Open Journal of Legal Science 法学, 2025, 13(3), 449-458
Published Online March 2025 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2025.133065

Hans汉斯

网络爬虫技术侵犯个人信息的定罪分析

李织宇

北京师范大学法学院，北京

收稿日期：2025年2月5日；录用日期：2025年2月19日；发布日期：2025年3月12日

摘　要

随着信息技术的飞速发展，网络爬虫技术在各个领域得到广泛应用，同时利用该技术侵犯个人信息的犯罪行为也不断增多。然而，由于我国目前的法律法规不够明确、完善，不同地区在司法实践中对相关法律法规的理解和适用存在差异，致使“同案不同判”的问题普遍存在。针对司法实践中对该行为的入罪定罪混乱问题，应该先确定行为人行为是否构成犯罪，再确定行为人的犯罪行为应该被判处的具体罪名。在入罪方面，既应判断行为对象，在区分数据和个人信息的基础上，进一步对个人信息进行归类分析；还应从客观方面和主观方面分析行为人的行为，即行为人是否具备授权、违法性认识、符合犯罪行为构成要件。在确定行为人行为构成犯罪时，则进一步确定其罪名。在综合考虑行为人的具体行为、行为实质上侵犯何种法益以及同一行为同时构成不同罪名时如何处理罪数关系等问题的基础上，最终明确行为人犯罪行为应该被判处的罪名。

关键词

爬虫技术，侵犯个人信息，入罪判断，侵犯公民个人信息罪

Conviction Analysis of Web Crawler Technology for Infringement of Personal Information

Zhiyu Li

School of Law, Beijing Normal University, Beijing

Received: Feb. 5th, 2025; accepted: Feb. 19th, 2025; published: Mar. 12th, 2025

Abstract

With the rapid development of information technology, web crawler technology has been widely

文章引用: 李织宇. 网络爬虫技术侵犯个人信息的定罪分析[J]. 法学, 2025, 13(3): 449-458.
DOI: 10.12677/ojls.2025.133065

applied in various fields. At the same time, criminal acts of infringing on personal information by using this technology are also on the rise. However, due to the lack of clarity and perfection of China's current laws and regulations, different regions have differences in the understanding and application of relevant laws and regulations in judicial practice, resulting in the widespread problem of "different judgments for the same case". In response to the chaotic situation of conviction and sentencing of such acts in judicial practice, it is necessary to first determine whether the act of the actor constitutes a crime, and then determine the specific charge for which the criminal act of the actor should be sentenced. In terms of determining criminal liability, not only should the object of the act be judged. On the basis of distinguishing between data and personal information, further classification and analysis should be carried out. It is also necessary to analyze the actor's behavior from the objective and subjective aspects, that is, whether the actor has authorization, awareness of illegality, and meets the constitutive requirements of the criminal act. When it is determined that the actor's behavior constitutes a crime, the charge is further determined. On the basis of comprehensively considering issues such as the specific behavior of the actor, what kind of legal interests are essentially infringed by the behavior, and how to deal with the relationship of the number of crimes when the same act constitutes different charges, the charge for which the actor's criminal act should be sentenced is finally clarified.

Keywords

Crawler Technology, Infringement of Personal Information, Conviction Judgment, Crime of Infringing on Citizens' Personal Information

1. 现状与困境

1.1. 网络爬虫技术风险性增加

大数据时代，收集数据信息技术被广泛应用。“网络爬虫”就是通过特定规则自动抓取收集信息的技术。它能够在未得到数据拥有者同意的状况下访问并获取海量数据，并且迅速地把目标网页的信息内容下载至本地。早期网络爬虫技术作为中立技术为人们搜索信息提供方便，但随着该技术的不断发展，滥用这一技术的行为人越来越多，网络爬虫技术的刑事风险性不断增加。

首先滥用网络爬虫技术会造成巨大的技术风险。太频繁的恶意抓取行为可能会造成网站拥堵甚至服务器崩溃，影响网站正常运行。多次重复的抓取行为也会大量浪费网络服务器资源[1]。这些行为所造成的技术风险可能严重影响互联网产业顺利发展。

其次滥用该技术会侵害多种法益。例如严重侵犯公民的个人信息权益、部分著作权人的著作权益、他人的商业秘密权益等。

最后滥用技术的行为本身可能也属于刑法规制的范畴。若行为人本身存在非法侵入、为明知的犯罪行为提供爬虫技术服务、恶意侵入他人计算机信息系统获取数据、破坏计算机信息系统等行为。若其行为符合犯罪构成要件，在未侵害其他法益时，行为本身就构成犯罪[2]。

