Dispute Settlement 争议解决, 2025, 11(9), 164-173
Published Online September 2025 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2025.119293

Hans汉斯

我国“流量劫持”行为的司法困境、原因检视与刑法因应

冯迎港，邓　领

伊犁师范大学新疆社会治理与发展研究中心，新疆　伊宁

收稿日期：2025年8月11日；录用日期：2025年9月3日；发布日期：2025年9月15日

摘　要

随着互联网行业竞争的加剧，“流量劫持”现象层出不穷，如DNS劫持、数据劫持、变造劫持等。当前，我国司法实践认定“流量劫持”行为时，主要存在罪与非罪界限不清晰、类案罪名适用不统一、犯罪认定缺少统一裁判等困境。出现上述问题的原因主要为刑法中“破坏”与“非法控制”的解释结论界限不明、“流量劫持”行为的日益复杂以及法益侵害的多元性。基于此，我国刑法及司法解释应当坚持以社会危害性为基础、以犯罪构成要件为标尺、以法益内容为实质的定罪标准。此外，我国应当根据“流量劫持”的技术类型明确其罪名适用。在罪数认定上，我国司法机关应当根据行为的数量和性质，正确适用想象竞合、牵连犯、数罪并罚的情形。

关键词

“流量劫持”，类型化归纳，非法控制，想象竞合

The Judicial Dilemma, Cause Analysis and Criminal Law Response to “Traffic Hijacking” in China

Yinggang Feng, Ling Deng

Xinjiang Social Governance and Development Research Center, Yili Normal University, Yining Xinjiang

Received: Aug. 11th, 2025; accepted: Sep. 3rd, 2025; published: Sep. 15th, 2025

Abstract

With the intensification of competition in the Internet industry, “traffic hijacking” phenomena emerge

文章引用: 冯迎港, 邓领. 我国“流量劫持”行为的司法困境、原因检视与刑法因应[J]. 争议解决, 2025, 11(9): 164-173.
DOI: 10.12677/ds.2025.119293

in an endless stream, such as DNS hijacking, data hijacking, and altered hijacking. Currently, in China's judicial practice, when identifying "traffic hijacking" behaviors, there are mainly predicaments such as unclear boundaries between guilt and innocence, inconsistent application of charges in similar cases, and lack of unified adjudication for guilt determination. The main reasons for the above problems are the unclear boundary between the interpretation conclusions of "destruction" and "illegal control" in the criminal law, the increasingly complex nature of "traffic hijacking" behaviors, and the diversity of legal interest infringements. Based on this, China's criminal law and judicial interpretations should adhere to the conviction standards based on social harmfulness, taking the elements of crime as the yardstick, and regarding the content of legal interests as the essence. In addition, China should clarify the application of charges according to the technical types of "traffic hijacking". In terms of determining the number of crimes, judicial organs in China should correctly apply the situations of imaginative joinder of offenses, implicated offenses, and combined punishment for multiple crimes according to the quantity and nature of the behaviors.

Keywords

"Traffic Hijacking", Typological Induction, Illegal Control, Imaginative Joinder of Offenses

1. 引言

"流量劫持"是行为人利用恶意软件非法修改浏览器配置，或者在应用软件上捆绑插件，用户在登录初始网页或者下载应用软件时，强制其登录指定网页(网站)或者捆绑下载插件，造成用户流量被迫流入特定网页(网站)或者应用程序，并将该部分流量卖送广告商或者软件推广商等流量需求方，最终实现流量变现[1]。随着网络的迭进发展，"流量劫持"案件近年来层出不穷，司法实践逐渐显示出网民入刑的态度。截至 2023 年 6 月 29 日，在裁判文书网搜索"流量劫持"可以检索到 66 篇法律文书，其中 11 个是刑事案由，55 个是民事案由。由于"流量劫持"案件属于新型网络违法犯罪行为，该类案件的定性成为各界关注的热点问题，换言之，"流量劫持"行为的各环节、各类型是否能为刑法规制所涵盖，司法实践与理论界对此尚不能形成统一意见。在最高人民法院发布 102 号指导性案例"付宣豪、黄子超破坏计算机信息系统案"之前，我国法院通常以不正当竞争案件看待。随着"360 奇虎与 QQ 腾讯大战"案件的发酵，"流量劫持"行为对网络秩序的破坏不容小觑，司法系统内部针对该类案件罪与非罪、此罪彼罪问题逐渐出现分歧，由此出现破坏计算机信息系统罪、非法控制计算机信息系统罪等判决结论。与之相对，刑法理论界更多聚焦如何在解构"流量劫持"类型的基础上提出科学的罪名适用，如有学者认为"流量劫持"分为硬性"流量劫持"和软性"流量劫持"，从而析出硬性"流量劫持"行为应成为刑法规制的重点[2]。在过滤出前置法规制的部分后，有学者进一步指出删除或者篡改原始网站代码后强制用户跳转至另外的网站，构成破坏计算机信息系统罪；未经用户同意，强制锁定网站首页或者指定网页，构成非法控制计算机信息系统罪[1]。随着学界对"流量劫持"行为类型的深入探讨，学者对"流量劫持"行为的定性仍未形成统一意见，其中对"流量劫持"行为各环节的违法性评价和罪数认定上仍存在较大争议。因此，我国仍需针对"流量劫持"行为建立一套统一的罪与非罪、罪名适用以及罪数认定的裁判标准，进一步完善我国关于"流量劫持"行为的刑法规制体系。

