收集和检索，同时也成为了违法犯罪的便捷工具。对具有主观恶意的网络爬虫行为进行有效的刑法规制迫在眉睫。基于我国司法实践中对网络爬虫行为入罪标准不一、罪名适用模糊的现状，应从构成要件入手，从形式和实质两方面界定恶意网络爬虫的入罪标准。形式上应限定爬取行为的非开放性及侵入手段的非授权性，实质界定的标准应是爬取行为的法益侵害性。在明确入罪标准后将恶意网络爬虫行为予以类型化定性分析，从而实现更加罪名适用的精准性和特定法益保护的有效性。

关键词

网络爬虫，非授权性，非法侵入计算机系统罪，破坏计算机信息系统罪

Criminal Law Regulation of Malicious Web Crawling

Zhengxiao Shi

Law School of Qingdao University, Qingdao Shandong

Received: December 20, 2025; accepted: January 13, 2026; published: January 23, 2026

Abstract

As a widely used technology in the internet industry, web crawlers have greatly facilitated people's information collection and retrieval, while also becoming a convenient tool for illegal and criminal activities. It is imperative to effectively regulate web crawling behavior with subjective malice through criminal law. Based on the current situation in China's judicial practice—where the standards for criminalizing web crawling behavior are inconsistent and the application of charges remains ambiguous—it is necessary to start from the constituent elements and define the criteria for criminalizing malicious web crawling from both formal and substantive aspects. Formally, the scope

文章引用: 石郑晓. 恶意网络爬虫行为的刑法规制研究[J]. 争议解决, 2026, 12(1): 199-207.
DOI: 10.12677/ds.2026.121026

should be limited to the non-open nature of the crawling behavior and the unauthorized nature of intrusion means; substantively, the criterion should be the infringement of legal interests caused by the crawling behavior. After clarifying the criteria for criminalization, a typological qualitative analysis of malicious web crawling behavior should be conducted, so as to achieve more precise application of charges and enhance the effectiveness of protecting specific legal interests.

Keywords

Web Crawler, Unauthorized Nature, Crime of Illegally Intruding into Computer Information Systems, Crime of Sabotaging Computer Information Systems

1. 引言

随着科技网络、信息技术发展进程的突飞猛进，我们已然踏入大数据时代。数据象征着互联网企业的核心竞争力，商业价值越来越高，人们对数据需求也越来越大，但因为互联网上的数据信息庞杂，因此为满足人们在互联网上高效的完成数据检索的需要，网络爬虫技术应运而生[1]。

华东政法大学张勇教授表示“技术是中立的，但技术应用永远不是中立的”。网络爬虫作为数据收集环节的一项重要的中立技术，其创建之初是为了帮助搜索引擎高效收集数据，本身并无好坏之分。但在认识到网络爬虫技术能给予用户便利的同时，也不能忽视因其滥用、恶意使用所带来的法律风险。各种利用网络爬虫技术爬取网站数据的行为正处于难以界定其行为性质的灰色地带，导致不正当竞争和数据泄露事件频发[2]，在此背景下，网络爬取数据行为刑法如何规制的探讨不绝于耳，由于爬虫行为手段不一、技术方式复杂、侵害后果不尽相同，司法实践对恶意网络爬虫行为涉及的入罪边界以及各个罪名的适用并不统一。

美国围绕《计算机欺诈与滥用法案》(CFAA)展开持续讨论，重点厘清“未经授权访问”的认定标准，通过典型判例明确爬虫行为不得突破网站明确设置的访问限制[3]。欧盟则基于 GDPR 框架，聚焦数据爬取中的“知情同意”原则，研究自动化采集场景下个人信息保护的具体规则，强调数据主体的权利保障与爬虫操作者的合规义务。国外普遍重视技术规制与法律规制的协同，研究涵盖爬虫协议(robots.txt)的法律效力认定、反爬技术措施的合法性边界等议题。同时，学界关注行业自律机制建设，探索通过技术标准、行业规范引导爬虫行为合法化，形成了“法律约束 + 技术规范 + 行业自律”的多元规制研究体系。且随着数据跨境流动需求增加，国外研究聚焦跨境爬虫行为的管辖权划分、不同法域规则冲突解决等问题，提出了基于数据类型、行为发生地、损害结果地的管辖认定思路，为跨境规制提供了理论支持[4]。

