个罪研究

计算机网络犯罪中的侵入行为及其规制

高仕银 *

摘　要　“侵入”在计算机网络犯罪中特指未经授权或超越授权访问计算机信息系统的行为。计算机网络犯罪中的侵入行为因具体罪名的不同而在体系性地位上呈现三种类型：犯罪成立的决定性要件、犯罪成立的基础性要件、犯罪成立的前提性条件。计算机网络犯罪中的侵入行为的不法本质是避开、突破计算机信息系统安全保护措施或不按既定程式操作，进而实现非法访问目的。由此，应根据程序编码设置的安全限制标准来确立侵入行为的刑事不法性，以使用服务协议和代理人法则建立的契约信任标准来确定侵入行为的民事违法性；应对突破计算机信息系统安全保护措施的侵入行为予以刑事惩罚，将违背既定告知条款要求或背弃约定信任义务的侵入行为纳入民事惩处。实现不同侵入行为类型下计算机网络不法行为的刑民规制，有利于数字经济时代正确厘定和界分计算机网络侵入行为的犯罪化和非犯罪化，实现对计算机信息系统特别是其中的数据的合理保护和有效利用的调衡。

关键词　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　非法控制计算机信息系统罪　破坏计算机信息系统罪　网络爬虫

DOI:10.19430/j.cnki.3891.2024.03.006

此前，河南新郑刘姓老师因不堪他人频繁闯入其网课直播间骚扰，破坏课堂秩序，在家中不幸去世，引发大众关注。刘姓老师的遭遇，被称作“网课爆破”，是指不法分子通过技术性或者其他非正当登录手段侵入教师直播的网络课堂，恶意干扰网上教学秩序，甚至对网课直播系统进行非法操纵或控制，导致线上课堂教学无法正常进行的行为。除“网课爆破”外，在一些网络平台，有不少声称专业“爆破”的博主发布视频称，各大网络会议室、在线办公平台皆可“爆破”。① 无论是“网课爆破”还是对其他在线活动的“爆破”，表面上好像只是耍技术伎俩的“恶作剧”或“捣乱”，但实质上

* 中国社会科学院机关党委副研究员。

本文系研究阐释党的二十大精神国家社会科学基金重大项目“建设中国特色社会主义法治体系的理论基础和实施方案”（项目编号：23ZDA073）的研究成果。

① 参见赵丽：《“网课爆破”污秽不堪涉嫌违法犯罪》，载《法治日报》2022 年 11 月 5 日，第 4 版。

属于类似黑客入侵的不法行为。特别是非法获取计算机信息系统数据、非法控制或破坏计算机信息系统等，都是通过网络侵入计算机信息系统，进而实施相关行为。“侵入”是危害计算机信息系统安全类犯罪的核心概念，但刑法和司法解释都没有明确对其进行界定，学界对其专门探讨也比较少。作为计算机网络犯罪的一个重要行为要件，有必要对“侵入”进行深入分析，明确其内涵，厘清其在计算机网络犯罪中的体系性位置、对不同类型计算机网络犯罪不法行为认定的作用，以利于合理有效地规制计算机网络犯罪。

一、侵入的内涵与行为类型

“侵入”是我国刑事法律用来描述有关犯罪行为的一种术语，在计算机网络犯罪中，主要是指危害计算机信息系统安全的相关不法行为。我国《刑法》关于危害计算机信息系统安全犯罪的主要规定是第285条和第286条。1997年《刑法》在第285条中规定了非法侵入计算机信息系统罪，2009年《刑法修正案（七）》在本条中增设两个条款，包括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和提供侵入、非法控制计算机信息系统程序、工具罪。从《刑法》第285条规定的罪状来看，无论是非法侵入计算机信息系统罪还是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都明确规定了侵入行为，并且都把“侵入”作为构成相应犯罪的重要要件。但是，本条所涉各罪中的侵入行为是否相同不无疑问，理论和实务界也未达成共识，需要从“侵入”一词本身的义涵以及《刑法》各罪关于“侵入”规定的罪状内涵着手并重点结合犯罪的行为特性予以逐一厘清。

（一）线下物理空间的侵入行为

“侵入”一词原本是用于描述在现实生活的物理空间实施的有关行为。根据现代汉语词典的解释，“侵入”是指用武力强行进入境内，或有害的或外来的事物进入内部。[①]可见，“侵入”一词主要用来描述外部的人或物以不当或不友好的方式进入内部，其基本的行为特征是“强行性”“有害性”或“不安全性”，反映了一个由外及内的“闯”的过程，且并不受内部所接受或欢迎，是一种莽撞的进犯或未经允许的进入。纵观我国现行《刑法》条文，目前在罪状表述中使用“侵入”的共有4条规定，分别是第219条、第245条、第285条和第293条之一。其中，第219条规定的是侵犯商业秘密罪，有关“侵入”的表述是该条第2款：“以盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取权利人的商业秘密的”。第245条是关于非法侵入住宅罪的规定，对“侵入”的表述非常简洁明了。第293条之一是关于催收非法债务罪的规定，其中“侵入”的表述是该条第3款：“限制他人人身自由或者侵入他人住宅的”。

从立法沿革上看，上述关于“侵入”规定的4个条文中，非法侵入住宅罪最早使用

① 参见中国社会科学院语言研究所词典编辑室编：《现代汉语词典》（第7版），商务印书馆2016年版，第1057页。

了“侵入”一词。1979 年《刑法》在第 144 条中专门就非法侵入住宅罪作出了明确规定，后来在 1997 年《刑法》修订时，非法侵入住宅罪主要内容都得以保留并被规定在现行《刑法》第 245 条。《刑法》第 219 条规定的侵犯商业秘密罪虽然在 1997 年《刑法》中就有设立，但其第 2 款关于“侵入”的规定是 2020 年《刑法修正案（十一）》所增设。《刑法》第 285 条有关计算机网络犯罪的几个罪名分别是在 1997 年《刑法》和 2009 年《刑法修正案（七）》中所新设。《刑法》第 293 条之一第 3 款也是在 2020 年《刑法修正案（十一）》中所增设，该款中关于“侵入”的规定其实与非法侵入住宅罪在行为本质上基本无异。因此，按照立法生成的时间顺序，“侵入”一词在刑法规定中最开始也主要是用来表述传统的在现实社会中发生的犯罪行为即非法侵入他人住宅。

非法侵入住宅罪中的“侵入”，无论是从文义上理解还是从法条规定的目的来解释，都是指对他人生活起居的场所或处所的侵犯，是行为人自身闯入到他人居所中，存在物理意义上的身体位移。这在社会一般大众中都能取得比较一致的认识，也符合自然法则的常识判断。因为现实社会中，人们对于自己的住宅、居所等属于私人的相对封闭的空间与场所都具有明确的权利与权限意识，会明示或告知他人是否可以进入或者继续停留在自己的居所等类似地方。相应地，一般的社会人也都知道或者懂得“闲人免进”或不得“擅闯私宅”是一项基本的社会交往规则，应当予以严格遵守。非法侵入的规定总体上是处罚那些明知是他人住所或场地而无故进入或进入后拒不退出的行为，尽管其知道权利人禁止其作出如此行为。① 比如，房屋所有人在住宅外的围栏上挂着“禁止进入”的标识，正常人非因法定事由置若罔闻闯而进之，则构成非法侵入。

在普通法上，任何未经许可的进入他人土地或非法停留在其房屋或建筑物的行为就是“侵入”，但单纯的侵入行为并不是刑事犯罪，可通过民事救济予以解决，除非侵入之后实施了侵害或意图侵害房屋安宁的行为。② 之后，刑法将非法侵入住宅的行为规定为犯罪，且只要证明侵入是非法的，即房屋的所有者或代理人对被告人进入或不退出的行为明确表示禁止，犯罪就成立。③ 正因为如此，在关于非法侵入住宅罪的理解和适用上，一般都认为符合该罪构成要件“侵入”的核心要求是行为人没有获得权利人的同意、许可而故意进入，或者在有权进入后被要求离开时没有其他正当性理由而继续停留。因此，从非法侵入住宅罪的层面来理解，“侵入”就是没有正当理由的强行进入或无理由的拒不退出。

（二）线上网络空间的侵入行为

在计算机问世后，特别是因特网的出现，由计算机和互联网组成的网络虚拟社会逐渐成为人们活动的“第二空间”。人们的行为在网络空间也发展变化成两大类。一是传统行为的网络化，即把计算机网络作为实现传统生活便捷化的一种新兴工具，主要是借

① See Model Penal Code § 221.2 (1962).

