资政专栏

文章编号:1008-4355(2021)04-0093-14

危害计算机信息系统安全犯罪中的“经济损失”

——以中美两国的对比分析为视角

高仕银

(中国社会科学院,北京 100732)

摘 要:“经济损失”在我国危害计算机信息系统安全犯罪中被作为衡量犯罪是否严重,行为人应否受到刑事处罚的决定性条件之一。通过对比考察中美两国关于“经济损失”的相关规定,结合两国法院判解和具体案例,对我国危害计算机信息系统安全犯罪中“经济损失”的内涵予以分析建构,分别对规定中的“给用户直接造成的经济损失”和“用户为恢复数据、功能而支出的必要费用”进行更精细的定义,以期能为司法更有力地打击犯罪和更合理地惩治罪犯及对被害人予以充分保护提供有益参考,确保刑法适用的明确精准。

关键词:价值减损;安全风险责任;合理与必要

中图分类号:DF636 **文献标志码**:A

DOI:10.3969/j.issn.1008-4355.2021.04.09 **开放科学(资源服务)标识码(OSID)**:

一、问题的提出

电子数据信息在现代社会是一种技术成果,具有同财物一样的价值。计算机数据信息作为无形物与有形实体物一样代表着一种经济财产,可以给所有或合法持有人带来经济上的利益。未经授权或没有法定原由不得侵入或侵害他人计算机信息系统及其中的数据信息,这涉及对计算机信息系统和数据信息安全及价值的保护。根据我国《刑法》第 285 条和第 286 条的相关规定,危害计算机信息系统安全犯罪的后果之一,就是导致计算机信息系统不能正常运行使用或者是其中的数据信息价值减少或灭失,进而给计算机用户或权利人造成经济损失。

“经济损失”在中美两国的规定中都被作为衡量犯罪行为是否严重的重要指标。我国相关司法解释规定,危害计算机信息系统安全造成经济损失一万元以上的,属于危害计算机信息系统犯罪入罪标准的

收稿日期:2021-04-20

作者简介:高仕银(1981),男,贵州湄潭人,中国社会科学院直属机关党委(纪委)副研究员,法学博士。

“情节严重”;美国联邦《计算机欺诈与滥用法》①中规定,行为人通过传播破坏性程序或未经授权访问计算机信息系统造成经济损失五千美元以上的,即构成犯罪。“经济损失”作为决定犯罪成立与否的重要条件,尤其是在“经济损失”这一规定本身比较模糊的情况下,有必要进行深入探讨,厘清其具体内涵,这对于更加精确地认定危害计算机信息系统犯罪、更合理地组织起对这类犯罪行为的反应以及更好地为犯罪被害人提供保护具有重要意义。笔者不揣浅陋,希望对比分析中美两国相关规定及司法案例,为我国规定中的“经济损失”的进一步完善提供参考。

二、危害计算机信息系统安全犯罪中的经济损失的规定考察

(一)我国的相关规定

在我国《刑法》中,危害计算机信息系统安全犯罪主要包括第285条和第286条规定之罪。从立法上看,我国《刑法》在1997年修订时和此后的历次修正案都没有对危害计算机信息系统安全犯罪中的“经济损失”作出规定。给“经济损失”以明确“身份”的是最高人民法院、最高人民检察院联合发布的《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》(以下简称《解释》)。“经济损失”的规定位于《解释》第1、3、4、6条和第11条,其中,第1、3、4、6条规定了“经济损失”的具体构成情况。《解释》明确了危害计算机信息系统安全犯罪的定罪量刑标准,对《刑法》第285条、第286条涉及的“情节严重”“情节特别严重”“后果严重”“后果特别严重”的具体情形作出规定。② 例如,把“非法获取计算机信息系统数据或控制计算机信息系统”“提供侵入、非法控制计算机信息系统的程序、工具”和“破坏计算机信息系统功能、数据或者应用程序”的行为造成经济损失1万元以上的,作为《刑法》第285条和第286条规定中“情节严重”和“后果严重”的一个具体量化标准。换言之,根据《解释》的规定,危害计算机信息系统安全犯罪以造成经济损失的数额作为入罪标准之一。③ 按照《解释》的规定,如果实施前述的危害计算机信息系统安全的犯罪行为造成的经济损失达到1万元以上的,属于刑法规定的“情节严重”或“后果严重”;如果造成经济损失达到5万元以上的,则是“情节特别严重”或“后果特别严重”。

值得注意的是,《解释》第11条第3款对“经济损失”进行了专门说明:本解释所称“经济损失”,包括危害计算机信息系统犯罪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。可以说,这是我国司法解释对专门术语或专项用语作出的为数不多的单独说明。同时,按照最高司法机关的有关认识,这里的“经济损失”应该是现实的,而非可期待的。需要注意的是,破坏计算机信息系统功能、数据给用户间接造成的经济损失,如用户损失的预期利益等,不能纳入“经济损失”的计算范围。④ 因此,可以说我国司法解释不但规定了“经济损失”在危害计算机信息系统安全犯罪中的存在范围、具体数额标准和主要作用,同时也赋予其一定的内涵,给司法机关在案件办理中划出了大体适用的方向。

---

① 《计算机欺诈与滥用法》(Computer Fraud and Abuse Act,简称“CFAA”)是美国联邦规制计算机网络犯罪的最重要法律,其被编入美国《联邦法典》第18编第1030条,详见:Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2018). 下文将以1030条来指代《计算机欺诈与滥用法》。

② 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,第24页。

③ 喻海松:《网络犯罪二十讲》,法律出版社2018年版,第22页。

④ 陈国庆、韩耀元、吴娇滨:《〈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《人民检察》2011年第20期,第53页。

(二)美国的相关规定

1030 条诞生于 1984 年美国国会关于计算机犯罪的立法,而该条与“经济损失”有关的规定是在 1986 年的修法中确立的,位于该条(a)(5)款。根据现行 1030 条(a)(5)款的规定,计算机犯罪的后果包括两个方面:损害(damage)和经济损失(loss)。① 不过从立法沿革上来看,损害与经济损失并非一开始就同时诞生于(a)(5)款的规定之中。在 1986 年以后 2001 年以前,该款关于危害计算机犯罪的后果规定只有损害而没有经济损失,其包含于损害的定义之内,且内涵也比较简单:实际维修和重装计算机系统或者恢复数据到其原来状态所花费的成本代价。② 2001 年遭受“9·11”恐怖袭击后,美国国会在“爱国者法案”③中将 1030 条(a)(5)款中的损害进行了修正,并把其中的经济损失与损害并列,作为危害计算机犯罪的两大后果。④ 2001 年修法不但将“损害”和“经济损失”分别加以规定,而且还重新规定了“损害”的概念,⑤并在 1030 条(e)款第 11 项对“经济损失”作出了专门的定义。⑥

