Dispute Settlement 争议解决, 2024, 10(1), 169-176
Published Online January 2024 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2024.101024

Hans汉斯

数据犯罪的保护法益研究

——以非法获取计算机信息系统数据罪为例

沈家仪

华东政法大学刑事法学院，上海

收稿日期：2023年11月1日；录用日期：2024年1月1日；发布日期：2024年1月9日

摘　要

非法获取计算机信息系统数据罪是数据犯罪的典型罪名，目前在实务中存在行为对象范围过大、行为方式认定等疑难问题，究其原因是对数据法益保护的定位及其内容的不明。数据安全法益独立于计算机信息系统，注重数据本身内容安全，包含数据控制安全与数据利用安全两个方面。非法获取计算机信息系统数据罪的行为对象不仅限于身份认证信息，包含一切经过数字化方式处理的数据，但不包括可公开获取的企业数据；认定行为方式应以是否“未经授权或超越授权”为标准，单纯违背数据网站服务协议的数据抓取行为不应入罪。

关键词

数据犯罪，非法获取计算机信息系统数据罪，保护法益，数据利用安全

Research on the Legal Benefits of Protecting Data Crimes

—Taking the Crime of Illegally Obtaining Computer Information System Data as an Example

Jiayi Shen

School of Criminal Law, East China University of Political Science and Laws, Shanghai

Received: Nov. 1st, 2023; accepted: Jan. 1st, 2024; published: Jan. 9th, 2024

Abstract

The crime of illegally obtaining computer information system data is a typical charge of data crimes. Currently, there are difficult problems in practice, such as the large scope of behavior objects and

文章引用: 沈家仪. 数据犯罪的保护法益研究[J]. 争议解决, 2024, 10(1): 169-176. DOI: 10.12677/ds.2024.101024

the determination of behavior methods. The reason for this is the unclear positioning and content of data legal interest protection. The data security law is independent of computer information systems and focuses on the security of data content, including two aspects: data control security and data utilization security. The object of the crime of illegally obtaining computer information system data is not limited to identity authentication information, but includes all digitally processed data, but does not include publicly available enterprise data; the manner in which the act is committed should be determined by the criterion of whether it is "unauthorized or exceeds the authorization", and the act of data capture that simply violates the service agreement of the data website should not be criminalized.

Keywords

Data Crime, The Crime of Illegally Obtaining Data from Computer Information Systems, Protecting Legal Interests, Data Utilization Security

1. 引言

如今网络已经发展进入了全方位互动的时代，这是一个以人工智能和大数据为主要特征的智能化网络时代，此时的数据不仅仅是单纯的数据，更是已经成为了市场资源配置中的关键性生产要素，其重要性不言而喻。近年来，非法获取“微信公众号”案、首例“爬虫”入刑案、“撞库打码案”等与数据相关的新型网络犯罪案件相继发生，数据的高速化、价值化、规模化以及脆弱性等特征导致数据安全不断面临新的威胁，数据已然成为网络空间的主要攻击对象。

作为数据犯罪的典型罪名，非法获取计算机信息系统数据罪在司法适用中争议较大，因此本文将以非法获取计算机信息系统数据罪为切入点，就解决当前数据犯罪中的疑难问题，对数据犯罪的法益保护问题进行相关研究。

2. 我国数据犯罪刑法规制之困境及其成因

2.1. 我国数据犯罪刑法规制之困境

以全国首例“爬虫”入刑案为例，上海晟品网络科技有限公司曾在 2016 年至 2017 年间抓取北京字节跳动网络技术有限公司服务器上保存的相关视频数据，主要包含头条号视频列表、分类视频列表、相关视频及评论等相关数据，造成了被害单位 2 万元损失。本案的数据是公开可访问的视频数据，行为人通过技术手段绕过服务器的身份校验和访问频率限制是本案在数据抓取过程中的主要行为方式。而在卫梦龙、龚旭、薛东东非法获取计算机信息系统数据案中，卫梦龙与龚旭原本共同就职于北京某大型网络公司，卫梦龙利用龚旭拥有的账号、密码、Token 令牌等权限异地登陆公司内部管理开发系统以获取公司内部数据，由薛东东在网络出售这些非法获取的数据，获利 37,000 元。本案的犯罪对象是其公司内部的计算机信息系统数据，行为方式是直接输入账号密码等。两案都是非法获取计算机信息系统数据罪的指导案例，但犯罪对象和行为方式却大有不同，对于企业的公开信息是否属于本罪中的数据主体，或是本罪的侵入行为的认定，都存在不少的疑难问题。