2. 我国"流量劫持"行为司法认定的困境

在以往针对"流量劫持"的法律实践中，法院多以民商事法律手段进行调整。然而，随着相关技术

的持续演进，此类行为的社会危害性逐渐增大，现已引起了刑法学界及实务界的关注。目前司法裁判中存在罪与非罪界限不清、相似案件罪名适用不一以及罪数认定缺少统一裁判等问题。

2.1. 罪与非罪的界限不清

根据当前“流量劫持”案件的司法实践，法律主要采取了两种规制路径：一是借助反不正当竞争法来进行管理和约束；二是依据刑法予以调整。但是，如上法律未明确指出法律的适用指向。在涉及猎豹、金山以及2345科技有限公司的一宗反不正当竞争纠纷中，争议焦点在于当用户安装或启动由被告方提供的驱动精灵应用程序时，该程序会在没有充分通知用户或者通过误导性提示的情况下，擅自更改用户浏览器内设定的2345导航主页。被告未经用户同意，借助其软件干预并改变了浏览器默认首页设置，进而转移了原本属于2345网站的访问流量。法院最终认定，该行为违背了公平竞争的基本原则，属于不正当竞争行为[1]。

在涉及卿烨科技有限公司的案例中，该公司被指控在其用户未被告知的情况下，通过程序自动给谷歌浏览器添加扩展插件。该插件在未经用户授权的情况下篡改浏览器默认启动页面，剥夺用户根据个人偏好选择启动页的权利，从而引导和控制用户的搜索和访问流量。法院最终认定，卿烨科技的行为构成对计算机信息系统实施破坏的犯罪行为[2]。从这些案例的比较中可以看出，尽管涉案主体均为企业，并且均涉及非授权修改浏览器设置的行为模式，但相似的“流量劫持”行为在不同的案件中可能面临民事诉讼或刑事指控的区别对待。这表明，相似的案件之所以会产生不同的法律判断，原因在于不同的案件之间存在各种各样的差异(见表1)。

Table 1. Comparison between criminal cases and unfair competition cases involving “traffic hijacking”
表1. “流量劫持”刑事案件与不正当竞争案件的对比

类案特征	修改浏览器主页		在他人网站植入广告	
案件名称	1) 北京猎豹、金山与上海2345不正当竞争(2018)沪0115民初728611号	2) 卿烨科技破坏计算机信息系统案(2018)京0108刑初714号	3) 南京聪明狗不正当竞争案(2019)京73民终1489号	4) 符耿琳破坏计算机信息系统案(2017)琼97刑终74号
行为模式	未经用户同意，利用电脑软件修改用户浏览器启动页	未经用户同意，利用插件修改用户浏览器启动页	未经允许利用插件在淘宝网插入广告	未经允许利用技术手段在网站中植入违法广告
裁判结果	构成不正当竞争	构成破坏计算机信息系统罪	构成不正当竞争	非法控制计算机信息系统罪

2.2. 相似案件罪名适用不一

在司法实践中，由于法官个人对法条理解的差异、法律法规本身可能存在的模糊性以及个案具体情况的不同，导致了即便是在相似案件中，适用的罪名也可能出现不一致的情况。虽然“流量劫持”这类案件在整个司法案件中的比例不高，但从现有的案例分析来看，对于何为犯罪行为的理解存在分歧。例如，在首例被认定为刑事犯罪的“流量劫持”案中，被告人针对“2345.com”实施了DNS攻击，并进行了黑客活动，法院基于这些行为对两名被告作出了相应的判决[3]。在另一起与DNS劫持有关的案例中，

[1]参见上海市浦东新区人民法院(2018)沪0115民初728611号民事判决书。
[2]参见北京市海淀区人民法院刑事判决书(2018)京0108刑初714号。
[3]参见上海市浦东新区人民法院(2015)浦刑初字第1460号刑事判决书