经济损失能够在 2001 年得以单独规定,主要是受美利坚诉米德尔顿案(United States v. Middleton)判决的影响。⑦ 这从美国司法部对该法修正案作出法律适用指南时的解释中可以得到印证:立法机关适当地对经济损失作出专门的定义并编入法典是接受了米德尔顿案的判解。⑧ 美国国会也承认,经济损失不仅仅是限于事实上的修复也应该包括损失的计算机使用时间,重装程序和数据的成本以及完善被修改的数据的支出等。⑨ 有些给被害人的计算机信息系统不一定造成损害,但依然会被认为是导致了经济损失,这是因为,在有些场合中既没有计算机系统也没有其中的信息遭到破坏,然而存在着诸如可以让入侵者收集系统登录的有效密码的犯罪行为,而使得所有的系统使用者都必须修改密码,也使得系统的管理员致力于运用资源来重新设置系统的安全性,因此在这一过程中虽无“损害”,但是被害人却因此遭受到“经济损失”。⑩

美国将危害计算机犯罪的损害和经济损失加以严格区分,是为了更好地打击这类犯罪。因为法条对损害的定义主要是指对计算机数据、程序、系统或者储存的信息直接的物理性危害或者删除,而经济损失的定义则对那些给被害人造成的其他类型的经济上的危害铺开了一张大网。⑪ 同时,按照 1030 条(c)(4)(A)款的规定,凡是因危害计算机信息系统犯罪而给他人在一年之内造成经济损失累计达到 5 千美元以上的即构成犯罪。⑫ 换言之,行为人实施危害计算机信息系统的行为造成经济损失的数额在一

① 18 U.S.C. § 1030(a)(5)(2018).

② Senate Report No. 99-432, at 11(1986), reprinted in 1986 U.S.C.C.A.N 2479, 2488-89.

③ 该法案的全称是《以适当而必要之方式团结与增强美国遏制恐怖主义法案》,英文为:Uniting and Streng-thening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act,简称 USA PATRIOT.

④ Pub. L. No. 107-56, § 814(d)(5), 115 Stat. 384.

⑤ 根据 1030 条(e)款第 8 项的规定,“损害”的定义是:对数据、程序、系统或信息的完整性或可用性的任何削弱损伤(impairment)。

⑥ 1030 条(e)款第 11 项对“经济损失”的定义为:任何被害人的任何合理性的付出花费,其不仅包括被害人针对计算机犯罪所采取的反应与措施的成本,评估计算机损害所需的开支和将数据、程序、系统以及信息等恢复到犯罪侵害以前状态的合理费用;还包括因计算机损害失去的任何收入或付出的成本和其他因中断服务带来的损害性结果。参见:18 U.S.C. § 1030(e)(11)(2018).

⑦ 在该案中,法院判决把修补安全漏洞等所花费的成本也作为经济损失加以计算,但其要求是对安全的修复是使之与原来状况一样,而不是更安全,即任何改良的成本不能当作为造成损害的数额。参见:United States v. Middleton, 231F.3d 1207(9th Circuit, 2000).

⑧ Department of Justice, *Computer Crime and Intellectual Property Section*, *Field Guidance on New Authorities that Relate to Computer Crime and Electronic Enacted in the USA Patriot Act of* 2001. 参见:http://www.cybercrime.gov/PatriotAct.htm.

⑨ Senate Report No. 99-432, at 11-12(1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2488-89.

⑩ George Roach and William J. Michiels, *Damage is the Gatekeeper Issue for Federal Computer Fraud*, 8 Tul. J. Tech. &Intell. Prop., 71(2006).

⑪ Sarah Boyer, *Computer Fraud and Abuse Act: Abusing Federal Jurisdiction?* 6 Rutgers Journal of Law&Public Policy, 692(2009).

⑫ 18 U.S.C. § 1030(c)(4)(A)(i)(2008).

年内累计达到五千美元即构成犯罪,五千美元是入罪或担责的门槛。[①] “经济损失”被单独规定并赋予其具体内涵和认定的数额标准后,美国法院在实践中又根据不同情况形成了较为丰富的判解,下文将在“经济损失的认定”分析中予以阐述。

(三)中美两国规定的对比分析

从上述中美两国关于危害计算机信息系统安全犯罪“经济损失”规定的梳理考察,可以看到两国为了更加严厉地打击计算机犯罪,都通过专门规定来确立“经济损失”的内涵,并且都将其作为入罪标准之一。特别是在美国,对“经济损失”在法条上从融合规定到单独列出,前后经历了15年,体现了美国立法和司法机关在这一问题上不断积累经验、提升认知和逐渐定型完善的过程。因此,从“经济损失”的内涵上,我们可以看到两国规定中有如下一些比较明显的差别。(1)计算的范围不同。我国司法解释所称的经济损失主要包括两个方面:犯罪行为给用户直接造成的经济损失和用户为恢复数据、功能而支出的必要费用;美国刑法规定中的损失包括四个方面:针对计算机犯罪所采取的反应措施的成本、聘请专业人士评估计算机受损而花出的费用、恢复计算机到受损前状态的合理费用以及因计算机受损带来的应有经济收入的流失。(2)涉及的被害对象不同。我国司法解释中所指的遭受损失的被害人是指计算机用户,主要是计算机信息系统的合法用户;[②]而美国刑法规定中损失的被害人不仅仅是指计算机用户,还包括因计算机犯罪而遭受损失的任何被害人。

通过对比考察可以看出,美国刑法规定中的“经济损失”在内涵上要比我国司法解释中“经济损失”更宽泛,其不但包括了因危害计算机信息系统造成系统本身及数据信息的损失还涉及评估和收入等方面的计算。同时,还值得注意的是美国刑法规定的经济损失在层次上更丰富一些,各项都有一定的涵摄范围,比如同样关于“恢复数据、功能”的表述,美国规定中将“恢复”限定为“受损前的状态”;我国司法解释没有对此做进一步的要求,只是以“必要费用”作为限制。这就使得一些用户如果在“恢复”过程中出现过度的情况下,即把数据、功能等恢复得比受损前的状态更优的情况下的花费,是否能算入“经济损失”,不无争议。另外,我国司法解释中关于“给用户直接造成的经济损失”这一表述也比较模糊,直接造成的经济损失是包括因计算机受到破坏而导致的经济收入的减少还是计算机受到破坏或损害本身的价值损失等,从这一规定并不能得出明确的结论。我们也应当看到,在美国的规定中,对经济损失的计算还包括“因计算机损害失去的任何收入”,这存在着较大的解释空间,不利于司法上的明确决断和对经济损失的合理计算,因为这可能导致在实践中将一些预期性的利益或收入也被纳入计算,从而超出了对犯罪本身的评价范围。

三、“经济损失”的司法认定分析

(一)美国法院关于“经济损失”认定及分析

如前文所述,美国2001年修法单独规定计算机犯罪造成的“经济损失”并明确其具体内涵之后,在司法实务中针对这一规定如何具体认定形成了一系列的重要判解,比较有代表性的有如下判例。在“美利坚诉米尔特案”(United States v. Millot)中,一名已离职的雇员侵入前公司计算机系统中删除了该公司另一名雇员的账户。该公司一直将其计算机安全防护外包给IBM公司。案发后,IBM公司的两名技术

① Mitchell Waldman, *Civil Actions*, *Enforcement*, *and Liability*; *Disciplinary Actions*, American Jurist 2D Computers and the Internet, 85 (2007).

