

试论我国网络刑法存在的缺陷和立法完善

□ 周 微

摘 要:网络的发展使得一个新的犯罪类型——网络犯罪应运而生。我国现行刑法对网络犯罪做出了相应的规定,但由于犯罪类型较新、相关理论相对滞后和不完善,这些规定还存在一些缺陷和漏洞,不能完全适应打击网络犯罪的现实需要,需要进一步探讨和完善。本文在介绍我国网络刑法立法现状的基础上,分析我国网络刑法存在的缺陷并提出立法改善的建议。

关键词:网络刑法;网络犯罪;立法完善

中图分类号:D914

文献标识码:A

文章编号:1671-8402(2008)12-0152-04

如果我们对我国网络犯罪立法状况加以细致考察可以看出,我国惩治网络犯罪的刑事法律体系尚未成形,仍处于探索性阶段。虽然我国正逐步加大网络安全和网络犯罪防控的力度,特别是近几年相关的立法非常活跃,但总的来说层次仍然偏低,大部分属于管理性的行政规章与司法解释。由于立法体系不完善,各个部门、层次多头管理,管理色彩浓厚,存在交叉、矛盾等很多问题。中国法学会刑法学研究会会长赵秉志就认为,“中国的网络犯罪立法活动尚处于就事论事阶段,主要集中在网络运行安全、网络经营秩序方面,关于滥用计算机行为所造成的危害,规定较少。”我国打击网络犯罪仍缺乏足够的法律依据,许多案件因此无法被法院受理,因此亟需加强相关立法,并对不合时宜的条文加以跟进式修改。

具体来说,目前我国的网络犯罪立法存在以下的不足:

一、非法侵入计算机信息系统罪所保护的範圍偏窄

《中华人民共和国计算机信息系统安全保护条例》第4条规定:“计算机信息系统的安全保护工作,重点维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的计算机信息系统的安全。”我国1997年新《刑法》将非法侵入计算机信息系统的行为规定为犯罪,但是该条明确规定侵入的是“国家事务、国防建设和尖端科学技术”三个领域的计算机信息系统,把“经济建设的计算机信息系统领域”排除在外。

许多学者提出,刑法规定的非法侵入计算机信息系统罪所侵入的“领域”狭小,与网络的发展及其在社会生活中的作用不相称。国家事务、国防建设和尖端科学技术三大领域的计算机信息系统需要刑法特别保护,但是,经济建设等重要行业中的计算机信息系统同样也需要重点保护。“事实上,计算机网络在我国经济建设中的作用越来越重要,国民经济信息化、网络化的速度在加快,近年,我国信息产业年均增长速度超过30%,以信息化带动工业化的经济发展战略的实施使我国网络经济插上腾飞的翅膀,成为国民经济持续发展的动力。从我国计算机犯罪案件的发生率看,金融行业计算机犯罪发案率占全部计算机犯罪的61%,这一点与许多其他国家情形相似,同时也充分说明大部分计算机犯罪以经济利益为驱动力不容怀疑。”^[1]

刑法将非法侵入计算机信息系统罪的犯罪对象限定为“国家事务、国防建设、尖端科学技术领域”的计算机信息系统,这在当时主要是考虑到“经济建设”的范围太宽,可能会扩大打击面。但是这样规定使得经济建设中的某些相当重要的领域得不到保护。在我国打击网络犯罪的司法实践中,由于非法侵入计算机信息系统罪将重要经济领域中的计算机信息系统排除在保护之外,使许多具有严重社会危害性的网络犯罪案件难以定性和起诉。因此,应当扩大本罪的犯罪对象,将金融、医疗、交通、航运等重要领域的计算机信息系统也纳入本罪的保护范围,加强对计算机信息