尽管被告施硕同样通过修改域名解析记录实施“流量劫持”，法院则是以非法控制计算机信息系统罪对涉及的个人进行判决[4]。在第一个案例中，被告人对“2345.com”的网络流量进行非法访问，法院以破坏计算机信息系统罪对被告人作出判决；而在施硕公司的案例中，与改变域名解析文件的方式来实现 DNS 劫持相似，但是法院最终依然以“非法控制”将其判决。从中我们可以看出两个案件尽管所实施的犯罪方式十分相似，但是在不同的法院裁判中，犯罪行为的认定却得到不一样的结果。这说明在司法实践中，同类行为可能被认定为不同罪名(见表 2)。

Table 2. Comparison of case examples of criminal cases involving “traffic hijacking”
表 2. “流量劫持”刑事案件案例对比

劫持类型	DNS 劫持型		植入推广 ID 型		植入广告型
案件名称	1) 付宜豪等破坏计算机信息系统案(2015)浦刑初 1460 号	2) 施硕等控制计算机信息系统案(2015)渝北法刑初字第 666 号	3) 陈志勇、王惺等非法获取计算机信息系统数据案(2016)渝 01 刑终 575 号	4) 沈捷等诈骗案(2017)沪 0104 刑初 8 号	5) 陈启商等破坏计算机信息系统(2019)沪 01 刑终 601 号
行为模式	修改互联网用户路由器的 DNS 设置	修改电信运营商域名解析配置文件	镜像网络端口数据，植入推广 ID，使用户带着 ID 访问百度	应用程序植入推广 cookie，促使用户带其下单	解析修改用户 http 数据包包头，植入预先设置的广告代码
裁判结果	破坏计算机信息系统罪	非法控制计算机信息系统罪	非法获取计算机信息系统数据罪	诈骗罪	破坏计算机信息系统罪

2.3. 罪数认定缺少统一裁判

在“流量劫持”案件中，行为人可能会多次实施相同类型的“流量劫持”行为，或者采用不同的方法进行“流量劫持”。因此，这类行为可能涉及多个不同的罪名。而现阶段司法实践中针对此种情况，往往缺乏统一的罪数认定标准，出现了裁判结果不统一的情况。造成这种现象的一个重要原因是，司法实践中尚未对“流量劫持”行为的罪数进行认定。

截至目前，仅在卿烨科技有限公司破坏计算机信息系统案件中，对涉及“流量劫持”的犯罪行为数量进行了具体的认定和分析。在该案件中，法院判定被告公司通过制作、分发特定源代码程序的方式，非法控制了计算机信息系统，而且该源代码程序未经用户许可擅自修改用户浏览器启动页面，剥夺了用户的自由选择权，而且对计算机信息系统的原有功能造成了破坏。法院认为，仅以“非法控制”来评价被告单位的行为并不充分，因为该单位所开发的源代码程序具有“非法控制”的功能，其最终目的是实现“破坏”[5]。在这种情况下，控制行为是手段，而破坏行为才是最终结果，二者系牵连犯。因此，法院认定被告单位破坏计算机信息系统罪。而在陈志勇等人涉及的案件中，他们非法获取计算机信息系统数据，并实施了一系列不同的行为，但法院最终却仅仅认定了一个罪名，该案可分为两个阶段，第一阶段，通过获得资料骗取推广费，因此符合牵连犯原则，按诈骗罪定罪；第二阶段，通过非法获取用户笔记本电脑数据实施对计算机的控制，法院依据牵连犯的原则，认定为非法控制计算机信息系统罪[6]，但忽视了犯罪情节的认定(见表 3)。

[4]参见重庆市渝北区人民法院(2015)渝北法刑初字第 00666 号判决书。
[5]参见北京市海淀区人民法院刑事判决书(2018)京 0108 刑初 714 号。
[6]参见重庆市沙坪坝区人民法院(2016)渝 0106 刑初 1393 号刑事判决书。

Table 3. Comparison of the determination of the quantity of crimes in “traffic hijacking” cases
表 3. “流量劫持”案件犯罪数量认定对比

案件名称	卿烨科技破坏计算机信息系统案(2018)京 0108 刑初 714 号	陈志勇等非法获取计算机信息系统数据案(2016)渝 01 刑终 575 号
行为个数	1) 利用源代码程序静默下载安装 crx 插件 2) 插件修改浏览器启动页	1) 镜像网络端口数据植入推广 ID 2) 抓取服务器上的 QQCookies 数据、控制 QQ 账户
可能触犯的罪名	1) 非法控制计算机信息系统罪 2) 破坏计算机信息系统罪	1) 诈骗罪 2) 非法获取计算机信息系统数据罪
罪数认定	手段和目的牵连	未认定
判决结果	破坏计算机系统罪	非法获取计算机信息系统罪

3. 我国“流量劫持”行为司法乱象的原因检视

当前，在网络领域中，“流量劫持”已然成为一个亟待解决的突出问题。通过深入探究“流量劫持”行为类型的现状，以及对其司法认定过程中所面临的重重困境进行剖析，造成上述一系列棘手问题的原因主要集中在刑法对计算机犯罪立法规定的混乱。

