

# 破坏计算机信息系统罪之司法 实践分析与规范含义重构

俞小海\*

---

## 目次

- 一、破坏计算机信息系统犯罪司法实践总体样态
- 二、破坏计算机信息系统犯罪司法实践分析与反思
  - (一) 数罪并罚问题认定不一
  - (二) 类似行为评价差异较大
  - (三) “后果严重”认定模糊
  - (四) 适用范围过度扩张
- 三、破坏计算机信息系统罪的文本还原与规范构造
  - (一) “后果严重”的规范解释
  - (二) 计算机信息系统数据的合理解释
  - (三) 利用计算机实施犯罪的认定
- 四、结语

**摘要** 通过对 43 个相关司法判例的梳理和分析,得出破坏计算机信息系统罪司法实践中存在数罪并罚问题认定不一、类似行为评价差异较大、“后果严重”认定模糊、适用范围过度扩张等问题。实践中,通过降低“后果严重”的标准和扩大对计算机信息系统数据之解释,使得破坏计算机信息系统罪具有极强的适用力,呈现“口袋化”之趋势,偏离了破坏计算机信息系统罪的文本含义和规范构造。为此,应当将本罪“后果严重”限定为与计算机信息系统安全具有关联性的后果,将计算机信息系统数据限缩为核心数据和核心应用程序,在此基础上准确认定利用计算机实施犯罪的罪数形态。

**关键词** 计算机信息系统 后果严重 司法判例

---

近年来,随着计算机信息技术的不断发展,针对网络或者利用网络从事犯罪的活动呈上升趋势,也使得传统意义上的破坏计算机信息系统罪获得了新的适用空间。尽管我国刑法已经较为明

---

\* 上海市高级人民法院法官助理。

确地区分了针对计算机信息系统犯罪和利用计算机实施犯罪的定罪规则,但是在现实中,随着财产的“数字化”“虚拟化”,以及与网络交织在一起的行为定性模糊,使得行为人针对计算机信息系统或利用计算机信息系统而实施的犯罪行为出现了定性上的争议。从搜集到的判例来看,这类犯罪的司法实践存在较多问题,有必要予以专门梳理,从而让破坏计算机信息系统罪回归本来含义,实现刑事司法调整的精确性。

## 一、破坏计算机信息系统犯罪司法实践总体样态

笔者在“北大法宝”司法案例中,将时间设定为2014年之前,在全文中精确检索包含“计算机信息系统”的案例,共有189件,其中刑事103件,民事81件,行政5件。对刑事103件逐一分析,与破坏计算机信息系统罪有关的有43件。<sup>[1]</sup>经分析,这类案件总体上呈现如下三个特点。

第一,案件逐渐增多,呈现高发态势。43个案件,发生于2005年以前的总共8件,2005年至2010年之间有15件,2011年以来共有20件,特别是2012年、2013年分别达到6件、11件。总体而言,与破坏计算机信息系统罪相关的案件,呈逐年增多之趋势。(图1)

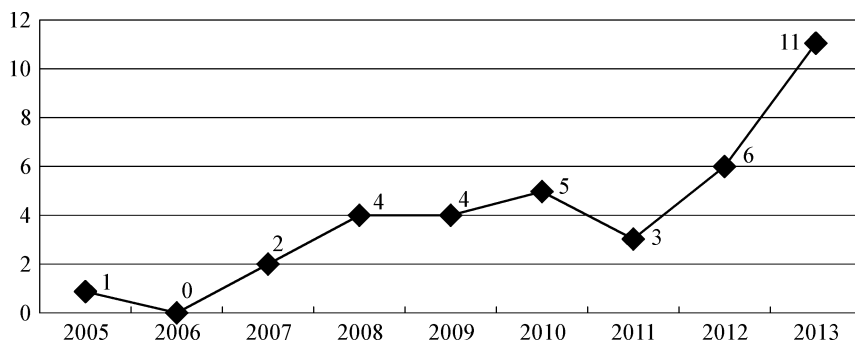


图1 2005年以来破坏计算机信息系统罪情况

第二,行为方式相对类型化。从收集到的判例情况来看,破坏计算机信息系统罪主要集中于四种行为方式:一是以干扰、破坏计算机信息系统作为威胁向他人索取财物,这类行为共有4件;二是非法进入公安机关计算机信息网络以帮助他人消除、变更交通违章信息,或者帮他人增加户口信息而获利,这类行为有6件;三是对计算机信息系统中的数据予以修改、变更,直接造成他人财物受损,这类行为有10件;四是开发、制作网络游戏外挂程序帮人代练升级牟利,这类行为有7件;五是典型的破坏计算机信息系统行为,比如删除他人计算机系统盘、硬盘所有数据、应用程序,通过拒绝服务攻击方式(DDOS)对网站进行攻击,制作、传播计算机病毒,植入木马程序,致使他人

[1] 这里需要说明两点:第一,全文中包含“计算机信息系统”的刑事裁判文书共有103篇,但是涵括了破坏计算机信息系统罪、提供侵入计算机信息系统程序罪、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等罪名,其中,全文包含“破坏计算机信息系统罪”的刑事裁判文书一共有43件。第二,在中国的语境下,司法实践不仅仅是指人民法院的定罪量刑活动,还包括了公安机关刑事拘留、检察机关审查起诉阶段,因此,要想获得对于破坏计算机信息系统罪司法实践的全面、客观、理性认识,需要对公安、检察、审判各刑事诉讼阶段予以把握,因此,本文关注的不仅仅是人民法院最终认定为破坏计算机信息系统罪的案例,还包括公安机关刑事拘留时认定为破坏计算机信息系统罪或检察机关审查起诉时指控破坏计算机信息系统罪之情形,甚至包括辩护人认为构成破坏计算机信息系统罪之情形,而这三种情形,极有可能在法院罪名认定时被否定。所以,本文尽管以破坏计算机信息系统罪为中心,但是,选取的案例却涉及法院最终认定为他罪的情形。换言之,本文所言的与破坏计算机信息系统罪有关的案例,并不仅仅指最终被人民法院认定为破坏计算机信息系统罪之判例,还包括公安机关、检察机关、辩护人认定破坏计算机信息系统罪而法院最终变更罪名之情形。

计算机、网站运行陷入瘫痪,等等,这类行为有11件;〔2〕六是其 他行为,即非典型的破坏计算机信息系统行为,这类情况共有5件。(图2)

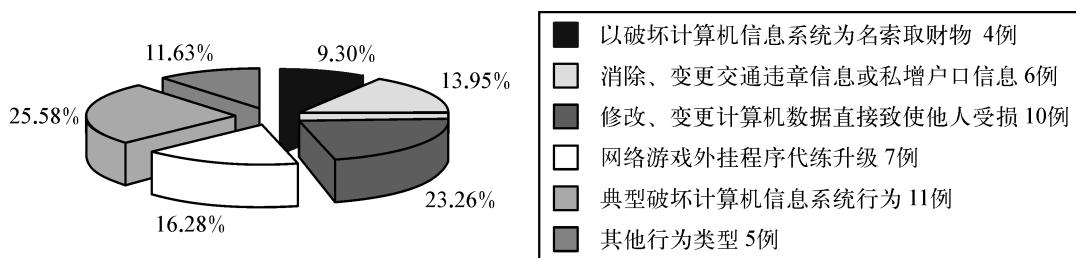


图2 破坏计算机信息系统犯罪行为方式

第三,定性争议较大。对实践中的破坏计算机信息系统犯罪加以梳理,发现该类犯罪实践认定中争议较大。在与破坏计算机信息系统罪相关的43个司法判决中,公诉机关指控罪名与法院最终认定罪名完全一致的有24个,而公安机关、检察机关、辩护人意见和法院最终认定罪名之间不一致的有19个,占44.19%。涉及不同罪名争议的共22次。〔3〕其中,与非法经营罪争议4次,与侵犯著作权罪争议3次,与盗窃罪争议7次,与非法控制计算机信息系统罪、变造、故意传播虚假恐怖信息罪、伪造国家机关证件罪、敲诈勒索罪、诈骗罪、故意毁坏财物罪、操纵证券交易价格罪〔4〕争议各1次。(图3)