作者简介:周微,女,厦门大学法学院研究生。

系统的刑法保护。

二、制作、传播计算机病毒罪的犯罪客体错位

我国的刑法理论认为,犯罪客体就是被犯罪行为侵犯的社会关系,犯罪行为侵害的社会关系不同,其社会危害性就不同,因而其犯罪的性质也就不同。刑法分则关于具体犯罪划分的十大类,就是根据犯罪客体不同而确定的。“制作、传播计算机病毒的犯罪行为侵犯的同类客体应该是社会公共安全。社会公共安全是指不特定多人的生命、健康、重大公私财产以及公共生产、工作、生活的安全,而故意制作、传播计算机病毒的犯罪行为侵犯的犯罪客体符合‘社会公共安全’这一概念。”^[2]《中华人民共和国计算机信息系统安全保护条例》第28条规定:“计算机病毒,是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据,影响计算机使用,并能自我复制的一组计算机指令或者程序代码。”由此可以看出,计算机病毒具有感染性、潜伏性、可触发性和破坏性等四个特点。“计算机病毒对计算机信息系统和其他文件有很强的感染性,即计算机病毒可以把自身或者其变体复制于其他程序或者文件,使其在虚拟的网络世界中具有与危害公共安全犯罪中使用的爆炸性、易燃性、放射性、毒害性、腐蚀性等物品相类似的扩张力和破坏力,从而侵害不特定的计算机信息系统,危害不特定的多数公民或者单位的合法权益。”^[3]可见,计算机病毒与其他计算机破坏性程序比较,可以侵害公众利益,其社会危害性比其他破坏性程序更大,具有危害公共安全的性质。其他计算机破坏性程序,例如设备炸弹、逻辑炸弹、野兔、特洛伊木马,虽然可以破坏系统,但没有感染性,因而不具有危害公共安全的性质。

同时,根据刑法规定,故意制作、传播计算机病毒等破坏性程序,后果严重的,才能予以处罚,这在刑法理论上称为结果犯。但是由于计算机病毒的潜伏性特点,即入侵的病毒有一段时间的潜伏期,被感染的计算机信息系统不一定马上受到病毒的影响,常常经过一段潜伏期后才会爆发。“根据计算机病毒具有的潜伏性,计算机病毒在潜伏期间就已经对计算机信息系统安全形成了隐患,被感染病毒的计算机系统随时都处于危险状态,如果等待计算机病毒发作造成严重后果才予以处罚,不利于实现预防犯罪的刑法目的。”^[4]所以,故意制作、传播计算机病毒罪,应该是危险犯,即只要故意制作、传播计算机病毒足以造成计算机信息系统严重破坏的危险状态,就可以构成犯罪的既遂。这样就与危害公共安全罪可以处罚危险犯的规定相衔接。

刑法将制作、传播计算机病毒的行为与制作、传播其他破坏性程序的行为合并规定为制作、传播计算机病毒等破坏性程序罪,并将其归入妨害社会管理秩序这一同类客体中,显然是犯罪客体错位。应当将制作、传播计算机病毒的行为从制作、传播计算机病毒等破坏性程序罪中分离出来独立成罪,并归入危害公共安全罪这一类罪中,同时将该罪规定为危险犯。

三、单位犯罪主体缺失

我国《刑法》第30条规定,“公司、企业、事业单位、机关、团体实施的危害社会的行为,法律规定为单位犯罪的,应当负刑事责任。”也就是说,单位犯罪以法律有明文规定为限。而我国刑法第285条、第286条均没有规定单位可以构成犯罪主体。但是从国内外司法实践看,已经出现单位实施网络犯罪的行为。如单位为了达到不正当竞争、获取商业秘密、刺探国家秘密等目的,而实施非法侵入计算机系统、破坏计算机信息系统功能、破坏计算机数据和应用程序,或者制作、传播计算机病毒等破坏性程序的行为。同时,近年来我国颁布的《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》、《计算机病毒防治管理办法》等行政法规和规章,对于单位或者法人所实施的故意输入计算机病毒等危害计算机信息系统安全的行为,都规定可予以行政处罚。“既然单位或者法人可以作为行政违法主体并被处以行政处罚,对于危害严重的犯罪主体为什么不可以给以刑事处罚?”^[5]