3.1. “破坏”与“非法控制”界限不明

在“流量劫持”案件中，关于“破坏”与“非法控制”这两个概念的界定存在不同分歧。《刑法》第二百八十五条第二款针对的是非法控制计算机信息系统的犯罪活动。这项法律规定采取了一种概括性的描述，指出如果有人对计算机信息系统进行非法控制，并且情节达到严重的程度，则会被视为犯罪行为。但是，该条款没有具体列举哪些特定的行为可以归为此类犯罪。此外，《刑法》第二百八十六条对破坏计算机信息系统罪进行了规定，该条款分为三款，分别描述了构成此罪的三种不同类型的行为。然而，从其法律条文来看，依然采用了较为宽泛和包容性的表述方式[3]。虽然这种立法为司法实践保留了一定程度的解释灵活性，但也引发了两种罪名在适用方面的复杂性及界限的模糊性。尤其是对犯罪行为进行界定时，非法控制计算机信息系统罪和破坏计算机信息系统罪呈现交叉竞合。这是由于计算机信息系统本质上属于由数据组成的集合，当对这类系统实施“非法控制”时，通常涉及对系统内数据的添加、移除或更改等操作。此外，要构成破坏计算机信息系统罪，还必须存在对系统功能、数据等造成相似修改或损害。因此，针对某些威胁网络安全的行为，难以简单地界定其性质究竟是非法控制还是破坏。

3.2. “流量劫持”行为类型繁杂

“流量劫持”并非单一行为，而是由多种行为聚合而成的类型化行为，这些行为呈现出显著的繁杂性，涉及多种不同的类型。各类“流量劫持”行为在操作手段、导致的危害后果以及所侵害的具体法益方面存在明显差异。因此，为保证司法裁判的稳定性，有必要对“流量劫持”行为进行分类和辨别，以便准确认定其性质。当前，学术界已充分认识到“流量劫持”现象的复杂性，并建立了分类标准以更好地识别和界定这些行为，为司法实践提供了理论支撑。依据其造成的不同影响，“流量劫持”可以被区分为两种主要形式：导向改变型与内容嵌入型。导向改变型通常涉及对计算机信息系统的非法干预；而内容嵌入型更多情况下被视为违反市场竞争规则[4]。根据不同技术手段的应用，“流量劫持”行为可以进一步分类为灰色“流量劫持”和黑色“流量劫持”[5]。前者被视为一种不正当竞争手段，而后者则可能被判定为违法行为。尽管这一见解认识到了“流量劫持”本身之间的差异，但其界定标准仍不够明确，

并且缺乏具体的分类指导原则。

3.3. 同一行为侵害法益的多样性

司法实践对同一犯罪行为会根据其侵害的具体法益类型来进行区分，使之适用于不同的罪名和法律条款。从“流量劫持”的行为来看，不同的行为可能表现出不同的行为效果，而同一行为在不同案件中也可能产生不同的法律后果。因此，在面对类似案件时，法官需要识别行为侵害法益的类型。在当前“流量劫持”案件中，行为人仅实施了单一的“流量劫持”行为，但是此类行为侵犯多重法益。以李孟龙、梁雄健、吴文仔等为例，在他们所涉及的帮助信息网络犯罪活动的案件中，行为人实施 DNS 劫持[7]，可能同时对网络秩序以及用户数据安全这两个法益造成侵害，法益侵害的实质出现是适用刑法的前提，故而罪名选择需严格依照法益识别准则。

4. 我国“流量劫持”行为的刑法规制因应

通过对“流量劫持”案件进行分析可知，在处理“流量劫持”案件的司法实践中，一方面存在罪与非罪界限不清晰的问题；另一方面，相似案件之间出现了罪名适用不一致的情况。这些问题的存在，不仅阻碍了对“流量劫持”行为的有效规制，也对司法公正造成了不利影响。因此，解决上述问题的关键在于建构一套完整清晰的罪与非罪、此罪彼罪及罪数认定的适用结论。

4.1. 以犯罪构成界别“流量劫持”行为罪与非罪的判定标准

确立一套明晰的衡量标准，既可对“流量劫持”行为的罪与非罪的区分划定提供参考，也能为司法实务提供指导准则。现行规制路径通常根据不同类型的“流量劫持”行为采取差异化管理。对于那些严重侵犯网络用户自主选择权的跳转型“流量劫持”，鉴于其对法益的侵害程度较为严重，可以采用刑法的相关规定予以打击；而对于植入型“流量劫持”以不正当竞争规制，上述分类方法不尽合理，跳转与否是跳转技术功能的结果，仅以是否发生跳转作为区分罪与非罪的标准显然是不够的。而更为合理的区分方式应从“流量劫持”行为的社会危害性、犯罪构成要件、侵害的法益内容等角度着手。