② See People v.Gudoto, 174 N.E.2d 385 (1961).

③ See Wayne R.LaFave, Criminal Law, 4th ed., West, a Thomson Business, 2003, p.1031.

助计算机网络实施现实空间本有的行为，如网上购物等。[①] 二是在网络中形成新的行为，这些行为在原本的传统社会中并不存在，只是因应计算机网络的出现而产生，如对网络大数据信息的访问、收集、获取或前述“网课爆破”等各种危害计算信息系统有关犯罪。随着网络空间的形成，该空间必然需要一定的秩序，在形成网络秩序的同时，就会出现扰乱网络秩序的犯罪，这些犯罪形态是超出传统犯罪范围的，因而在网络空间就出现了传统犯罪与新型犯罪的掺杂，使发生在互联网中的犯罪类型更为纷繁复杂。信息技术快速发展带来的行为模式变化，特别是网络空间中的新行为样态倒逼刑法不得不适时调整其规定，特别是在罪状的表述上，赋予传统词汇在新行为样态下新的内涵，以求更精确地认定犯罪和更合理地组织起对这类犯罪行为的应对，“侵入”一词的使用就是一个典型。

“侵入”这一原本用于描述传统犯罪的用语因计算机网络犯罪的规制需要而被再次使用在刑法条文中，具体通过《刑法》第285条的规定展现出来。同一用语在不同类别的规定中使用，虽然规制的范围不同，但其行为构成具有一定的参照可比性。正如学者所言，如果与传统的犯罪行为方式进行对比，我们可以发现，非法侵入计算机信息系统罪和人身犯罪中的侵入住宅罪具有一定的可比性，非法获取计算机信息系统数据罪和财产犯罪中的盗窃罪具有一定的可比性，非法控制计算机信息系统罪和人身犯罪中的绑架罪具有一定的可比性。[②] 从行为方式和类型上看，将计算机网络犯罪中的“侵入”和传统犯罪中的“侵入”进行对比理解，具有积极意义。因为将“侵入”这一计算机网络犯罪构成中的具体行为要件纳入法条的整体规定中进行比较分析，有利于更好发现其中的差异。法律条文只有当他处于与它有关的所有条文的整体之中才显出真正的含义，或它所出现的项目会明确该条文的真正含义；有时把它与其他的条文——同一法令或同一法典的其他条款——一比较，其含义也就明确了。[③] 因此，从法条规定的整体性来看，“侵入”这一原本用于传统犯罪的词语所表征的行为在网络空间是否被赋予了新的意义，须通过与行为构成相似的传统犯罪进行体系性、通盘式的对比，才能更准确清晰地厘定其在计算机网络犯罪中的具体内涵。

从解释论而言，对于不同条文中相同用语的解释，需要用体系解释的方法根据关联条文阐明刑法规范的真实含义，做到解释结论与整个刑法特别是相关条文保持协调，避免前后左右矛盾。但是，体系解释并不等于对同一用语作出完全统一的解释。[④] 这是因为，虽然法律条文使用的词语是相同的，但是如果该用语所指称的行为方式、发生场域和危害后果等方面有了新的变化，特别是所侵犯的法益内容有了根本性的变化，解释时

① 当然，还存在把计算机网络作为犯罪工具而利用计算机网络实施传统犯罪的情况，如网络诈骗、网络盗窃等。对此，《刑法》第287条规定：“利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照有关规定定罪处罚。”

② 参见陈兴良：《网络犯罪的刑法应对》，载《中国法律评论》2020年第1期，第91页。

③ 参见［法］亨利·莱维·布律尔：《法律社会学》，许钧译，上海人民出版社1987年版，第70页。

④ 参见张明楷：《刑法分则的解释原理》（第2版），中国人民大学出版社2011年版，第326页。

既要看其统一性，更要注意其差异性、特殊性和合理性，在避免前后左右矛盾的同时，更要杜绝解释结论不合法条逻辑和立法本意要求。同样都是“侵入”一词，《刑法》第 285 条中规定的“侵入”和《刑法》第 245 条中规定的“侵入”就不能作完全统一或相同的解释。因为《刑法》第 245 条规定中的“侵入”是针对现实物理空间而言的，其核心要求是行为人进入到他人的房屋等场所才符合本罪的构成要件；而《刑法》第 285 条规定中的“侵入”是针对网络虚拟空间而言的，行为人自身并没有也不可能闯入到他人的计算机信息系统或网络空间中。现实空间的行为和虚拟空间的行为虽然在相同用语上具有相对的可比性，但行为的具体实施方式并不存在绝对的同一性。总之，计算机网络环境下行为样态具有新颖性和特殊性，需要根据不同场合作出不同解释。对于《刑法》第 285 条规定中的“侵入”，在与传统犯罪对比得出差异性结论的基础上，其基本内涵需要结合法条规定和计算机网络犯罪的具体行为特征才能进一步明确。

如上所述，《刑法》第 285 条中规定“侵入”行为的罪名是非法侵入计算机信息系统罪和非法获取计算机信息系统数据罪、非法控制计算机信息系统罪。① 非法侵入计算机信息系统罪和非法获取计算机信息系统数据罪、非法控制计算机信息系统罪的根本区别在于，前罪与后两罪的犯罪对象不同。非法侵入计算机信息系统罪的犯罪对象是国家事务、国防领域、尖端科学技术领域的计算机信息系统，非法获取计算机信息系统数据罪、非法控制计算机信息系统罪的犯罪对象是国家事务、国防领域、尖端科学技术领域以外的计算机信息系统。因此，从法条规定的内容来看，这三个犯罪仅仅在犯罪侵害的对象范围上有所差异。需要指出的是，非法获取计算机信息系统数据罪、非法控制计算机信息系统罪是在同一款规定中的选择性罪名，其关于侵入行为的构成要件在规范要求上都相同，从计算机网络技术层面来看，都是非法的网络访问行为。至于这三个罪名是否因为犯罪对象的不同而将所涉的“侵入”作出不同的解释，仍然需要深入分析。

关于非法侵入计算机信息系统罪中的“侵入”，有学者认为是“未取得有关部门的合法授权与批准，通过计算机终端访问国家事务、国防建设、尖端科学技术领域的计算机信息系统或者进行数据截收的行为”。② 也有观点认为，非法侵入计算机信息系统罪中的“侵入”是指无权或者超越权限进入国家事务、国防建设、尖端科学技术领域计算机信息系统的情形；就规范意义而言，行为人非法获悉了他人的用户名和密码，直接进入计算机信息系统，亦属于无权进入，构成“侵入”；非法获取计算机信息系统数据罪、非法控制计算机信息系统罪中的“侵入”，是指未经授权或者超越授权，获得删除、增加、修改或者获取计算机信息系统储存、处理或者传输的数据的权限。③ 从司法实践上看，司法机关在卫某、龚某、薛某非法获取计算机信息系统数据案中将“侵入”界定为