法益的功能是由其作为犯罪本质特征的属性所决定的。这就决定了只要是与定罪和量刑有关的问题，法益都能发挥作用和影响[1]。学术界在数据犯罪领域对于数据犯罪的保护法益的认定依然存在了较大的分歧，这将直接导致数据犯罪的边界不明，在司法适用时使得司法判决缺乏统一标准而存在同案不同判或是面对疑难个案时无所适从的现象。

2.2. 我国数据犯罪刑法规制困境之成因

究其根本，我国在最初立法时对于计算机犯罪及其保护法益就没有给予其独立的地位。在传统刑法理论中，计算机信息系统中存储、处理或者传输的数据指一切在计算机信息系统中处理的文字、图像、声音等有意义的组合[2]。在互联网最初兴起的时代，数据的范围就相当于计算机信息系统的范围，然而，随着数据犯罪技术性的快速代际升级，数据不在局限于计算机信息系统内。两高在 2011 年的相关解释中明确，包括计算机、通信设备、网络设备、自动化控制设备在内的计算机信息系统，是指具备自动处理数据功能的系统。此解释扩大了数据犯罪的惩罚范围，新型数据载体如移动智能终端、APP 应用软件以及蓝牙等纳均可以包含在内。在 2013 年的相关解释中明确，信息网络不仅包含使用计算机为终端的信息网络，还包括使用电视机为终端的广播电视网、使用移动电话机为终端的移动通信网等各种信息网络，以及向公众开放的局域网络。此时的“计算机信息系统安全”通过技术性扩张已成为了“信息网络安全”，即通过扩大“计算机信息系统安全”的范围为来扩大计算机信息系统安全的法益范围，并没有提出独立的数据犯罪保护法益。同时，在司法实务中往往根据“计算机信息系统”的技术性问题来判定数据侵害行为是否构成犯罪，导致数据的独立价值被长期忽视，与数据日益增长的重要性不相符合。

其次，2011 年《解释》特别指出了“身份认证信息”的特殊性，并明确了以计算机系统台数或是违法所得的金额等具体情节。以计算机信息系统数量或是行为人违法所得等入罪标准，可以在实务认定数据犯罪时更具针对性和可操作性，但忽视了数据本身所具有的新型价值。只重视其所反映的传统价值，容易导致数据犯罪与财产犯罪、侵犯公民个人信息罪、非法控制计算机信息系统罪等罪名之间的边界不明，从而难以准确定性相关犯罪行为。

3. 数据犯罪保护法益的研究现状与认定

3.1. 数据犯罪保护法益的研究现状

法益侵害性作为犯罪本质，其在刑法教义学中的重要性不言而喻，法益概念的立法批判与规范解释机能也为学理普遍肯定。而数据犯罪在司法适用中的诸多问题在于法益含混导致其立法批判机能与规范解释机能难以有效发挥[3]。对于数据犯罪的保护法益目前在学术界依然存在较大争议，主要分为单一法益与复合法益两大阵营。

持单一法益观点的学者认为数据犯罪的保护法益具有单一性，主要包括计算机信息系统安全说、数据载体安全说、数据安全法益说等观点。传统观点认为非法获取计算机信息系统数据罪的保护法益是计算机信息系统的安全，实质上包括存储数据安全、处理数据安全和传输数据安全三个方面[4]。数据载体安全说认为，数据犯罪的保护法益是数据载体安全，只对数据进行技术性特征的判断，不区分记录信息的数据与冗余数据。数据安全法益说认为，数据犯罪的保护法益是数据的保密性、完整性和可用性[5]。持复合法益观点的学者认为数据犯罪的法益具有复合性，同时包含安全和财产法益两方面内容，应当通过数据的专门化和财产化保护二元的保护路径进行数据保护[6]。无论是单一法益还是复合法益，对于数据犯罪保护法益的争议点主要有以下三点，一，数据犯罪的法益是否独立于计算机犯罪法益；二，数据犯罪的法益内容是数据载体安全还是数据内容安全；三，数据犯罪法益的具体内容。

3.2. 数据犯罪保护法益的独立性

无论是单一法益论将本罪保护法益解释为计算机信息系统安全或计算机信息系统运行安全的观点，还是复合法益论认为的数据安全与系统功能多方面内容，都未能正视数据犯罪的独立性。