② 喻海松:《网络犯罪二十讲》,法律出版社2018年版,第22页。

人员用了 407 小时来修复被删除的账户以及其他问题。受害公司之前与 IBM 公司签订的协议是两名员工全职负责受害公司的计算机安全,IBM 公司支付给员工每小时 50 美元薪酬。控方以 407 小时乘以 50 美元每小时得出 20350 美元的损失数额。被告人提出抗辩认为这一计算不成立,因为技术员是全职工作,即使没有被告人的侵害发生,他们也要从事其他安全职责,IBM 也要付出同样的薪酬。联邦第八巡回法院采纳了控方的意见,认为虽然受害公司已经定额外包安全问题给 IBM,但经济损失依然可以按照控方提出的标准来计算。① 在“Nexans Wires S. A v. Sark-USA, Inc. 案”中,原告是一家德国公司。被告公司的员工侵入到原告公司计算机信息系统窃取了该公司相关生产精铜和光纤的资料并用来开办新公司与之竞争。在判决中,法院认为德国公司的两名主管经理从德国飞美国的费用不能算作是“经济损失”,证据表明主管经理的到访是讨论被窃取的信息而非计算机受到的潜在危害,如果他们在纽约检测其中的一台计算机,则旅途费用都可以算在“经济损失”数额中。法院还否决了原告公司诉称的因数据被窃而失去了两个商业机会的价值也算入损失之中。理由是法条规定的“收入损失”必须是因计算机系统中断服务而造成,但本案中原告并没有诉称受侵入的计算机不能运行。②

在“B&B Microscopes v. Armogida 案”中,一个名为阿姆吉达的雇员在 B&B 显微镜公司(以下简称 B 公司)工作时为 B 公司开发了一套很有价值的 K 软件系统用于出售给客户。由于某些原因,阿姆吉达辞职并认为 K 系统属于他个人而非 B 公司,于是在离开前他将公司配发给他使用的笔记本电脑中的几千个文档进行了“选择性的删除和复写”。③ 随后,阿姆吉达将 K 系统的复件以 1 万美元卖给了犹他州政府。B 公司聘请了一家技术公司来检测该笔记本电脑,发现阿姆吉达对他所开发的 K 系统中的文件实施了删除和复写行为。在 B 公司中只有阿姆吉达才能使该系统正常运转。阿姆吉达的这一行为使得 B 公司的笔记本电脑以及客户的系统遭受到了“损害”,因为行为人对于“计算机系统、程序等的完整性和可用性造成了削弱损伤”。B 公司提出遭受到 51400 美元的损失,并诉称根据以下项目得出:聘请技术公司论证分析和修复 K 系统花费 1400 美元,在一年之内失去的销售 K 系统的预期收入 5 万美元。法院判决认定 B 公司损失了 11400 美元,其中 1400 美元是聘请技术公司的支出,1 万美元是由于 K 系统文件被删除和复写而遭受损害且 B 公司无法复制该系统产生的“服务中断”所带来的经济损失,并以被告人卖给犹他州的复件价值来计算。④

上述美国法院对“经济损失”认定的判解,虽然侧重不一,但共同点都在于要求认定“经济损失”时对相关数额的计算必须是“合理的”(reasonable),这主要源于米德尔顿案判解的创造。不过从法条的原文来看,该定义并没有指明“合理”的具体内涵。换言之,究竟是那些列举在法条中的关于损失计算的各种类型本身就被立法机关认为是合理的还是在这些列举的类型中当进行损失的计算时必须仔细检查其涉及的价值是否合理。⑤ 米德尔顿案的判决意见认为应该是后一种的合理性,能作出这一说明的是该案法院所赞同的对陪审团的指引:“在逻辑上要排除陪审团认为是过多的任何支出”。⑥ 虽然法院判决要求对“经济损失”的计算必须是“合理的”,但如何才能确定是“合理的”,法院并没有加以详细说理,在美国学界则主要有两种主张。

一种是从刑法上的因果关系来看损失合理性的计算。比较有代表性的观点认为:法律上考虑的问

① United States v. Millot, 433 F. 3d 1057(8th Circuit, 2006).

② Nexans Wires S. A v. Sark-USA, Inc., 319 F. Supp. 2d 468(S. D. N. Y. 2004).

③ B&B Microscopes v. Armogida, 532 F. Supp. 2d 744, 749(W. D. Pa. 2007).

④ B&B Microscopes v. Armogida, 532 F. Supp. 2d 744, 758(W. D. Pa. 2007).

⑤ Orin S. Kerr, *Computer Crime Law*, 2nd ed., West, a Thomson business, 91(2009).

⑥ United States v. Middleton, 231F. 3d 1207, 1215(9th Circuit, 2000).

题是看是否由法定禁止的行为引起了(caused)经济损失,刑法上的因果关系原理通常都不会要求被害人的遭遇是否合理,唯一考虑的问题是禁止的行为与导致的结果之间是否存在"除非"(but for)和"直接的"(proximate)关系。基于此,被告人通常都必须因犯罪行为而对被害人负责。例如,犯罪人抢劫老太太,老人因身体虚弱而死于遭抢时的过度惊吓,罪犯不可能逃脱老人死亡的刑事责任;尽管同样的抢劫对于年轻妇女而言不会导致惊吓死亡。被害人只有在参与到不可预见的行为中,且该行为打破了原有的因果关系链并在行为与结果的可罚性之间有所作用时,才可以考虑被害人的因素。① 因此,从刑法上的因果关系原理出发,这类观点对"经济损失"定义中的"合理的"要求表示质疑。

与之相反,第二种观点认为将计算机再安全化之类的支出归入经济损失的范围并不合理,认为应当排除安全性提高的成本作为"经济损失"的计算范围。主要提出两点理由:一是在计算机犯罪语境下,1030条的规定使得入侵者要为计算机所有人随意地对他们自己数据信息安全性的忽视而负责。大多数的公司企业都意识到他们计算机系统存在安全缺陷,但却忽视这一危险。因而选择适当程度的安全性是机主的职责,社会并不认为谴责入侵者为安全性的支出负责是妥当的。当然,对于那些技术高深的黑客而言,可以突破良好的安全防护,但1030条这样规定对于一般的入侵者从普通的安全漏洞攻入而言并不公平。二是将再安全的支出费用等算到入侵者头上会使得形成犯罪的核心基础与再安全费或调查费的起因之间出现脱节(disjuncture)。当计算机信息系统被发现受到入侵,系统管理员都会竭力追踪入侵者是怎样获得访问的。当安全漏洞被发现并得到控制以后,管理员的工作并未结束,应该检测所有的与这一漏洞有关的其他部分是否安全,以确保不会再受到侵入。但很多受害的公司都是忙于收集证据和进行调查并将这些算作是因损害的发生而导致的经济损失。因而,计算机的入侵者最终受到刑事追诉是因为被害人的调查所产生的费用。②