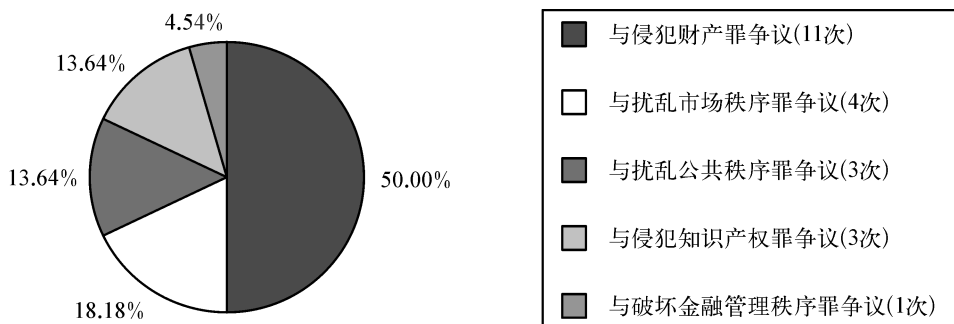


图3 破坏计算机信息系统罪与其他犯罪争议情况

〔2〕 分别参见广西壮族自治区南宁市青秀区人民法院(2008)青刑初字第375号判决书、广西壮族自治区南宁市中级人民法院(2008)南市刑一终字第172号刑事裁定书;浙江省湖州市中级人民法院(2013)浙湖刑终字第44号刑事判决书;《江苏省无锡市滨湖区人民检察院诉马志松等破坏计算机信息系统案》,载《最高人民法院公报》2009年第2期;湖北省仙桃市人民法院(2007)仙刑初字第350号刑事判决书;云南省昆明市五华区人民法院(2001)五法刑初字第328号刑事判决书、云南省昆明市中级人民法院(2001)昆刑终字第600号刑事裁定书;上海市第二中级人民法院(2009)沪二中刑终字第321号刑事裁定书;上海市浦东新区人民法院(2010)浦刑初字第1428号刑事判决书;河北省唐山市路北区人民法院(2005)北刑初字第305号刑事判决书;北京市海淀区人民法院(2008)海法刑初字第3461号刑事判决书;上海市嘉定区人民法院(2010)嘉刑初字第184号刑事判决书、上海市第二中级人民法院(2010)沪二中刑终字第670号刑事裁定书;上海市嘉定区人民法院(2010)嘉刑初字第490号刑事判决书。

〔3〕 需要说明的是,一般情况下,一个案子主要存在两种不同罪名的争议,但在个别案件中公安机关刑事拘留罪名、检察机关批准逮捕罪名、辩护人意见和法院最终认定罪名均不一致或者其中三方意见不一致,便涉及三个罪名或四个罪名之争议,为了更加如实、客观反映统计情况,本文将前者定义为两次罪名争议,将后者定义为三次或四次罪名争议,因此罪名争议次数就会大于公安机关、检察机关、辩护人意见和法院最终认定罪名之间不一致情形之数量。

〔4〕 经1999年《刑法修正案》和2006年《刑法修正案(六)》两次修改之后,最高人民法院、最高人民检察院《关于执行〈中华人民共和国刑法〉确定罪名的补充规定(三)》(2007年10月25日)将我国《刑法》第182条原来的操纵证券、期货交易价格罪改为操纵证券、期货市场罪。

## 二、破坏计算机信息系统犯罪 司法实践分析与反思

如果对 43 个司法案例进一步分析,则会发现破坏计算机信息系统罪在司法实践中存在较多问题,一定程度上偏离了破坏计算机信息系统罪的文本含义和规范构造。

### (一) 数罪并罚问题认定不一

实践中,行为人单纯出于报复、泄愤动机而实施对计算机信息系统功能进行删除、修改、增加、干扰,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,或者故意制作、传播计算机病毒等破坏性程序,影响计算机系统正常运行的情况较为少见,更多的是通过实施破坏计算机信息系统行为而实现其他目的,由此极有可能出现一个行为同时侵犯数个法益触犯不同罪名之情形。在此情况下,关于破坏计算机信息系统罪是否与其他犯罪数罪并罚,司法实践持有不同的立场。

43 个司法案例中,有 4 件系以干扰、破坏计算机信息系统作为威胁索取财物,但在认定上出现了差异。比如在胡磊、李权利破坏计算机信息系统案中,被告人胡磊、李权利连续多次对某公司游戏平台服务器实施攻击干扰,最终造成机房内的服务器瘫痪,造成该公司严重损失,并以此为要挟,勒索该公司游戏币“银子”5 亿两。后两被告人销赃得款人民币 18 750 元(以下简称“案例一”)。<sup>〔5〕</sup>在喻某、李某破坏计算机信息系统案中,喻某等人对他人公司游戏服务器进行 DDOS 攻击,致使该公司经营的网络游戏无法正常运行,并以此索要网络安全保护费,先后共获利一百七十余万元(以下简称“案例二”)。<sup>〔6〕</sup>在李永破坏计算机信息系统案中,李永非法获取他人网站服务器的管理员权限,登录他人网站服务器,在未予以备份的情况下删除了服务器上所有网站程序文件和数据库文件,并以恢复被破坏的网站数据为名向受害公司索取人民币五万余元(以下简称“案例三”)。<sup>〔7〕</sup>在欧阳俊曦破坏计算机信息系统案中,欧阳俊曦利用其个人网站传播病毒软件,并以修复丢失资料、获得正版软件序列号为名,向被感染的计算机用户索取款项共两千七百余元(以下简称“案例四”)。<sup>〔8〕</sup>上述四个案例,尽管形态各异,但基本行为方式是一样的,即通过攻击他人网络服务器索要财物。对此,案例一和案例二均认定为破坏计算机信息系统罪一罪,在案例三中,审理法院认为,“李永违反国家规定,对计算机系统功能进行删除,造成计算机信息系统不能正常运行,后果严重,其行为已构成破坏计算机信息系统罪,依法应予惩处;被告人李永又以非法占有为目的,采用要挟的方法索取他人财物,数额巨大,其行为又已构成敲诈勒索罪,依法亦应予惩处并予以两罪并罚”。<sup>〔9〕</sup>遂认定为行为人同时构成破坏计算机信息系统罪和敲诈勒索罪。在案例四中,公诉机关指控的罪名为破坏计算机信息系统罪和敲诈勒索罪两罪,但是法院对公诉机关认为应数罪并罚的意见予以纠正,最终仅认定破坏计算机信息系统罪一罪,不过与案例一、案例二直接认定为破坏计算机信息系统罪一罪不同的是,案例四是在肯定同时构成破坏计算机信息系统罪和敲诈勒索罪两罪的基础上依据“择一重罪”之原则做出最终认定。在该案判决理由中,一审法院认为,“被告人欧阳俊曦为了牟取非法利益,制作、传播计算机病毒的行为同时触犯破坏计算机信息系统