我国刑法中，数据犯罪的最初形态表现为纯技术性的非法入侵计算机信息系统罪、破坏计算机信息系统罪。此时的数据指的是由计算机信息系统运行产生的内部系统资料，具有封闭、静态和限定的特点。《刑法修正案(七)》增设了非法获取计算机信息系统数据罪、非法获取公民个人信息罪等直接有关数据的相关罪名，大力加强了对数据的保护，并不再将其局限于静态的计算机信息系统的一部分或其运行结果，而是转变为动态而开放的网络信息群。立法上虽然表述为“计算机信息系统中存储、处理或者传输的数据”，但其重点不在于计算机信息系统本身，而是“数据”。计算机信息系统的作用只是对数据类型进行限制，以便将这些内容的保护对象与传统纸质介质上存储的数据或其他形式的数据区分开来。2021 年通过的《数据安全法》第一条明确指出了立法目的，“规范数据处理活动，保障数据安全，促进数据开发利用”，维护数据安全已经成为一项独立于国家安全、社会安全和个人人身财产安全之外的法益，且在立法上对于数据安全的重视程度逐渐增加。

其次，随着数字化技术的发展，计算机犯罪经历了从利用计算机攻击计算机信息系统到运用计算机实施传统犯罪再到利用计算机窃取数据的变迁。计算机犯罪的重心已经从以炫耀技术为目的的黑客行为转向以牟取利益为动机的数据窃取和转售行为。随着云计算技术和移动终端设备的进步，数据本体与所含信息的分离越来越明显。电子数据的收集、储存和处理已经超越了计算机信息系统的限制，对计算机信息系统的侵害不一定危及数据安全，反之亦然。

最后，随着大数据与人工智能时代的到来，数据的量级呈指数型增长，早期的计算机网络已经扩展到各类通信网络、工业互联网和物联网，人们的生活每时每刻都产生着海量数据。与此同时这些海量数据也早已成为创造财富的一种方式，是如今数字经济的重要生产要素。数据具备了当今社会的基础资源价值，因此对数据法益的独立保护不仅关乎经济生产的稳定运行和国家社会的安全稳定，也与个人的隐私和财产等权益息息相关。

3.3. 数据犯罪保护法益为数据内容安全

数据作为信息网络的基本语言，本身不具有任何目的，具有价值中立的特点。数据载体安全说存在对法益概念与行为对象概念的混淆问题，数据载体的功能仅限于对事实的判断，不包括价值判断，因此数据载体属于行为对象而不是保护法益。首例网络爬虫入刑案的主审法官认为，本案被爬取的是公开但不共享的数据，虽然用户可以观看这些公开视频、浏览评论等，但并不提供下载，且网站加工视频过程中冗余的计算机语言、代码也没有公开，因此侵害了数据的保密性。将数据的保密性建立在本身不包含内容的冗余数据上，是以数据的技术特征取代数据的法益本质，认为数据载体安全才是数据犯罪的保护法益。以中立性的技术标准来确定法益内容，将数据犯罪的保护法益等同于数据本身，使其失去实质性的法益根据，进而丧失其指导具体构成要件解释的方法论意义[7]。

其次，将数据载体作为保护法益的观点忽略了法益理论的哲学根基。法益理论基于防止刑罚权的滥用，要求刑罚的实施必须以保护个人的生命、身体、自由、尊严、财产为目标。将数据载体本身作为的保护对象，忽视了个体的价值追求，使人在法益的概念中丧失了主体地位，展现了强调工具理性忽视价值理性的数据主义思想[8]。

数据犯罪案例所涉及数据类型广泛，包括身份认证、公民个人信息、结构化数据集合以及有知识产权属性的数据等，几乎覆盖了数据载体所能包含的绝大部分内容。将数据安全法益认定为数据载体安全，不加区别认定为非法获取计算机信息系统罪无疑扩张了数据犯罪的范围，使其有成为“口袋罪”的嫌疑。

我国刑法在涉及到数据安全保护方面，设立了“侵犯商业秘密罪”、“侵犯公民个人信息罪”等不同罪名的规定，将数据内容区分为商业秘密、个人信息等也正是说明了数据犯罪的保护法益应是数据的内容本身。