总体来看,上述两种观点都试图从两个侧面来明确经济损失定义中的"合理性"是否合理,虽然都有一定的道理,但是法条的规定有时只能选择符合大众公平的折中,从而实现宽严相济。正如米德尔顿案的判解所体现的那样:被害人不能以一个小的安全问题受到侵害为借口就升级其计算机的安全性,使得花费的"损失"数额达到五千美元以上,从而突然将一个轻微的安全漏洞攻击行为变成一项重罪。③ 从上述法院判解中,可以概括出其关于"经济损失"的具体认定主要包括三个方面的内容:一是对计算机信息系统损害(包括数据恢复、信息重建等)本身修复的必要成本;二是算入的损失必须是与计算机信息系统危害本身直接相关的合理工作成本;三是对计算机信息系统中数据信息的经济损失的计算除了包括因损害导致的维修成本外,还包括且限于数据信息本身的价值(以市场交易价值为参考),而不包含预期的可能收益。

(二)我国司法实践中关于"经济损失"的认定检视

根据实务部门的有关研究来看,在实践中危害计算机信息系统安全犯罪经济损失的认定同其他财产犯罪相比,存在以下三个显著的特点④:第一,被害单位与司法机关认定的数额存在重大差异。侵犯计算机的犯罪行为会导致损害后果的多样性、程度的差异性、评估的技术性以及责任的不确定性,涉及不同层级被害人、同一层级多名被害人、多次侵害被害人的认定,因此实际损失的大小与范围确定非常困

① Orin S. Kerr, *Computer Crime Law*, 2nd ed., West, a Thomson business, 91(2009).

② Reid Skibell, *Cybercrime & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 Berkeley Technology Law Journal, 929-31(2003).

③ United States v. Middleton, 231F. 3d 1207, 1213(9th Circuit, 2000).

④ 刘惠、邓超:《计算机犯罪经济损失认定的实证解析》,载《检察调研与指导》2016年10月辑刊,第84-85页。

难。同时,经济损失的确定也缺乏客观明确的标准。具体反映到司法实践中,体现为被害单位、公安机关、检察院和法院对于经济损失数额的认定存在重大分歧。第二,被害单位与司法机关认定的内容存在显著差异。原因在于经济损失的内容具有多样性,直接经济损失和间接经济损失的计算范围和计算标准存在明显区别。被害单位认定遭受的经济损失一般包括被损毁数据费用、人力资本支出、应得利益受损、司法成本和防卫安全支出等方面。被害单位往往倾向于将所有与计算机相关联的损害结果均认定为犯罪嫌疑人的行为所致,而司法机关则需要甄别经济损失计算方法是否科学合理。实践中,司法机关对于被害单位提供的经济损失的内容往往未全部认定,甚至在部分案件中全部未予认定。第三,计算机犯罪与一般犯罪的证据采信标准差距较大。在计算机犯罪中,认定存在经济损失的证据主要包括:被害单位提供的证人证言,证明存在财产损失的情况说明及相关票证等书证,会计师事务所出具的司法会计鉴定意见书、损失鉴证报告、评估报告书、司法鉴定检验报告书、资产损失鉴定评估报告,价格认证中心出具的价值认证书、估价认证结论等。在财产犯罪和经济犯罪中,认定财产损失的主要证据为鉴定意见,通常情况下,鉴定意见因其科学性和客观性而具有很高的证明效力。在计算机犯罪中,对经济损失的鉴定意见采信率则相对较低,未予采信或部分采信的现象较常见。

应当说,上述归纳非常确切中肯,较为客观全面地反映了我国司法实践部门在“经济损失”认定上的现实状况。不过,与其讲这是司法实务部门关于认定“经济损失”存在的三大特点,不如说是三大难点。在我国,自《解释》明确将“经济损失”规定为危害计算机信息系统犯罪的入罪标准之一以来,由于“经济损失”本身内涵比较简单,《解释》在第 11 条第 3 款用一句话予以“解释”之外,也没有再给予更多的解释,同时也没有权威典型案例判解予以指引。因而在实务中形成了“何人受损不易确定、多少人受损不易确定、损失大小也不易确定”①等系列难题。另一方面,有关危害计算机信息系统安全犯罪“经济损失”的认定及其研究成果在我国也非常少,这一问题没有得到深入的探讨,未能给司法实践提供有效参照借鉴。

尽管如此,在我国司法实践中对于“经济损失”的认定,一些法官、检察官还是结合案例敢于担当地提出了一些非常积极的观点。如有学者认为,根据《解释》的规定,“经济损失”具体而言包括:(1)危害计算机信息系统犯罪行为给用户直接造成的经济损失。对于非法获取计算机信息系统数据犯罪而言,合法用户获取该数据应当支付的费用属于行为给用户造成的经济损失;对于通过非法控制计算机信息系统使用的计算机信息系统资源,合法用户使用该计算机信息系统资源应当支付的费用属于行为给用户直接造成的经济损失;计算机信息系统不能正常运行期间支付的网络宽带费用等合理支出费用。(2)用户为恢复数据、功能而支出的必要费用。在计算机信息系统功能或者数据破坏后,通常需要采取各种应急响应措施使其恢复到正常状态,如对被删除的数据采取数据恢复措施,被拒绝服务攻击的网站增加数据分流设备、增加带宽等,都属于造成的经济损失。② 有学者指出,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。③ 也有学者指出,经济损失应与破坏计算机信息系统行为具有直接因果关系。④ 还有学者从《解释》给定的内涵着手,对“给用户造成直接经济损失”和“用户为恢复数据、功能而支出必要的费用”

① 刘惠、邓超:《计算机犯罪经济损失认定的实证解析》,载《检察调研与指导》2016 年 10 月辑刊,第 84 页。

② 喻海松:《网络犯罪二十讲》,法律出版社 2018 年版,第 22-23 页。

③ 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,第 70 页。

④ 吴波、俞小海:《破坏计算机信息系统罪的司法适用中,争议性问题集中于——怎样理解“后果严重”与“计算机信息系统数据”》,载《检察日报》2019 年 4 月 19 日,第 03 版。

的具体情况进行了分门别类的具体认定。[①] 这些无疑都是很好的探索和经验积累,有利于对“经济损失”认识的不断深化和认定的不断精准。下文结合张某犯破坏计算机信息系统罪和程某林犯非法获取计算机信息系统数据罪来检视我国司法实践对“经济损失”的认定。