单位犯罪主体在我国网络犯罪中的缺失,致使单位实施的严重网络不法行为无法可依。因此,立法者有必要明确规定单位可以构成上述几类网络犯罪,以有效规范和控制单位网络犯罪。

四、刑种单一,起刑点过低

对网络犯罪的刑罚措施,国外通常综合运用自由刑、财产刑和资格刑,有些甚至处以生命刑。而我国刑法对网络犯罪的刑罚方式仅仅规定了自由刑,没有规定财产刑、资格刑和生命刑,刑种单一。对网络犯罪没有规定财产刑和资格刑,与网络犯罪的特点不适应。网络犯罪大都以非法牟取经济利益为目的,给受害人带来巨大的经济损失。因此,在对犯罪人处以自由刑之外,应当并处罚金或没收一定财产。对单位犯罪应实行“双罚制”,即对单位主管人员和直接责任人处以刑罚,并对单位处以罚金。“财产型的处罚能在经济上惩戒犯罪人,提高计算机犯罪的潜在经济成本,有利于打击和预防计算机犯罪。”^[6]同时,一些网络犯罪人

在受到刑事处罚后,不仅没有被改造,反而从反面琢磨、总结出作案的经验,具有更大的社会危害性,因此有必要对他们的执业资格进行限制,剥夺其在一定时间之内不得从事与网络相关的职业或进行与网络相关的活动。

此外,从刑法的法定起刑点看,刑法第286条规定的破坏计算机信息系统罪“后果特别严重的,处五年以上有期徒刑”,而刑法第124条规定的破坏广播电视设施、公用电信设施罪“后果特别严重的,处七年以上有期徒刑”,同样具有危害公共安全的性质和特别严重的后果,而破坏计算机信息系统罪的法定最高起刑点较低,这就出现了罪行和处罚不适应的情况。同时,刑法第285条规定的非法侵入计算机信息系统罪的法定刑是“处三年以下有期徒刑或者拘役”。但是,根据《刑法》第7条和第8条的规定,中国公民在我国领域外犯罪的,按刑法规定的最高刑为三年以下有期徒刑的,可以不予追究;外国人在我国领域外对中华人民共和国国家或者公民犯罪,按刑法规定的最低刑为三年以上有期徒刑的,可以适用我国刑法,但是按照犯罪地的法律不受处罚的除外。因此,我国公民或者外国人在我国领域外实施的非法侵入我国领域内的计算机信息系统的跨国犯罪,由于法定最高刑是在三年以下有期徒刑,往往不能追究其刑事责任,不利于严厉打击非法侵入计算机信息系统的犯罪活动。^[7]因此,应当适当提高起刑点。

五、刑事罪名的规定不完善

根据刑法的规定以及《最高人民法院关于执行〈中华人民共和国刑法〉确定罪名的规定》的司法解释,我国刑法仅仅规定了2个网络犯罪的罪名,即非法侵入计算机信息系统罪和破坏计算机信息系统罪,利用计算机实施其他犯罪的按照刑法已经规定的相关罪名处罚。而从上文的分析中可以看出,除了刑法规定的非法侵入计算机信息系统罪仍然可以独立成罪外,破坏计算机信息系统罪应当分解为破坏计算机信息系统功能罪(即《刑法》第286条规定的“对计算机信息系统功能进行删除、修改、增加、干扰,造成严重后果的”行为)、破坏计算机信息系统数据和应用程序罪(即《刑法》第286条第2款规定的“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和应用程序进行删除、修改、增加的操作,后果严重的”行为)和故意制作、传播计算机病毒等破坏性程序罪三个罪名。而故意制作、传播计算机病毒等破坏性程序罪又可以分解为故意制作、传播计算机病毒罪和故意制作、传播除计算机病毒外的其他破坏性程序罪,并将