1) 以社会危害性为基础

众所周知，犯罪的本质特征是具有社会危害性。在网络环境中发生的“流量劫持”，其社会危害性最直接地体现在具体的行为手段和性质上。第一，从“流量劫持”的手段来看，可以区分不同的行为手段及其衍生后果。当采用误导性广告、搜索引擎默认选项或输入法软件功能等技术方法来引导流量时，这类行为虽然促进了商业竞争且完成了流量导向的目标，但它们对用户行为的影响以间接形式呈现。这些手段不直接回应用户的请求数据，也不涉及侵入他人计算机系统或破坏信息系统及网络设备的正常运作，因此不宜作为犯罪行为来处理。然而，当“流量劫持”涉及使用木马程序、恶意代码入侵等更具侵入性的技术时，此行为直接威胁到计算机信息系统的安全性和完整性，以及网络设备的功能，具有严重的社会危害性，应当受到刑法的约束和惩处。在进行具体判断时，可参考是否使用了黑客工具、“抓包”技术等。第二，从“流量劫持”行为性质来看，“流量劫持”行为具有植入功能，往往依托于其他平台，可通过获取用户授权在他人网络上植入插件。虽有对数据的修改，但系以互联网行业的盈利模式等作为盈利手段。总之，如果说出于为赌博网站推广的目的而修改他人网站的代码或程序时作出定罪处理的，鉴于某些“流量劫持”行为所具有的严重社会危害性，对这些行为进行定罪是合理的。从实证研究的角度出发，评估“流量劫持”行为的社会危害程度，可以初步形成关于这些行为是否构成犯罪的判断准则。

[7]参见广东省中山市第一人民法院(2020)粤 2071 刑初 835 号刑事判决书。

2) 以犯罪构成要件为标尺

在刑事司法实践中，不管认定行为是否构成犯罪，以及构成何种类型的犯罪，必须依赖犯罪构成要件。这是因为刑法中的定罪依据是建立在犯罪构成理论之上的。在我国的法律框架下，这一理论的一个重要特征在于它不仅定性还定量。例如，在我国刑法的具体条款中，一般会先把某类行为界定为特定的罪行，然后依靠附加条件，像“情节特别严重”或“导致重大后果”来进一步划定更严重的犯罪标准。在处理涉及“流量劫持”案件时，要认定某行为是否构成破坏计算机信息系统罪，除了必须确认行为人实施了符合《刑法》第二百八十六条所描述的破坏行为之一，并对系统的运行安全造成实际侵害之外，还必须验证该行为引发了“严重的后果”。若无法满足这些条件，则不足以将“流量劫持”等行为定性为犯罪。关于“造成严重后果”的界定，应当依据最高人民法院、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》中的相关规定进行评估。根据这一标准，在判断是否破坏了计算机信息系统时，应该综合考虑多个因素，包括但不限于受影响的计算机信息系统的数量、违法行为所带来的非法获利以及造成的经济损失等，以此来全面评价行为的严重性。而行为不满足法律规定的各项构成要件时，不存在犯罪问题，即不应将其判定为犯罪。当行为人以“流量劫持”为手段获取财物时，如果该行为满足了诈骗罪等特定罪名的构成要件，则应依据具体情形依法进行定性和处理，采用相应的刑法规定予以规制。

3) 以法益内容为实质

在确认事实上的社会危害性之后，通过进一步衡量是否侵害了具体法益来确认是否存在法益侵害，使得该种社会危害现象蜕变为具有法益侵害的一种司法选择[6]。从“流量劫持”所导致的后果分析，此类行为可能侵犯的合法权益至少涵盖三个方面：首先，涉及网络用户或运营商的流量财产权益；其次，影响运营商的正常业务运营；最后，关乎计算机信息系统的安全性。因此，在评价“流量劫持”行为是否构成犯罪时，可以从上述三类法益侵害角度进行考量。