〔5〕 参见江苏省苏州市虎丘区人民法院(2009)虎刑初字第 0363 号刑事判决书。

〔6〕 参见湖南省长沙市中级人民法院(2012)长中刑一终字第 0329 号刑事判决书。

〔7〕 参见上海市青浦区人民法院(2010)青刑初字第 117 号刑事判决书。

〔8〕 参见广州市越秀区人民法院(2007)越法刑初字第 402 号刑事判决书、广州市中级人民法院(2007)穗中法刑一终字第 310 号刑事判决书。

〔9〕 上海市青浦区人民法院(2010)青刑初字第 117 号刑事判决书。

罪、敲诈勒索罪两个犯罪客体,构成我国刑法理论的想象竞合犯,按对想象竞合犯‘从一重罪处断’的处罚原则,本案应以破坏计算机信息系统罪论处”。<sup>[10]</sup> 对此,二审进一步指出,“破坏计算机信息系统罪的动机是多种多样的……对其牟取非法利益的主观犯罪动机和非法取得他人钱财的客观后果,属于破坏计算机信息系统罪的构成要素,对以上情节已在认定此罪过程中给予了评价,不应单独定罪,否则是重复评价。行为人为了牟取非法利益,制作、传播计算机病毒的行为同时触犯破坏计算机信息系统罪、敲诈勒索罪两个罪名这种是基于一个犯罪行为而同时侵犯两个犯罪客体的犯罪,是刑法理论的想象竞合犯。”<sup>[11]</sup> 可见,对在破坏计算机信息系统的同时索要他人财物的行为如何定性,司法实践层面做法并未统一。

## (二) 类似行为评价差异较大

43个案例中,行为方式为研发、制作游戏软件外挂程序出售或通过制作的外挂程序从事有偿代练升级的共有7例,7个判例中,有3件法院在认定时将研发、制作游戏软件外挂程序出售的行为解释为未经著作权人许可,复制发行计算机软件之行为,进而将该种行为认定为侵犯著作权罪。<sup>[12]</sup> 有2件法院在认定时将研发、制作游戏软件外挂程序出售、有偿代练的行为解读为违反国家规定,未经国家主管部门批准,也未获得游戏软件公司许可和授权的出版非法互联网出版物的行为,从而认定构成非法经营罪。<sup>[13]</sup> 因其中1例公诉机关指控构成破坏计算机信息系统罪,法院在判决理由中指出,“破坏计算机信息系统罪侵犯的客体是计算机信息系统的安全,本案被告人制作的外挂软件的运行,只是改变了网络游戏软件设定的游戏规则,影响程序的正常运行,导致服务器的加重,但并没有破坏计算机系统本身运行的安全性;其次,被告人制作、销售外挂程序的行为侵害了网络游戏经营者、游戏消费者的合法权益,扰乱的是网络游戏经营的正常秩序,这与破坏计算机信息系统罪所要求的扰乱公共秩序不相符……故公诉机关对于本案被告人行为的定性有误,本院予以纠正”。<sup>[14]</sup> 还有2例,则被认定为对计算机信息系统中传输的数据进行修改的操作,干扰网络游戏服务端计算机信息系统功能,实施危害计算机信息系统安全的行为,进而认定构成破坏计算机信息系统罪。<sup>[15]</sup> 在其中1例案件中,针对控辩双方破坏计算机信息系统罪还是非法经营罪之争议,法院指出,“被告人邬某某利用他人制作的外挂程序为不特定游戏玩家提供针对网络游戏的有偿代练升级服务,其代练服务本身并非违反国家规定,故意从事非法经营活动,扰乱市场秩序,情节严重的行为,不属于非法经营罪的规制范畴,被告人邬某某不构成非法经营罪。本案被告人邬某某的犯罪行为客观上严重破坏了该款游戏的正常操作流程和运行方式,本质上属于修改网络游戏运行数据,干扰网络游戏服务端计算机信息系统功能,危害计算机信息系统安全的行为,符合破坏计算机信息系统罪的犯罪构成要件”。<sup>[16]</sup> 可见,针对研发、制作游戏软件外挂程序出售或通过制作的外挂程序从事有偿代练升级这一行为,司法实践中

[10] 广州市越秀区人民法院(2007)越法刑初字第402号刑事判决书。

[11] 广州市中级人民法院(2007)穗中法刑一终字第310号刑事判决书。

[12] 参见上海市徐汇区人民法院(2011)徐刑初字第256号刑事判决书、上海市静安区人民法院(2012)静刑初字第478号刑事判决书、上海市浦东新区人民法院(2010)浦刑初字第3240号刑事判决书和上海市第一中级人民法院(2011)沪一中刑终字第411号刑事裁定书。

[13] 参见《董杰、陈珠非法经营案》,载《最高人民检察院公报》2011年第5号;《江苏省南京市江宁区人民检察院诉董杰、陈珠非法经营案》,载《最高人民法院公报》2012年第2期;上海市浦东新区人民法院(2008)浦刑初字第384号刑事判决书。

[14] 参见上海市浦东新区人民法院(2008)浦刑初字第384号刑事判决书。

[15] 参见上海市徐汇区人民法院(2013)徐刑初字第281号刑事判决书、上海市徐汇区人民法院(2013)徐刑初字第641号刑事判决书。

[16] 上海市徐汇区人民法院(2013)徐刑初字第281号刑事判决书。

就出现了三种不同的定性。

### （三）“后果严重”认定模糊

根据我国《刑法》第 286 条，破坏计算机信息系统罪之成立，需满足“后果严重”之条件。但是实践中有些案例在“后果严重”之判定上比较模糊。比如在吕薛文破坏计算机信息系统案中，<sup>〔17〕</sup>尽管被告人非法入侵他人主机，增设最高权限的账户，修改最高权限密码，但是其随后将新设的密码告知网络管理员，并非想获得对计算机的绝对控制权。从其行为来看，被告人吕薛文也没有对计算机信息系统的功能、数据和应用程序进行破坏，其入侵行为没有使计算机信息系统无法正常运行，没有产生严重后果。但最终法院认定为其行为“后果严重”。该案判决理由中提到，“计算机信息系统上的账号和密码，是以数据形式表现出来的计算机信息系统功能的一部分。无论出于何种目的，非法入侵他人计算机信息系统对管理账号和密码进行修改、增加，致使网管员也不能进入主机系统进行管理工作，已经危害了计算机信息系统的安全，造成他人主机管理失控、不能正常运行的严重后果，构成破坏计算机信息系统罪……”<sup>〔18〕</sup>类似的情形还有，非法获取人事考试网网管员权限，进而获取他人用户名及密码，被认定为“后果严重”。<sup>〔19〕</sup>又比如在罗露破坏计算机信息系统案中，<sup>〔20〕</sup>控辩双方针对本案是否属于“后果严重”存在分歧，辩护人认为，罗露虽违反国家规定，对计算机信息系统中存储、处理或者传输的数据进行了删除的操作，但既未造成省教委计算机信息系统无法正常运行，更未由此产生任何严重的危害后果和经济损失。所有的数据都存在备份，全省的学校又分别将其数据进行了上传，考生数据实际上已经得到恢复。因此，罗露的行为不构成破坏计算机信息系统罪。公诉机关则认为，罗露对计算机信息系统的入侵，已构成最高程度的“控制”或“攻破”，具备造成计算机信息系统无法正常运行甚至瘫痪的潜在威胁，且罗露已破译了管理人员的密码，可以无限制地存储、删改计算机信息系统资源，并且已经实际实施了删除文件的行为，造成涉及全省 30 万名考生的系统关闭了一段时间，后果不能说不严重。因此，应以破坏计算机信息系统罪对罗露定罪处罚。法院最终支持了公诉机关的指控，指出“被告人罗露作为计算机专职教师，主观上明知自己的行为会造成文件删除的后果，客观上仍实施了非法登录江苏省中小学生信息技术等级考试网站和删除文件的行为，并造成 9 991 名考生成绩被删除的严重后果，符合破坏计算机信息系统罪的构成要件”。<sup>〔21〕</sup>后来针对本案的法理评析中，该案