故意制作、传播计算机病毒罪归入危害公共安全这一类罪中。

同时,随着计算机网络的发展,犯罪工具和手段不断翻新,犯罪方式和侵犯对象不断变化,司法实践已经出现某些违法乃至足以构成犯罪的网络严重违法行为,但是由于我国刑法未作出相关的犯罪规定,因而导致无法可依,轻纵了犯罪人。我国的网络刑事立法中规定的刑事罪名已经不适应网络犯罪的变化。“犯罪问题越演越烈,已经严重威胁着社会的发展和进步。于是我们就想办法遏制它、打击它,不惜一切代价。但是,当我们试图通过法律来控制网络犯罪的时候,我们却面临一个难题:对于危害社会的网络行为如何界定网络犯罪的界限和范围,尤其是如何处理公民的自由权利和社会公共利益之间的关系。在网络刑事立法中,我们应当坚持保障公民的自由权利与保护社会公共利益有机结合的原则。法律应当在个人利益与社会利益、个人自由与社会秩序之间形成平衡,使其不偏向某一方面。”^[8]基于此点考虑,在我国刑法典中,应增设如下罪名。

(一)非法使用网络资源罪

非法使用网络资源罪,是指以无偿使用为目的,未经授权或超出授权范围占用或控制网络资源的行为。表现为不经电信部门许可私自入网,或者非法取得合法用户的计算机网络账户和密码以秘密手段使用其网络的行为。

根据最高人民法院《关于审理扰乱电信市场管理秩序案件具体应用法律若干问题的解释》第8条的规定:“盗用他人公共信息网络上账号、密码上网,造成他人电信资费损失数额较大的,依照《刑法》第264条的规定,以盗窃罪定罪处罚。”但是,非法使用网络资源不同于一般的盗窃罪。“一方面,非法使用网络资源的行为常常体现行为人突破计算机网络的安全系统,非法占用或控制计算机及其网络资源,因而这种行为不仅是窃用了服务,而且在窃用的同时也造成了计算机网络系统的安全性问题;另一方面,盗窃罪以非法占有为构成要件,而非非法使用网络资源的行为并不一定以非法占有为目的。”^[9]同时,“盗用互联网络行为所侵犯的客体不是网络本身,而是互联网络经营者的收益权,以及合法用户的使用权。经营者向用户提供网络,实际上提供的是一种服务,是一种特殊的商品。经营者付出服务劳动,是为了实现收益权;用户付出服务费用是为了得到网络的使用权。盗用网络不一定破坏网络,也不一定利用网络进行违法犯罪活动,但其行为结果却一定使网络经营者和合法使用者

蒙受财产损失,具体表现为互联网络经营者收益的减少,以及合法用户网络使用费的增多。”^[10]

因此,从刑法规范的角度看,为使刑法发挥应有的规范功能,立法者有必要将这种行为作为单独的犯罪类型予以犯罪化。在网络背景下,将针对虚拟财产的“使用”盗窃行为加以入罪化,已经成为一个迫在眉睫的事情。因此,此次刑法修正的法条设计过程中,建议增设的“使用盗窃型”新罪名“非法使用网络资源罪”,已经被纳入新的刑法修正意见草案之中。

(二)擅自中断计算机网络、通信服务罪

擅自中断计算机网络、通信服务罪,是指从事互联网信息系统的管理人员或者通信服务人员,违反国家规定,擅自中断计算机网络或者通信服务,造成计算机网络或者通信系统不能正常运行的行为。

