

# CCED5.0 著作权保护中的问题及探讨

王 迁

(西北大学法律系学生)

**摘 要** CCED5.0的作者为了防止盗版、惩治盗版者,编制了能破坏硬盘数据的加密程序。本文分析探讨了此加密程序对计算机安全的影响、在法学上的性质以及它的合法性等问题。认为此加密程序能破坏盗版用户的计算机安全;通过将此与计算机病毒进行比较,试将其界定为“报复性准计算机病毒”;根据我国民法规定的民事责任制度,认为其合法性值得商榷。并建议用立法手段对其加以制约和规范。

**关键词** 著作权 盗版软件 朱崇君 破坏性加密程序 侵权

CCED5.0是中国著名计算机专家朱崇君先生编写的一个文字表格处理软件,自问世以来,受到了普遍的好评与欢迎。为了防止猖獗的盗版行为侵害其合法权益,朱崇君先生首次采用了一种针对盗版使用者的计算机数据的破坏性加密程序。《电脑》杂志在1995年第一期刊登了《朱崇君先生告诫电脑用户》的声明:“为了惩治个别违背版权法,不尊重他人劳动的人,经加密的CCED程序如果确切地发现其中一个要素被解开,它并不及时警告和立即瘫痪,仍然佯做可正常运行,但它会不定期地对硬盘数据起破坏作用。CCED5.0问世后,以其自身功能的吸引力和其特殊的加密方法,引起了解密者纷纷跃跃欲试。事实是:经朱崇君先生对目前出现的CCED5.0版‘解密’结果的考察,还没有一个是彻底的!至少文件存盘时不定期抽查密点以及不定期检验自身文件完备性还没有被解密者发现并解除!为了大家的数据安全,建议您不要使用来历不明的CCED软件。”

我们认为,朱崇君先生的这一作法,给计算机安全和著作权保护的研究提出了一系列新的课题:1. 破坏性加密程序对计算机安全的影响;2. 破坏性加密程序在法学上的性质;3. 破坏性加密程序的合法性。本文试从保护著作权与保护计算机安全的关系及民法中民事权益的保护方法入手,对以上问题作一探讨。

## 一、破坏性加密程序对计算机安全的影响

保护计算机安全是指保证计算机的正常运行、防止对计算机数据和数据通讯的破坏。当今对计算机安全的威胁主要来自于计算机病毒。

朱崇君先生的破坏性加密程序是否可以破坏计算机安全呢?这从其声明中可以得到肯定的答案。由于它对盗版用户的硬盘数据会起不定期的破坏作用,则载有盗版

软件的硬盘所存储的一切数据都会受到威胁。用户使用盗版的行为尽管可能非法,但他们对硬盘中其他来源合法的软件仍拥有法定所有权,这些数据的安全受法律保护。因此,朱崇君先生“惩治”“个别违背版权法,不尊重他人劳动的人”的含义,就是破坏盗版用户的计算机安全。

我国是一个计算机普及尚为落后的国家,软件用户的专业素质较低,法律意识较淡薄。很多软件用户还没有建立起“花钱买软件”的法律观念,甚至不知道计算机软件受著作权法保护,故意使用盗版是违法行为。因此,我国使用盗版现象较为普遍。据美国商业软件联盟(Business Software Alliance缩写BSA)的调查报告,中国盗版软件数量与用户使用全部软件量的比例竟高达95%,即每卖出5套正版软件,就会有95套盗版。按照这个比例,假设销售1000套CCED,就会有19000套盗版的CCED被使用。这19000个盗版用户计算机安全如何得到保护,是朱崇君先生对中国计算机事业提出的挑战。

## 二、破坏性加密程序在法学上的性质

通过对破坏性加密程序对计算机安全影响的分析,可以发现,它与计算机病毒有着共同的重要特点,但同时又有本质不同。比较两者之间的异同,有利于准确把握破坏性加密程序的性质。计算机病毒有如下几个显著特点,其中前两条是根本特点。