数据内容安全相较于数据载体安全更能体现刑法的谦抑性。数据作为当今社会的重要生产要素，通过不断流动、聚合，扩宽了应用场域，从而创造出新的数据和价值，达到数据价值的飞跃，加强数据流动有助于推动数字经济的发展。面对具有巨大价值的数据信息，为了实现经济利益，各大数据平台必然会不断加强技术壁垒，以阻止他人获取和利用数据，导致不正当竞争。以数据载体作为保护法益可能会导致互联网领域的大型企业愈演愈烈的排他性竞争以巩固其垄断地位[9]。更好的做法是将数据内容安全作为保护法益，将这类行为交由民法、经济法和行政法进行调规制，既符合刑法的谦抑性，又能有效防止优势地位企业以所谓的数据载体保密为借口，阻止他人获取和使用数据，从而避免数据垄断和不正当竞争的发生，推动数字经济健康有序地发展。

因此，就首例爬虫行为入刑案来说，没有侵害到数据的保密性，本案爬取公开可获取数据的行为应当属于未经授权的获取行为，不应被认定为非法获取计算机信息系统数据罪，由民事侵权领域予以规制。

3.4. 数据安全法益的具体内容

2017 年起施行的《网络安全法》第七十六条提到的“数据的完整性、保密性、可用性”这一数据安全三要素的概念借鉴于欧盟《网络犯罪公约》、德国刑法等域外立法，将数据的完整性、保密性、可用性作为数据犯罪的保护法益。完整性是指数据的准确与完备，不被随意修改和破坏；保密性是指数据的获取和使用需要经过授权；可用性是指数据的拥有者可以及时、可靠获取和使用数据。相较于其他的观点，该模式符合数据复杂多样、侵害侧重各不相同的特点，基于数据本身进行独立的规范评价[10]。不难看出，这是一种消极防御的模式，侧重于数据的控制安全，是针对数据泄露、篡改、灭失等静态数据安全风险，并确立以安全边界防护为核心的理论体系[11]。数据控制安全侧重于数据权利者对于数据的控制力，此时的数据利益是作为权利主体所绝对排他性的独享的。这在非法获取计算机信息系统数据罪的立法中也有所体现，将“侵入”或“采用其他技术手段”等条件作为本罪的构成要件。

在数据时代，数据和信息的流通是国家发展和社会基础条件，纯粹消极防御的数据控制模式要求收集和利用数据获得数据权利者的授权，这无疑会导致企业和个人获取数据的成本增加，一些互联网企业日常需要大规模收集并分析数据，这些企业无疑也会面临更高的刑事法律风险，非常不利于企业的创新与发展。如今民法价值取向已经由个人本位迈向社会本位，赋权理念需更多融入社会公共利益基因[12]。数据的使用日渐普遍且多样化，促进数据流通对数据赋权具有重要意义。因此我们既要承认数据的私权属性，同时也不能否认数据的公共产品属性，以充分发挥数据的公共价值，《数据安全法》就指明了的“保障数据安全，促进数据开发利用”的立法目的。

数据利用模式并不禁止他人获取或利用数据，而是通过重点规制数据滥用行为，兼顾数据主体与数据利用者的利益，以最大程度释放数据所蕴含的社会价值，以积极利用数据为目标，充分发挥数据所蕴含的社会价值。其次，数据利用模式弱化了对数据拥有者的保护，更侧重于对数据利用者的引导。刑法的补充性要求将刑法作为保护法益的最后手段，而通常情况下的数据获取行为并没有对数据权利者造成重大损失，是随后对数据的不正当利用才导致数据权益者的权益收到侵害。在这一点上数据利用模式与刑法作为补充性法益保护工具的功能定位相符。

综上所述，数据安全法益的基本内容应包含数据控制安全与数据利用安全两个方面。数据控制安全适用于保障数据内容层的安全性，保证数据的静态安全。其基于数据排他性原则，建立静态安全边界来保护数据，起到被动防御的作用。数据利用安全适用于促进数据应用层的流通共享，确保数据的有效利