① 《刑法》第 286 条规定的破坏计算机信息系统罪没有明文规定侵入行为，但这是一种毁坏型的计算机网络犯罪，主要是针对计算机信息系统的功能。这种毁坏行为是否需要以侵入计算机信息系统为前提，下文将进一步展开分析讨论。

② 张明楷：《刑法学（下）》（第 6 版），法律出版社 2021 年版，第 1372 页。

③ 参见喻海松：《网络犯罪二十讲》（第 2 版），法律出版社 2022 年版，第 38、44 页。

违背被害人意愿，非法进入计算机信息系统的行为，其表现形式既包括采用技术手段破坏系统防护进入计算机信息系统，也包括未取得被害人授权擅自进入计算机信息系统，还包括超出被害人授权范围进入计算机信息系统。①

值得注意的是，有观点认为，非法获取计算机信息系统数据罪中的“侵入”是指行为人在没有权限、没有获得访问许可的情况下，违背计算机信息系统控制人的意愿，进入到无权访问的除国家事务、国防建设和尖端科学技术领域之外的计算机信息系统中，常见的方式是利用他人网上认证信息进入计算机信息系统，或在系统中植入木马、后门程序，获取存储、处理或传输的信息数据。② 将本罪中的“侵入”解释为包括“获取存储、处理或传输的信息数据”似有不妥。这是因为，侵入行为和获取数据或非法控制行为在《刑法》第 285 条规定中是两个不同的行为，侵入在先，获取或非法控制在后。“在侵入计算机信息系统以后又获取计算机信息系统数据的情况下，由于这里侵入的计算机信息系统并非国家事务、国防建设、尖端科学技术领域的计算机信息系统，并不构成独立的罪名。”③ 在非法获取计算机信息系统数据罪、非法控制计算机信息系统罪中，单纯的侵入行为在现行规定下不具有刑事非难性，如果将“侵入”扩大解释到包括后续的获取数据或非法控制行为，既与法条规定的文义不符，也可能会导致犯罪认定不适当。

综上所述，从体系解释出发，结合刑法规定的整体性和合目的性要求，我们可以将计算机网络犯罪中的“侵入”理解为使用计算机信息系统或具有类似功能的设备非法访问他人计算机信息系统的行为，这里的非法访问是指没有获得权利人许可、同意（即未经授权），或虽获得访问的许可、同意，但超出了许可、同意的范围（即超越授权）。对于《刑法》第 285 条前两款规定的三个罪名而言，不能因为第一款和第二款规定的犯罪对象不同而将本条中行为构成、发生场域、侵害法益类型相同的侵入行为在内涵上作不同的解释。

二、侵入行为的体系性定位

《刑法》第 285 条明确规定了侵入行为，但第 286 条规定的破坏计算机信息系统罪在罪状中没有侵入行为的明文表述。对此，不能简单地从字面上判断破坏计算机信息系统罪不存在侵入行为，需要结合法条规定具体分析把握。从行为要件上看，非法侵入计算机信息系统罪的“侵入”是决定性构成要件，决定犯罪的成立与否。非法侵入计算机信息系统罪是行为犯，只要有非法侵入行为，即具备本罪的行为要件，一旦侵入即构成既遂。④ 在非法获取计算机信息系统数据罪、非法控制计算机信息系统罪中，侵入是基

① 卫某等非法获取计算机信息系统数据案（检例第 36 号），最高人民检察院第九批指导性案例（2017 年）。

② 参见江溯主编：《网络刑法原理》，北京大学出版社 2022 年版，第 136 页。

③ 陈兴良：《网络犯罪的类型及其司法认定》，载《法治研究》2021 年第 3 期，第 4 页。

④ 参见江溯主编：《网络刑法原理》，北京大学出版社 2022 年版，第 132、139 页。

础性行为要件，须同时与非法获取行为或非法控制行为相结合才能成立相应犯罪。换言之，非法获取计算机信息系统数据或非法控制计算机信息系统均须以侵入为基础。① 下文结合具体规定，对侵入行为在《刑法》第 285 条各罪中作为犯罪成立的决定性要件、基础性要件和侵入行为在《刑法》第 286 条中的存在性及体系性地位予以逐一分析厘清。

（一）对犯罪成立具有决定性地位的侵入行为

《刑法》第 285 条第 1 款规定的非法侵入计算机信息系统罪中，侵入行为是单一行为，其本身对犯罪成立起着至关重要的作用。在本罪中，侵入行为不从属于任何一个犯罪行为，而是一个独立的行为要件，行为人一旦实施，犯罪即成立。正如学者所言，“行为人只要在客观上实施了侵入国家事务、国防建设、尖端科学技术领域计算机信息系统的行为，无论是否进一步实施其他行为，均可以构成本罪”。② 单一的侵入行为之所以能直接决定犯罪的成立，是由于犯罪对象的特殊性。立法作出如此规定是一种特别明示，即“动手（侵入）就是犯罪”，表明国家刑罚权对专门领域计算机信息系统的格外重视。换言之，国家将这类计算机信息系统的安全置于最重要的位置，一旦安全受到威胁就科以刑事惩戒，这是对特殊法益的特殊保护。需要进一步考察的是，虽然“侵入”在本罪中具有决定犯罪成立的唯一性，但如果侵入国家事务、国防建设、尖端科学技术领域计算机信息系统后，又实施了后续的其他行为，如非法获取其中的数据、控制或破坏计算机信息系统等，如何定罪处罚？

《刑法》第 285 条第 1 款只规定了侵入行为，没有对获取数据、控制或破坏等行为予以进一步规定。而《刑法》第 285 条第 2 款和第 286 条虽然规定了获取数据、控制或破坏行为，但其规定的犯罪对象（即计算机信息系统）并不相同，刑罚幅度也有较大差异。如果实施第 285 条第 1 款规定的侵入行为，又实施了第 285 条第 2 款或第 286 条规定的行为，似乎还是只能依据第 285 条第 1 款来惩处，立法出现了保护不周延之嫌。有学者甚至指出，“第 285 条第 1 款确认了国家事务、国防建设、尖端科学技术领域计算机信息系统及其中的数据是受法律重点保护的计算机信息系统，理应得到更全面的法律保护，《刑法》第 285 条第 2 款的立法逻辑与第 1 款相悖”。③ 对于这一问题，有观点从解释论上提出，《刑法》第 285 条第 2 款中的“前款规定以外”并不是真正的构成要件要素，只是表面要素或界限要素：行为人侵入国家事务、国防建设、尖端科学技术领域计算机信息系统，获取该计算机信息系统中储存、处理或传输的数据，或者对该计算机信息系统实施非法控制，情节特别严重的，应认定为非法获取计算机信息系统数据罪、非法控制计算机信息系统罪。④ 也有学者认为，刑法如此规定不仅有悖于对计算机信息