1. 破坏性。计算机病毒会破坏系统的正常运行。一般后果为:删除或篡改系统内部分或所有数据;使计算机的运行效率降低。2. 传染性。计算机病毒会主动攻击正常软件,使之染上病毒,并带病毒扩散、传染。3. 潜伏性。指病毒可依附于其他文件而寄生,长时间地隐藏在合法文件中对其进行传染而不被发现。4. 可触发性。设计者可为病毒设置一个激发条件,如日期、特定的操作等,激

活后对系统发起攻击。5. 衍生性。指病毒的核心代码可能被他人破解并利用,而改造成变种病毒。

破坏性加密程序与计算机病毒的根本区别,在于它不具备病毒严格意义上的传染性,表现在:病毒的传染是主动进行的,一个成功的病毒,会自动感染进入系统的一切正常文件,通过不断复制自身完成传染,无需人的主动干预。而破坏性加密程序自己不会复制破坏模块到其他文件,它是通过用户购买盗版,或非法拷贝而进入其系统的。从这个意义上说,破坏性加密程序只具有“传播”性,而无“传染”性。这个差异也造成了它们在破坏力大小上的区别。由于病毒可不断复制自身感染正常文件,因此它的传染速度快,范围广,一旦被激发,破坏力极强。而破坏性加密程序仅靠用户“人工传播”,无论是速度上、范围上都无法同病毒相比,其破坏性仅局限在使用盗版软件的用户中。

但是,破坏性加密程序和病毒又有其类似性,正如声明所说的“它并不及时警告和立即瘫痪,仍然佯做可正常运行,但它会不定期地对硬盘数据起破坏作用”。这正是典型的“破坏性”和“潜伏性”的表现,而“CCED 程序如果确切地发现其中一个要素被解开”则是触发破坏模块的条件。而且,破坏性加密程序一旦被高手解密,其核心思想完全可能被模仿,其加密模块也完全可被利用,从而可能被人通过对原有加密程序的加工,如增加传染模块、加强破坏程度等,改造成一种恶性的计算机病毒。由于更改一个程序代码比编制一个程序要简单得多,因此,在计算机病毒的产生途径上,恶性病毒往往是良性病毒的变种,而这种变种造成的破坏后果比原版病毒严重得多,在当今世界流行的几千种计算机病毒中,大多数是变种病毒。虽然现在朱崇君先生声称还没有能彻底解密的版本出现,但这并不能保证 CCED 将来不可能被解密,而一旦被恶意的人利用来编制计算机病毒,后果是不堪设想的。声明中提到的“引起解密者纷纷跃跃欲试”正是一个不祥的征兆。因此,它也具有“衍生性”的特征。

通过以上分析可以看出,破坏性加密程序具有除传染性外的一切计算机病毒的特点,同时可以通过软件的传播而进行有限的扩散,它的编制目的不同于计算机病毒,病毒纯粹是为了破坏而设计,而它在于警告用户不得使用盗版,同时“惩治”盗版用户。

为了准确地考察破坏性加密程序对计算机安全的影响并确定其法律地位,有必要界定其法律性质。我们认为,它是一种“报复性准计算机病毒”。“报复性”是表示它的设计不是为了主动攻击,而在于对使用盗版者进行报复。“准”说明由于传播机制的不同,使其接近但又不同于计算机病毒。

### 三、破坏性加密程序的合法性

我们试从分析软件著作权者和盗版使用者之间的关系入手,探讨报复性准计算机病毒的合法性和它对立法的影响。

#### 1. 著作权享有者和盗版使用者之间的法律关系

为了便于问题的讨论,本文引入“盗版用户”这一概

念。包括是从《计算机软件保护条例》第 30 条第 6 项“未经软件著作权人或者其合法受让者的同意,复制或者部分复制其软件作品”者和第七项“未经软件著作权人或者其合法受让者的同意,向公众发行、展示其软件的复制品”者手中购买或获得软件的人。按其是否知道软件为未经权利人授权使用的非法软件,分为善意使用者和恶意使用者。下面分别分析他们与著作权享有者之间的法律关系。