基本案情1[②]:被告人张某通过拒绝服务攻击方式(DDOS),对新浪互联信息服务有限公司UT网络服务器进行攻击,造成该公司UT服务器堵塞,无法提供网络服务,总时长达500余分钟,经鉴定经济损失达人民币48.42万元。被告人张某认可指控罪名,但对攻击时长500余分钟及由此造成的经济损失48.42万元提出异议,辩称攻击总时长为100分钟左右,损失数额不应全部承担。其辩护人认为:张某对新浪公司UT网络服务器攻击的总时长应是在240分钟至270分钟之间,并非控方指控的500余分钟,现有证据无法证实张某的攻击行为会造成新浪网广告页面、博客等业务的损失,同时不排除他人也在攻击新浪网。

北京市海淀区人民法院认为,对张某破坏计算机信息系统罪的指控成立。对于攻击时长及经济损失数额的认定,通过对被告人张某的供述与控方当庭出示的受攻击端口流量图的分析,可以证实被告人张某第一次的攻击时长为两个小时左右,第二次攻击时长为335分钟,因此控方所提供的第一份评估报告中所显示的攻击时长为465分钟是具有事实依据的,法院予以认可。对该份评估报告所得出的经济损失数额为人民币196875.2元的结论亦予以认可。但由于被告人张某声称第二次攻击结束后,后续的攻击总时长仅有十余分钟,次数亦很少,而控方所提供的这一期间新浪UT服务器所受攻击时间长度、次数的证据未能充分证明哪些攻击系由被告人张某实施,因此控方关于这一期间张某的攻击时长为118.7分钟,以及由此造成的经济损失额为人民币287251.61元的结论,法院不予认可。最后,北京市海淀区人民法院结合张某与受害公司达成民事和解并积极赔偿等情况,判决被告人张某犯破坏计算机信息系统罪,判处有期徒刑一年六个月。

通过上诉案例可以看出,在造成经济损失的数额认定问题上虽然控辩双方存在着较大的分歧,但对于经济损失的内容则并没有多大异议。这些经济损失都是指新浪公司UT服务器遭受张某通过拒绝服务攻击方式攻击后因全面堵塞,无法对外提供网络服务而造成的营业上的经济减损。因为在该案中关于损失的证据为,经相关机构评估,第一次攻击被害公司通讯软件产品UT遭受连续攻击所造成的直接损失金额为人民币19.69万元,第二次攻击被害公司通讯软件产品UT遭受连续攻击所造成的直接损失金额为人民币28.73万元。法院在认定造成经济损失的数额时,并没有具体确认最后的损失总额,而是按照最有力证据证明的最低损失额度为标准判定张某的行为符合刑法规定上的“后果严重”。虽然本案的判决是在2011年两高出台的司法解释之前,但是在该案中的经济损失及其认定对于我们理解《解释》中的“给用户直接造成的经济损失”具有重要的参考价值。司法解释中的规定一部分是源自司法实践中的有益经验,在理解新的解释内涵时,不可忽视既有判决的结论,尤其是一些典型的重要案例。因此,我们认为《解释》中的“直接造成的经济损失”就是指因计算机信息系统受到破坏或干扰等而导致的应有经济收入的减损。

基本案情2[③]:被告人程某林系深圳市科脉技术股份有限公司(以下简称“科脉公司”)员工,负责软件研发工作。2018年4月至11月22日期间,被告人程某林下载并运行Teamviewer12远程控制软件,利用其个人笔记本电脑远程控制公司工作电脑并访问公司服务器,在工作环境下未经公司授权并绕开公

① 刘惠、邓超:《计算机犯罪经济损失认定的实证解析》,载《检察调研与指导》2016年10月辑刊,第86-87页。

② 张某破坏计算机信息系统案,北京市海淀区人民法院(2008)海法刑初字第3461号刑事判决书。

③ 程某林非法获取计算机系统数据案,深圳市中级人民法院(2019)粤03刑终1735号刑事判决书。

司的代码安全防护措施,私下将科脉公司服务器中“快食慧”“好餐谋”等软件源代码使用屏幕拷贝方式复制到个人笔记本电脑,后又将软件源代码上传至个人微信中。科脉公司于2018年11月上旬接到举报并聘请专业公司对代码被窃进行技术安全检查,支付费用人民币2.12万元,同时向公安机关报案。经鉴定,程某林个人笔记本电脑中的“快食慧”“好餐谋”软件源代码与科脉公司“快食慧”“好餐谋”软件源代码的相似率为99.92%。深圳市南山区人民法院于2019年6月6日作出《(2019)粤0305刑初735号刑事判决》,认为程某林违反公司规定,绕过公司多种防范措施,将软件代码和文档非法获取后存储在个人电脑中,并因此导致公司聘请网络安全单位对其行为进行查找、发现漏洞,给公司造成经济损失,情节严重,判决被告人程某林犯非法获取计算机信息系统数据罪,判处有期徒刑一年四个月,并处罚金人民币一万元。

程某林提起上诉,认为原审判决认定事实不清,适用法律错误。辩称其是为学习、工作及研究的方便才获取涉案计算机信息系统数据,起诉书将科脉公司聘请专业公司对代码进行技术安全检查,支付2.12万元作为科脉公司的经济损失进行指控,不属于《解释》第11条规定的“经济损失”。深圳市中级人民法院认为,上诉人程某林非法获取科脉公司的软件源代码,导致科脉公司聘请第三方对源代码被窃进行技术安全检查并支付人民币2.12万元,已达到《解释》第1条第1款第(四)项之情节严重的规定,其犯罪动机以及是否将获取的源代码出售获利,均不影响构成非法获取计算机信息系统数据罪的认定,于2019年9月30日作出《(2019)粤03刑终1735号刑事判决》:依法裁定驳回上诉,维持原判。

上述程某林案涉及的具体罪名是我国《刑法》第285条第2款规定的非法获取计算机信息系统数据罪。设立该罪的主要目的,是保护计算机信息系统中有关数据的使用安全和独有或专有价值,他人未经授权或许可,不得随意获取这些数据,表明了数据所有或使用的排他性。其中,规定的“获取”不限于对数据的复制、拍照、刻录转化乃至“死记硬背”等,只要将数据从储存的计算机信息系统或有关介质中使用不当手段形成同样的信息样态,并且这一样态完全不受原数据正当所有人或使用人的控制,而能够被非法获得者支配使用,就应认为是获取。本罪属于结果犯,即不但要求行为人违反有关规定侵入计算机信息系统,还要获取到计算机信息系统中存储、处理或传输的数据。

从程某林实施的行为看,其明知公司对所研发软件采取多种手段进行严格保密的情况下,依然无视公司规定,通过远程控制软件介入公司电脑,绕过公司设置的多种防范措施,采取屏幕截图的方式,将公司的软件代码和文档非法获取后存储在个人电脑中,符合非法获取计算机信息系统数据罪的构成要件。无论其是出于学习、工作及研究的方便,还是其他想法,在所不问。因为《刑法》第285条只规定了非法获取的构成要件,并没有规定诸如牟利或其他要求,一旦非法获取到数据,犯罪即既遂。因此,从这一点来看,一审和二审法院的认定无疑是恰当的。问题的关键在于,一、二审法院据以认定的科脉公司聘请专业机构进行安全检查花费的2.12万元是否属于经济损失,不无疑问。因为,这既涉及对“经济损失”的准确理解,更涉及程某林的行为是否“情节严重”,应否定罪处刑。一审法院并未就此展开深入分析,二审法院针对程某林上诉提出的“2.12万元不属于经济损失”的辩解也未充分论证。因此,只有对《解释》规定的“经济损失”内涵进行必要的厘清,才能进一步认定程某林的行为是否构成相关犯罪。