本文针对这一问题展开探讨，以明确网络爬虫行为的罪质，把握网络爬虫行为入罪的标准及罪名的适用，避免产生刑法过度干预与轻纵犯罪分子的两极现象，保障市场主体的合法权益，营造数字经济市场公平竞争环境。弥补了现有研究中技术与法律融合不足的缺陷，提出“技术特征－风险层级－规制强度”的对应关系理论，丰富了网络爬虫刑事规制的理论体系。构建的量化认定标准与差异化规制规则，可为司法机关办理爬虫相关案件提供明确指引，减少同案异判现象；跨部门法衔接机制的完善，为执法与司法实践提供了系统性解决方案。针对深层网络爬虫等新型技术场景的规制建议，回应了大数据时代的技术发展需求，为数据安全保护与数字经济健康发展提供了法律保障。

2. “网络爬虫”：一种自动抓取信息的程序

网络爬虫作为一项在互联网应用广泛的程序，为人们的生活带来了极大的便利。网络爬虫作为一项中立的技术，在其提高检索效率帮助人们事半功倍的同时，越来越多利用网络爬虫侵犯他人利益的情况亟需得到合理规制。

(一) “网络爬虫”的语意辨析

网络爬虫，又称为网络蜘蛛、网络机器人，是一种高效的、自动抓取信息的计算机程序。它按照预先设定的规则，对互联网上的数据信息进行识别、提取和汇总等并建立索引，以满足互联网用户与日俱增的网络数据与资源需求。网络爬虫因其结果精准、过程高效、范围广泛而在精准搜索、数据深度挖掘、网页漏洞检修等方面广泛应用，现如今已经成为各大网站普遍使用以及相关专业人士所必备的技能。

网络爬虫作为技术而言是具有中立性的，既可以充分发挥上述优点加快信息流通速度，帮助人们实现快速精准搜索，也存在着技术风险例如抓取过程中易造成网络拥堵、服务器瘫痪以及侵害个人法益风险如个人信息等问题。理论上网络爬虫分为善意网络爬虫和恶意网络爬虫。善意网络爬虫遵守行业规则，即 Robots 协议，能够增加网站的曝光率和知名度，而恶意网络爬虫则无视 Robots 协议。Robots 协议是网站所有者通过置于网站根目录下的文本文件 Robots.txt，提示网络爬虫网页是否可被抓取。因其简单高效，故而被认定为搜索引擎行业内公认的、应当被遵守的行业道德[3]。

善意网络爬虫如白帽子技术也被称为“道德黑客”，虽有侵入网站的抓取行为，但由于其目的并不抱有恶意，而是出于实验新技术或是检测安全漏洞并反馈给互联网平台等使其能够及时修复完善系统的善意目的，因此被认定是善意网络爬虫。道德黑客的判断分析需坚持形式与实质并重：先审查客观构成要件，再通过法益侵害性判断与正当化事由排除违法性，最后以主观故意、目的与期待可能性限制有责性。多数善意测试行为因无实质法益侵害、存在阻却事由或无犯罪故意而不构成犯罪；仅在造成实质损害且主观有责时，才可能被归责。Robots 协议并不属于强制性法规，违反 Robots 协议强行爬取数据被视为违反诚实信用原则和不具有商业道德的行为。而恶意网络爬虫无视 Robots 协议，违背网站意愿，强行突破反爬规则暴力爬取网站数据，不仅可能导致个人隐私、商业秘密的泄露，并且同时间内大量投放爬虫也易引起网站拥堵、服务器崩溃的问题，给企业造成损失。