1.2. 出现大量网络爬虫技术案件

截止至 2024 年 11 月，在中国裁判文书网、中国人民案例网、威科先行等网站，通过“爬虫”、“爬

取”、“抓取数据”等关键词进行检索，共搜索到案件近 600 个。在这些案件中，民事案件占比高达 77%，刑事案件占比在 21%。至 2018 年，因网络爬虫技术行为犯罪的案件数量仅为 11 件。2019 年开始近 6 年的时间，网络应用爬虫技术行为进行犯罪的案件量迅速攀升，其中 2019 至 2021 年的 3 年时间中，利用网络爬虫技术进行犯罪案件高达 60 多件。虽然自 2022 年，刑事案件数量有所下降，但是每年都存在运用该技术进行犯罪的案件。随着科技的不断发展，近几年稳定的案件数量并不能保证未来案件数量没有继续上涨的趋势。

1.3. 规制网络爬虫技术犯罪困境

1.3.1. 是否入罪模糊不清

截止至 2024 年 11 月，在中国裁判文书网、中国人民案例网、威科先行等网站，通过“爬虫”、“爬取”、“抓取数据”等关键词进行检索，共收集到不起诉决定书 72 份。综合阅读以上不起诉决定书，主要以“犯罪事实不清、证据不足，不符合起诉条件”和“犯罪情节轻微，不需要判处刑罚”两种理由不对犯罪嫌疑人提起诉讼。通过对比不同案件的具体情节，可以发现不同地区的司法机关会对相同情节案件作出入罪与不入罪的不同决定。例如邹某某侵犯公民个人信息、非法获取计算机信息系统数据案[1]，被告人邹某某负责编写爬虫程序，非法保存个人信息达到 21,241,504 条。这些信息以每笔 0.1 至 0.3 元不等费用提供给网贷平台。被告人被认为犯罪情节轻微，不予起诉。而在熊鹏、谭统权侵犯公民个人信息案[2]，同样是通过爬虫程序爬取信息提供给贷款公司，共爬取并提供个人信息 2,853,111 条。在这一案件中被告人被认为反侵犯公民个人信息罪，被判处有期徒刑三年，缓刑四年。

上述入罪问题存在是因为在从对象不法的角度判断时，难以通过被抓取的数据来判断行为的不法性。例如抓取何种数据是合法的，何种是违法的；能否将被抓取的数据进行类型化分析等。而在从行为不法角度判断时，第一，认定非法行为的标准模糊，没有对该行为规制的具体限度。第二犯罪行为的构成要件认定标准也比较模糊，例如如何判断“违反国家有关规定”、“非法方法”、“情节严重”等。

1.3.2. 此罪彼罪难以区分

通过对近几年涉及“网络爬虫技术”的刑事案件进行分析，出现了“同案不同判”的司法适用现象。

首先，刑事案件判决书中网络爬虫行为所涉及的罪名纷繁复杂，例如侵犯公民个人信息罪、非法获取计算机信息系统数据罪、非法经营罪等，其中“侵犯公民个人信息罪”和“非法获取计算机信息系统数据罪”这两项罪名占比最高。

其次，在刑事案件判决书中不同法院针对相同行为判决所涉及罪名数量不同。例如在李某甲侵犯公民个人信息案[3]，李某甲存在编写“爬虫软件”进入系统获取公民信息并出售给他人的犯罪行为。法院认为该行为同时符合非法侵入计算机信息系统罪和侵犯公民个人信息罪，但应当按照处罚较重的罪名，即侵犯公民个人信息罪定罪处罚。而在张某拔非法获取计算机信息系统数据罪、侵犯公民个人信息罪案[4]，张某拔同样是存在编写代码进入多个交管平台获取公民信息并向其他公司提供查询信息服务的犯罪行为。法院也认为张某拔行为同时符合上述两个罪名的构成要件，但最后判决是其同时构成两个罪名并数罪并罚。上述两个案件中行为人行为类似，两个法院也均认可行为同时符合两个罪名的构成要件，但是在最后的判决中却出现判处一个罪和两个罪的差异。

[1]浙江省杭州市西湖区人民检察院西检一部刑不诉[2020] 777 号不起诉决定书。
[2]四川省峨眉山市人民法院(2020)川 1181 刑初 49 号判决书。
[3]河南省开封市龙亭区人民法院(2024)豫 0202 刑初 19 号判决书。
[4]广东省广州市海珠区人民法院(2022)粤 0105 刑初 795 号判决书。