① 当然，《刑法》还规定了“采用其他技术手段”非法获取计算机信息系统数据或非法控制计算机信息系统，但并不排斥侵入行为是构成犯罪的基础性要件。

② 陈兴良：《网络犯罪的类型及司法认定》，载《法治研究》2021 年第 3 期，第 4 页。

③ 皮勇：《我国新网络犯罪立法若干问题》，载《中国刑事法杂志》2012 年第 12 期，第 45 页。

④ 参见张明楷：《刑法学（下）》（第 6 版），法律出版社 2021 年版，第 1372 页。

系统安全的分类分级保护的要旨，而且还明显违背罪责刑相适应原则；在刑法解释无法解决条文之间不协调与处罚不均衡的问题时，有必要适时在立法层面对相关法条进行调整，将侵入计算机系统或采用其他技术手段，非法获取重要领域计算机信息系统数据或控制计算机信息系统的行为分别作为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罪的加重情形，并设置相较现行《刑法》第285条第2款更严厉的法定刑，以实现对计算机系统安全的分类分级保护。① 还有观点认为，《刑法》第285条第1款在立法上应当属于保留条款，即备用条款，不应当大范围地适用；案件能够靠上其他罪名的，就不应当适用非法侵入计算机信息系统罪。② 可以说，上述观点对侵入行为在《刑法》第285条第1款中作为决定犯罪成立的要件上并无认识分歧，只是对侵入后又实施其他行为如何定性处理有不同看法。质言之，这关涉定罪和处罚两个层面关系如何协调的问题。

从非法侵入计算机信息系统罪的构成要件来看，侵入行为在认定犯罪的成立与否上具有决定性作用，实质上充分体现了立法的价值取向。把本罪中的侵入行为作为认定犯罪成立的唯一行为要件，处于独一无二的位置上，就是明示任何未经授权或超越授权访问国家事务、国防建设、尖端科学技术领域计算机信息系统的行为都是禁止的。当然，从司法实践中处理的案件来看，很少出现只是单纯侵入上述三大领域计算机信息系统而不进一步实施其他危害行为的犯罪。③ 上述通过立法修改完善刑法规定的主张固然是最佳解决方案，但现实并非立即可行；认为“前款规定以外”只是表面的构成要件要素，不是成立犯罪必须具备的要素，从而直接打通第285条第1款和第2款在行为多重性下的叠加适用，以图求得“罚当其罪”的观点，可能会因为解释过渡实质化而将刑法明文规定的区分此罪与彼罪的重要行为要件忽略，特别是立法明确表达的对特殊领域计算机信息系统予以单独区别对待和特殊保护的目的模糊化，不利于正确全面认识和合理惩治这类犯罪。同样，认为不应当大范围适用第285条第1款，而主张案件只要能够靠上其他罪名就用其他罪名的看法也有“稀释”法条规定甚至不遵守罪刑法定原则之嫌。如果在侵入国家事务、国防建设、尖端科学技术领域计算机信息系统后，行为人又进一步实施了其他犯罪行为的，可以按照牵连犯的理论思路来予以规制，即按照侵入后所实施的犯罪以从一重处的原则来处罚。

（二）对犯罪成立具有基础性作用的侵入行为

《刑法》第285条第2款规定的两种犯罪都将侵入计算机信息系统作为手段行为，再将非法获取计算机信息系统数据或非法控制计算机信息系统作为目的行为。这表明侵

① 参见刘宪权：《“互联网3.0”时代计算机系统犯罪刑法规制的重构》，载《华东政法大学学报》2022年第5期，第78页。

② 参见喻海松：《网络犯罪二十讲》（第2版），法律出版社2022年版，第42页。

③ 当然，也存在只是侵入国家事务、国防建设、尖端科学技术领域计算机信息系统，并没有意图进一步实施非法获取数据、控制或破坏计算机信息系统的情况，或是以非法获取数据、控制或破坏计算机信息系统为目的，侵入上述特殊领域计算机信息系统，但由于意志以外的原因未能实施目的行为的情况。这些情况都以非法侵入计算机信息系统罪论处。

入计算机信息系统是非法获取或非法控制的基础要件，是一种必需的先行行为。如果没有这个先行行为，即使非法获取到计算机信息系统数据或非法控制了计算机信息系统，也很难成立本条规定之罪。因此，本款规定的犯罪都有前后两个相互接续的行为，属于复行为犯。如果用简短的结构示意形式来描述本款之罪的行为构成，可表示为“侵入—获取”或“侵入—控制”，这两对行为模式在构成相应的犯罪上缺一不可，并且都是以“侵入”为基础的“彼此成就”。

总之，没有作为基础性要件的侵入行为，也就难以成立《刑法》第 285 条第 2 款规定之罪；同样，即使有侵入行为，如果没有后续的非法获取或非法控制行为，《刑法》第 285 条第 2 款规定之罪也不能完全成立。当然，如果行为人为了非法获取计算机信息系统数据或非法控制计算机信息系统，在侵入非属于国家事务、国防建设、尖端科学技术领域的计算机信息系统后，由于意志以外的因素未能实施后续非法获取或非法控制行为的，则属于犯罪的未遂，完全不影响侵入行为作为犯罪成立基础性要件的评价。

（三）作为犯罪成立前提性条件的侵入行为

《刑法》第 286 条规定的破坏计算机信息系统罪是一种毁坏型的犯罪，虽然其与故意毁坏财物罪具有一定的可比性，但两者之间又存在重大差异。刑法没有将破坏计算机信息系统的行为直接纳入故意毁坏财物罪中予以规制，而是单独成罪，主要原因在于这里的破坏行为不是从外部对计算机信息系统设备硬件进行物理性损坏，而是对计算机信息系统内部的功能与内容（包括软件、数据等）进行影响和破坏。这从刑法关于该罪的罪状表述“造成计算机信息系统不能正常运行”可以得出肯定性结论。详言之，破坏计算机信息系统行为是非法对计算机信息系统功能进行删除、修改、增加、干扰，或非法对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，亦或故意制作、传播计算机病毒等破坏性程序，影响或导致计算机信息系统不能正常运行。因此，破坏计算机信息系统罪与故意毁坏财物罪的主要区别在于前者的破坏是导致计算机信息系统不能正常运行，后者的毁坏“既包括从物理上变更或者消灭财物的形体，也包括通过对财物施加有形力或者影响力，使财物的效用丧失或者减少的一切行为”，① 即导致财物既有的物理功能丧失或经济上的价值减损。

由于第 286 条并没有像第 285 条那样在罪状表述上明确规定侵入行为，在行为要件的要求上，破坏计算机信息系统罪是直接实施所规定的破坏行为即可，还是须以侵入为前提？特别是在以干扰方式破坏计算机信息系统的情况下，是否需要侵入行为？对此，存在两种截然不同的看法。肯定的观点认为，破坏计算机信息系统罪是一种毁坏型的网络犯罪，因其毁坏对象并非计算机的物理设备而是计算机的信息系统，所以这种毁坏行为必然以侵入计算机信息系统为前提，对计算机信息系统的程序进行删除等，由此导致计算机信息系统丧失其功能。② 否定论者认为，侵入计算机信息系统并非影响计算机信

① 张明楷：《刑法学（下）》（第 6 版），法律出版社 2021 年版，第 1342 页。

② 参见陈兴良：《网络犯罪的类型及司法认定》，载《法治研究》2021 年第 3 期，第 8 页。

息系统功能的前提条件，两者之间并不具备唯一性关系；即使侵入计算机信息系统内部也并不意味着一定会造成计算机信息系统功能不能正常运行之结果，如非法侵入计算机信息系统后获取一般数据的行为，充其量对数据安全造成影响，但不会影响计算机信息系统本身的运行状态。①