(二) 恶意爬虫行为亟需规制

随着互联网行业日新月异的发展以及在当代人生活中应用的进一步普及，恶意网络爬虫的不正当行为也可能涉嫌非法。在大数据时代，数据的经济价值进一步凸显，而人工智能的兴起更使得恶意网络爬虫如虎添翼，进一步增强了网络爬虫的信息识别与收集能力。因此再加上网络爬虫本身所具有的低门槛、高隐蔽性等特征，恶意滥用网络爬虫技术所造成的损失也在进一步扩大。在此情形下，探讨恶意网络爬虫的刑事违法性已迫在眉睫[4]。

首先，网络爬虫行为本身即存在技术风险。网站通常提示的“网页无法显示”“下载失败”等问题即可能是大量网络爬虫在短时间内访问此网站系统，导致其拥堵卡顿，网站负荷过大无法正常运行。虽然实践中极少出现网络爬虫引起服务器崩溃而构成犯罪的情况，但不能忽视国家计算机信息系统有可能受到网络爬虫侵入的情形。

其次，是网络爬虫爬取数据信息将会滋生下游犯罪。恶意网络爬虫行为可能会导致商业秘密泄露、侵犯公民的个人信息、造成不正当竞争、危及国家秘密等一系列后果[5]。例如曾经风靡一时的“AI 换脸”即是利用网络爬虫技术收集公民公开发布的照片视频，从中提取出人脸信息，再进行深度伪造，合成新视频来进行诈骗活动。不正当的网络爬虫行为使其下游犯罪更加多样与便捷。同时，网络爬虫也显现出成为上游犯罪技术手段的特征，被称为“数据掮客”。例如在很多放贷案件当中，都是利用网络爬虫收

集不能按时还款的对象信息进行下一步操作，精准识别其借贷需求从而骗取被害人财物。

3. 恶意网络爬虫行为的司法规制困境

现如今，各种利用网络爬虫技术爬取网站数据的行为正处于难以界定其行为性质的灰色地带，导致不正当竞争和数据泄露事件频发。当前学届对于网络爬虫技术多存在误读且我国对于网络爬虫的立法并不完善，出现了口袋罪趋向以及部分违法行为无法可依的状况。

(一) 现行刑法的规制现状

近年来，我国不断强调数据安全，数据作为网络爬虫行为的对象与其息息相关。由此我国对于网络爬虫的司法规制呈现出一种“严厉态势”，由民事领域逐步转向刑事领域。在上海晟品公司爬虫入罪案中司法机关提到“在大数据时代，数据的独立价值与权利属性已经越来越得到广泛重视”；在酷米客诉车来了非法获取数据案中也提出“数据能够为原告带来现实或潜在的经济利益，已经具备无形财产的属性。”越来越多因数据抓取而被起诉或定罪的案例表明，我国对于网络爬虫的法律评价正逐步由违反商业道德的不正当竞争行为、侵权行为转向违法犯罪行为。

当前，我国关于恶意爬取数据的相关规定主要分布于《反不正当竞争法》《民法典》侵权责任编、《刑法》及《网络安全法》等中。而在《刑法》当中主要涉及第 217 条“侵犯著作权罪”、第 219 条“侵犯商业秘密罪”、第 253 条之一的“侵犯公民个人信息罪”、第 285 条“非法侵入计算机信息系统罪”“非法获取计算机信息系统数据罪”与“非法控制计算机信息系统数据罪”及第 286 条“破坏计算机信息系统罪”等。然而上述法律并未对爬取数据的行为做出明确具体的规定，更多只是为规制网络爬虫行为提供指导性立场。由逐年递增的关于爬取数据行为的刑事司法审判中可知，实践中对恶意爬取数据行为的规制罪名主要集中于侵犯公民个人信息罪、非法侵入计算机信息系统罪、侵犯著作权罪三个罪名上。