依照《解释》第1条第1款的规定,构成非法获取计算机信息系统数据罪规定中的“情节严重”至少包括四种情形之一:第一项,获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组以上的;第二项,获取第一项以外的身份认证信息五百组以上的;第三项,违法所得五千元以上或者造成经济损失一万元以上的;第四项,属于兜底条款,即其他情节严重的情形。从上述程某林案来看,在其行为符合非法获取计算机信息系统罪的构成要件的同时,是否达到“情节严重”的标准,则要看其是否符合上述四种情形之一。很明显,第一项和第二项不符合,唯有可能的就是第三项,有违法所得或造成经济损

失。经济损失数额和违法所得数额都是破坏计算机信息系统犯罪中定罪量刑的标准,公安机关、检察机关对上述两个数额都应当进行侦查和指控。[①] 按照这一认定思路,程某林在获取到科脉公司服务器中的“快食慧”“好餐谋”等软件源代码后,先是将其存放于个人笔记本电脑中,后又将软件源代码上传至其个人微信。至案发时,程某林自始至终并没有将获取到的“快食慧”“好餐谋”等软件源代码予以出售或用作其他用途而获得相应的收入或任何其他利益。因此,违法所得的认定排除,剩下的就是造成经济损失。从《解释》第11条第3款给“经济损失”的确立的内涵来看,认定为“经济损失”,符合三个条件之一即可:一是给用户直接造成经济损失;二是用户为恢复数据支出的必要费用;三是用户为恢复功能支出的必要费用。三个条件满足其一即可认定造成的经济损失,但三个条件应该也可以叠加认定造成“经济损失”的总数。

(三)司法认定的启示

从美国法院关于“经济损失”认定的判解和学界关于对“经济损失”计算的“合理性”的不同主张,可以看出,司法实践中要准确的厘定“经济损失”的具体范畴,需要在遵循法条规定的基础上结合具体案例形成对“经济损失”含义的不同要件的单独体系性的判解(比如对数据信息损害的修复成本认定的判解、数据信息的具体价值认定的判解、计算机信息系统危害有关的工作成本认定的判解等),从而将“经济损失”定义中的核心要件部分都以具体案例判解来解释和确定具体内涵。概而言之,“经济损失”在美国除了立法给予其单独规定并赋予具体内涵之外,还通过判例来不断发展丰富,形成了——立法“条文定调”指明主要方向——司法“判例定型”形成具体结论——的模式,使得对“经济损失”的认定不断与时俱进,越发清晰和全面。同时,从美国法院判解中还可以看出,虽然法条规定经济损失的计算包括“因计算机损害失去的任何收入”,但法院对此保持了相当谨慎的立场,对可能的预期性收入没有予以确认,也是受到了学界关于“合理性”不得额外增加被告人负担主张(即前述第二种)的影响。因此,美国这种对经济损失先通过立法进行内涵丰富的定义,再通过司法对内涵中各个类型的具体丰富的做法,对我们认定相应犯罪的经济损失具有一定的参考价值。

结合上述分析,并从“程某林案”的司法认定来看,科脉公司被程某林通过远程屏幕截图复制的“快食慧”“好餐谋”等软件源代码的原数据依然在科脉公司服务器中完好的存储着,没有受到任何的损害,并且“快食慧”“好餐谋”等软件源代码的有关功能也未受到任何影响。因此,在该案中不需要对数据被复制后进行恢复,也不用对有关功能进行修补,也即不会产生相关任何费用。按照《解释》关于“经济损失”的规定来看,本案中涉及的2.12万元的安全检查费用,可以明确判断其不属于科脉公司为恢复数据或有关功能而支出的必要费用。问题的焦点在于,这2.12万元是否属于“给用户直接造成经济损失”?一般而言,给用户造成直接的经济损失应当是行为人实施危害计算机信息系统的犯罪行为后,在用户未采取有关补救措施之前致使用户因计算机信息系统受到侵害或暂停服务产生的实际的现实损失。具体到本案中,就是看程某林在复制“快食慧”“好餐谋”等软件的源代码后,是否给科脉公司因代码被复制而造成经济上的减损。这既包括源代码被出售的获得的价值,也包括源代码被他人使用而产生的经济价值,但不包括可能会带来的预期收益。事实上,程某林复制代码后,并没有出售,也没有本人使用或转给他人使用,因此并没有让科脉公司蒙受任何直接的经济损失。至于科脉公司发现“快食慧”“好餐谋”等软件源代码被程某林复制后,而聘请专业公司对该公司的服务器相关日志进行分析和安全检查鉴定,属于后续的防控行为,其产生的2.12万元技术协查服务费并不能认定为属于《解释》规定中的“经济损失”。因此,在本案中程某林的行为虽然符合非法获取计算机信息系统数据罪的构成要件,但因为达不

① 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,第72页。

到《解释》规定的“情节严重”标准,可以免予刑事处罚,采用相关的非刑罚处罚措施。通过以上检视分析,我们认为,可以对我国规定中的“经济损失”分别从“给用户直接造成的经济损失”和“用户为恢复数据、功能而支出的必要费用”两个方面的内涵再予以细化明确。

四、我国危害计算机信息系统犯罪中“经济损失”的完善思考

在对我国危害计算机信息系统犯罪中“经济损失”相关规定进行完善建构的同时,必须要看到传统财产犯罪与危害计算机信息系统犯罪中“经济损失”的差异,否则就没有必要对危害计算机信息系统犯罪中“经济损失”进行单独认定和建构。传统的财产犯罪中,如盗窃、抢(夺)劫、诈骗等,一般情况下都主要是因侵财行为而导致被害人的财产在价值上受到减损,从而表现为经济损失。总的来说,侵犯财产罪的构成要件结果是使被害人财产遭受损失。① 因此,我国《刑法》对于传统的财产型犯罪,起刑点都主要是以“数额”作为参照,以“数额较大”作为犯罪成立的标准,而司法解释更是以明确的数字划定了“数额较大”的具体内容。例如盗窃罪,盗窃公私财物价值 1000 元至 3000 元以上就是《刑法》第 264 条规定的“数额较大”。虽然刑法规定了“数额较大”作为传统侵财犯罪的入罪标准,但是法律规定上或司法解释确定的“数额”是否为犯罪导致的经济损失,不无疑问。就常态化的取财行为而言,取得财物往往意味着被害人失去财物,财物的数额就是被害人损失的数额,将“数额”与“损失”等同也没多大疑问。② 但是传统财产犯罪导致的“经济损失”,单从财物的数额来看似乎不太完整,具体应包括哪些内容,还需要进一步予以厘清。