如前所述，破坏计算机信息系统罪与故意毁坏财物罪的重要区别，在于前者是对计算机信息系统内部功能产生影响，其直接结果是导致计算机信息系统不能正常运行。“破坏计算机信息系统功能的行为，是指行为人在不法侵入计算机信息系统内部后，再对系统的功能本身进行破坏，从而使得计算机信息系统不能运行或者不能按原先的设计要求运行。”② 在破坏计算机信息系统犯罪中，特别是以干扰方式构成破坏计算机信息系统罪的情况下，如果不需要侵入行为就可以直接构成犯罪，不但会导致犯罪认定结论的不适当，③ 也会使得破坏计算机信息系统罪与毁坏财物罪的区别进一步模糊化，恐怕与立法本意不符，还可能导致对此类犯罪认定的不当扩大。非通过技术侵入手段，在计算机信息系统之外实施的物理性干扰行为，如果没有导致计算机信息系统本身不能正常运行或没有导致计算机信息系统不按预设的既定程式运行，则不能简单认为构成破坏计算机信息系统罪，否则其不符合一般社会大众的认识判断和预期要求。

例如，在现代医疗健康检查中，检测仪器如 CT、X 光、核磁共振等一般都是通过计算机信息系统来综合控制的，如果行为人没有通过技术手段侵入控制检测仪器的计算机信息系统并修改有关运行参数、软件程序，或没有通过技术手段干扰计算机信息系统正常运行，而是简单通过使用特殊金属或其他材料遮挡检测仪器前端的方式，使得被检测者与检测仪器不能充分接触，从而导致体检数据不正常或检查结果出不来，无论如何也不能认为构成破坏计算机信息系统罪。《刑法》第 286 条第 1 款中的“删除、修改、增加、干扰”行为，应当直接针对计算机信息系统的软件功能发生作用，而非间接影响计

① 参见阎二鹏：《干扰型破坏计算机信息系统罪的司法认定》，载《中国刑事法杂志》2022 年第 3 期，第 130、131 页。

② 周光权：《刑法软性解释的限制与增设妨碍业务罪》，载《中外法学》2019 年第 4 期，第 958 页。

③ 典型案例如李某、何某民、张某勃等人破坏计算机信息系统案。该案中，被告人李某、张某勃多次用棉纱堵塞采样器的方法，干扰环境空气质量自动监测系统的数据采集功能，造成环境空气自动监测站的监测数据多次出现异常，多个时间段内监测数据严重失真。法院裁判认为，被告人用棉纱堵塞采样器的采样孔，造成采样器内部气流场改变，造成监测数据失真，影响对环境空气质量的正确评估，属于对计算机信息系统功能进行干扰，构成破坏计算机信息系统罪。参见李某等破坏计算机信息系统案，最高人民法院指导性案例 104 号（2018 年）。本案中，李某等人通过在计算机信息系统的物理设备外部，用棉纱隔断自然空气在采样器的流通，使得计算机信息系统监测到的空气污染数值失真，但计算机信息系统本身的正常运行功能没有受到任何影响，系统的数据处理功能也没有遭到破坏。如果该案中的手段行为不是用棉纱堵塞采样器，而是行为人在采样器周围甚至整个计算机信息系统设备外围修建一个可以隔绝环境自然空气流动的“玻璃罩”，同样会导致空气监测数值失真，这种情况下能否认为构成破坏计算机信息系统罪？答案应该是非常明确的，肯定不能认定为构成本罪。

算机信息系统的数据处理结果即可构成。破坏计算机信息系统罪乃是网络空间针对计算机信息系统的毁弃型犯罪，如不严格把握破坏行为的“直接性”要求，势必会导致本罪适用范围不当扩张；如果认为以任何方式影响计算机信息系统最终输出数据的行为都符合构成要件，无疑会使本罪偏离毁弃型犯罪的本质，从而削弱罪刑法定这一基本原则。① 纵观《刑法》第 285 条和第 286 条的规定，从犯罪对象、行为要件和保护法益的设定而言，无论是体系解释还是目的解释，都应把侵入行为作为这两条规定所列犯罪的重要构成要件，这也是危害计算机信息系统犯罪区别于其他犯罪的重要体现。因此，破坏计算机信息系统是以侵入为前提的破坏，计算机信息系统不能正常运行，是侵入之后的不能正常运行。

三、侵入行为的判断与规制

（一）侵入行为的判断考察

前述学理观点和有关司法指导性案例的定义，对于计算机网络犯罪中的侵入行为都强调一个关键的问题，即对计算机信息系统的登录访问是否有权限，或是否取得他人的许可或同意。如果行为人访问计算机信息系统的行为没有得到授权、同意或虽有授权但超出授权范围的，就属于侵入。“侵入的本质特征是未经授权或超越授权。”② 我国《刑法》在计算机网络犯罪的相关规定中，虽然有侵入行为的表述，但并未对何为侵入行为作进一步的说明，立法上更没有关于“未经授权”“超越授权”的相关规定。只有《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》（法释〔2011〕19 号）（以下简称《解释》）第 2 条对《刑法》第 285 条第 3 款进行解释时，专门使用了“未经授权”与“超越授权”的表述。虽然这里的“未经授权”与“超越授权”并非直接针对《刑法》第 285 条第 1 款和第 2 款规定中的侵入行为所作的进一步解释，但是结合解释的语境和解释的内容可以认为是司法机关对侵入行为本质特征的描摹。《解释》第 11 条专门就《刑法》规定中涉及的几个专门术语，如“计算机信息系统”“计算机系统”“身份认证信息”“经济损失”的具体内涵进行了说明，但是对“未经授权”和“超越授权”这两个在《解释》中使用的、用来表征侵入行为重要特性的新词，既没有说明其使用理由，也没有对其内涵作出具体定义，使得《解释》存在一定的缺憾，依然未能给司法机关在认定侵入行为上作出明确的指引。因此，只有进一步厘清“未经授权”和“超越授权”，才能更好地对侵入行为作出准确判断。

立法和司法解释对侵入行为及表征其重要本质特征的“未经授权”与“超越授权”均未作出明确说明，可能是因为在信息社会背景下，计算机网络技术的发展变化和升级

① 参见王华伟：《破坏计算机信息系统罪的教义学反思与重构》，载《东南大学学报（哲学社会科学版）》2021 年第 6 期，第 96、97 页。

② 喻海松：《网络犯罪二十讲》（第 2 版），法律出版社 2022 年版，第 44 页。

更新比较快，社会认识赶不上时代变化的情形凸显，立法和司法解释以稳慎的态度作了善意保留，采取了“技术性”回避，不以当时的认知经验和相对不太成熟的结论来作统一的、较为僵硬的规定或定义，而是将这个问题作为“开放式要件”，留给司法实践部门在发展中去认识并在发展中予以解决，通过结合实际的案件情况特别是新兴技术样态来作出具体的认识判断。因为在司法运行中，案件的素材是非常丰富的，遇到的情况也是极为鲜活的，刑事法官可以根据不同个案中表现出来的情况并结合相同类型的前在生效判决，不断对“未经授权”和“超越授权”的内涵进行归纳、提炼和总结，在前人判解结论的基础上形成新的裁判结论，作出符合当下案件情况的恰当定义，通过司法实践的经验积累，最终形成司法实践部门认识比较一致的判断标准。然而，在司法实践层面，最高司法机关没有发布专门的指导性案例作为参考，地方各级司法机关在判决中也没有就此展开深入论证分析。从已有的相关刑事生效判决来看，司法人员对这两个用语的说理阐释程度并不理想。① 我国立法和司法在“未经授权”和“超越授权”判断标准上付之阙如，有必要从域外相似规定和司法实践中探寻恰当做法，以助力对我国《刑法》规定中的侵入行为进行有效合理的判断。