有学者指出我国当前对网络爬虫行为的刑法规制同样呈现扩张化的倾向。主要表现在两个方面。其一，司法机关忽视了数据本身的公共性与流通性，将一切突破或者绕过反爬虫技术措施的行为皆认定为非法侵入[6]，扩大了此行为违法性的认定范围。生活中常见的“验证码”实际上就是一种反爬措施，主要有短信验证、拖动滑块至正确位置以及按照提示点击图片等等。这些技术的主要目的在于区分访问者是否为真实人类用户，以免被网络爬虫大量访问造成网站拥堵等问题，而不在于阻止用户的访问其相关数据，限制访问权限。上文中规定是否为可爬取内容的“Robots 协议”也是一种反爬措施。其二，理论上网络爬虫在其中存在概念外延的现象，将不属于网络爬虫技术范围的行为也视为网络爬虫行为。例如在网络爬虫罪名集中的侵犯公民个人信息罪当中，除却爬取行为还有后续的传播、牟利等行为。而法院认定构成犯罪的行为可能并非其爬取行为而是后续行为。但在认定网络爬虫的入罪标准时，某些学者却并未对其进行甄别。

(二) 现行刑法的规制反思

基于上述规制网络爬虫的司法现状可知我国对于网络爬虫的法律规制正在进一步强化，但在实践中由于相关立法并不精确以及对爬取行为和后续行为分辨模糊致使对于网络爬虫的入罪标准并未统一。而网络爬虫本身作为一种工具，再加之司法实践中兜底性罪名适用居多，也会导致罪名适用模糊的问题。

1、入罪标准不一

有学者指出，我国司法对网络爬虫的规制有不识别网络爬虫技术特征而一律入罪和不识别网络爬虫抓取的数据类型一律入罪的特征。不识别网络爬虫的技术特征是指司法机关未能考虑到网站技术排他性不同，违背网站意愿，故意避开或强行突破等抓取行为所应承担的法律责任也不同。不识别网络爬虫抓取的数据类型是指网站数据的开放程度不同，既有完全开放可被摘用的数据，也有仅限用户注册后浏览，不允许不当使用的数据，以及完全不允许访问的数据例如商业秘密等。而司法实务中对于不同数据类型

抓取的入罪标准并无完全细分，我国相关法律条文也并未做出明确规定。我国刑法中并无直接针对网络爬虫的条款，在其他关于数据安全方面的法规仅强调“不得以非法方式收集数据”。

同时，上文中所提到的网络爬虫的概念外延，使得网络爬虫几乎包含一切自动性的数据获取行为，以及相关犯罪的关联行为[7]。网络爬虫本身是一项高效的中立技术，其恶意行为的危害性主要在于大量投放后自身带来的垃圾流量问题，恶意侵入、破坏系统问题以及后续相关数据信息的使用行为带来的社会危害性两方面。由于网络爬虫本身所具有大量抓取数据的技术特性，本身很容易达到以数据信息数量为衡量标准的入罪界限。而根据形式与实质相统一原则，不仅要明确恶意网络爬虫具体的可罚性的侵入方式及相关数据标准，还应明确恶意网络爬虫行为本身的法益侵害性[8]。在司法实例中，既存在法益侵害性大于“晟品公司案”而作为民事案件处理的情况，也有忽略网络爬虫的工具属性，不结合网络爬虫在案件中具体造成的社会危害性大小而“打包式”入罪的情形。

2、罪名适用模糊

如今我国的司法实践中对于恶意网络爬虫行为的定罪量刑呈现出模糊性的特点。一方面是由于网络爬虫行为的行为本身与其爬取的对象、爬取的后续行为在某些案件中存在交叉，各主体之间法益边界较为模糊。这种交叉会导致司法实践中对行为取向的定性不同，因而带来保护法益和量刑幅度的不同[9]。同时随着对信息与数据概念的进一步细分以及对数据法益的深入研究，对行为对象的解释模式不同也会导致罪名适用的不准确性。另一方面由于规范恶意网络爬虫行为的法律规范并不完善，相较快速发展的信息网络具有滞后性且缺乏具体的可操作性，我国恶意网络爬虫定罪的罪名主要集中在非法获取计算机信息系统数据罪、侵犯公民个人信息罪和侵犯著作权罪三个罪名上，愈发呈现出一种兜底性的趋势。这不仅会强化恶意网络爬虫刑法规制领域口袋化罪名的适用，也会导致具体个案中的特定法益得不到有效的保护[10]。