用。其基于数据的公共属性，旨在充分挖掘数据的经济价值，构建动态流通利用框架，发挥积极利用的作用。

4. 数据安全法益与非法获取计算机信息系统数据罪构成要件的重释

4.1. 行为对象

首先，通过前文的论述可知，数据安全法益保护的是数据的独立性以及内容安全，因此本罪的行为对象仅包含有内容记录的数据，不包含冗余的、不记录信息的数据。

其次，依据数据安全法益的具体内容，在数据控制安全层面，数据的内涵不仅是存储在计算机信息系统内的数据，还包括维护信息系统功能的数据、存储在应用程序、云端或他专门存储介质中的数据。尽管《计算机刑事案件解释》将非法获取计算机信息系统数据罪的行为对象缩小为“身份认证信息”，但实际证明，其他非身份认证数据也可以识别用户的相关信息，从而导致数据安全风险暴露，如网站建立连接时在用户本地终端上产生的数据(Cookies)，Cookies 包含了网页、下载、关键词搜索等信息，虽然不属于身份认证信息，但网站可以通过 Cookies 收集和分析用户的行为数据，实现精准的广告投放。因此，本罪行为对象中的数据涉及所有经过数字化方式处理的数据。

最后，在数据利用安全层面，本罪的行为对象不包括可公开获取的企业数据。数字经济蓬勃发展，具有垄断地位的数据企业往往采取禁止抓取的手段来打压竞争对手，从网络效应、先发优势以及数据存储控制中获得利益。具有垄断地位的数据企业援引数据犯罪相关法律的目的并非为了防止黑客入侵，而是通过其他企业数据的获取和使用行为为“未经授权”这一点来限制竞争，不利于数字经济市场的发展。对于公开可获取的企业数据，本就只要用户注册并登录即可自由访问这些数据，在首例“爬虫”入刑案中，虽然被告上海晟品网络科技有限公司抓取的被害单位的视频数据的手段是“未经授权”，但所抓取的视频数据是所有注册用户可公开访问的，此时刑法应采取更为谨慎的态度，对于抓取企业公开可获取的数据的行为，应该通过实质性的标准予以出罪[13]。即使公开可获取的企业数据中可能包含了个人公开信息，但只要在合理的范围内，符合个人信息公开的目的和公开时的用途，没有侵害其重大利益，刑法也无需进行干预。目前，欧洲并未将个人的信息自决权视为排他性的绝对权力，美国在数据犯罪的刑法规定方面也逐渐趋于宽松。大数据领域的反垄断政策要求限制优势企业滥用数据控制权，以及采取技术性、排他性措施阻碍数据共享的行为。在大数据时代下积极获取企业公开数据并进行合理使用，促进了数据流通、共享，理应得到竞争法的支持。根据法秩序的统一性原则，对于民法、经济法上不违法甚至鼓励的行为，刑法不应当作犯罪处理。对“数据利用安全”法益层面上数据范围的认定，必须考量社会激励和经济后果，优先考虑反垄断的政策需求，谨慎规制获取可公开获取企业数据的行为。

4.2. 行为方式

依据我国关于非法获取计算机信息系统数据罪法条的规定，构成本罪具有“侵入计算机信息系统或者采取其他技术手段”的行为方式限定。随着数字技术的发展，行为人可能采取从云端直接获取的方式非法获取数据，不需要侵入计算机信息系统，或者行为人仅侵入云端，但并未采取技术手段获取数据载体，而是通过自己的记忆或是拍照录像等手段复制数据造成严重后果，是否依据法条并不构成对数据的非法获取，这显然并不合理。最高检在“卫梦龙等非法获取计算机信息系统数据案”中提到，非法获取计算机信息数据罪中的“侵入”包括：采用技术手段破坏或者规避系统防护进入计算机信息系统；未取得被害人授权擅自进入计算机信息系统；超出被害人授权范围进入计算机信息系统。“未经授权或者超越授权”成为了该罪的行为要件的认定关键。

美国的《计算机欺诈和滥用法案》(CFAA)同样对数据犯罪的表现形式认定为“未经授权访问”或者“超越授权访问”，主要包含四种理论：代理理论、代码理论、违反合同协议和撤销机制，其中代理理论在认定违反犯罪时赋予雇主过多权限，因判断标准过于主观而被认为是不合理的。

代码规制理论通过判断用户是否通过虚假认证或利用代码漏洞等行为来认定是否属于“未经授权”[14]。数据网站通常会采取数据技术保护措施以维护自身数据安全，只有规避或强行突破其保护措施的数据获取和访问行为才被认为是“未经授权”的数据犯罪行为。非法获取计算机信息系统数据罪存在“侵入型”和“利用其他技术手段型”两种行为方式，对于“利用其他技术手段型”法律并没有予以明确规定，但可以参考刑法对于第二百八十五条提供侵入计算机信息系统程序罪的解释，将非法获取计算机信息系统数据罪中的“利用其他技术手段型”的表现形式解释为规避或突破其数据安全保护措施的行为[15]，具体有侵入手段、利用技术手段绕开数据安全保护措施、利用技术手段破解网络安全措施、利用“撞库”手段等方式。