从时间维度上看，关于计算机网络犯罪的相关立法，美国最早也相对较为成熟。② 同时，美国在计算机网络犯罪立法中对“未经授权”与“超越授权”作出了明文规定，并且还在司法判例中形成了不同的判断标准。立法上，美国联邦《计算机欺诈与滥用法》（Computer Fraud and Abuse Act）是联邦规制计算机网络犯罪的主要法律。根据其规定，“未经授权”或“超越授权”访问计算机信息系统，是构成计算机网络犯罪的基础性行为之一。③ 这里的“未经授权”或“超越授权”访问相当于我国刑法规定中的侵入行为。美国立法在明文规定“未经授权”和“超越授权”的同时，还对“超越授权”的内涵进行了专门界定：在获得计算机网络一定访问权限的情况下，修改或获取计算机网络中的数据信息，但这种修改或获取数据信息的行为并没有得到权利人的授权。④ 对于“未经授权”，美国联邦立法没有像“超越授权”那样作出具体的定义，而是将这一任务交给了联邦司法部门来完成。联邦司法部门通过多年实践探索，对“授权”与否的具体判断形成了丰富的经验法则，发展出了相对较为成熟的判定体系。综合来看，主要

① 参见高仕银：《计算机网络犯罪规制中的“未经授权”与“超越授权”——中美比较研究》，载《时代法学》2020 年第 1 期，第 103-106 页。

② 在大陆法系主要国家中，德国 1986 年制定了关于计算机犯罪的刑法，日本在 1987 年修改刑法典和 1999 年制定的《未经授权访问计算机法》中规定了计算机犯罪条款，意大利于 1992 年颁布了关于计算机犯罪的专门立法。在英美法系主要国家中，美国于 1984 年颁布了规制计算机犯罪的相关法案，英国在 1990 年出台了计算机滥用法，澳大利亚于 1989 年制定了专门保护计算机及其数据的刑事法律。参见高仕银：《计算机犯罪规制中美比较研究》，中国社会科学出版社 2021 年版，第 6-10 页。

③ 美国法规定了 7 种“未经授权”或“超越授权”访问计算机信息系统行为。See 18 U.S.C § 1030（a）（1）-（a）（6）（2008）.

④ See 18 U.S.C § 1030（e）（6）（2008）.

有三类：根据程序编码设定的权限作出判断（程序编码标准），根据使用服务协议条款约定的权限作出判断（使用服务协议标准）和以代理人法规定的权限作出判断（代理人法则标准）。①

在对计算机信息系统访问的权限设定上，计算机权利人根据系统的安全性要求和与计算机用户之间的关系，分别以设置访问计算机信息系统的程序编码、制定访问网站的服务协议条款对开放的计算机用户或按照代理人法则的规定对处于雇佣关系的员工赋予不同级别或层次的访问权限。计算机用户（包括处于雇佣关系的员工）如果不按照计算机权利人设定或约定的方式访问计算机信息系统，就会触发访问行为是否授权或超越授权的问题，即是否存在侵入的问题，进而会引发司法机关的问责。实践中，美国联邦司法部门紧密结合计算机信息技术特征，一方面考虑计算机权利人合理利益的保护，另一方面注意对计算机用户正当权利的保障，在对这两者考量的基础上依照立法规定并结合判例结论，对计算机访问行为的违法性判断因计算机权利人设定的访问路径有别，而实行不同的认定进路，并采取不同的惩戒措施。② 美国关于计算机访问授权与否的上述三种判断标准，对于我们认定我国法律规定中的侵入行为具有一定的启示意义。鉴于计算机网络的国际性特征，立法（和司法）上的同步与同态有利于我们加强国际合作以及建立平等的对话基础，更有利于全面彻底地遏制计算机网络犯罪。下文以侵入行为中所涉问题最多的非法获取计算机信息系统数据为核心，采用民刑结合的规制思路，从我国实际出发并在我国法律语境下分别从程序编码标准、使用服务协议标准和代理人法则标准来判断，以期更有利于实现对计算机信息系统特别是其中数据信息合理保护和有效利用的调衡。

（二）侵入行为的规制进路

计算机的交互性和互联网的开放性特征，决定了现代刑法不可能把用于现实社会的传统规制模式，简单套用到对计算机网络虚拟空间的行为范式中。事实上，大多数情况下是计算机网络发生的新行为样态倒逼刑法规制方式作出调整，并且让现代刑法在技术的发展中不断革新条文内容，延展规制范围。一般而言，计算机网络犯罪规制最核心的问题，是如何实现用户上网自由、计算机信息系统及数据安全、个人隐私保护等方面的有效平衡。严厉的规制可以有效保护数据安全与个人隐私，但若用之过度或规制方式走

① 参见高仕银：《计算机网络犯罪规制中的“未经授权”与“超越授权”——中美比较研究》，载《时代法学》2020 年第 1 期，第 100-102 页。需要指出的是，当下在国内也有学者将美国的标准归纳为四种，除了上述三种相关标准外，还结合美国晚近以来的司法判例总结出了第四种，即“违反数据网站撤销机制的判断标准”或“撤销范式”（参见杨志琼：《美国数据犯罪的刑法规制：争议及启示》，载《中国人民大学学报》2021 年第 6 期，第 160 页）。但是，本文认为，这种标准或范式的本质依然是网站的所有者或权利人通过“二次声明”的方式与访问行为人达成的合同或新的使用服务协议条款，只不过内涵更为明确具体，因此仍应当视为“使用服务协议标准”，其只不过是这一标准的加强版或升级版。

② 关于具体的认定和惩戒方式，参见高仕银：《计算机犯罪规制中美比较研究》，中国社会科学出版社 2021 年版，第 237-268 页。

偏，则会影响个人上网自由，更阻碍信息产业发展，特别是影响网络数据资源的有效流通，与大数据时代的开放性和共享性精神相悖。正因如此，侵入行为的规制既要注重对计算机信息系统特别是其中的数据安全予以全面有效的保护，也要兼顾计算机信息系统中的数据资源能够让合法的计算机用户得到恰当充分的利用。从计算机网络及其数据保护与利用的基点出发，对不同的侵入行为应结合具体情形作出判断，分别通过民事惩处和刑事惩罚的方式对其进行规制，进而保障计算机网络空间针对以数据为核心要素的各类行为良性有序开展。

1. 民事惩处：范围及方式

违反网站使用服务协议的侵入行为，实质是“超越授权”的侵入，应纳入民事案件范畴来处理。日常生活中，无论是工作、学习还是生活，普通的计算机网络用户在登录网站浏览网页、搜索资料、下载有关数据资源或开展线上交易等活动时，经常会碰到登录界面显示的对话框，提示使用者认真阅读网站设定的格式性服务条款，主要内容一般都是告知访问权限、行为规范、责任和义务等。使用者都会被要求阅读完这些条款，并在标有“同意”或“知悉”的方框或按钮内作出选择后，网页才会跳转到访问者需要的界面。如果访问者没有按照其网站服务条款规定的要求来行使访问行为，就有可能会被认为是超越访问权限，从而涉及是否存在侵入的问题。按照我国现行刑法和有关司法解释的规定，这种超越网站服务协议条款的访问行为一旦被认定为符合法定的侵入行为构成要件，就可能面对刑事追究的危险。计算机网站的权利人出于保护自己网站信息或计算机信息系统及其数据安全利益的需要，可以在法定框架内建立符合有利于自己的服务条款，为用户设定系列访问权限与责任义务。这种网站服务协议条款可以用来约束用户的访问行为，但不能以此作为判断构成“超越授权”的侵入行为进而被认定为犯罪。