4. 恶意网络爬虫行为的入罪标准考量

将网络爬虫限缩至具备主观恶意的行为领域，才有了刑法规制的必要性。由于网络爬虫技术的不断异化使用，爬虫行为所呈现的犯罪模式亦有所不同。司法实践中的判决案例表明，网络爬虫行为的刑事案件中被判处的罪名主要有非法侵入计算机信息系统罪、非法获取计算机信息系统数据罪、破坏计算机信息系统罪以及侵犯公民个人信息罪。可以概括的讲，各项罪名的构成要件有所差异，但主体构成一致，在构成要件上具有共同点。下文将以数罪的共同构成要件要素展开分析，为恶意网络爬虫行为的刑事解决提供清晰的可行方案。

(一) 形式界定：爬虫行为具备客观不法

恶意网络爬虫行为的犯罪对象为计算机信息系统中的数据，上述提及的数据犯罪所侵犯的法益为计算机信息系统的安全和秩序。在此意义上讲，以数据为目标对象的行为未必纳入刑法规制的范围，此类行为只有侵犯了数据犯罪的法益才具有了社会危害性和可谴责性，需要刑法规范予以科处刑罚[11]。

1、爬取的“数据”应具有非开放性

前文所述，网络爬虫行为以数据为犯罪对象，而如今的网络数据万千，层出不穷。根据数据的分级分类规则，按照数据的敏感程度分级，数据分为公开数据、秘密数据、机密数据和绝密数据。在此为方便区分，可以称之为公开数据和非公开数据两大项。

有学者将数据是否具有公开性作为爬虫行为入罪的界限，如吴卫认为，不应认为通过网络爬虫爬取公开数据的行为具有不法性。按照此分级规则来确定爬虫行为的社会危害性是不恰当的。首先，对于非公开数据，爬虫行为显然侵犯了数据的秘密性与内在价值，无疑在客观上已构成行为不法。其次，对于公开数据的爬取是否全部意味着行为的限度合法，是否不会造成数据的价值破坏？此问题不能一概而论[12]。

在此需明确，数据的公开性与开放性是两种不同程度的属性，数据虽已公开但并不意味着一定开放获取，当数据的公开程度升高至允许人们自由获取时，数据便具有了开放性。开放性意味着数据不受约束，可以供人们免费获取并不对使用获取次数做出限制，可以认为数据在此具有公共产品属性。高富平教授就认为，“数据是否公开不是合法性判断的标准，是否为开放数据才是判断爬虫合法性边界的考虑因素之一。”因此，应将数据的开放性作为网络爬虫行为合法与否的关键，只有所爬取的数据不具有开放性，此行为才具备了入罪可能。

2、“侵入”手段应具有非授权性

虽然网络爬虫是一项中立的网络技术，行为人通过此项技术获取规则之内的信息更有利于社会经济发展。然而当爬虫行为超越了一定的边界，便产生了爬虫行为入罪的风险。不同类型的爬虫行为其中都蕴含着对于“侵入”的认定。侵入行为无疑是影响网络爬虫行为罪与非罪的关键。

在非法获取计算机信息系统数据罪的认定过程中，根据《中华人民共和国刑法释义(第六版)》内容，“侵入”是指未经授权或者他人同意，通过技术手段进入计算机信息系统。采用网络技术手段以外的其他手段不属于本款规定的行为。结合《计算机安全解释》第 2 条对“侵入、非法控制计算机信息系统程序、工具”的规定，根据该司法解释，考虑到数据传输模式的特殊性，“非法侵入”应当初步解释为“未经授权或超越授权进入计算机信息系统”。

例如，在卫某、龚某等非法获取计算机数据罪一案[1]中，被告人龚某在明知卫某使用账号目的的情况下，向被告人卫某提供自己所掌握的百度凤巢系统内部账号和密码。被告人卫某利用龚某所提供的账号和密码，违规登陆百度在线网络技术(北京)有限公司凤巢系统，查询、下载该计算机信息系统中存储的客户数据，并交由被告人薛某出售给他人，违法所得共计人民币 37,000 元。本案中的行为人进入计算机信息系统的方式有所不同——本案被告人龚某系被害公司的员工，外部人员利用其内部权限登陆被害公司系统，获取存储于被害公司的数据。对于这种利用内部权限登陆计算机信息系统获取数据的行为能否认定为刑法规定的“侵入”？这是本案定罪的关键。