此外，通过浏览不同案件法院所撰写的判决书发现，判决书中的说理部分也较为模糊空洞。只有部分会厘清争议焦点，详细论证被告人行为为何符合这项罪名。其他仅仅笼统地将被告人行为概括分析为“认为其违反国家规定，情节严重，构成该项罪名。”这一模糊的说理行为说明目前司法机关对这一行为认知不够充分，在判案过程中回避评价该行为。

上述定罪问题存在是因为一方面网络爬虫犯罪行为所侵犯的法益难以清晰确定。法益是分析行为究竟构成哪项罪的核心，它具有指导解释不同罪名构成要件的作用。不同法益立场不仅决定了罪名，还决定了罪行的处罚范围。而网络爬虫技术灵活多变，不同类型的数据表征权益各不相同，爬虫行为可能触及多项罪名[3]。另一方面当网络爬虫行为同时触犯不同罪时，罪与罪之间的关系，即是法条竞合关系还是想象竞合关系存在争议。

综上所述，网络爬虫行为在是否入罪、如何定罪问题上存在大量分歧。究其现象的表面原因是不同地区对法律的理解适用存在差异，无法达到统一。而根本原因则是涉及网络爬虫行为的入罪、定罪法律法规模糊不清。这一根本原因会对司法产生诸多不利影响，例如破坏法制统一、降低公众对司法公正的信任、难以树立司法权威等。因此急需通过分析探讨，构建出网络爬虫技术侵犯个人信息的定罪路径。

2. 网络爬虫技术侵犯个人信息入罪分析

对网络爬虫行为侵犯个人信息是否入罪主要从两个方面进行考量。从行为对象角度，即该行为所爬取的何种数据可以被归纳为个人信息；是否不对该行为爬取的全部个人信息进行区分，均认为其属于实施行为的犯罪对象。从行为手段角度，何种行为应该被评判为犯罪行为；如何理解《刑法》中相关罪名的构成要件等。

2.1. 行为对象分析

2.1.1. 区分数据与个人信息

针对网络爬虫行为侵犯个人信息的入罪分析，首先要确定行为对象是否是个人信息。依据法律，数据是指任何以电子或其他方式对信息的记录。[5]因此在互联网时代，各式各样以电子形式被记录的信息都可以被称作是数据。但根据所载信息可以将其分为个人和非个人。个人信息是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。[6]依据这一概念，数据划分为个人数据的核心就是具有“可识别性”。那么又应该如何理解“可识别性”这一概念？

欧盟对个人数据“可识别性”采取的外延单位较大，对个人数据的保护范围和强度都较大。依据我国的司法解释[7]，若是不可以直接识别，并且需要结合大量其他信息才可以识别特定自然人的个人信息就不属于刑法保护的范畴。因此，利用能否直接通过该信息识别特定自然人身份，可以将个人信息分为直接和间接两类。直接个人信息当然属于保护范畴；间接个人信息则通过是否需要大量计算或者结合许多其他信息才可识别特定自然人身份进行区分。存在这种区分的原因主要是，若将经过多次技术处理或转化后才能指向特定自然人的信息视为具有“可识别性”的个人信息，会破坏并限制数据和信息的合理利用，打破互联网利益和个人权利之间的平衡[4]。

综上所述，数据是否被归类为个人信息的核心是该信息是否具有识别特定自然人的“可识别性”。同时刑法对个人信息的保护范畴也需要对“可识别性”进行限缩解释，即排除需要经过海量计算处理或结合大量技术才能识别特定自然人身份的间接信息。

[5]《中华人民共和国数据安全法》第3条。
[6]《中华人民共和国个人信息保护法》第4条。
[7]《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第1条。

2.1.2. 个人信息归类分析

在确定网络爬虫行为所爬取的数据为个人信息范畴后，不能不对个人信息进行区分，全部认为是犯罪行为所侵犯的对象。而应该将这些个人信息依据是否已经在网络上公开区分为公开以及非公开的个人信息。