从我国《刑法》规定来看,对于因犯罪而导致经济损失的有关规定在总则中有所体现。《刑法》第 36 条第 1 款规定,由于犯罪行为而使被害人遭受经济损失的,对犯罪分子除依法给予刑事处罚外,并应根据情况判处赔偿经济损失。这里规定的“由于犯罪行为而使被害人遭受经济损失的”,既包括由犯罪行为直接造成被害人物质损失的,如毁坏财物、盗窃、诈骗等直接侵害财产的犯罪行为,也包括由于犯罪行为的侵害间接造成的被害人经济上的损失,如伤害行为,不仅使被害人身体健康受到损害,而且使被害人遭受支出医疗费用等经济损失。③ 从这一论述来看,其对《刑法》第 36 条第 1 款规定中犯罪行为人导致的经济损失分为直接损失和间接损失两部分。直接侵害财产就是侵财行为直接导致的财物本身经济价值数额的减损。例如,在盗窃罪中,盗窃数额指的是损失数额(而非获利数额),且损失数额以被盗财物本身的价值为上限。④ 间接损失则是指与财物本身经济价值无关的但是与侵财行为有联系的经济上的损失,比如抢劫罪中导致的人身伤害而形成的医疗费用等。但从侵财犯罪的本体来看,其中导致的经济损失主要是指直接的财物本身的经济价值。在财产损失判断过程中,应当排除非物质性主观价值和利他主义目的的商品化和经济化。⑤ 在传统的侵财型犯罪中,经济损失的内涵主要限于财物本身的经济价值即财物数额,一般存在着“此消彼长”的关系(即被侵害一方所失,就是侵害一方所得),在有些情况下还同时表现为附加侵财犯罪行为直接导致的非财物性价值(如抢劫中导致人身伤害产生的医疗费用等)。

在信息化时代,计算机安全有几个基本的目标要求,即保护计算机信息系统及其中的数据或者信息

① 张明楷:《刑法学(下)》,法律出版社 2016 年版,第 938 页。
② 王俊:《财产罪中“损失”要素的体系性定位》,载《政治与法律》2019 年第 1 期,第 35 页。
③ 胡康生、李福成主编:《中华人民共和国刑法释义》,法律出版社 1997 年版,第 45 页。
④ 马乐、刘奕禄:《论盗窃罪的法益与财产损失定位》,载《河南财经政法大学学报》2020 年第 4 期,第 90 页。
⑤ 陈毅坚:《诈骗罪中财产损失的概念与认定——以混合型交易为中心》,载《政法论坛》2019 年第 1 期,第 43 页。

的安全性、机密性、完整性和可用性。[①] 相应地,在危害计算机信息系统犯罪中特别强调计算机信息系统的安全性和数据信息本身的"机密性""有用性"和"完整性",这种状态一旦被打破,即使数据信息在计算机信息系统中完好存在并没有被删除,其价值也受到了削弱,给权利人造成了消极影响,从而导致经济损失。"经济损失"在危害计算机信息系统犯罪中主要从三大方面体现其重要性:一是其为犯罪的构成要件之一;二是其为量刑的主要决定性因素;三是其为被害人获得赔偿的基础。[②] 这也使得在危害计算机信息系统犯罪中,经济损失产生的情况比较复杂,既有可能是因为对系统功能本身的损害导致的经济损失,也有可能是对系统中储存的数据信息的损坏或获取泄露导致的经济损失。

在这类犯罪中不一定直接表现为财物本身数额的减少而形成经济损失,相反,有时计算机信息系统中的数据信息本身并没有直接减少,但依然出现了经济损失。这是因为在计算机信息系统中所涉及的主要不是实在的有形财物,而是以数据信息表现出来的财产性利益。计算机滥用中所侵害的东西与既有的法律关于财产规定的类别与形态并不很符合,比如计算机程序或软件,其可能只以电子脉冲或磁性方式存在于储盘中,即使这些程序或软件被盗用,原件依然存在,没有被夺取。[③] 这些表现为程序或软件的电子数据信息虽然通过犯罪方式从此计算机中经由网络或特定的程序工具被复制转移到彼计算机中,但并没有对原来的程序数据做任何改变,其依然好端端地在原来计算机中运行着。因此,在危害计算机信息系统犯罪中,由于其中的数据信息的特殊性导致了这类犯罪的经济损失和传统财产犯罪存在较大差异。

从上述关于传统犯罪和危害计算机信息系统犯罪的经济损失的简要分析来看,两者虽在结果上都主要表现为导致他人经济上的价值减损,并且在法律的评价上也都主要以数额作为入罪和量刑的参照标准,但两者又有较大的不同。从形式上看,在传统的财产犯罪中是直接可见的损失,主要体现为财物的转移、灭失、减少等直观可见的价值减损;危害计算机信息系统安全犯罪既有直接可见的损失,还有系统不能正常运行或者安全运行导致的损失,还包括系统中的数据信息受到获取或使用而导致本身的价值减损。因此,既存在"此消彼长"的关系,还存在"此未消彼未涨,但经济损失也发生"的情况。从范围上看,危害计算机信息系统安全犯罪中经济损失的生成既有可能是有形实体,还包括无形物。一般而言,传统财产犯罪中规定的是实际存在并可识别的财产,甚至在一些条文中明确规定的是"物",这样才可能在窃取过程中拿走属于他人的东西。[④] 在危害计算机信息系统犯罪中,受到侵害的数据信息则属于无形物。这些无形的数据信息在计算机空间具有价值是因为其表征着一种财产利益,人们可以拿来在现实世界中花费使用,那些软件、域名以及纯粹的信息等,本身都具有经济价值。[⑤] 这些数据信息作为无形物与有形实体物一样代表着一种经济财产,可以给所有或合法持有人带来经济上的利益。

打击危害计算机信息系统安全犯罪的主要目的是保护数据信息,最重要的是谨慎地对数据信息及其体现的权益加以保护。[⑥] 这种保护体现了危害计算机信息系统安全犯罪所导致的"经济损失"和传统犯罪所导致的"经济损失"在认定上的路径差异:危害计算机信息系统安全犯罪中强调的是计算机数据

① Matt Bishop, *Introduction to Computer Security*, Addison-Wesley Professional, 259-275(2004).

② Jennifer S. Granick, Faking It: Calculating Loss in Computer Crime Sentencing, 2 ISJLP 209 (2006).

③ Michael Gemignani, *Computer Crime: The Law in '80*, 13 Ind. L. Rev. 689,690(1980).

④ Orin S. Kerr, Note, *The Limits of Computer Conversion: United States v. Collins*, 9 Harv. J. L. & Tech. 205, 209 (1996).

⑤ Marc D Goodman and Susan W Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, 10 International Journal of Law and Information Technology no. 2, 145(2002).

⑥ Donn B. Parker, *Fighting Computer Crime: A New Framework for Protecting Information*, Wiley Computer Publishing, John Wiley&Sons, Inc., 55(1998).