本案中被告人的行为首先客观上超越了被害方的授权范围。具体表现在其一，被告人龚某将账号、密码、token 令牌等提供给非公司员工卫某使用：被害公司允许员工使用公司内部的账号和密码，但公司明令禁止员工擅自出借账号、密码；其二，行为人登陆系统后下载了无权下载的数据：被告人龚某虽有权限进入管理系统，但根据被害方规定，并没有权限下载与其正常业务无关的客户信息。同时，被告人进入系统的主观目的也在于超越授权范围去获取相应信息系统内数据。综上所述，虽然本案中被告人采取了相对“温和”的手段，但却符合超越被害公司的授权范围去获取计算机信息系统数据这一行为本质，因此应认定为“侵入”。此案例佐证了“超越授权”对于爬虫行为客观方面“非法侵入”的认定。

(二) 实质界定：爬虫行为造成法益侵害

持有“规范违反说”的学者认为，网络爬虫行为涉及刑事犯罪的边界即为法律构成中“违反国家规定”的成立，要求爬虫主体在客观上违反了“Robot”协议，或者违反其他反爬虫协议等未经授权和超越授权之方式。此观点强调爬虫行为的刑事违法性的同时忽略了其行为是否达到实质可罚的程度。

于数据规制而言，由于反爬虫措施的制定与实施的目的不同，所使用的技术手段亦有所区别，因此具备刑事违法性的爬虫行为未必具备在实质上侵害了相关网络主体的法益[13]。

比如“道德黑客”的网络数据抓取行为，“道德黑客”(也称“白帽子”)是一种网络修复工具，他们通过测试，检查并发现网络漏洞，不会进行攻击，而是反馈给相关平台或者企业，从而促进其修复和完善。所谓的“每一朵乌云都有一朵金边，每一顶白帽子也都有一道黑边。”[14]从法律构成看，“道德黑

[1]参见北京市海淀区人民法院(2017)刑初 392 号刑事判决书。

客”行为未经授权侵入了网站，浏览并获取的网站存储的数据，属于违反国家规定抓取数据，具备刑事违法性，可以构成非法获取计算机信息系统罪。但在主观方面，此种浏览网站存储数据的目的是为了证实安全漏洞是否存在，并非明知而故意侵入，实质上并未给网站带来了实质性的损害。根据我国刑法学理论，犯罪是具有相当程度的社会危害性的行为，“道德黑客”善意目的在一定程度上降低了其主观恶性和社会危害性，如果其非法获取计算机信息系统数据的数量不大，综合主客观方面的情节评价为情节显著轻微，应当按照我国刑法第十三条“但书”的规定，不认定为非法获取计算机信息系统数据罪。

5. 恶意网络爬虫行为的罪名适用考量

在整体上对于爬虫行为的刑事边界予以厘清之后，需要具体分析不同类型的爬虫行为所涉及的罪名，着眼于爬虫行为的阶段性与实现状态，基于类型化的研究方法，可将其分为“侵入型”爬虫、“获取型”爬虫和“破坏型”爬虫三种类型。将复杂多样的爬虫行为予以类型化，便于精准地适用不同的罪名，以期对爬虫行为实现正当的刑法规制[15]。

(一) “侵入型”爬虫行为的定性分析

在网络爬虫行为异化之后，行为的动态过程包括初始化、访问、突破爬虫防范措施和获取数据四个阶段，其中初始化过程是不具备任何风险性的，爬虫主体从访问阶段开始进入计算机系统，此时进入的网站性质成为了其行为合法与否的关键。爬虫程序作为一种人为编写的技术手段，其使用行为的主观目的决定了其产生的法益影响。随着反爬措施的进步，爬虫程序亦在内卷式发展，当其进入特定领域的系统网站而被评价为“侵入型”爬虫行为，即存在的非法侵入计算机信息系统罪的适用空间。