公开的个人信息是指已经在网络上公开，不特定自然人可以在网上随意搜索浏览，并且可以对这些信息进行复制的个人信息。目前学界针对网络爬虫随意爬取公开信息是否定罪存在争议。部分学者认为虽然公开数据可以由任何自然人进行分享、获取和使用，但从保护公民人身和财产权利角度出发，侵犯公民个人信息，情节严重的仍然构成侵犯公民个人信息罪。但同样有学者认为一旦数据处于公众自由获取、利用的状态，这些数据就是公共物品[5]，此时并不构成犯罪。在司法实践中，最高人民法院在最高法指导性案例 194 号熊昌恒等侵犯公民个人信息案的裁判要旨中说明行为人违法处理公开个人信息并获利，违背公开目的或明显改变用途，该信息被进一步利用后危及个人的人身或财产安全，情节特别严重，构成侵犯公民个人信息罪[6]。还需要进一步对公开的数据进行划分，依据权利人的意愿分为主动公开以及被动公开数据；依据公开方式可以分为合法和非法公开数据。因此在判断爬取公开的个人信息是否构成犯罪时，不应该仅从数据是否被公开的形式判断，而应该从实质性角度考量。例如行为人收集行为是否违背公开数据的目的，行为人后续是否存在利用、向他人提供、出售公开信息等行为。针对明显违背公开信息的目的，改变公开信息的用途，利用公开信息实施可能危害公民人身、财产安全的行为应该构成犯罪。因此，实质判断承担着是否构成犯罪的终极评价任务。

非公开的个人信息则是指数据控制者通过技术手段限制不特定第三方访问数据，排除数据被公开获取的可能性[7]。非公开信息的保护范围广泛，依据行为人能否浏览、收集数据的条件不同，可以将其分禁止访问的个人信息，限制访问的个人信息，可以访问却不能被复制的信息。禁止访问的个人信息当然归属于非公开数据范畴。限制访问信息也属于其范畴。在“微梦诉云智联公司案”裁判文书中“对于微梦公司通过登录规则或其他措施设置了访问权限的数据则应属新浪微博中的非公开数据。”[8]可以访问却不能复制的信息同样是数据控制者采取技术手段通过限制行为人对数据进行浏览、收集的渠道，进而限制数据被进一步公开的可能性。依据上述分类，根据限制条件的不同，可以区分信息保护程度。信息的防护力度越大，刑法的保护层级就越高，网络爬虫行为需承担的法律责任也越重。与公开个人信息相比，非公开信息不仅因其存在事实上的排他性更需要法律保护。同时，行为人的非法行为在侵犯他人信息时，还破坏了计算机系统，干扰网络秩序稳定。这时此行为可能同时触犯不同的罪名。

2.2. 行为手段分析

2.2.1. 网络爬虫行为

网络爬虫行为是否是犯罪行为可以从行为的客观方面和主观方面分别分析。

在客观方面，网络爬虫行为可以被分为有授权的行为、超越授权的行为和无授权的行为。有授权的行为是网络爬虫行为事先取得数据所有者的同意，可以对数据进行自由爬取。该行为通常基于授权而具备合法性。但需要判断该授权不仅是形式上的授权，更是实质上的授权。因此应该明确授权是否以不正当方式获取，在获取过程中是否违背信息所有者意愿或真实意思表示。若行为人通过隐瞒、欺诈等方式取得了信息所有者的授权。虽然爬取行为在形式上为有授权的行为，但是在实质上它并没有遵循“知情同意原则”。该授权行为的合法性会基于虚假的授权行为消失，成为违法行为。超越授权行为的判断关键则在行为人被授权的行为范围。例如行为人利用工作便利，超出工作职责范围爬取个人信息、超出单位内部管理规定范围等[8]。无授权的行为则是指网络爬虫行为根本未获得许可。它依据网站是否存在防

[8]北京市海淀区人民法院(2017)京 0108 民初 24512 号民事判决书。

护行为分为无防护措施行为和有防护措施的行为。无防护措施的行为是指网站仅公开发表拒绝爬取的说明，但并未采取防护措施；有防护措施的行为则是行为人侵入、破坏系统，获取数据。两种行为的侵害性程度不同，爬取无防护措施的行为侵害性程度更轻、破坏防护措施的行为侵害性程度更重。依据侵害程度不同分别构成民事违法和刑事违法。

在主观方面，需要判断行为人是否具备违法性的认识。在考量行为人违法认识时要从多方面考量。第一，考察行为人所处的行业，若其本身就为互联网的从业人员，那么他对网络爬虫技术的风险以及规则都有更深刻的理解，应要求其具有更高的规范、风险意识。第二，考虑行为人的主观目的。行为人在实施行为时本身是否带有违法性的恶意目的。例如，他的爬取行为是为了收集个人信息来牟取利益或是为了避开、突破网站防护所实施的行为等。第三，需要从客观行为综合倒推行为人的主观目的。例如，行为人是否采取隐蔽、秘密的行为方式，在技术层面行为人是否采取破坏性明显的强制措施等。