〔17〕 该案基本情况为：吕薛文入侵广州主机系统并取得最高权限后先后 3 次修改广州主机系统的 root 密码，后吕薛文上网主动要求与网管员对话，并将 root 密码已经改为 root123 密码一事通知了网管员。网管员经试验 root123 密码可用后，为安全起见，又把 root123 设置为另一密码。但是网管员随后即发现，他刚改过的这一密码，又被改回为只有吕薛文和网管员知道的 root123 密码。随后，广州主机采取了封闭普通用户登录进入该主机的措施后，只有吕薛文仍能以非法手段登录进入，期间该主机的 root 密码第三次失效，吕薛文再次主动与网管员交谈，虽然仍否认自己修改了主机的密码，但是将能够进入主机的新 root 密码告诉了网管员。吕薛文实施了入侵行为后，将其使用的账号记录删除，还将拨号信息文件中的上网电话号码改为 12345678 或 00000000，以掩盖其入侵行为。参见广东省广州市中级人民法院（1999）穗中法刑经初字第 11 号刑事判决书。

〔18〕 广东省广州市中级人民法院（1999）穗中法刑经初字第 11 号刑事判决书。

〔19〕 参见南京市鼓楼区人民法院（2013）鼓刑初字第 26 号刑事判决书。

〔20〕 该案基本情况为：2002 年 5 月 18 日，被告人罗露利用其事先从客户端 SQL SERVER 企业管理器获取的江苏省普通高中会考办公室 FTP 站点服务器的 IP 地址、账号、用户名及密码，从苏州市第十中学计算机学校信息中心办公室其个人使用的计算机上，先后两次使用 Leapftp 软件非法登录江苏省中小学生信息技术等级考试网站（江苏省普通高中会考办公室专用服务器），执行删除文件命令，删除了 100 个 RST 文件（江苏省中小学生信息技术等级考试考生成绩文件），造成 85 所学校 9 991 名考生的成绩被删除。后经江苏省普通高中会考办公室组织各考点将备份文件重新上传，方将数据恢复。参见江苏省苏州市沧浪区人民法院（2002）沧刑初字第 254 号刑事判决书。

〔21〕 江苏省苏州市沧浪区人民法院（2002）沧刑初字第 254 号刑事判决书。

承办法官进一步提到,“作为破坏计算机系统罪构成要件的‘后果’,其性质是指现实的已经发生的危害。本罪应该属于刑法理论中的实害犯……公诉机关在举证过程中,没有明确提出实际给省教委和其他学校因为重新上传数据所造成的直接经济损失的证据……从客观上说,在经济上并无直接的损失。但作为本案中罗露的行为,在一场涉及全省30万考生的考试过程中,主观上故意侵入会考办的服务器,删除了大量考生的考卷数据文件。在会考办发现文件灭失后,立即关闭了服务器,并向全省各考点通知改变文件上传的时间。其产生的影响还是比较大的。如果处理不当,近万名考生就有可能要重新进行考试,后果就可能相当严重了。目前虽然在经济上没有造成明显的直接损失,但是存在一定的社会影响,而网站也在一段时间无法正常运行,应该属于后果严重的范畴……考虑到其后果严重性不是特别明显,法院在量刑上就定为有期徒刑六个月,并适用了缓刑”。〔22〕

笔者认为,上述3个案例被认定为“后果严重”均存在一定问题。吕薛文破坏计算机信息系统案中,尽管被告人增设最高权限的账户,修改最高权限密码,在形式上获得了对他人计算机信息系统的控制权,但其随后将新设的密码告知了网络管理员。从其行为来看,其对单个计算机单个数据的修改,并没有造成经济损失,也没有导致计算机信息系统无法正常运行,获取人事考试网管理员权限,进而获取他人用户名及密码,也是这种情况。在罗露破坏计算机信息系统案中,由于被告人删除的数据与计算机信息系统安全的关联性不大,所有被删数据均存在备份,而审理法院以被告人的行为具备造成计算机信息系统无法正常运行甚至瘫痪的潜在威胁以及“一定的社会影响”认定“后果严重”,而后又因“后果严重性不是特别明显”而从轻处罚并适用缓刑,偏离了破坏计算机信息系统罪实害犯的本质属性,也反应出破坏计算机信息系统罪“后果严重”认定上的随意性。

#### (四) 适用范围过度扩张

从司法判例中还可以看出,能够被认定为破坏计算机信息系统罪的范围不断扩大,呈现一定的“口袋化”倾向。比如,上文提及的对于研发、制作游戏软件外挂程序出售或通过制作的外挂程序从事有偿代练升级的行为,司法实践存在将之纳入破坏计算机信息系统罪的冲动。43个案例中,这类犯罪行为共有7例,其中公安机关刑事拘留或检察机关指控罪名为破坏计算机信息系统罪的有6例,最终被法院认定为破坏计算机信息系统罪的仍有2例。又比如,上文提及的并无明显严重后果的删除、修改、增加计算机信息系统中存储、处理或者传输的数据的行为,也被认定为本罪。除此之外,司法实践还将以下几种行为纳入了破坏计算机信息系统罪的范围,从而使得本罪日益“膨胀”。

一是将盗用用户名和密码进入公安机关网络系统,以帮助他人消除、变更交通违章信息,或者帮他人增加户口信息而获利的行为纳入破坏计算机信息系统罪。43个司法案例中,该类行为一共有6件,均被认定为破坏计算机信息系统罪,分别是陈厦辉、章剑峰破坏计算机信息系统案、〔23〕李某某、周某某破坏计算机信息系统案、〔24〕孙小虎破坏计算机信息系统案、〔25〕武峻破坏计算机信息系统案、〔26〕杨

〔22〕 顾军、华健义:《罗露破坏计算机信息系统案——破坏计算机信息系统罪“后果严重”的认定》,载张耕主编:《刑事案例诉辩审评——扰乱公共秩序罪》,中国检察出版社2005年版,第42~47页。

〔23〕 参见泉州市丰泽区人民法院(2003)丰刑初字第183号刑事判决书。

〔24〕 参见江苏省赣榆县人民法院(2013)赣刑初字第493号刑事判决书。

〔25〕 参见江苏省泗洪县(2011)洪刑初字第0337号刑事判决书、江苏省宿迁市中级人民法院(2012)宿中刑终字第0042号刑事判决书。

〔26〕 参见江苏省溧水县人民法院(2012)溧刑初字第65号刑事判决书。

某、蒲某某破坏计算机信息系统案、<sup>[27]</sup>童莉、蔡少英破坏计算机信息系统案。<sup>[28]</sup>对于上述6个案件,尽管公安机关、检察机关的认定与法院最终认定存在部分不一致(其中,童莉、蔡少英破坏计算机信息系统案中公安机关刑事拘留和检察机关指控罪名均为盗窃,武峻破坏计算机信息系统案中公安机关刑事拘留罪名为诈骗,李某某、周某某破坏计算机信息系统案中公安机关刑事拘留罪名为伪造国家机关证件),但是从法院最终均认定为破坏计算机信息系统罪这一情况来看,对于这类行为按照破坏计算机信息系统罪处理已成常态。但是应当看到,公安系统内部网站消除、变更交通违章信息,或者帮他人增加户口信息,由于并未涉及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不可逆的操作,其消除、增加或变更痕迹均可通过计算机系统操作日志中被核查出来,且公安机关在案发后可以通过相关途径把被删除的数据恢复到交通管理综合应用平台进而恢复对相关违章车辆的处罚,故行为人对违章数据的处理行为并不必然造成相关经济损失。实际上,就连孙小虎破坏计算机信息系统案承办法官也认为,“公安机关可以通过对相关数据进行恢复以便于及时对车辆违章行为做出处罚。所有经孙小虎非法处理的车辆违章数据并没被其删除,仍然存放于电脑系统中,只是数据处理的状态发生了变化,由原来的‘未处理’变为‘已处理’,公安机关随时可以通过行使职权把有关数据恢复到未处理状态以便于对违章行为做出处罚”。<sup>[29]</sup>这种情况下,将这些行为一概纳入破坏计算机信息系统罪,就显得较为冲动。