从犯罪构成看，非法侵入计算机信息系统数据罪的犯罪对象仅限于国家事务、国防建设、尖端科学技术领域的计算机信息系统。该罪的保护法益是特定领域的计算机信息系统安全，其重点在于对系统入侵的限制与防御，属于典型“行为犯”的构成。其中，根据《危害计算机解释》第十一条，对于三种领域的计算机信息系统有着更为精确的释义，即“计算机信息系统”和“计算机系统”皆指具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备等；第十一条亦明确规定：确认上述三大领域计算机系统与否应当委托省级以上负责计算机信息系统安全保护管理工作的部门检验。

比如，在滕守昆等非法侵入计算机信息系统案[2]中，被告人滕守昆等人为在帮人处理车辆交通违章业务时方便查询车辆信息，违规在其手机下载安装“四川公安交警警务云平台”APP 软件，并通过非法获取的用户名及密码登录网站平台，对相关车辆的交通违章信息非法查询。经四川省公安厅网络安全保卫总队认定：《四川公安交警警务云平台》和四川公安交警警务云平台 APP 计算机信息系统属于国家事务类网站，属于前文所述三大领域内的计算机系统，法院依法判处滕某等人非法侵入计算机系统罪。

(二) “获取型”爬虫行为的定性分析

爬虫主体突破防范措施之后的数据获取行为是刑法亟需规制的主要内容。本文从保护法益的角度出发，通过对爬取对象的类型化阐释以便准确适用不同的刑事罪名。从现有的爬虫程序所获取的对象来看，根据其特点可以大致分为个人信息数据、商业秘密数据、独创性数据和其他数据。

首先，对于利用爬虫技术侵入计算机信息系统，抓取具有“可识别性”的个人信息数据的行为，宜以侵犯公民个人信息罪予以规制。如今的信息网络时代，公民的个人信息大都于网络上进行存储，容易受到爬虫程序的获取。其中，公民个人信息的范畴不仅仅局限于姓名、身份证号等一对一识别性的数据信息，还包含公民的财产线索、家庭住址、私人账户信息等数据，这些数据虽不具有一对一识别的特征，但依然可结合相关信息捕捉个人身份，具有“可结合识别”的特征。当行为人违反国家规定，恶意适用

[2]参见四川省攀枝花市仁和区人民法院(2017)刑初字 135 号刑事判决书。

爬虫程序出售、提供、窃取或以其他方法获取该信息时，有侵犯公民个人信息罪的适用空间。其次，对于利用爬虫技术侵入计算机信息系统，抓取涉及“商业秘密”的企业数据的行为，宜以非法获取计算机系统数据罪予以规制。司法实践中，由于企业的运营管理需要广泛的数据支撑，其数据资源可以直接用于商业活动，具有实用性；能够创造商业利润，为秘密持有者带来收益，具有经济性；同时由于数据的实用性和经济性而具有保密性。因此，基于企业数据对于企业的发展及运营方面的重要作用，行为人通过爬虫技术非法获取企业数据的行为将会侵犯企业对数据的排他性占有权，侵犯了信息网络平台良好的竞争秩序。在此，需要强调刑法第二百八十五条[3]之规定，该犯罪构成为行为犯，因此应将被爬取企业的损失作为“情节严重”的构成要件要素予以考虑，无需将企业的实际损失作为罪名适用的必要条件。最后，作为普通企业数据的一种——独创性数据，通过爬虫技术获取该类数据作品的行为宜以侵犯著作权罪予以规制。在企业的运营中，不乏出现新的产品设计与研发，从产品创新导宣传销售的产业链中不可避免的通过信息网络形成自己的竞争优势。因此在企业对具有独创性的数据作品设置反爬虫的措施与规则之后，行为人仍以营利的目的未经授权或者超越授权，回避反爬虫措施从而获取数据作品，违法数额较大或者其他具有严重情节的行为，侵犯了所有权人的专有控制力以及排他性处分、使用收益权能，则可能构成侵犯著作权罪。