2.2.2. 行为构成要件

在网络爬虫犯罪行为爬取个人信息所集中涉及的几项罪名中，大多具备“违反国家规定”、“非法方法”、“情节严重”等几项标准，因此判断行为人行为是否符合法条规定可以分别从以下三方面进行理解。

依据现有的司法解释，“国家有关规定”这一范围包括法律、行政法规、部门规章。但依据我国《刑法》96 条，“国家规定”指法律、行政法规、国务院规定的行政措施、发布的决定和命令[9]。可以看出，针对“违反国家有关规定”的范围在法律层面存在争议。不同学者也存在不同的理解。有学者认为，虽然二者表述不同，但是多添加的“有关”只是一个虚词，没有扩张或限缩国家规定的能力，本质上不会超越《刑法》规定的范围[10]。也有学者认为，这一范围应当扩大至地方性法规和部门规章、地方政府规章[11]。虽然纳入某些部门规章规定有利于依据各个领域、行业的特点保护，扩大了规制犯罪的范围，有利于保护个人信息[12]。但是涉及保护个人信息的部门规章较少，规章的立法性质又决定这些规定较为泛化、内容碎片化，法律操作性不强。此时将全部部门规章纳入进来不仅无法起到保护个人信息的实质效果，还会破坏法秩序统一。综上，笔者认为，不同学者之间的考量均存在合理性，因此应该选择折中的办法进行解释，可以考虑通过采取司法解释的方法，对侵犯公民个人信息罪中的“国家有关规定”进行解释，明确将某些部门规章的规定纳入进来，而非将部门规章直接作为前提条件全部纳入其中。这种理解一方面有利于加强对自然人的个人信息权益保护；另一方面这一理解能够维护法秩序统一、实现不同部门法之间的有效衔接。

判断行为中的“非法”要素可以分别从原则层面以及行业规则层面分析。第一，违反“合法性”原则的行为应被认定“非法方法”。其中针对“合法性原则”可以从《个人信息保护法》的“正当必要原则”以及“知情同意原则”[13]进行判断。即处理个人信息必须遵循正当、必要原则。此原则强调收集、处理个人信息的行为需要具有明确、合理目的，行为人的处理目的与处理行为需直接相关，同时行为人信息收集范围被限制到最小，不能过度收集。且处理行为必须保证个人充分知情、自愿并明确同意。那么行为人收集处理个人信息时，若数据所有者为第三方平台，行为人不仅要获得平台的授权，还应征集个人的知情同意，此时其行为才不构成非法方法。此外《网络安全法》通过具体规定来体现“合法性原则”，即行为人不得进行侵入网络、干扰网络正常功能、窃取数据等非法行为。以上与网络爬虫行为息息相关的法律法规中的规定共同确立了行为人行为需遵循的“合法性原则”[14]。第二，违法行业规则，即“爬虫协议”获取个人信息的行为可以被认定为“非法”。“爬虫协议”是规范网络爬虫行为的公认行业规则，该协议能够提示网络爬虫行为人哪些网页、数据可以被抓取收集[15]。目前“爬虫协议”的效力尚有争议，即其作为行业公认规则是否具有法律属性、具备规范行为的强制力。笔者认为违反“爬虫协议”

行为可以被认定为“非法方法”的主要原因有以下几点。在理论层面，该协议公认程度极高。它不仅被搜索行业认可，并具有国际通行的行业惯例与商业规则地位。在法律滞后、缺失的情况下，遵守这一行业协议能够更好保护自然人的信息权益，规制滥用网络爬虫技术行为。在实践层面，通过归纳司法判决结果，法院在审判中认可爬虫协议。此外，判断爬虫行为是否违反爬虫协议则通常以行为人是否采取突破反爬程序的强行或暴力爬取数据的行为为依据。[9]因此，行为人行为是否属于“非法方法”可以分别从“合法性原则”以及“行业规则”两个层面进行分析。

网络爬虫技术爬取个人信息入罪标准中“情节严重”需同时达到形式上和实质上的“严重”。在形式上，依据现有司法解释，通过规定个人信息数据的数量以及行为人的违法所得金额以及造成的经济损失金额判断是否严重[16]。但目前在实际应用中，司法解释通过规定数据数量、违法所得金额评判“情节严重”的规定已经出现局限性，难以满足现实需求。因此，在判断情节严重时更应该从实质上考量行为对被害人权益的损害。