全国人大常委会《关于维护互联网安全的决定》第1条第3款规定,“违反国家规定,擅自中断计算机网络或者通信服务,造成计算机网络或者通信系统不能正常运行”的,依照刑法有关规定追究刑事责任。但是,刑法中并没有直接规定该罪的罪名和法定刑。如何适用刑法认定罪名?有学者认为,本罪适用刑法第286条规定的破坏计算机信息系统罪的罪名。也有学者认为,该罪可能适用刑法不同的罪名。计算机网络管理人员和服务人员利用计算机技术非法侵入计算机互联网信息系统进行破坏活动,从而中断网络通信系统,对其可以适用破坏计算机信息系统罪的罪名。网络管理人员或者服务人员如果出于泄愤报复或者其他个人目的,利用职务之便中断计算机网络或者通信服务,造成计算机网络或者通信系统不能正常运行,可以适用刑法第276条规定的破坏生产经营罪的罪名。如果行为人破坏公用电信设施,危害公共安全的,可以适用刑法第124条规定的破坏公用电信设施罪的罪名。^[11]

由于刑法没有对擅自中断计算机网络、通信服务的行为作出明确的规定,对于该行为在刑法罪名的认定上存在着争议,这样不利于对该行为的刑事规范和处罚。因此,应当在刑法上增设擅自中断计算机网络、通信服务罪,对此类行为做出单独的规范,设置法定刑。

(三)窃取计算机信息资源罪

窃取计算机信息资源罪,是指以非法占有为目的,利用计算机秘密窃取他人信息资源,数额较大的行为。

计算机信息资源作为一种虚拟财产需要刑法的特别保护。“所谓虚拟财产,是指只能以数字化的方式

而存在的财产。”^[12]虚拟财产的存在方式只能是数字化,即只能以二进制的逻辑结构为存在的空间,而不能以具有时空性质的物理空间为存在方式,这种财产若离开数字化方式便不复存在。

结语

网络空间所具有的开放性和资源共享性,给掩藏其中的各种类型的犯罪行为提供了广阔的滋生空间,同时也对传统的刑法理论形成冲击,传统法律在处理网络犯罪时明显力不从心。完善我国网络犯罪立法已势在必行。刑法规范如何应对日新月异的涉及网络的犯罪并适时调整,无疑显得非常重要。这是健全现有法律体系的需要,是调整网络犯罪引起的社会冲突关系的需要,是保障网络健康发展的需要,是维护个体权利、同网络犯罪作斗争的需要,也是教育人守法、预防犯罪的需要。

注释:

[1] 刘秋香:《我国计算机犯罪刑法完善之构想》,载《河南社会科学》2007年9月第15卷第5期。

[2] 黄泽林、陈小彪:《计算机犯罪的刑法规制缺陷及理论回应》,载《江海学刊》2005年第3期。

[3] 李文燕主编:《计算机犯罪研究》,中国方正出版社2001年版,第318-319页。

[4] 李文燕主编:《计算机犯罪研究》,中国方正出版社2001年版,第318-319页。

[5] 黄泽林、陈小彪:《计算机犯罪的刑法规制缺陷及理论回应》,载《江海学刊》2005年第3期。

[6] 刘秋香:《我国计算机犯罪刑法完善之构想》,载《河南社会科学》2007年9月第15卷第5期。

[7] 黄泽林、陈小彪:《计算机犯罪的刑法规制缺陷及理论回应》,载《江海学刊》2005年第3期。

[8] 孙景仙、安永勇:《网络犯罪研究》,知识产权出版社2006年版,第192页。

[9] 孙景仙、安永勇:《网络犯罪研究》,知识产权出版社2006年版,第195页。

[10] 韩崇华:《盗用互联网络的法律问题》,载《政治与法律》1999年第3期。

[11] 参见黄泽林:《网络犯罪的刑法适用》,重庆出版社2005年版,第110页。

[12] 许富仁、庄啸:《传统犯罪对象理论面临的挑战——虚拟犯罪对象》,载《河北法学》2007年2月。

参考文献:

[1] 高惠珠:《论当代信息伦理学视阈中的“责任”伦理》,《贵州社会科学》2007年第12期。

(作者单位:厦门大学法学院,福建 厦门 361005)

(责任编辑:夏也)