从文本内容和所涉主体来看，网站服务条款在本质上是一种基于双方合意订立的民事合同。用户在访问过程中不遵守网站服务条款，从根本上而言是违背了计算机网站的权利人对访问者的诚实信用要求，这种违反与背离应属于民事违约行为，完全可以按照民法典中关于合同的相关规定加以救济，通过民事诉讼的方式来解决纠纷，而不能随意开启国家刑罚权予以追责。把访问过程中对网站服务条款的违反当作刑事违法性判断的依据，就相当于是让计算机网站的权利人来决定什么样的访问行为会构成犯罪。① 因此，如果将违反网站服务条款的访问行为当作超越授权的侵入行为而认定为犯罪，可能会导致一个严重的问题，即网站服务条款架空刑事法的有关规定，变成实质上的刑法内容，从而背离罪刑法定原则的根本要求。结合我国《刑法》规定，除第 285 条第 1 款规定之罪和非法控制计算机信息系统、破坏计算机信息系统外，在违反网站服务条款访问计算机信息系统构成“侵入”的同时，又获取其中存储、处理或传输的数据，给权利人造成经济损失的，应依据民法典的有关规定，予以相应经济赔偿。但是，如果违反网站服务条款实施访问并通过技术手段大批量“抓取”“收集”数据的，则应根据不同情形作出

① See United States v. Drew, 259 F.R.D.465 (2009).

判断并予以分类规制，下文将进一步展开分析。

违反代理人法则的侵入行为在实质上也是“超越授权”的侵入，亦可通过民事惩处来实现规制。基于雇佣关系的员工使用老板（或企业）的计算机信息系统或登录所在单位的网站完成工作任务，是基于一种“代理”关系的履职行为，表明了老板（或企业）对员工在履行工作职责或交办任务范围内的计算机信息系统访问授权行为。按照普通法关于代理人的有关法理，员工与老板之间的雇佣关系明确了员工在职期间须严格遵守雇佣协议的要求，在工作上的行为应符合雇主的利益；如果员工的所作所为并不是代表雇主本意甚至有损于雇主利益，那么其已经不具有代理人的资格，雇主的相应授权也即终止。① 根据普通法上的这种观念，如果员工在访问老板（或企业）的计算机信息系统或数据网站时并非出于工作需要，而是有利于本人或第三人，甚至是与受雇企业形成竞争性利益，其相应的访问行为就不符合代理人的要求，属于超越授权。纵观近年来国内外发生的这类案件，大多表现为员工通过已获授权去访问工作单位的计算机信息系统从中获取数据信息，将其出售给与本单位有竞争关系的企业，或者带着从原单位获取的重要数据“跳槽”到有相同业务的公司工作，更有甚者“另起炉灶”自己经商办企与原单位展开竞争。② 这类行为实则违反的是代理人法则上的忠实守诚义务，行为人超出了雇主对计算机信息系统授权使用的范围，违反雇佣合同的有关约定，在不涉及侵犯商业秘密、个人隐私和知识产权有关刑事问题的情况下，也应通过民事诉讼方式，让此类“内部黑客”承担民事责任，及时予以高额的经济惩处，这恐比刑事打击更具有积极性意义：其一，代理人法则无法准确厘定雇员的行为在什么情形下超出了忠诚的范围，会让雇主或企业获得过多权限来定义犯罪，特别是当雇员的行为发生后，通过代理人法则去进行追溯式的违法性判断，会导致犯罪认定的不精准甚至刑事处罚的扩张；③ 其二，民事惩处措施的实行，使得那些企图实施侵入行为的“内部黑客”认识到必须要为自己的行为付出经济上的重大代价，如果得不偿失，就会放弃相关行为，从而达到震慑预防的

① See William A.Gregory, The Law of Agency and Partnership, 3rd ed.West Group, 2002, pp.11-15.

② 另外，还有的表现为内部员工将自己掌握的单位内部计算机信息系统的登录账号、密码提供给无权访问的第三人，让第三人登录计算机信息系统下载获取有关数据信息。典型的如前述最高人民检察院公布的卫某、龚某、薛某非法获取计算机信息系统数据案中龚某向卫某提供登录账号、密码的行为。或者，单位内部员工没有访问计算机信息系统的权限，但通过盗取本单位有访问权限员工的登录账号、密码的行为。例如，在张某非法获取计算机信息系统数据案中，同案犯魏某每月通过盗取同事郭某的工号和密码登录珠海市人民医院的管理信息系统提取医生处方用药信息的统计数据（参见张某亮、吴某武非法获取计算机信息系统数据，非法控制计算机信息系统，掩饰、隐瞒犯罪所得、犯罪所得收益案，广东省珠海市香洲区人民法院刑事判决书（2017）粤 0402 刑初字第 1879 号）。对于上述两种情形（即卫某和魏某登录计算机信息系统的行为），因其本身没有获得登录的任何授权，对于这种“未经授权”的侵入行为，本文认为并不适用代理人法则，不能简单以民事惩处的方式来规制。

③ See Annie Lee, Algorithmic Auditing and Competition under the CFAA: The Revocation Paradigm of Interpreting Access and Authorization, 33 Berkeley Technology Law Journal 1307, 1316 (2018).

目的。

2. 刑事惩罚：边界及要求

计算机信息系统或数据网站的权利人为了防止侵入行为，都会通过技术性手段建构安全屏障来限制并规范用户的访问行为。比如，设置类似“防火墙”的安全软件或程序，通过设定专门的访问程式或编制网络密钥等对不同类别的计算机网络用户分配不同的使用权限，从而保障系统安全运行、数据有序使用。用户只有按照设定的程序或使用合法的密钥，才能实现正常的访问。如果用户不按照给定的有效登录方式、程序访问计算机信息系统或数据网站，而是使用技术性手段绕开设定的安全程序，或者通过技术手段破解网络密钥、突破访问限制措施等方式访问计算机信息系统或网站，就类似于现实生活中盗贼使用工具撬开上锁的门或者架设梯子翻墙入院，属于“未经授权”的侵入行为。专门使用技术性手段或非法获取账号密码的方式使他人的计算机信息系统安全程序破防，进而实施非法访问的行为，体现了行为具有严重的法益侵害性和刑事非难可责性。① 这种突破计算机信息系统或数据网站设定的安全保护措施，违反网络秩序的访问行为，无视权利人的正当性利益并将计算机信息系统及数据置于严重的安全风险之中，破坏了社会对计算机信息系统及数据安全保护的正义期待，无论是从一般的道义责任上讲还是就其造成的危害性而言，都应施以刑罚的惩戒。

结合我国刑法和相关司法解释的规定，凡是利用技术性手段避开或者突破计算机信息系统安全保护措施访问计算机信息系统的，都是应受刑事惩罚的侵入行为，按照侵入或侵入后实施的后续行为来定罪处罚，典型的如计算机病毒、账号密码破解、撞库等。② 需要指出的是，这类侵入行为的刑事惩罚边界在于是否规避、突破了权利人设定的安全保护措施。如果行为人没有规避、突破计算机信息系统或数据网站的安全保护措施，只是在权利人设定的安全措施范围内，采用一定的技术手段获得比一般普通大众访问系统或获取数据更为优势的地位，以创造“捷径”或提升速率等方式登录进入系统或网站，则不能简单地认为一律构成犯罪，典型的如网络爬虫行为。

3. 民刑双重适用的特殊情形：网络爬虫行为

网络爬虫行为的主要特征是通过技术手段对计算机网络空间中数据进行非常规化获取。如何对其规制是晚近以来刑事法学界讨论非常热烈、司法实务界也高度关注的一个问题。网络爬虫作为一种自动下载网页内容的软件程序，是当下网络空间抓取数据的常用工具。对于网络爬虫行为的规制，本文认为应聚焦爬取对象和爬取后果两个维度来考察：关于爬取对象，须考察爬取的数据是公开数据还是非公开数据；关于爬取后果，须考察爬取过程中是否突破了计算机信息系统或数据网站安全保护措施。如果爬取的是已

① See Ethan Preston, Finding Fences in Cyberspace: Privacy and Open Access on the Internet, 6 Journal Technology Law & Policy 57, 91-92 (2001).