3. 网络爬虫技术侵犯个人信息罪名分析

通过上述入罪分析确定犯罪嫌疑人的行为构成犯罪时，下一步需要分析的问题就是这一行为应该被定为何种罪名。罪名与犯罪嫌疑人的具体行为、不同罪名所要保护的法益以及罪数之间的关系息息相关。因此，下文主要从以上三方面分析。

3.1. 不同类型的具体行为分析

网络爬虫是随着时代发展的一种新兴网络技术，这一技术本身是中立的，但是因为犯罪嫌疑人的主观恶意成为犯罪行为。在对中国裁判文书网中的判决书归纳分析后，目前网络爬虫犯罪行为主要有以下几种。第一，使用网络爬虫技术获取个人信息的行为；第二，利用网络爬虫技术突破系统权限的非法侵入行为；第三，利用网络爬虫技术攻击计算机系统的破坏行为；第四，明知他人利用他人信息进行犯罪而提供网络爬虫技术的技术提供行为。基于行为人的目的以及不同行为所侵害的法益，行为人的不同行为应构成不同罪名。

第一，使用网络爬虫技术获取个人信息的行为可能构成侵犯公民个人信息罪。公民个人信息区别于其他数据，因其与信息主体存在关联，能够识别特别个人，侵犯到信息主体的权益。因此，为更好保护自然人的权益，该行为应以侵犯公民个人信息罪论处。需要注意的是，并非全部使用行为都被认定为犯罪。在对行为进行判断时，要综合信息类型以及行为人的行为方式、目的、后果等综合判断。第二，为获取个人信息，利用网络爬虫技术突破系统权限的非法侵入行为可能构成非法侵入计算机信息系统罪或非法获取计算机信息系统数据罪。此时主要是通过判断行为人所侵入的系统进行判断。若行为人侵入国家事务、国防建设、尖端科学技术领域的计算机系统则构成非法侵入计算机信息系统罪，若是其他普通的计算机信息系统则构成非法获取计算机信息系统数据罪。第三，为获取个人信息，利用网络爬虫技术攻击计算机系统的破坏行为可能构成破坏计算机信息系统罪。其中破坏行为可以包括行为人利用爬虫技术爬取数据造成网站拥堵、破坏系统的行为以及对信息系统的安全措施进行暴力破解的行为。第四，明知他人利用个人信息进行犯罪而提供网络爬虫技术的技术提供行为可能构成提供侵入、非法控制计算机信息系统程序、工具罪或以侵犯公民个人信息罪的共同犯罪或非法获取计算机信息系统数据罪的共同犯罪。此时，针对犯罪活动专门设计的网络爬虫程序的行为人应该定为什么罪名应着重判断行为人之间是否存在共同犯罪的意思联络。若行为人之间存在明确的意思联络表示，应该将该行为确定为共同犯罪。若共

[9]《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第 5 条；《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 1 条。

同意思联络不明确，则不能认定为共同犯罪，而是判为提供侵入、非法控制计算机信息系统程序、工具罪[17]。

综上所述，在行为人利用网络爬虫侵犯个人信息的行为可以进一步细化为不同的具体行为，这些具体行为可能分别构成不同罪名。在确定行为人的具体行为后，需要通过对行为人行为所侵害法益以及行为人行为所涉及的罪数进一步分析。

3.2. 不同罪名的法益分析

为更好解决数字犯罪，应该明晰罪名所保护法益的基本内涵，立足于不同数据法益类型及法益侵害的形态，实现对数据犯罪的规制[18]。目前在网络爬虫行为侵犯个人信息应该被判处什么罪名中，适用侵犯公民个人信息罪还是非法获取计算机信息系统数据罪是最主要的争议焦点。因此下文着重分析这两个罪名所保护的法益。