首先，从财产法益角度考察，有观点认为流量属于财产性利益，因此实施“流量劫持”行为构成盗窃罪[7]。该观点值得进一步商榷。虽然网站流量能带来经济效益，但它并非构成传统意义上的有形资产或法律上的财产权益，故而不能被当作盗窃罪的对象，也不会对盗窃罪旨在保护的法益造成干扰[8]。所以，把“流量劫持”简单地判定为盗窃罪并不恰当。不过，随着相关技术的发展，“流量劫持”可能已经超越了其最初主要针对计算机网络和互联网基础设施的原始形态，转变为一种依托这些平台实施更为复杂犯罪行为的手段。其次，从运营商正常运营的角度来看，“流量劫持”确实给运营商带来了某种负面影响，运营商投入了大量资源和成本以吸引和维持用户流量，在此过程中流量却因劫持者的拦截而流失，但这尚不足以成立破坏生产经营罪。破坏生产经营罪主要针对机器设备、耕畜等生产工具和生产设备的物理性破坏行为，其保护的具体法益主要是处于实际存在状态的生产活动。显然，“流量劫持”行为更为侧重的是功能性损害而非物理性损害，因而不应当简单地判定为破坏生产经营罪。最后，从计算机信息系统的安全性角度考察，“流量劫持”可能符合计算机犯罪构成要件。“流量劫持”案件在实际中常常涉及行为人利用网络技术非法侵入、控制或损害计算机信息系统，这些系统的安全是法律重点保护的重要利益之一。因此，当“流量劫持”行为对计算机信息系统的安全构成直接而紧迫的威胁时，就达到了构成犯罪的必要条件。所以，在认定“流量劫持”行为究竟是罪与非罪的实质判断中，应把握“流量劫持”行为扰乱计算机信息系统安全的危害性及具体犯罪构成要件的合法性。

4.2. 以技术底色明确“流量劫持”行为的适用罪名

不同的“流量劫持”行为，在实施目的、所采用的行为手段、造成的损害后果以及侵害的法益等方面，都有可能存在显著差异。判断一个行为构成此罪还是彼罪的关键衡量标准是该行为侵犯了何种法益。

因此，应围绕“流量劫持”行为的侵害法益以选择相应的罪名，从而确保类似案件罪名适用的一致性。

1) DNS 劫持：破坏计算机信息系统罪

目前，对于 DNS 劫持行为所侵犯的法律利益性质的认定，理论上的观点存在分歧，主要存在“非法控制”与“破坏”的两种观点，在责任竞合上形成法律适用上的分歧[9]。在 DNS 劫持案件中，行为人通过攻击或未经授权修改域名解析记录，导致这些记录指向非预期的网站而非原定的所有者或管理者指定的地址。这种行为被视为“破坏计算机信息系统功能”，构成破坏计算机信息系统罪。由于域名系统是关于计算机网络所指 ID 的一系列规范文件，当检测到针对特定排名的域名信息网络接口的解析配置被篡改，从而改变了该域名系统的正常工作模式。当域名系统被劫持，导致其无法按照原有的路径进行解析时，这种情形符合《刑法》第二百八十六条中所述的“致使计算机信息系统不能正常运行”的规定。此类行为损害了计算机信息系统的运行安全，构成了对相关法律保护利益的威胁[10]。同时，行为人修改域名解析文件后，域名系统将仅按照行为人设定的新路径进行解析，引导用户访问指定的网站。这不仅改变了原本由权利人控制的域名信息系统的状况，还导致权利人失去了对计算机信息系统的实际控制权，无法掌控系统的运行及信息流动的方向，致使权利人合法权益受到损害。

2) 数据劫持：非法控制计算机信息系统罪

在分析数据劫持是否应被视为犯罪行为的问题上，通过在主机上安装插件或代码强制更改用户浏览器首页、利用程序修改 HTTP 请求的首页信息等途径非授权地展示广告时，这些行为被认为是针对计算机信息系统的非法操纵。该行为侵害了合法权利持有人对其系统应有的控制权，因此需认定为非法控制计算机信息系统罪。当行为主体在目标服务器或计算机信息系统内实施特定动作，如嵌入额外的插件、插入广告代码或修改数据包的首页信息等操作时，实际上是在对这些系统的信息进行变更或添加。此种模式与刑法第二百八十六条第二款描述的行为特征相一致。从技术层面来看，非法控制计算机信息系统通常首先需要侵入该系统，并获取相应的权限[11]。因此，在处理数据的变更或添加时可能同时满足“破坏”与“非法控制”。然而，在探讨破坏计算机信息系统罪时，重点应该放在“破坏”这一概念上。虽然《刑法》第二百八十六条第二款没有明确指出“数据的增加、删除或修改”需要致使“计算机信息系统无法正常运作”作为犯罪成立的前提，但从立法科学性和合理性考虑，对于性质相似的行为应当施以相同程度的法律制裁。因此，不应以数据的增加、删除或修改理解为构成破坏计算机信息系统罪的行为。若如此理解，不仅难以区分那些仅借助非关键数据的修改或添加来实现控制与真正破坏系统运行的行为，这种模糊还可能会导致非法控制计算机信息系统罪的适用范围宽泛过度，变成一个囊括多种行为的“口袋罪”[12]，从而削弱了法律的精确性和针对性。