信息安全和数据信息产生的财产性利益,而传统财产犯罪中强调的主要是财物的安全。诈骗和盗窃的法律只反映了传统的关于财产的观念——有形的并常常是可以移动的实体物——这种按照惯例所定义的财产已经在信息化时代不能被接受了,在信息社会下登录程序或访问金融账号就像记一个数字那么简单,不能以传统财产犯罪的眼光和法律来对计算机犯罪中的财产进行相应认定①。对危害计算机信息系统安全犯罪的“经济损失”的确定和厘清要充分体现信息化时代要求,通过合理归因和有效判定,突出对计算机信息系统本身及其中的数据信息价值的双重保护功能。综合上述分析,危害计算机信息系统安全犯罪的“经济损失”既有别于传统侵财犯罪的“经济损失”,又在相关规定和司法认定中有其特殊性,应结合《解释》的规定,分别从“给用户直接造成的经济损失”和“用户为恢复数据、功能而支出的必要费用”两个方面予以完善。

(一)“给用户直接造成的经济损失”的进一步细化

通过仔细对比美国法关于“经济损失”规定的内涵,就会发现我国《解释》中对“经济损失”的规定显得相对单一和粗疏,容易导致认定上的困难,特别是其中关于“给用户直接造成的经济损失”的表述,易造成误判。如前文所述,1030 条中的“经济损失”内涵至少可以分解为四个方面。② 如果将这种划分具体分解适用到上述程某林案中,科脉公司所花费的 2.12 万元,其实最接近于其中的第二项,即评估计算机损害所需的开支。我国《解释》中规定的“给用户直接造成的经济损失”,如果与 1030 条规定的“经济损失”内涵向对应,最相似的应该是其中的第四项,即因计算机被犯罪损害而失去的任何收入或付出的成本和其他因中断服务带来的损害性结果。程某林的行为如果按照 1030 条的“经济损失”内涵规定,其超越授权获取所在公司“快食慧”“好餐谋”等软件源代码致使该公司不得不聘请第三方公司来进行安全检测鉴定所花费的 2.12 万元,无疑属于造成了经济损失,应该被定罪处刑。但是按照我国《解释》对“经济损失”的规定,其并未对所在公司造成直接的经济损失,也就达不到“情节严重”的要求,故而可以免除刑罚处罚。因此,在关于“经济损失”的规定上,我们应该区分不同情况进行更精细的规定,进一步明确“给用户直接造成的经济损失”是指行为人实施危害计算机信息系统犯罪行为后,在用户未采取有关补救措施之前致使用户产生的实际的损失,包括失去的应有经济收入或付出的经济成本和其他因中断服务带来的现实经济价值的减损。

(二)“用户为恢复数据、功能而支出的必要费用”的进一步明确

用户恢复数据、功能到何种状态算是恢复以及怎么来确定支出的费用是“必要”的?这是关键的问题。前文分析了美国法院在 1030 条的“经济损失”规定下,对计算机“再安全”和损失计算的“合理性”的判解③以及学界关于“合理性”的不同主张。其中的“再安全”与“合理性”类似于我国司法解释规定上的“恢复”和“必要”。在美国判例中对“再安全”的认识是,要求对计算机系统安全进行修复并使之与原来状况一样,而不是更安全,即任何改良的成本不能当作犯罪造成的损失数额,“合理”是指进行经济损失的计算时必须仔细检查其涉及的价值是否合理,也就是在逻辑上要排除陪审团认为是过多的任何支出。④ 美国法院判例对于“再安全”和“合理性”的判解观点可以作为我们对我国《解释》规定的“恢复”和“必要”进行理解时的参考。恢复数据、功能就是使之达到计算机遭受攻击或破坏以前的完好或安全

① Jill S. Newman, *The Comprehensive Crime Control Act of* 1984: *Filling the Gap in Computer Law*, St. Louis Bar Journal, 32(1986).

② 即:1. 被害人针对计算机网络犯罪所采取的反应与措施成本;2. 评估计算机损害所需的开支;3. 恢复数据、程序、系统以及信息等到原有状态的合理费用;4. 因计算机被犯罪损害而失去的任何收入或付出的成本和其他因中断服务带来的损害性结果。

③ United States v. Middleton, 231F. 3d 1207(9th Circuit, 2000).

④ United States v. Middleton, 231F. 3d 1207, 1215(9th Circuit, 2000).

状态;支出的必要费用就是指为了恢复计算机信息系统中的数据或功能到原来的完好或安全状态而支出的必需的合理费用,同时用户在恢复数据、功能过程中采取安全防护、检测鉴定、弥补安全漏洞等有关必要的措施使计算机信息系统恢复到受害之前的状态而产生的必要合理成本也应属于“用户为恢复数据、功能而支出的必要费用”。

(三)简要的结论

综合上述分析,我国《解释》中“经济损失”的内涵应进一步解释为:给用户直接造成的经济损失,是指行为人实施危害计算机信息系统的犯罪行为后,在用户未采取有关补救措施之前致使用户产生的实际的损失,包括失去的应有经济收入或付出的经济成本和其他因中断服务带来的现实经济价值的减损;用户为恢复数据、功能而支出的必要费用,是指用户为恢复计算机信息系统数据、功能使之达到遭受攻击或破坏以前的完好或安全状态而支出的必需的合理费用以及用户为使数据、信息、系统功能达到受害之前的状态而采取的安全防护、检测鉴定、弥补安全漏洞等措施所产生的必要成本。按照这一解释,上述程某林案中,科脉公司所花费的 2.12 万元无疑可以计算入“经济损失”的范围,而程某林的行为则构成犯罪,应受到刑罚处罚。另外,在对“经济损失”的内涵予以解释建构的基础上,还建议最高司法机关适时发布相关的指导性案例,为“经济损失”的认定提供有力参考,使定罪处刑更准确,避免误解误判。JS

“Economic Losses” in Crimes against Computer Information System Security: A Comparative Analysis of China and the United States

GAO Shi-yin

(Chinese Academy of Social Sciences, Beijing 100732, China)

Abstract: “Economic loss” is used as one of the decisive conditions to measure the seriousness of the crime and whether the perpetrator should receive criminal punishment in crimes against the security of computer information systems in China. By comparing and examining the relevant provisions on “economic loss” in China and the United States, the study analyzes and constructs the connotation of “economic loss” in crimes against the security of computer information systems in China, taking into account the court rulings and specific cases of the two countries. The definition of “economic loss directly caused to the user” and “the necessary expenses incurred by the user to restore data and functions” is more refined, with a view to providing useful reference for the judiciary to combat crimes more vigorously and punish criminals more reasonably, as well as to provide adequate protection for victims. It is hoped that this will provide a useful reference for the judiciary to combat crime more vigorously and to punish offenders more reasonably, as well as to protect victims adequately, and to ensure that criminal law is applied clearly and precisely.

Key Words: impairment of value; safety risk responsibility; reasonable and necessary

本文责任编辑:李晓锋

青年学术编辑:张永强