3.2.1. 侵犯公民个人信息罪的法益

目前有关公民个人信息罪的法益主要存在超个人法益、个人法益等学说。但当前的学说均存在问题，超个人法益存在过于限缩犯罪圈、与司法解释相矛盾等问题。个人法益学说中所考虑保护的公民个人信息权益和个人自由则过于宽泛。判断该罪的法益应首先考虑其犯罪对象、罪名、法条位置以及司法解释等多方面，即本罪的犯罪对象是公民的个人信息；从法律体系角度考虑，该罪名在刑法第四章，该罪所保护的法益应该属于个人法益；“该罪的本质是侵害公民所享有的个人信息不被披露、泄露的个人信息安全权。”因此侵犯公民个人信息罪的法益应该属于个人法益范畴。但这一范畴过于宽泛，需要进一步分析。通过考虑该罪的规范本质和不法行为、实现全面保护个人信息、解决不完全否定被害人同意阻却犯罪的作用等多方面问题[19]，侵犯公民个人信息罪的法益应该是保护公民的“个人信息安全权”。公民个人信息泄漏后，整个信息的处于不安全状态，公民的人身财产利益也面临极高的风险。为避免公民的利益进一步受损，应保证其个人信息处于安全状态之中。

3.2.2. 非法获取计算机信息系统数据罪

从我国刑法的立法导向来看，保护数据更强调的是保护它的动态流转功能，保护信息则更强调保护它的静态内容。非法获取计算机信息系统数据罪的犯罪对象是“数据”，因此该罪名强调对数据本身的保护作用，即保护数据所有者对数据的控制以及操作自由的秩序法益。但是该罪名并不是仅仅只涉及秩序法益，这一罪名同样保护信息内容安全这一法益。当前刑法规制网络犯罪行为存在部分漏洞，例如传统罪名无法规制加工处理后获取公民个人信息的行为。而通过强调该罪名保护信息内容安全法益能够弥补这些漏洞。该罪名在保护信息安全时，打击非法获取数据的前端行为，进而打击到后续加工处理数据行为。综上，非法获取计算机信息系统数据罪保护的法益是“数据控制与操作自由和信息内容安全”的阶层式法益。

3.3. 罪数关系分析

网络爬虫技术侵犯公民个人信息应该判处何种罪名同样与罪数关系紧密相连。目前针对罪数关系中的争议主要有以下几点。首先，犯罪嫌疑人的行为应该整体看为一个行为以一个罪名论处，还是将其分为多个行为分别论处。其次，当一个行为同时触犯多个罪名时，如何对该行为定罪。

3.3.1. 行为数量分析

判断行为人的行为构成几项罪名首先要判断行为人在犯罪过程中存在几个犯罪行为，即这些具体行为应该全部归纳为一个犯罪行为还是将其分为多个行为分别论处。对行为人的行为数量主要从行为人的

行为目的、性质以及所侵害的法益分别分析。例如，若行为人最初设计网络爬虫技术的目的是为获取、贩卖公民个人信息，则行为人的所有行为应整体看为一个行为，以侵犯公民个人信息罪判处。若行为人在为他人犯罪提供网络爬虫技术时，同时获取个人信息，该行为就存在不同的行为目的，即以技术非法获取利益以及侵犯他人信息，此时行为人行为就应该分开评定，分别构成提供侵入、非法控制计算机信息系统程序、工具罪以及侵犯公民个人信息罪。

3.3.2. 罪名竞合关系分析

当同一行为同时构成两种罪名的构成要件时，这两种行为的竞合关系是法条竞合还是想象竞合对行为人的定罪存在主要影响。针对这一问题，学界同样存在争议。有学者认为，个人信息与计算机数据存在概念上交叉，但计算机数据内容复杂、外延广泛，它包含了公民个人信息[20]。两个罪名是特殊法和普通法的关系，应根据特别法优于普通法的法条竞合处理原则，以侵犯公民个人信息罪论处。也有学者认为，如果信息主体和数据控制者都享有受刑法保护的权益，在只有一个非法获取行为时，则成立两种罪行的想象竞合[21]。

评价不同罪名之间的关系，应该以形式标准和实质标准分别评价。形式标准主要通过判断不同法条之间的关系。法条之间主要存在对立、包容、交叉、中立等关系。涉及竞合的法条关系主要有包容关系和交叉关系，其中包容关系应属于法条竞合，交叉关系属于想象竞合。实质标准是判断法益的同一性和不法的包容性。在法益的同一性中，“法条竞合只有一个法益侵害事实，适用一个法条；想象竞合则存在数个法益侵害事实，适用全部法条评价，避免遗漏行为人的不法内容。”[22]在不法的包容性中，为对违法行为进行完整的评价、符合罪刑适应的原则，对于不法内容重、法定刑轻的情况归为想象竞合。综上，评判罪名应综合考虑形式和实质标准，若司法机关判断行为人的行为可以通过一个法条对所用不法内容进行完整评价，则成立法条竞合，否则为想象竞合。