3) 变造劫持：诈骗罪

在施硕涉及的未经授权操控计算机信息系统案件中，行为人通过更改域名解析配置，导致用户在访问指定网站时，在不知情的情况下被嵌入了推广商的代码，使得被影响的网站基于误导而向推广商支付了相关费用；而在陈志勇的数据窃取案件中，被告人在用户网络流量的数据包中注入了包含特定推广 ID 的信息，行为人通过百度平台上获得了推广佣金。而在涉及沈捷的欺诈案件中，被告人则是通过在成果网上发布包含推广链接的内容，诱导用户进行点击，从而在用户的浏览器中设置推广关联的 cookie，以此方式赚取了购物平台的推广奖励[8]。这些情形可以被视为典型的“流量劫持”行为。尽管行为人利用计算机技术植入推广 ID，但此类行为更适合以诈骗罪进行定性，而非归类为计算机犯罪。从具体实施手段来看，行为人借助把特定的推广标识植入网络用户的通信数据流中的途径，此种方式并未致使计算机信息系统功能出现异常或失效，同时也未涉及广告弹窗的生成。它仅仅在网络使用过程中附带地植入了推

[8]参见重庆市沙坪坝区人民法院(2016)渝 0106 刑初 1393 号判决。

广 ID，因此不适宜将其判定为计算机犯罪。

4.3. 以刑法立法统一“流量劫持”行为的罪数认定标准

准确界定“流量劫持”行为的罪数形态对于定罪准确和量刑公正尤为关键。依据当前“流量劫持”案件的判决，可以看出司法实践对于罪数认定的标准存在不统一的现象。因此，有必要根据行为的具体数量和性质，对“流量劫持”行为进行详细的评估，以实现全面且一致的法律认定。

1) 想象竞合的情形

想象竞合指的是当某一行为同时违反多项罪名，或者符合多个犯罪构成要件的情况[13]。虽然我国刑法没有直接采纳“想象竞合”这类表述，但该罪数理论已深刻影响司法实践。由于“流量劫持”行为大多具有推广引流的效果，因此容易与其他犯罪竞合。然而在现有的案例中，法院对于此类竞合情形的界定不够明晰。例如，在李孟龙、梁雄健、吴文仔等人涉及的帮助信息网络犯罪活动案件中，他们利用 DNS 劫持手段为赌博网站提供推广服务，并从中获利 17 万元[9]。尽管在此案中法院并未详细分析域名劫持行为的具体性质，但该行为已触犯破坏计算机信息系统罪。依据《最高人民法院、最高人民检察院、公安部关于办理网络赌博犯罪案件适用法律若干问题的意见》，为赌博网站提供广告推广服务的行为被认定为开设赌场罪的共犯行为。就“流量劫持”行为带有宣传和引导的特性而言，实施此类行为的个人可能会被认定为共犯。从犯罪行为的结构分析，当行为人实施 DNS 劫持行为即构成开设赌场罪、帮助信息网络犯罪活动罪以及破坏计算机信息系统罪的竞合，以开设赌场罪认定只能认定为帮助犯，另外两罪基准刑虽为五年，但性质和帮助信息网络犯罪活动罪不同，故而该案以破坏计算机信息系统罪处理更恰当。

2) 牵连犯的情形

“流量劫持”行为不仅展现了显著的产业链特征，而且在这一犯罪链条的各个环节上，都可能得到特定技术手段的支持，从而使其更加复杂和多样化。由此，个人或单位可能涉及多种相互关联的违法活动[14]。“流量劫持”往往处于非法产业链的前端，既可在同一层面，也可跨层级与其他犯罪行为相关联。以沈捷诈骗案为例，行为人通过域名劫持植入 cookie，后使电商陷入错误认识获取推广费，实施了“流量劫持”和诈骗两个行为，存在手段目的牵连，应从一重罪处罚，但该案缺少对“流量劫持”行为的认定。在陈志勇案中，被告通过架设服务器镜像和复制网络端口间接获取运营商用户数据，并在未授权情况下植入推广 ID 以赚取广告费用。前者构成非法获取计算机信息系统数据罪，后者则为变相“流量劫持”[10]。因此，仅以此罪评价被告行为是不全面的，应同时构成两罪，且鉴于其严重性，更适合以较重的诈骗罪论处。

3) 数罪并罚的情形

当行为人参与多种不同形式的“流量劫持”活动时，每种行为所导致的后果及其对法律利益的侵害各有差异。因此，对于行为人之间无关联且行为无吸收关系的多个违法行为，应当数罪并罚。例如，在陈志勇和王惺等非法获取计算机信息系统数据案中，被告人陈志勇实施了两种性质不同的行为[11]。

首先，关于陈志勇的第一个行为，他通过建立服务器镜像和复制网络端口数据的方式，设立虚拟身份建立网络端口的行为，可以认定为非法获取计算机信息系统数据罪。植入推广 ID 以获取推广费的行为属于典型的变造劫持行为，应被认定为诈骗罪。然而，镜像数据本身并不直接形成“流量劫持”。实际上，陈志勇通过第一个行为获取的这些数据成为后续实施变造和劫持活动的工具或手段，两行为之间具有手段和目的的牵连关系，按照法条规定可能判处较重刑罚，因此应以诈骗罪定罪。