(1) 善意使用者。《计算机软件保护条例》第 32 条对善意使用者的法律责任作出了明确规定:“软件持有者不知道或者没有合理的依据知道该软件是侵权物品,其侵权责任由该侵权软件的提供者承担。但若所持有的侵权软件不销毁不足以保护软件著作权人的权益时,持有者有义务销毁所持有的侵权软件,为此遭受的损失可以向侵权软件的提供者追偿。”可以看出,由于不具备侵权行为的主观要件,即主观过错,善意使用者除负有销毁软件义务外,不对著作权享有者负法律上的责任。需要指出的是,“声明”虽然呼吁“为了大家的数据安全,建议您不要使用来历不明的 CCED 软件”,但这不能排除存在善意使用者的可能性,因为声明本身并不具有法律上的强制效力。

(2) 恶意使用者。对明知或应当知道所持软件为侵权物品者的法律责任,《计算机软件保护条例》并未规定。根据民法侵权行为和民事责任的一般原理及该条例第 30 条对侵权行为的规定,恶意使用者侵犯了著作权人的合法财产权益,应当停止侵害(即立即销毁非法软件和备份)和赔偿损失(即补交使用费)。可见,由于恶意使用非法软件这一侵权行为,使著作权享有者和恶意使用者之间产生了特定的权利义务关系,即著作权享有者享有要求停止侵害和赔偿损失的请求权,而恶意使用者则必须履行这个义务。

#### 2. 编制报复性准计算机病毒的法律性质

编制报复性准计算机病毒的目的,声明中说得清清楚楚,是“‘惩治’个别违反版权法的人”。那么,对于盗版使用者,是否应当“惩治”?著作权享有者是否又有权单方面自行“惩治”呢?

前文已分析过,善意盗版使用者不对权利人承担赔偿义务,更无所谓要受“惩治”。而恶意盗版使用者侵犯了著作权享有者的合法权益,理应赔偿,但他与权利人之间的关系是民事关系,适用民事赔偿,应遵循民事法律所规定的范围、方式、程序。首先,民事法律关系的核心是平等,当事人任何一方都不具有凌驾于另一方的特权。因此,“补偿性”是民事责任制度的根本特点,是区别于行政、刑事责任制度的主要标志。而“补偿”的基本含义是:使受到的损失在量上得到相同的偿付,即完全根据损害范围确定赔偿数额。对财产侵权的补偿,主要是通过返还原物、替代物、或折价赔偿等方式来完成的。报复性准计算机病毒则无论如何不能体现这一平等原则,CCED 的市场售价是 660 元,这个数目也应当成为盗版用户赔偿的最高限度。而事实是,一旦对硬盘进行破坏性操作,对用户造成的损害则可能远远大于这个价额。可以设想,如

果一位作家存储长篇小说的硬盘遭到破坏,那损失是CCED的价值根本无法抵偿的。

其次,解决民事侵权行为引起的赔偿问题的途径:一是当事人自行协商解决,它体现了民法的自治原则,而“惩治”则完全是单方面行动;另一方法是通过诉讼,由法院作出司法裁判,最终从实体上解决是非和责任承担的争议,“惩治”显然不符合法定程序。

再次,应当着重指出,所谓“惩治”并不是解决民事纠纷的方式,它是在不平等的法律关系中,由居于主导地位的主体代表国家对相对人实施的具有强制性的行为。具体而言,只有在行政法律关系和刑事法律关系中,才可能由行政机关和司法机关对违反行政、刑事法律的人实施。这一权力,属于国家,只能由宪法规定的国家机关代表国家行使,其他任何机关、团体、个人都不得拥有。因此,个人是无权“惩治”他人的。