4. 结语

网络爬虫技术的广泛应用方便人们的同时，其犯罪风险也与日俱增，如何将网络爬虫技术爬取个人信息的行为定罪已成为规制该行为的关键。当前，这一领域面临着诸多棘手困境，例如入罪标准模糊不清，此罪与彼罪难以准确区分，罪名认定充满了不确定性。

本文从剖析其入罪要素出发，分别判断行为对象和行为手段。从行为对象来看，数据应该先从类别区分是否为个人数据，然后进一步从形式和实质判断数据是否公开。在行为手段方面，需分别从客观和主观两方面判断其合法性，同时，准确理解“违反国家有关规定”“非法方法”“情节严重”等关键要素。在确定行为入罪后，对该行为的定罪需综合考虑具体行为、法益和罪数关系。一方面不同类型的网络爬虫行为对应不同罪名。另一方面，同一行为构成不同罪名时，则从法益等方面综合评定判断，确定行为人的罪名。通过这一逻辑顺序考量才能确保认定罪名准确无误，进而维护法律秩序的权威性，切实保障公民的合法权益免受侵害。

参考文献

[1] 刘艳红, 杨志琼. 网络爬虫的入罪标准与路径研究[J]. 人民检察, 2020(15): 26-31.

[2] 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.

[3] 姜岚. 大数据时代下网络爬虫行为的刑法规制[J]. 中阿科技论坛(中英文), 2024(4): 163-167.

[4] 周光权. 侵犯公民个人信息罪的行为对象[J]. 清华法学, 2021, 15(3): 25-40.

[5] 高富平. 数据经济的制度基础——数据全面开放利用模式的构想[J]. 广东社会科学, 2019(5): 5-16, 254.

[6] 中华人民共和国最高人民法院官网《指导性案例》, 载指导性案例 194 号: 熊昌恒等侵犯公民个人信息案-中华

人民共和国最高人民法院[EB/OL]. https://www.court.gov.cn/shenpan/xiangqing/384431.html, 2025-01-06.

[7] 项定宜. 数据分类确权的司法探索与规则重构[J]. 河北法学, 2024, 42(12): 110-129.

[8] 宋行健. 滥用网络爬虫技术收集个人信息的刑法规制[J]. 湖南科技大学学报(社会科学版), 2021, 24(4): 139-148.

[9] 冀洋. 法益自决权与侵犯公民个人信息罪的司法边界[J]. 中国法学, 2019(4): 66-83.

[10] 吴允锋, 纪康. 侵犯公民个人信息罪的司法适用——以《网络安全法》为视角[J]. 河南警察学院学报, 2017, 26(2): 91-97.

[11] 江耀炜. 大数据时代公民个人信息刑法保护的边界——以“违反国家有关规定”的实质解释为中心[J]. 重庆大学学报(社会科学版), 2019, 25(1): 152-161.

[12] 王秀哲. “侵犯公民个人信息罪”司法解释之局限性及其破解[J]. 河南大学学报(社会科学版), 2018, 58(5): 25-32.

[13] 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

[14] 刘鹏. 利用网络爬虫技术获取他人数据行为的法律性质分析[J]. 信息安全研究, 2019, 5(6): 548-552.

[15] 杨华权, 曲三强. 论爬虫协议的法律性质[J]. 法律适用, 2013(4): 30-34.

[16] 姜金良, 张丹丹. 网络爬虫技术使用过界的刑事责任认定[J]. 阅江学刊, 2024, 16(3): 101-109.

[17] 吴沛泽. 数据犯罪的刑法规制: 法益内涵与体系构建[J]. 中国刑事法杂志, 2024(5): 121-138.

[18] 徐剑. 侵犯公民个人信息罪法益: 辨析与新证[J]. 学海, 2021(2): 118-126.

[19] 曹岚欣. 恶意爬取数据行为的刑法规制边界——以非法获取计算机信息系统数据罪为视角[J]. 中国石油大学学报(社会科学版), 2024, 40(2): 130-138.

[20] 宋行健. 滥用网络爬虫技术收集个人信息的刑法规制[J] .湖南科技大学学报(社会科学版), 2021, 24(4): 139-148.

[21] 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.

[22] 万雨馨. 解构与重塑: 法条竞合和想象竞合区分之二元化路径[J]. 东华理工大学学报(社会科学版), 2022, 41(3): 250-255.