二是将有偿删帖行为纳入破坏计算机信息系统罪。比如在曹黎、吕孝华案中,被告人曹黎、吕孝华在互联网上从事有偿非法删除各类网站帖子的网络公关工作,其通过技术手段利用网络论坛的安全漏洞,远程上传木马程序,非法获取论坛数据库内的管理员账号和密码后实施删帖行为,并以每帖500元至1800元的费用向客户收取费用,分别获利人民币9万余元和8万余元。<sup>[30]</sup>尽管法院最终认定为非法控制计算机信息系统罪,但是公安机关刑事拘留罪名为破坏计算机信息系统罪。

三是将破坏非计算机信息系统的行为认定为破坏计算机信息系统罪。比如在倪山林破坏计算机信息系统案中,司法机关将“惠普”牌HPE5100A网络分析仪认定为计算机信息系统,从而将设置致使屏幕黑屏的程序导致网络分析仪黑屏的行为认定为破坏计算机信息系统罪。<sup>[31]</sup>尽管HPE5100A网络分析仪具备中央处理器、存储器、输入接口、输出接口和控制器等硬件,能够对电子元器件等对象进行特定的信息数据采集、加工,并且按照一定的应用目标和程序对采集的数据进行处理,然后提供处理结果。但是,这仅仅说明网络分析仪具备了类似于计算机信息系统的功能,而与实际的计算机信息系统相差甚远。根据《中华人民共和国计算机信息系

[27] 参见重庆市黔江区人民法院(2013)黔刑初字第00012号刑事判决书。

[28] 参见吕梅青、朱宏伟:《童莉、蔡少英破坏计算机信息系统案》,载中华人民共和国最高人民法院刑事审判第一、第二、第三、第四、第五庭主编:《刑事审判参考》(总第86集),法律出版社2013年版,第70~75页。

[29] 冯莉:《破坏计算机信息系统犯罪中的经济损失》,载《人民司法》2013年第6期。但承办法官这一论述系针对公诉机关将被告人消除的1156条车辆违章信息所对应的罚款金额共计人民币14万余元作为孙小虎的犯罪行为造成国家经济损失(14万余元)从而认定被告人的行为“后果特别严重”这一指控的否定性解释,并未涉及对本案定性的分析。

[30] 参见海口市龙华区人民法院(2012)龙刑初字第481号刑事判决、海南省海口市中级人民法院(2013)海中法刑终字第57号刑事裁定书。

[31] HPE5100A网络分析仪是美国“惠普”公司制造的智能化电子测量仪器(宝通公司用来测量其生产的陷波器、滤波器等元器件的电参数)。该案参见江苏省无锡市滨湖区人民法院(2001)锡滨刑初字第395号刑事判决书、江苏省无锡市中级人民法院(2001)锡刑终字第213号刑事裁定书。



统安全保护条例》第2条,“本条例所称的计算机信息系统,是指由计算机及其相关的和配套的设备、设施(含网络)构成的,按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统”。通过该条可知,计算机信息系统必须由计算机和其他相关、配套的设备、设施构成,其前提是必须存在计算机。网络分析仪并不存在计算机,故无法拟制为计算机信息系统。

从上述情况来看,某一行为被纳入破坏计算机信息系统罪的解释路径主要依据两条:一是降低“后果严重”的标准,将无明显后果、仅有潜在后果、后果无法量化或者后果与计算机信息系统安全关联性不高等情形界定为破坏计算机信息系统罪中的“后果严重”。应当看到,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》(2011年8月1日,以下简称《解释》)将“违法所得五千元以上或者造成经济损失一万元以上的”认定为破坏计算机信息系统罪“后果严重”的标准之一,<sup>[32]</sup>尽管强调了“后果严重”的可量化,但也进一步弱化了“后果”与计算机信息系统安全的关联性,使得仅仅通过计算机非法获利或者造成他人经济损失而未影响计算机信息系统安全的行为极易被纳入破坏计算机信息系统罪之范围。从这个角度来说,《解释》极有可能进一步扩张破坏计算机信息系统罪的适用范围。二是对计算机信息系统功能和计算机信息系统中存储、处理或者传输的数据予以扩大解释,将计算机信息系统中的任何数据等同于该罪中的计算机信息系统或作为该罪犯罪对象的数据,并进而将对计算机信息系统数据所作的任何修改、删除、新增等行为都解释为破坏计算机信息系统罪中的“破坏行为”。正如有学者指出的,“将‘计算机信息系统功能’扩张解释为‘计算机信息系统数据’,进而,所有对于计算机信息系统数据的删除、增加、修改、干扰行为,无论是否危及计算机信息系统功能的正常运行和安全状态,都会被司法机关视为符合‘破坏计算机信息系统罪’的罪状描述,这一罪名因而被‘口袋化’”。<sup>[33]</sup>通过上述两条路径,破坏计算机信息系统罪在司法实践中获得了极强的解释力和适用力,成为网络信息时代新生的“口袋罪”。<sup>[34]</sup>

### 三、破坏计算机信息系统罪的 文本还原与规范构造

破坏计算机信息系统罪司法实践中的乱象,亟须在学理上厘清该罪适用边界,进而合理限定该罪处罚范围,提高刑法调整的精确性。但颇为遗憾的是,截至目前,我国已有的相关文献侧重于

[32] 《解释》第4条规定,破坏计算机信息系统功能、数据或者应用程序,具有下列情形之一的,应当认定为刑法第二百八十六条第一款和第二款规定的“后果严重”: (一) 造成十台以上计算机信息系统的主要软件或者硬件不能正常运行的; (二) 对二十台以上计算机信息系统中存储、处理或者传输的数据进行删除、修改、增加操作的; (三) 违法所得五千元以上或者造成经济损失一万元以上的; (四) 造成为一百台以上计算机信息系统提供域名解析、身份认证、计费等服务或者为一万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的; (五) 造成其他严重后果的。《解释》第6条规定,故意制作、传播计算机病毒等破坏性程序,影响计算机系统正常运行,具有下列情形之一的,应当认定为刑法第二百八十六条第三款规定的“后果严重”: (一) 制作、提供、传播第五条第(一)项规定的程序,导致该程序通过网络、存储介质、文件等媒介传播的; (二) 造成二十台以上计算机系统被植入第五条第(二)、(三)项规定的程序的; (三) 提供计算机病毒等破坏性程序十人次以上的; (四) 违法所得五千元以上或者造成经济损失一万元以上的; (五) 造成其他严重后果的。

[33] 于志刚:《口袋罪的时代变迁、当前乱象与消减思路》,载《法学家》2013年第3期。

[34] 43个案件裁判文书中,可以直接看出公安机关刑事拘留罪名的有21个,未明确刑事拘留罪名的有22个。公安机关刑事拘留的21个罪名中,18个为破坏计算机信息系统罪,而最终被检察机关或法院改变罪名的有11个。这说明,在公安机关阶段,破坏计算机信息系统罪的“口袋化”倾向更为明显。