编制报复性准计算机病毒的实质,是一种“复仇”行为,意在对使用盗版的用户实施报复,使其硬盘数据受到破坏。个人复仇在现代法律制度确立之前是普遍存在的,古代法律大多对私人间的复仇加以认可,进入资本主义社会后,由于被证明为是一种野蛮行为而被彻底废除,代之由司法机关裁判并实施惩罚,社会主义国家则从根本上否定了这种作法。

编制报复性准计算机病毒的后果,是盗版用户硬盘数据遭到破坏。由于用户硬盘中存储有其他合法程序,这一作法可能转化成对盗版用户合法数据权益的侵权行为。

因此,编制报复性准计算机病毒的行为是否符合中国现行法律精神,是很值得商榷的。

### 3. 报复性准计算机病毒对中国计算机安全的影响及解决途径

中国必将走向信息时代,无论是对现在的单用户、多用户网络还是将来的信息高速公路而言,计算机数据安全不仅涉及千家万户的切身利益,还将影响社会的正常活动和国家的安全和利益。下面我们从我国实际出发,对报复性准计算机病毒对我国计算机安全的影响作进一步探讨,希望能引起立法者的注意,将这一新现象纳入保护计算机安全的法律体系。

一般而言,报复性准计算机病毒与计算机病毒相比的突出特点,在于它传播的速度较慢、对象特定。然而,在当今中国的特定国情下,计算机病毒的流行有着特殊的规律。由于大规模的计算机网络体系尚未在我国建立,因此计算机病毒主要靠装载感染上计算机病毒的程序软盘的拷贝、携带而传播。近年因用户反病毒意识有所提高,重要软盘一般使用写保护,这使得计算机病毒对其他用户软盘的主动传染率大大降低,而主要局限于对用户个人系统内部的破坏。换言之,系统内病毒要复制自身到其他用户的软盘,只有在此用户打开写保护进行文件操作时才有可能。这样,使一般计算机病毒的传播速度降到类似于报复性准计算机病毒了。

就传播的范围而言,由于计算机病毒可自由地对用户硬盘内其他文件进行感染,使得其他用户文件在与系统作信息交换时染上病毒的可能性较大,而报复性准计算机病毒不会主动感染其他文件,因而只有其他用户拷贝带有报复性准病毒的源程序时,才会导致其传播,从这个意义上看,计算机病毒扩散的范围仍然较大。但考虑到一旦编制报复性准计算机病毒的作法被广泛采用,用户系统内的传播源变得足够多时,则它们的整体传播范围就会接近计算机病毒。

因此,如果不及时控制报复性准计算机病毒的发展,而任意由软件作者将它当作防止盗版的一般性方法应用时,它造成的破坏就会接近于计算机病毒,这是对我国计算机安全的极大威胁。

综上所述,报复性准计算机病毒是CCED5.0作者用以保护著作权的手段,是计算机安全学和法学研究中出现的新课题,它造成的社会影响在于:1. 报复性准计算机病毒对单用户的破坏类似于计算机病毒。2. 报复性准计算机病毒可以通过软件复制而进行传播。3. 报复性准计算机病毒可能被加工成真正的计算机病毒。4. 报复性准计算机病毒可能侵犯善意使用者的合法权益。5. 报复性准计算机病毒可能侵犯恶意使用者对除盗版软件本身以外的其他合法数据的权利。鉴于我国有关保护计算机安全的立法尚未涉及到这方面的问题,我们建议今后在进行有关计算机安全的立法时,应慎重考虑报复性准计算机病毒问题,并制定出相应的符合我国国情的法律。

### 参 考 文 献

- 1 《正版的功能意外的价格》,《电脑》1995年第1期第64页。
- 2 成林:《不能再让盗版软件横行》,《电脑》1995年第1期第3页。

(责任编辑:刘 欢)