[9]参见广东省中山市第一人民法院(2020)粤 2071 刑初 835 号刑事判决书。
[10]参见上海市徐汇区人民法院(2017)沪 0104 刑初 8 号刑事判决书。
[11]参见上海市徐汇区人民法院(2017)沪 0104 刑初 8 号刑事判决书。

其次，对于第二个行为而言，陈志勇因采用技术方法获取 cookie，此行为构成非法获取计算机信息系统数据罪。随后，他通过这些数据实施了控制 QQ 账户的操作，并将这些账户用于淘宝平台上的广告推广活动，这一系列行为则属于数据劫持，同时也触犯了非法控制计算机信息系统的相关法规。鉴于前期获取 cookie 的行为是为了后续控制 QQ 账户做准备，可以视为实现非法控制目的的一种手段。因此，陈志勇的前后两种行为分别构成了变造劫持和数据劫持，这两种行为侵害了不同的法律利益，并导致了不同的危害结果。而且，这两种行为在实施方式与造成的法益侵害之间缺乏高度伴随性，不具备牵连犯的特征。为了刑法的充分评价，应对陈志勇变造劫持行为和数据劫持行为分别定性并实行数罪并罚。

5. 结语

随着互联网科技与数字经济日益紧密结合，网络空间中的“流量劫持”现象也逐渐演变出更为复杂的形式。这种变化持续地对刑法在网络环境下的适用性构成挑战。在“流量劫持”被正式纳入刑法之前，这类行为通常依据反不正当竞争法进行处理。首例“流量劫持”刑事案为类似案件设立了法律标准，明确了此类行为的罪与非罪界限。近年来，随着“流量劫持”犯罪增多，由于其形式多样、复杂，导致司法裁判中仍存在罪与非罪界限不清、相似案件罪名适用不一致及罪数认定缺乏统一裁判等现象，亟需解决。因此，治理“流量劫持”行为的关键在于构建足够完善的网络“流量劫持”治理体系框架，通过构建“罪与非罪－罪名适用－罪数认定”三位一体的裁判规则体系，精准廓清“流量劫持”行为的刑法规制边界，实现对“流量劫持”行为全维度精确整治与网络空间法治生态深层次优化，为数字经济稳步推进打造坚实的法律后盾。

基金项目

本文系 2024 年新疆维吾尔自治区高校基本科研业务费科研项目“我国非法数据跨境流动的刑法规制研究”(项目编号：XJEDU2024P074)阶段性成果。

参考文献

[1] 肖怡. 流量劫持行为在计算机犯罪中的定性研究[J]. 首都师范大学学报(社会科学版), 2020(1): 37-44.

[2] 陈禹衡. 流量劫持的刑法规制思考——以第 102 号指导性案例为视角[J]. 西南石油大学学报(社会科学版), 2019, 21(6): 76-83.

[3] 程红, 赵浩. 计算机信息系统犯罪中“非法控制”和破坏的界限与竞合[J]. 中共山西省委党校学报, 2022, 45(6): 72-78.

[4] 刘佳欣. 反不正当竞争法视角下的“流量劫持”——以流量劫持典型案例为分析样本[J]. 法律适用, 2019(18): 80-88.

[5] 钱海玲, 张军强. 流量劫持不正当竞争行为的司法规制[J]. 法律适用, 2018(22): 95-106.

[6] 柳洁, 彭永雄, 曾城. 流量造假行为刑法规制的合理性判断[J]. 社会科学家, 2022(11): 121-128.

[7] 闻志强, 何嘉昕. 流量劫持的刑法认定研究[J]. 西部法学评论, 2022(5): 55-75.

[8] 贾银生. 流量造假犯罪刑法规制核心问题研究[J]. 当代法学, 2023, 37(2): 88-89.

[9] 叶良芳. 刑法教义学视角下流量劫持行为的性质探究[J]. 中州学刊, 2016(8): 45-49.

[10] 阎二鹏. 干扰型破坏计算机信息系统罪的司法认定[J]. 中国刑事法杂志, 2022(3): 122-137.

[11] 王燕, 石磊. 《张竣杰等非法控制计算机信息系统案》的理解与参照[J]. 人民司法, 2022(14): 23.

[12] 喻海松. 网络犯罪黑灰产业链的样态与规制[J]. 国家检察官学院学报, 2021, 29(1): 41-54.

[13] 张明楷. 论“依照处罚较重的规定定罪处罚” [J]. 法律科学, 2022, 40(2): 59-73.

[14] 姜敏, 冯迎港. 流量劫持行为的刑法定性与治理对策[J]. 南海法学, 2021, 5(3): 11-21.