对破坏计算机信息系统罪的学理分析,无论刑法理论界或司法实务界均未对破坏计算机信息系统罪之司法实践状况予以充分关注,未对其“口袋化”倾向予以充分评估,更未在实践案例的基础上形成专门性的研究成果,在很大程度上遮蔽了破坏计算机信息系统罪的实践乱象,影响了本罪研究的深入。只有从对已有破坏计算机信息系统罪实践案例的反思出发,以司法判例为基点发现问题、分析问题,才可以真正还原破坏计算机信息系统罪的文本含义与规范构造,从而为将来的司法实践提供可操作性的指引。笔者认为,这主要包括以下几个方面。

#### (一)“后果严重”的规范解释

根据《刑法》第286条,破坏计算机信息系统罪的行为方式有三种,分别为对计算机信息系统功能进行删除、修改、增加、干扰,造成计算机信息系统不能正常运行,后果严重;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,后果严重;故意制作、传播计算机病毒等破坏性程序,影响计算机系统正常运行,后果严重。从犯罪对象上来说,三种行为方式分别针对的是计算机信息系统功能、计算机信息系统中存储、处理或者传输的数据和应用程序以及计算机系统。显然,“后果严重”是三种行为方式入罪的必要条件。由于第一种行为和第三种行为“后果严重”之前分别有“造成计算机信息系统不能正常运行”和“影响计算机系统正常运行”之表述,可以得出该两种行为方式中的“后果严重”之含义必须包含对计算机信息系统本身的影响。但是,这一解释对于“后果严重”之前并无“造成计算机信息系统不能正常运行”或“影响计算机系统正常运行”之限制的第三种行为方式,是否同样适用,便成疑问。对此,有学者予以认同。比如有学者认为,这里的后果严重,是指使国家重要的计算机信息系统功能、数据和应用程序被破坏,严重破坏计算机信息系统的运行,造成重大经济损失,或者影响重要计算机信息系统正常运行,使正常的工作秩序遭到严重破坏,等等。即因计算机系统不能正常运行而造成了各种各样的严重后果。<sup>[35]</sup>还有学者针对《刑法》第286条规定的三种行为方式,分别对“后果严重”进行解读,并且在三种“后果严重”的解读中,分别加入了“使重要的计算机信息系统功能遭受损害”,“严重破坏计算机信息系统的有效运行”,“影响重要计算机信息系统的正常运行”。<sup>[36]</sup>有人则将第二种行为方式中“后果严重”的认定标准,等同于第一种行为方式。<sup>[37]</sup>而有学者则并不认同上述观点。该学者将第一种行为中的“后果严重”解读为“使重要的计算机系统功能遭受严重损害,严重破坏计算机系统的有效运行,给国家、集体或者个人造成重大损失,或者造成恶劣的社会影响等”,将第二种行为方式中的“后果严重”解读为“指使用户重要的计算机数据和资料遭到不可恢复的严重破坏,影响正常的工作和生活,因数据和应用程序被破坏而造成重大经济损失等”,将第三种行为方式中的“后果严重”解释为“影响重要计算机系统的正常运行,致使工作秩序遭受严重破坏,造成重大经济损失以及恶劣的影响等”。<sup>[38]</sup>

笔者认为,《刑法》第286条对于破坏计算机信息系统罪的三种行为方式做出了不同的文字表述,并非立法上的笔误,从1997年《刑法》新增这一罪名的起草过程来看,对于破坏计算机信息系统罪的三种行为方式的罪量要素并无争议,<sup>[39]</sup>因此,应当承认的是,《刑法》第286条中规定的三

[35] 陈兴良:《规范刑法学(第二版)》(下册),中国人民大学出版社2008年版,第814页;曲新久:《刑法学》(第三版),中国政法大学出版社2012年版,第490页。

[36] 参见郭立新、黄明儒主编:《刑法分则典型疑难问题适用与指导》,中国法制出版社2012年版,第411页。

[37] 参见周道鸾、张军主编:《刑法罪名精释(下)》(第四版),人民法院出版社2013年版,第713页。

[38] 参见邢永杰:《破坏计算机信息系统罪疑难问题探析》,载《社会科学家》2010年第7期。

[39] 参见高铭喧:《中华人民共和国刑法的孕育诞生和发展完善》,北京大学出版社2012年版,第513~514页。

种行为方式在构成“后果严重”的理解上并不完全一致。这也得到了司法解释立场的印证。<sup>[40]</sup> 据此,尽管《解释》在破坏计算机信息系统“后果严重”的规定中采取了分别解释的做法,将第一款、第二款的“后果严重”一并解释,而将第三款的“后果严重”单独解释,但是在界定第一款行为“后果严重”时,仍应同时满足“造成计算机信息系统不能正常运行”这一前置性条件,而在界定第二款行为“后果严重”时,不需要同时满足“造成计算机信息系统不能正常运行”这一条件。

但是,无论是将本罪客体解释为计算机信息系统安全,<sup>[41]</sup> 还是国家对计算机信息系统的运行管理制度和计算机信息系统的所有人与合法用户的合法权益,<sup>[42]</sup> 其首要的、主要的犯罪客体为计算机信息系统安全,因此,对于破坏计算机信息系统犯罪行为边界的划定,首先应当在犯罪客体的指引下完成。考虑到该罪名在司法判例中的扩张、本罪与其他财产性犯罪的交织性、计算机信息系统中存储、处理或者传输的数据和应用程序的多样性、删除、修改、增加的操作所引起的后果各异以及《解释》在“后果严重”上所持有的宽泛化的立场,总体上应遵循对破坏计算机信息系统罪中“后果严重”从严把握的思路。具体而言,有必要对《解释》第4条特别是《刑法》第286条第2款中的“后果严重”情形进一步限定:一是后果必须与计算机信息系统具有关联性。尽管不需要“造成计算机信息系统不能正常运行”(《刑法》第286条第1款所需标准),但是至少要影响到计算机信息系统安全。二是违法所得必须是基于删除、增加、修改等行为本身所产生的违法所得,而非通过删除、增加、修改等行为将他人的财物转为自己所有。三是造成的经济损失仅指该类行为给用户直接造成的经济损失,以及用户为恢复数据、功能而支出的必要费用。经济损失与破坏计算机信息系统行为具有直接因果关系。实施犯罪时尚未实际产生,将来有可能产生的利益损失,以及可通过数据恢复并采取必要措施避免的损失,不能认定为该类犯罪所造成的经济损失。

## (二) 计算机信息系统数据的合理解释

根据《解释》第11条,“计算机信息系统”和“计算机系统”,是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。其是一个整体性概念,并非等于计算机信息系统数据。对于计算机信息系统数据的性质,有人认为,《刑法》第286条第1款针对的对象是“计算机信息系统功能”,具体而言,主要是对计算机的系统文件进行非法操作,使系统紊乱、丧失部分或全部运行功能,甚至崩溃。第二款中的对象为“计算机信息系统中存储、处理或者传输的数据和应用程序”,具体而言,主要是对数据和应用程序(不包括系统文件和系统程序)进行非法操作,使相应的数据或程序丢失、更改、损坏。<sup>[43]</sup> 笔者认为,将《刑法》第286条犯罪对象计算机信息系统中存储、处理或者传输的数据和应用程序界定为非系统文件和系统程序,并不妥当。对于第2款中计算机信息系统数据和应用程序的解释,还是应当回归本罪犯罪客体,即计算机信息系统安全。“计算机信息系统是一个动态的数据系统,无论多么简单的操作行为,例如,打开一个文件夹,都会在后台增加一条操作记录,增加了该计算机信息系统的数据。”<sup>[44]</sup> 因此,任何在计算机上的操