(三) “破坏型”爬虫行为的定性分析

爬虫主体对于网站、平台中而言，除了具有侵入和获取数据带来的风险，其风险性还可以进一步体现在对于数据的处理或者对于网站平台的访问表现上。根据刑法第二百八十六条的规定，违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，或者对计算机信息系统中存储、处理、传输的数据和应用程序进行删除、修改、增加操作的，都构成破坏计算机信息系统罪。在此，可以将以上多种表现模式分为两类行为：其一是故意频繁多次访问计算机系统的行为，因为计算机信息系统都有其本身的承载负荷，大量多次地访问该系统，会使得系统压力过大，甚至出现系统崩溃现象，干扰该系统的正常使用与运行秩序；其二是随意删除或者修改、增加计算机系统数据的行为，该行为是直接破坏计算机信息系统的行为，行为造成的严重后果同样能够导致计算机信息系统运行受阻。以上两类行为即为恶意爬虫程序的存在的行为类型，在违反前置性规定的基础之上，出现以上行为表现的，则具有破坏计算机信息系统罪的适用余地。

如在王博一文、黄业兴破坏计算机信息系统案[4]中，法院查明，2017 年 7 月间，被告人王博一文曾受全运会组委会工作人员委托对接待服务管理系统的美工进行改善。王博一文为获得对该系统的安全维护业务，指使被告人黄业兴对系统进行攻击。同年 8 月 8 日，黄业兴编写“爬虫”程序后，利用王博一文提供的登录信息，将“爬虫”程序植入全运会组委会接待服务管理系统。由于“爬虫”程序在运行中自动点击了“删除”按钮，导致该系统内存储的 4000 余条参赛运动员及技术官员来津抵离信息、酒店住宿信息、人员身份信息被删除，组委会接待服务部额外投入人力，对被删除的信息进行人工补录，并对部分参赛运动员以及技术官员进行“举牌”接送服务，给全运会组委会的接待服务工作造成了严重影响，其行为均已构成破坏计算机信息系统罪。

参考文献

[1] 张莉. 数据治理与数据安全[M]. 北京: 人民邮电出版社, 2019.

[3]刑法第 285 条规定：“非法获取计算机信息系统数据、非法控制计算机信息系统罪，是指违反国家规定，侵入国家事务、国防建设、尖端科学技术领域以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，情节严重的行为。

[4]参见天津市第一中级人民法院(2018)刑终 300 号刑事裁定书。

[2] 王立梅, 郭旨龙. 网络法学研究[M]. 北京: 中国政法大学出版社, 2022.

[3] Kerr, O.S. (2003) Cybercrime's Scope: Interpreting Access and Authorization in Computer Misuse Statutes. *NYU Law Review*, **78**, 1596-1668.

[4] Zamora, A. (2019) Making Room for Big Data: Web Scraping and an Affirmative Right to Access Publicly Available Information Online. *The Journal of Business*, *Entrepreneurship & the Law*, **12**, 203.

[5] 刘宪权. 元宇宙空间中数据的分类分级与刑法保护[J]. 比较法研究, 2023(4): 51-64.

[6] 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.

[7] 劳东燕. 个人数据的刑法保护模式[J]. 比较法研究, 2020(5): 35-50.

[8] 张勇. 数据安全法益的参照系与刑法保护模式[J]. 河南社会科学, 2021, 29(5): 42-52.

[9] 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.

[10] 张明楷. 新刑法与法益侵害说[J]. 法学研究, 2000(1): 19-32.

[11] 王昭武. 法秩序统一性视野下违法判断的相对性[J]. 中外法学, 2015, 27(1): 170-197.

[12] 吴冬兴. 论法秩序统一性原则的司法应用逻辑[J]. 法学, 2022(7): 23-39.

[13] 周光权. "刑民交叉"案件的判断逻辑[J]. 中国刑事法杂志, 2020(3): 3-20.

[14] 陈家林. 法益理论的问题与出路[J]. 法学, 2019(11): 3-17.

[15] 田宏杰. 刑法法益: 现代刑法的正当根基和规制边界[J]. 法商研究, 2020, 37(6): 75-88.