② 在这类侵入行为中，如果侵入后的行为是有益的，比如是出于帮助发现计算机信息系统设计缺陷、漏洞或安全隐患的侵入，且没有实施后续的数据侵犯或其他危害计算机信息系统行为，虽然行为不法，但可以不用追责。

经公开的数据，[①] 且在爬取过程中使用的技术手段并没有突破计算机信息系统或数据网站的安全保护措施，而仅仅是增加了访问数据的速度或强度，即在单位时间内比一般人获取的数据量更大，则不属于刑法上的侵入行为，也不构成相关的犯罪，应予民事惩处，通过经济赔偿的方式弥补数据权利人的损失或利益。

公开数据是开放给大众访问的，相当于数据权利人给每一位用户进行了授权，只不过计算机信息系统或数据网站的权利人预先设定了限定性的访问方式，要求用户在访问和获取数据中须遵守这种方式。例如，在访问条款中声明反爬行为、设置人机验证机制和其他反爬措施等，相当于是对访问者明确的合约性告知。行为人一旦实施访问就意味着接受权利人的这些要求和约束。这种做法类似于“使用服务协议标准”，如果行为人违反权利人设定的访问要求，使用爬虫技术访问公开数据并大批量抓取，事实上就是违反合同要约的行为，应受到民事追究，承担权利人因此受到的损失。当然，如果在使用爬虫程序的过程中，由于数据抓取过于频繁，导致计算机信息系统“死机”或网站运行故障，后果严重的，在追究行为人民事责任的同时，还应以干扰型破坏计算机信息系统罪定罪处罚。

如果在爬取公开数据的过程中，采取的技术性手段避开、突破了计算机信息系统或数据网站的安全保护措施，则应认定这种“爬”的行为符合侵入性的构成要件行为，结合后续的数据抓取行为，构成非法获取计算机信息系统数据罪应无疑义，关键的问题在于如何准确厘定避开或突破计算机信息系统的安全保护措施。一般而言，计算机信息系统或数据网站都是按照事先编写好的程序来实现既定的运行逻辑，提供规定或预设的服务功能，并授权用户在使用过程中按照设定的程序和要求使用计算机信息系统或数据网站提供的功能，但并不允许用户通过技术发现的程序漏洞或软件功能缺陷去使用原程序并没有的运行逻辑或功能。[②] 从这一角度看，是否按原定的运行程序和运行逻辑来实施访问，是判断是否避开或突破安全措施的重要参考。网络爬虫行为在爬取公开数据的过程中，即便使用了一定的技术手段避开或突破计算机信息系统或数据网站中的反爬措施，比如绕开访问限制措施（如登录限制、流量限制、Cookie 限制、验证码限制等），但没有超出计算机信息系统中预设的运行程序或功能进行访问，或没有利用程序中的漏洞或软件缺陷来爬取数据，则应认为不属于避开或突破了计算机信息系统的安全保护措施。

---

① 公开数据包括已公开的个人身份信息。个人身份信息与普通数据相比，具有信息内涵的特殊性、适用场景的复杂性和法律规定的单独性。对于使用爬虫技术获取已公开的个人身份信息的规制，应重点从行为的“权限性”、信息的“可识别性”和权利人的“知情同意性”三方面进行判断，分别作出不同的定性处理：如果行为人是在访问授权范围内爬取了可识别的个人身份信息，并且得到身份信息的权利人的同意，则不构成犯罪；如果行为人未经权利人同意爬取其可识别的个人身份信息，则构成侵犯公民个人信息罪；如果行为人虽然没有得到授权或权利人许可，但爬取的信息不能够单独或者与其他信息结合识别出个人身份，则视为对普通公开数据的爬取，具体规制范式将在下文中进一步展开分析。

② See Pekka Himanen, The Hacker Ethic and the Spirit of the Information Age, Random House, 2001, p.181.

从计算机信息系统或数据网站编定的预设程序和功能来看，反爬措施并不是计算机信息系统或数据网站的安全防护措施，其在本质上只是阻止爬虫程序短时间内大批量获取计算机信息系统中的数据或为大批量获取数据制造障碍、增加难度，是权利人为了在保证符合预设条件的一般用户正常访问数据的同时，屏蔽、阻挡非正常用户，不至于使自己辛苦建立的数据遭到不当的高频访问和“不劳而获”的海量攫取，从而防止自身的数据利益减损。① 此外，以网络爬虫为代表的数据收集、使用行为是当前数据互联网行业不可或缺的技术措施，也是当前大数据产业发展的关键，对其予以过度的刑事规制，实质是变相强化“数据寡头”的市场优势地位，最终阻碍数字经济的发展。② 如果把避开或突破反爬措施简单等同于避开或突破计算机信息系统或数据网站的安全防护措施而入刑，不但会助推数据权利人不断建立反爬措施形成自己的保护屏障，而且还会把刑事惩罚作为重要后盾，始终据守在数据“城堡”的顶端或处于数据控制的优势地位，导致本已公开的数据不能流动，难以实现新的数据集成和有效利用，不利于数据业态的有序有效竞争和充分发展。刑法作为最后手段原则，在适用上应有其相当性和必要性，尤其是针对诸如网络爬虫行为的规制，要谨慎平衡数字产业发展现实需要和数据安全维护利益诉求，避免因刑法介入过度而抑制数据共享目标的实现，最终影响数字经济的良性发展。

四、结 语

计算机网络中的侵入行为和现实物理空间中的侵入行为，虽然字面用语相同，但内涵存在重大差别。对计算机网络中的侵入行为，需要根据不同场景并结合不同判断标准作出不同的规制。民刑结合的规制进路有利于在数字经济时代正确厘定和界分计算机网络侵入行为的犯罪化和非犯罪化。特别是针对诸如公开数据的网络爬虫行为，应注意其中的利益机制、保护方式和法律适用效果，明确其首先违背的是数据利益（数据控制者建构、运行数据需要的成本和数据资源优势在市场竞争中获得的更好经济效益），大批量数据抓取损害的是数据控制者的应得利益或期待利益。对没有避开或突破计算机信息系统安全保护措施，或没有导致计算机信息系统故障或原有数据损坏的网络爬虫行为，不作为犯罪论处，而是给予相应的民事赔偿，更符合数字经济时代关于数据合理保护与数据充分利用的要求。

（责任编辑：高磊）

① 例如，在百度诉奇虎360案、新浪微博诉脉脉案、大众点评诉百度地图案、酷米客诉车来了案中，原告都是为了防止竞争对手大批量地从本公司计算机信息系统爬取数据并利用获得的数据建构新的同业竞争体系，从而通过诉讼来维护自身权利。

② 参见杨志琼：《美国数据犯罪的刑法规制：争议及启示》，载《中国人民大学学报》2021年第6期，第157页。