<sup>[40]</sup> 最高人民法院有关人员在解读《解释》时明确指出,根据《刑法》第286条第1款、第2款的规定,破坏计算机信息系统功能和破坏计算机信息系统数据、应用程序行为的入罪要件并不相同,前者要求“造成计算机信息系统不能正常运行”,而后者不需要这一要件。因此,在司法实践中,需要依据刑法和《解释》的规定,根据具体案件情况进行分析判断,确保定罪量刑的准确。参见喻海松:《〈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〉的理解与适用》,载《人民司法》2011年第19期。

<sup>[41]</sup> 见前注[37],周道鸾、张军书,第714页。

<sup>[42]</sup> 高铭暄、马克昌主编:《刑法学》(第五版),北京大学出版社、高等教育出版社2011年版,第536~537页。

<sup>[43]</sup> 参见前注[28],吕梅青、朱宏伟文,第74页。

<sup>[44]</sup> 见前注[33],于志刚文。

作,都会对计算机信息系统数据产生影响。同样的,计算机信息系统中存储、处理或者传输的数据和应用程序也多种多样,关键是要区分该种影响的性质。对于第二款中计算机信息系统数据和应用程序,不能从形式上以系统文件、系统程序和非系统文件、非系统程序加以区分,而应从更为实质的角度,从该文件、程序对计算机信息系统安全的影响程度加以甄别,无论是系统文件、系统程序还是非系统文件、非系统程序,只要是对计算机信息系统安全有影响的,都可以认为是《刑法》第286条第2款中的数据 and 应用程序。在此,笔者认为应区分核心数据、应用程序和非核心数据、应用程序,前者系直接关系到计算机信息系统能否正常运行、关系到计算机信息系统安全的数据和应用程序,包括但不限于系统文件和系统程序;后者系计算机信息系统中无关计算机信息系统正常运行和计算机信息系统安全的数据和应用程序,比如文档、照片、自行安装的各类软件等。破坏计算机信息系统罪中涉及的数据和应用程序,必须是核心数据和核心应用程序,唯此,才能为破坏计算机信息系统罪划定合理边界,实现刑事处罚的准确性。

### (三) 利用计算机实施犯罪的认定

笔者收集的43个判例中,行为人对他人计算机信息系统中的数据予以修改、变更,直接造成他人财物受损或者谋利的行为共有10件,分别是曾亮、曾霞、杨华破坏计算机信息系统案、<sup>[45]</sup>董某某等破坏生产经营案、<sup>[46]</sup>鄢某某盗窃罪、<sup>[47]</sup>赵喆操纵证券交易价格案、<sup>[48]</sup>严峻故意毁坏财物案、<sup>[49]</sup>张某某等盗窃罪、<sup>[50]</sup>章某某等盗窃罪、<sup>[51]</sup>郑某某等盗窃罪、<sup>[52]</sup>周某某盗窃罪、<sup>[53]</sup>沈某破坏计算机信息系统案。<sup>[54]</sup>(表1)

表1 修改、变更数据致使他人财物直接受损案件类型

序号	刑拘罪名	批捕罪名	认定罪名	直观后果	行为方式	来源
1	未明确	盗窃罪	破坏计算机信息系统罪	造成电信公司损失40余万元	盗取账号和密码 修改电信公司数据 为他人宽带开通和提速	重庆市渝中区人民法院(2009)中区刑初字第854号
2	破坏计算机信息系统罪	破坏生产经营罪	破坏生产经营罪	被害单位损失6.9万元	虚假恶意订票	上海市静安区人民法院(2013)静刑初字第345号
3	破坏计算机信息系统罪	盗窃罪	盗窃罪	获利4500余元	盗取他人账号密码 通过技术手段用已过期的积分兑换礼品	上海市虹口区人民法院(2012)虹刑初字第1137号

[45] 参见重庆市渝中区人民法院(2009)中区刑初字第854号刑事判决书。

[46] 参见上海市静安区人民法院(2013)静刑初字第345号刑事判决书。

[47] 参见上海市虹口区人民法院(2012)虹刑初字第1137号刑事判决书。

[48] 参见上海市静安区人民法院(1999)静刑初字第211号刑事判决书。该案后来入选最高人民法院公报案例。参见《赵喆操纵证券交易价格案》,载《最高人民法院公报》2000年第2期。

[49] 参见上海市静安区人民法院(2004)静刑初字第35号刑事判决书、上海市第二中级人民法院(2004)沪二中刑终字第208号刑事判决书。

[50] 参见浙江省余姚市人民法院(2013)甬余刑初字第188号刑事判决书。

[51] 参见北京市石景山区人民法院(2012)石刑初字第446号刑事判决、北京市第一中级人民法院(2013)一中刑终字第115号刑事裁定书。

[52] 参见宁波市北仑区人民法院(2013)甬仑刑初字第57号刑事判决书。

[53] 参见宁波市北仑区人民法院(2013)甬仑刑初字第326号刑事判决书。

[54] 参见上海市闸北区人民法院(2008)闸刑初字第444号刑事判决书。

(续表)

序号	刑拘罪名	批捕罪名	认定罪名	直观后果	行为方式	来源
4	破坏计算机信息系统罪	故意毁坏财物罪	故意毁坏财物罪	造成他人经济损失 13 余万元	破解客户资金账号及股票交易密码后买卖股票	上海市静安区人民法院(2004)静刑初字第 35 号;上海市第二中级人民法院(2004)沪二中刑终字第 208 号
5	破坏计算机信息系统罪	盗窃罪	盗窃罪	获利 36 万余元	植入木马程序远程控制服务器,删除收银数据窃取网吧钱款	浙江省余姚市人民法院(2013)甬余刑初字第 188 号
6	破坏计算机信息系统罪	盗窃罪	盗窃罪	获利 12 万余元	侵入他人网络服务器窃取游戏币	北京市石景山区人民法院(2012)石刑初字第 446 号;北京市第一中级人民法院(2013)一中刑终字第 115 号
7	未明确	操纵证券交易价格罪	操纵证券交易价格罪	获利 7 000 余万元,造成他人损失 200 余万元	修改计算机系统中股票数据库,引起股票价格异常上涨时抛售股票获利	上海市静安区人民法院(1999)静刑初字第 211 号
8	破坏计算机信息系统罪	盗窃罪	盗窃罪	获利 1 万余元	植入木马程序远程控制服务器,删除收银数据窃取网吧钱款	宁波市北仑区人民法院(2013)甬仑刑初字第 57 号
9	破坏计算机信息系统罪	盗窃罪	盗窃罪	获利 1 万余元	植入木马程序远程控制服务器,删除收银数据窃取网吧钱款	宁波市北仑区人民法院(2013)甬仑刑初字第 326 号
10	未明确	破坏计算机信息系统罪	破坏计算机信息系统罪	造成他人损失 25 万余元	对客户信息、用电计费数据进行修改,减少电费计算	上海市闸北区人民法院(2008)闸刑初字第 444 号