违法合同协议认为，在行为人违反明确或隐含的合同协议访问、获取网络数据时属于“未经授权”。数据网站的合同协议在最大程度保护自己的数据利益，若完全依据合同协议的规定来认定数据犯罪的边界这无疑会扩大了处罚范围，将一些并不合理的一般违法行为认定为犯罪。其次，在使用网络服务时，用户对于合同协议的内容通常没有太多关注，即使有无法提出反对意见，因为在不勾选“同意”的情况下用户就无法继续使用。因此，违背网站使用条款的数据侵权行为通常适用于不正当竞争或者知识产权侵权责任等民事责任的情形。

撤销机制认为一旦数据网站发送停止、终止访问的指令就相当于撤销授权，用户就不能再访问和爬取数据。通常情况下的违反合同行为并不会被认定为侵害数据安全法益，但如果用户明知自己访问、获取数据的权利已被撤销而继续进行访问行为，此时可能就属于 CFAA 的管辖范围。撤销机制站在数据网站利益的角度维护数据安全，改变了数据流通、共享的局势。为促进数据的良好竞争，应要求数据网站具备充分的合理理由才可以撤销数据授权，同时撤销行为应遵循法律规定，通过向用户发送停止或终止函的方式进行撤销。

综上所述，单纯违背数据网站服务协议的数据抓取行为不应入罪，而应交由前置法规制；对于避开或突破计算机信息系统安全保护措施的数据抓取行为、在明知授权被撤销的情况下依然继续访问获取数据的行为，则应由刑法予以规制。

5. 结语

数据的重要性随着网络与信息技术的发展已经达到了前所未有的高度，为了促进数据经济和信息化社会的发展，保护数据法益的相关研究刻不容缓。大数据时代下的数据独立于计算机信息系统，具备独立的保护价值，数据安全法益重视保护数据内容本身的安全以及具备数据控制安全与数据利用安全两方面内容。本文在明确数据安全法益内容的基础之上重释非法获取计算机信息系统数据罪的构成要件，规范本罪的适用范围，为解决实务中存在的认定疑难问题提供思路，以更好应对数据时代所带来的新问题、新挑战。

参考文献

[1] 彭文华. 法益与犯罪客体的体系性比较[J]. 浙江社会科学, 2020(4): 47-55+156-157.

[2] 高铭暄, 马克昌. 刑法学[M]. 北京: 北京大学出版社, 2011: 536.

[3] 童德华, 王一冰. 数据犯罪的保护法益新论——“数据内容的保密性和效用性”的证成与展开[J]. 大连理工大学学报(社会科学版), 2023, 44(3): 54-64.

[4] 王倩云. 人工智能背景下数据安全犯罪的刑法规制思路[J]. 法学论坛, 2019, 34(2): 27-36.
[5] 刘一帆, 刘双阳, 李川. 复合法益视野下网络数据的刑法保护问题研究[J]. 法律适用, 2019(21): 109-117.
[6] 王华伟. 数据刑法保护的比较考察与体系建构[J]. 比较法研究, 2021(5): 135-151.
[7] 赵春玉. 大数据时代数据犯罪的法益保护: 技术悖论、功能回归与体系建构[J]. 法律科学(西北政法大学学报), 2023, 41(1): 95-107.
[8] 许可. 自由与安全: 数据跨境流动的中国方案[J]. 环球法律评论, 2021, 43(1): 22-37.
[9] 苏桑妮. 从数据载体到数据信息: 数据安全法益本位之回归[J]. 西南政法大学学报, 2020, 22(6): 97-108.
[10] 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.
[11] 杨志琼. 数字经济时代我国数据犯罪刑法规制的挑战与应对[J]. 中国法学, 2023(1): 124-141.
[12] 于改之. 从控制到利用: 刑法数据治理的模式转换[J]. 中国社会科学, 2022(7): 56-74+205.
[13] 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.
[14] 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.
[15] 杨志琼. 美国数据犯罪的刑法规制: 争议及其启示[J]. 中国人民大学学报, 2021, 35(6): 155-164.