可以肯定的是,无论是盗取账号和密码修改电信公司数据为他人宽带开通和提速,还是恶意订票,抑或是盗取他人账号密码通过技术手段用已过期的积分兑换礼品、破解客户资金账号及股票交易密码后买卖股票、植入木马程序远程控制服务器删除收银数据窃取网吧钱款、侵入他人网络服务器窃取游戏币、修改计算机系统中股票数据库引起股票价格异常上涨时抛售股票获利、对客户信息、用电计费数据进行修改,减少电费计算等行为,其共同点在于均通过网络完成,其行为必然会对计算机信息系统中存储、处理或者传输的数据进行一定的删除、修改或增加,影响计算机信息系统存储数据的正常管理秩序,从行为人获利或者其行为给被害方造成的损失来看,也符合破坏计算机信息系统罪中“后果严重”之条件,总体而言上述 10 个案子中的行为方式在形式上符合破坏计算机信息系统罪,这或许是公安机关介入时首选定性破坏计算机信息系统罪的原因(从表 1 可以看出,10 个案件中,公安机关明确以破坏计算机信息系统罪刑事拘留的有 7 个)。但是最终被法院认定为破坏计算机信息系统罪的仅有 2 例,即曾亮、曾霞、杨华破坏计算机信息系统案和沈某破坏计算机信息系统。其余 8 例均被认定为其他罪名。在赵喆操纵证券交易价格案中,

裁判理由对此有过表述，“被告人赵喆的整个行为，从现象上看是非法侵入了他人的计算机信息系统，修改了他人计算机信息系统中存储的数据，致使他人计算机信息系统的部分信息遭到破坏。这些表象，与刑法第二百八十六条第二款规定（即破坏计算机信息系统罪——笔者注）的犯罪行为相似。但是赵喆并非以破坏国家对计算机信息系统设立的安全保护制度为目的的实施犯罪行为，其行为主观上是想在引起股票价格异常上涨时抛售股票获利，客观上引起了股市价格的异常波动，结果也确实使自己及朋友获得了利益，而给三亚营业部造成 295 万余元的损失。赵喆的犯罪，虽然使用的手段牵连触犯了刑法第二百八十六条第二款的规定，但是侵犯的客体是刑法第一百八十二条所保护的国家对证券的管理制度和投资者的合法权益，因此构成的是操纵证券交易价格罪，不是破坏计算机信息系统罪”。<sup>[55]</sup> 由此看来，之所以认定为其他罪名，一方面是上述行为方式客观表现、行为性质、行为人主观目的均与破坏计算机信息系统罪存在差异；另一方面，在破坏计算机信息系统罪之外，也确实存在其他罪名可以更为准确地评价上述行为。

我国刑法就利用计算机实施犯罪作了提示性规定。根据《刑法》第 287 条，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，依照本法有关规定定罪处罚。据此，有学者认为，“对利用计算机病毒等破坏性程序非法占有他人财物的或者实施其他犯罪的，应当依照刑法的有关规定定罪处罚。例如，利用计算机病毒盗窃财物的，应认定为盗窃罪”。<sup>[56]</sup> 有人进一步指出，“根据上述条文规定（指《刑法》第 287 条——笔者注），凡是以计算机为工具所实施的犯罪，均应当以行为人所实施的危害行为所符合的具体犯罪来定罪量刑，构成什么罪，就以什么犯罪来追究刑事责任”。<sup>[57]</sup> 应当看到，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，往往也需要对计算机信息系统中存储的数据和应用程序进行删除、增加和修改，这种情况下，是否意味着只要是利用计算机实施的其他犯罪，就一概排除破坏计算机信息系统罪的适用空间？对此，有人认为，“行为人利用计算机实施金融诈骗、盗窃、贪污、挪用公款犯罪一般也要对计算机信息系统中存储的数据和应用程序进行删除、增加和修改。行为人金融诈骗罪、贪污罪、盗窃罪、挪用公款罪与破坏计算机信息系统罪之间形成了目的行为与手段行为的牵连关系。对此也应按牵连犯处理原则处理”。<sup>[58]</sup> 笔者认为，《刑法》第 287 条是一个注意性规定，其表明行为人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，一般按照相应的罪名（破坏计算机信息系统罪以外的罪名）处理，但是其并未完全排除破坏计算机信息系统罪的适用空间。这里最关键的还是要看行为人利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密犯罪过程中，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予以删除、修改、增加的操作，是否直接导致了严重后果。可以肯定的是，通过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行为，必然会或多或少地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予以相应操作，但是，不可能将任何对计算机信息系统中的数据施加影响的行为都定性为破坏计算机信息系统罪中的删除、修改、增加行为。如果行为人利用计算机实施金融诈骗、盗窃、贪污、挪用公款犯罪过程中对计算机信息系统中存储的数据和应用程序进行删除、增加和修改，并且这些操作已经现实地对计算机信息系统造成了严重后果，符合破坏计算机信息系统罪的构成要件，由于二者之间存在手段和目的的关系，那么就应当按照牵连犯来处理

[55] 参见前注〔48〕。

[56] 张明楷：《刑法学》（第四版），法律出版社 2011 年版，第 929 页。

[57] 赵秉志主编：《中国刑法实用》，河南人民出版社 2001 年版，第 1045 页。

[58] 柳王君、王贵东：《关于破坏计算机信息系统罪的几个问题》，载《河北法学》2002 年第 1 期。

理,择一重罪处罚。但是,对于干扰、破坏计算机信息系统后临时起意向他人索取财物的行为,或者行为人将计算机作为犯罪工具,在实施相应犯罪之后以破坏计算机信息系统的方法来消灭罪证,因存在两个相对独立的行为和主观故意,均宜按照数罪并罚来处理。

## 四、结 语

近年来,我国信息网络环境下的犯罪行为频发,给信息网络空间秩序和信息网络安全造成了严重影响。由此,破坏计算机信息系统罪受到了司法机关的某种“青睐”,在惩治危害计算机信息完全犯罪行为方面得到了较为广泛的适用。但是,由于信息网络这一公共空间的新颖化、复杂性、易变性,对于危害计算机信息安全的犯罪行为予以刑法规制存在一定程度的“进退”难题。一方面,基于当前惩治信息网络犯罪的现实需要,应当对破坏计算机信息系统罪的构成要件进行重新解释,从而发挥刑法在保护信息安全方面的积极作用;另一方面,基于刑法谦抑性和刑罚合理性的考虑,破坏计算机信息系统罪并非“万能钥匙”,有其固定的文本含义和调整范围,司法实践中不宜轻易扩张和突破,特别是在其行为本身符合其他犯罪构成要件的前提下,基于追求“定性准确”而采取的“保险式”定性,退而求其次,避开其他罪名而用破坏计算机信息系统罪囊括这些行为,尽管带来了某种司法“便利性”,但无疑不具有正当性。通过降低“后果严重”的标准和扩大对计算机信息系统数据之解释,使得破坏计算机信息系统罪在实践中呈现种种乱象,“口袋化”趋势日益明显,偏离了破坏计算机信息系统罪的文本含义和规范构造。司法实践在该问题上所表现出来的适法不统一、处罚失衡等现象,与刑法调整的公正性、精确性要求相去甚远。颇为遗憾的是,目前我国学界对这一问题并未投入足够的关注,且对于通过实证研究将大量刑事裁判文书所展现出来的刑事司法实践中的一些集体智慧加以整理或分析进而纳入到繁荣刑法理论研究和完善未来的规则构建这一刑法学研究方法运用不够充分,使得理论研究在某种程度上脱离了司法实践的需要。正是基于这种考虑,笔者收集了103份涉及“计算机信息系统”的刑事裁判文书,对其中涉及破坏计算机信息系统罪的43个司法判例逐一梳理、分析,得出了当前我国关于破坏计算机信息系统罪司法实践的第一手资料,对于该罪在司法实践中的诸多问题及其“口袋化”倾向进行了反思,在此基础上对于目前学界尚未足够关注、司法实践争议较大、新型信息网络安全观下极有可能大量适用的破坏计算机信息系统罪的构成要件进行了重新解释,提出了可行性的对策。笔者认为,这对于刑事司法实践的适法统一、完善相关刑法学理论研究,无疑是一个有益的尝试。

(责任编辑:林喜芬)